TestStream™ Management Software 5.3.0 Administrator Guide

733-1696 Rev. A

Contacting NETSCOUT SYSTEMS, INC.

Customer Support

The best way to contact Customer Support is to submit a Support Request:
https://my.netscout.com/mcp/Support/Pages/Home.aspx

Telephone: In the US, call **888-357-7667**; outside the US, call **+800 4764 3337**.
Phone support hours are 8 a.m. to 8 p.m. Eastern Standard Time (EST).

E-mail: support@netscout.com

When you contact Customer Support, the following information can be helpful in diagnosing and solving problems:
— Your organization's name, contact name, phone number, and location of system
— Type of nGenius 3900 series switch model
— TestStream Management Software version
— Detailed description of the problem, or source of the problem based on its symptoms
— Error text messages, supporting screen images, logs, and error files, as appropriate

Sales

Call **800-357-7666** for the sales office nearest your location.

Chapter 1 About This Document

Chapter 2 TestStream Management Software

Chapter 3 Configuration and Control

Chapter 4 Tools

Chapter 5 Favorites

Chapter 6 Connectivity

Chapter 7 Diagnostics and System Tests

Appendix A Command Line Interface Commands

Appendix B Restoring the TestStream Management Server

Appendix C TestStream Restful API

Chapter 1
About This Document

This document is intended to assist with the operation of NETSCOUT SYSTEMS, INC. (NETSCOUT®) TestStream™ Management Software used on NETSCOUT's nGenius 3900 Series Switches, OS-96 / OS-192 Optical Switches, HS-3200, and HS-6400 Switch for Test Optimization.

IMPORTANT

Please read and understand the *TestStream Management Software 5.3.0 Administrator Guide* (this document) before operating the equipment. Failure to do so may result in incorrect usage or damage to the nGenius 3900 series Switches, OS-96 / OS-192 Optical Switches, HS-3200, and HS-6400 Switch.

TestStream Management Server Notice

The *TestStream Management Software 5.3.0 Administrator Guide* assumes that the TestStream Management server software is installed and servers are defined and initialized. While most of the TestStream Management server operating parameters are selected during software installation, it is advisable to verify and/or revise these parameters before activating a TestStream Management server and starting switch functions.

Note: If changing the Linux shell password from the default NETSCOUT setting (refer to Changing SSH System Access Passwords on page 7-23), please contact Customer Support (refer to Contacting NETSCOUT Customer Support on page 1-2).

Related Documentation

For information related to this publication, refer to the following:

nGenius 3900 Systems

- ***nGenius® 3900 Series for Test Optimization Hardware Installation Guide***
  This document provides information on nGenius 3900 series system installation and hardware maintenance.
- ***TestStream™ Management Server Hardware Installation Guide***
  This guide provides information for installing, cabling, and starting the TestStream Management server.
- ***nGenius® 3901 for Test Optimization Quick Connection Guide***
  This guide provides overview information for installing, cabling, and starting the nGenius 3901 system.
- ***nGenius® 3901R for Test Optimization Quick Connection Guide***
  This guide provides overview information for installing, cabling, and starting the nGenius 3901R system.
- ***nGenius® 3903 for Test Optimization Quick Connection Guide***
  This guide provides overview information for installing, cabling, and starting the nGenius 3903 system.

- ***nGenius® 3912 for Test Optimization Quick Connection Guide***
  This guide provides overview information for installing, cabling, and starting the nGenius 3912 system.

OS-96 and OS-192 Optical Switches

- ***OS-96 and OS-192 Optical Switches for Test Optimization Hardware Installation Guide***
  This document provides information on the installation and hardware maintenance of the OS-96 and OS-192 Optical Switches.
- ***OS-96 Optical Switch for Test Optimization Quick Connection Guide***
  This guide provides overview information for installing, cabling, and starting the OS-192 Optical Switch.
- ***OS-192 Optical Switch for Test Optimization Quick Connection Guide***
  This guide provides overview information for installing, cabling, and starting the OS-192 Optical Switch.

HS-Series Switch

- ***HS-Series Switch for Test Optimization Quick Connection Guide***
  This guide provides overview information for installing, cabling, and starting HS-Series Switches.
- ***HS-Series Switch for Test Optimization Hardware Installation Guide***
  This document provides information on the installation and hardware maintenance of HS-Series Switches.

Contacting NETSCOUT Customer Support

Customer Support:
The best way to contact Customer Support is to submit a Support Request:
https://my.netscout.com/mcp/Support/Pages/Home.aspx

Telephone: US Toll Free: **+1-888-357-7667**; International Tol Free **+800 4764 3337**.
Phone support hours are 8 a.m. to 8 p.m. Eastern Standard Time (EST).

E-mail: support@netscout.com

When contacting Customer Support, the following information can be helpful in diagnosing and solving problems:
— Your organization's name, contact name, phone number, and location of system
— Your NETSCOUT MasterCare ID
— TestStream Management Software version
— Detailed description of the problem, or source of the problem based on its symptoms
— Error text messages, supporting screen images, logs, and error files, as appropriate

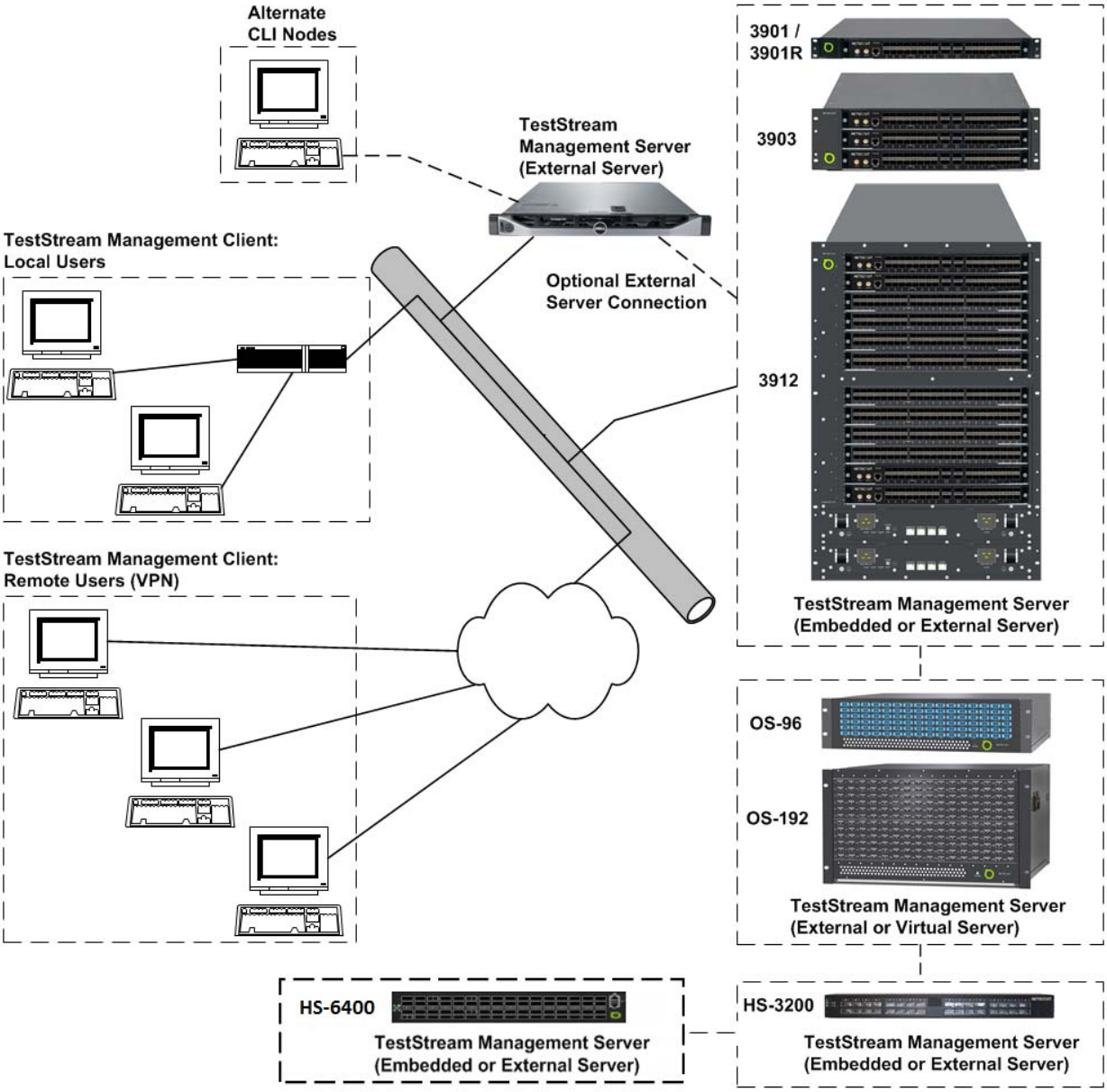
NETSCOUT Web Site

Visit our Web site at http://www.netscout.com.

Chapter 2
TestStream Management Software

This section covers startup, login, and initial user setup of the TestStream Management Software used with the NETSCOUT Test Optimization and TestStream Management Server.

TestStream Management Client is a Java-based application providing connectivity management of the nGenius switches from virtually any location. A user with an approved username and password can access their nGenius switches using a PC with an Internet browser (e.g., Internet Explorer, Firefox, etc.) or TestStream Launcher and, if required for remote usage, a Virtual Private Network (VPN) connection.



TestStream Management Supported Interfaces

Refer to the following sections for the interfaces TestStream Management supports in the nGenius switches.

- "G-Blade Port Configurations" on page 59
- "S-Blade Port Configurations" on page 62
- "S-Blade Pro Port Configurations" on page 66
- "S-Blade 64 Port Configurations" on page 73
- "T-Blade Port Configurations" on page 78
- "HS-3200/HS-6400 Blade Port Configurations" on page 84

TestStream Management Software Requirements

The following details the system requirements to run TestStream Management Software.

Operating Systems currently supported for use with TestStream Management Software include:

- Microsoft Windows 7 SP2(32 bit)
- Microsoft Windows 7 Professional (64 bit)
- Microsoft Windows 10 (64 bit)
- macOS 10.15: Catalina (Jazz) - 7 October 2019
- macOS 11: Big Sur - 12 November 2020
- macOS 12: Monterey - ETA October 2021

Web browsers supported for use with TestStream Management Software include:

- Microsoft Internet Explorer, versions 9, 10, and 11
- Mozilla Firefox (preferably the latest version)
- Google Chrome (preferably the latest version)

TestStream Management Server Requirements

The following details the system requirements to run the TestStream Management server application.

nGenius 3900 Series Switches

The TestStream Management server application is embedded onto the system blades allowing for standalone nGenius 3900 series switch operation, requiring only workstations for TestStream GUI access. However, to support multiple nGenius 3900 series switches through a network, TestStream Management must reside on the TestStream Management External Server.

Note: The TestStream Management server application supports a maximum of 32 nGenius 3900 switches networked to the TestStream Management External Server.

TestStream Management Server Requirements

Operating System: Refer to TestStream Software Components for operating system requirements for the TestStream Management External Server and the nGenius 3900 Blades.

TestStream Software Components

The following lists the current software components comprised in TestStream Management.

Component	Platform	Command	Output
Java Client	User PC	N/A	Supported Java version: JRE 1.8.1+ (except 1.8.221)
Operating System	External Server Dell, VM	cat /etc/redhat-release	CentOS Linux release 7.8.2003 (Core)
	S-Blade and SFM	uname -a	Linux HorizON 3.2.63-Debian-v3.3 #98 Mon Sep 14 16:10:38 EDT 2015 ppc GNU/Linux
	T-Blade		Linux HorizON 3.0.34-rt55_v2_1_Serv #7 SMP Tue Apr 14 15:06:55 EDT 2015 ppc GNU/Linux
	S-Blade Pro, SFM Pro, S-Blade 64		Linux HorizON 3.8.13-ts-powerpc-rt9_V2_3_Serv #28 SMP Thu Jul 13 11:08:11 EDT 2017 ppc GNU/Linux
	HS-6400		Linux localhost 4.9.75-OpenNetworkLinux #1 SMP Thu Sep 24 23:37:54 UTC 2018 x86_64 GNU/Linux
	HS-3200		Linux localhost 4.9.75-OpenNetworkLinux #1 SMP Fri Jul 6 18:12:12 UTC 2018 x86_64 GNU/Linux
Web Server	S-Blade	/usr/sbin/apachectl -V	Apache/2.2.22 (Debian)
	HS-3200, HS-6400		Apache/2.4.25 (Debian)
	T-Blade, S-Blade Pro, S-Blade 64	/usr/bin/httpd -v	Apache/2.4.52 (Unix)
	External Server Dell, VM	/usr/bin/httpd -v	Server version: Apache/2.4.6 (CentOS)
OpenSSL	External Server Dell, VM	openssl version	OpenSSL 1.0.2k-fips 26 Jan 2017
	S-Blade, SFM		OpenSSL 1.0.2l 25 May 2017
	HS-3200, HS-6400		OpenSSL 1.1.0l 10 Sep 2019
	T-Blade, S-Blade Pro, S-Blade 64, SFM Pro		OpenSSL 1.0.2d-fips 15 Mar 2022

Component	Platform	Command	Output
OpenSSH	External Server Dell, VM	/usr/sbin/sshd -v (ignore the illegal option message)	OpenSSH_7.4p1, OpenSSL 1.0.2k-fips 26 Jan 2017
	S-Blade, SFM		OpenSSH_7.5p1, OpenSSL 1.0.2l 25 May 2017
	HS-6400		OpenSSH_7.4p1, Debian-10+deb9u7, OpenSSL 1.0.2u 20 Dec 2019
	HS-3200		OpenSSH_7.4p1, Debian-10+deb9u2, OpenSSL 1.0.2u 20 Dec 2019
	T-Blade, S-Blade Pro, S-Blade 64, SFM Pro		OpenSSH_8.8p1, OpenSSL 1.0.2zd-fips 15 Mar 2022
bash	External Server Dell, VM	bash --version	GNU bash, version 4.2.46(2)-release (x86_64-redhat-linux-gnu)
	S-Blade, SFM		GNU bash, version 4.3.30(1)-release (powerpc-unknown-linux-gnu)
	HS-3200, HS-6400		GNU bash, version 4.4.12(1)-release (x86_64-pc-linux-gnu)
	T-Blade, S-Blade Pro, S-Blade 64, SFM Pro		GNU bash, version 4.4.0(1)-release (powerpc-timesys-linux-gnu)
PostgreSQL	External Server Dell, VM	psql --version	psql (PostgreSQL) 9.2.24
	S-Blade		psql (PostgreSQL) 9.1.14
	HS-6400		psql (PostgreSQL) 9.6.17
	HS-3200		psql (PostgreSQL) 9.6.6
	T-Blade, S-Blade Pro, S-Blade 64		psql (PostgreSQL) 8.3.9
NTP	External Server Dell, VM	ntpd --version	ntpd 4.2.6p5
	S-Blade, SFM		ntpd 4.2.6p5
	HS-3200, HS-6400		ntpd 4.2.8p10@1.3728-o
	T-Blade, S-Blade Pro, S-Blade 64, SFM Pro		ntpd 4.2.8p15@1.3728-o
GNU libc	External Server Dell, VM	ldd --version	ldd (GNU libc) 2.17
	S-Blade, SFM		ldd (Debian GLIBC 2.19-13) 2.19
	HS-6400		ldd (Debian GLIBC 2.24-11+deb9u4) 2.24
	HS-3200		ldd (Debian GLIBC 2.24-11+deb9u1) 2.24
	T-Blade, S-Blade Pro, S-Blade 64, SFM Pro		ldd (GNU libc) 2.19

TestStream Management Software - Permitted / Invalid User Text Characters

The following chart lists the permitted characters used for data/information entry throughout TestStream Management Software.

Permitted TestStream Management Text Characters	
Alpha (upper case):	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alpha (lower case):	abcdefghijklmnopqrstuvwxyz
Numeric:	0123456789

The following chart lists the characters that must not be used for data/information entry throughout TestStream Management Software.

Invalid TestStream Management Text Characters	
Text Entry:	' \ " ( ) %
SNMP Entry:	' \ " ( ) % & # * ; < > | (white space) ` $?
Backup Database Entry:	' \ " ( ) % / : * ? < > |
User Name Entry:	=

TestStream Management Server Ports / Processes

The following lists the external server communication ports and processes attached to each port.

	Port	Port # Configurable	By Default	Can be Disabled	Comment	Process
ssh	tcp/22	No	On	No	Redundant external servers use tcp port 22 for ssh and scp and ICMP echo request/echo reply for ping	sshd
http	tcp/80	Yes	On	Yes		httpd
https	tcp/443	Yes	Off	Yes		httpd
SSH CLI	Tcp/22022	Yes	Off	Yes		horizONsshd
CLI	Tcp/53058	Yes	On	Yes		UDBServ (HorizONServ in external server)
GUI	Tcp/50100	No	On	No		UDBServ (HorizONServ in external server)
	Tcp/50101	No	On	No	GUI Client polls server using this port.	UDBServ (HorizONServ in external server)
GUI (TLS)	Tcp/60100	No	On	No		UDBServ (HorizONServ in external server)
	Tcp/60101	No	On	No	GUI Client polls server using this port.	UDBServ (HorizONServ in external server)

	Port	Port # Configurable	By Default	Can be Disabled	Comment	Process
Postgres	Tcp/5432	No	On	No	Access is managed by pg_hba.conf (determines clients that can connect). Embedded server does not allow external connections. External server allows only redundant server to connect.	postmaster
Switch Discovery	Udp/65500	No	On	No	Used by the switch to listen for external servers sending discovery cmds. Will only answer to well formatted packets.	UCSMgmt
	Udp/65501	No	On	No	Used by the server to process the answers from the switches.	HorizONServ
Ntp	Udp/123	No	Off	Yes		ntpd
Server Redundancy	Tcp/58990	No	Off	Yes	Used only when redundancy in external server is enabled.	UDBMonitor
Server Redundancy (TLS)	Tcp/60103	No	Off	Yes	Used only when redundancy in external server is enabled with TLS.	UDBMonitor
Server/Switch Communication	Tcp/3500	No	On	No	Proprietary payload carries commands and responses.	UCSMgmt
Server/Switch Communication (TLS)	Tcp/60102	No	On	No	Proprietary payload carries commands and responses.	UCSMgmt
Server/Polatis Switch Communication	Tcp/5025	No	On	No	Communication port for Polatis Switch	HorizONServ
Server/MRV Switch Communication	Tcp/23	No	On	No	Communication port for MRV Switch	HorizONServ
RESTful API (http)	Tcp/8080	Yes	Off	Yes		httpd
RESTful API (https)	Tcp/8443	Yes	Off	Yes		httpd

TestStream Management System Maximum Usage Guidelines

The following maximum usage guidelines should be observed when operating TestStream Management Software:

- Defined nGenius 3900 switches: 32
- Concurrent GUI users: 16
- Concurrent CLI users: 32

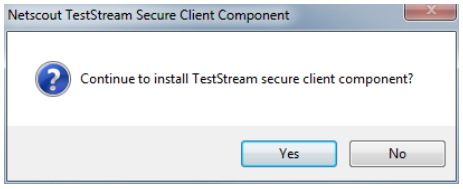
Installing the TestStream Client TLS/SSL Component

Note: Refer to *Setting Client Configuration: Select TLS Secure Server Communication* portion of **Configure Remote Access on page 4-25**.

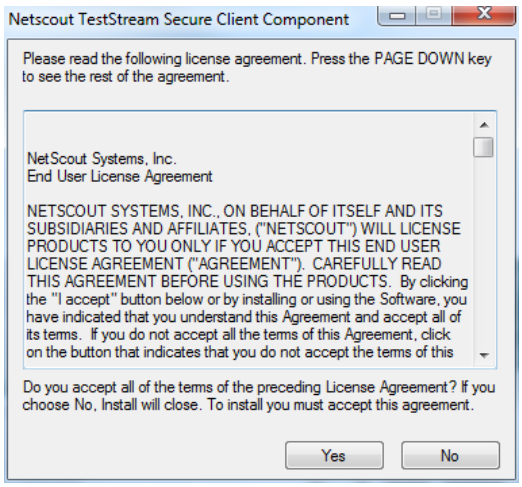
Use the following procedure to load the TLS/SSL component on your Teststream Client system.

1 Click on *Client TLS/SSL Component* from the TestStream Management Software welcome screen (also available on the TestStream Launcher screen). Click **Run** to begin the installation.

2 Click **Yes** to the *TestStream Secure Client Component* prompt.



3 Click **Yes** on the NETSCOUT End User License Agreement.



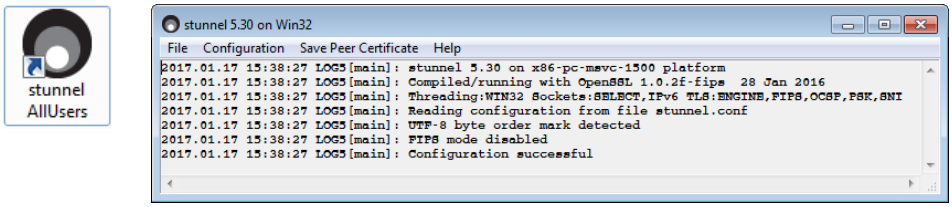
4 Click **Yes** to the *vcredist_x86.exe* installer prompt.

5 Click **Yes** to the *Win32OpenSSL.exe* installer prompt.

6 Click **Yes** to the *stunnel.exe* installer prompt.

7 Click **OK** to the *TestStream Secure Component Installation Completed* announcement.

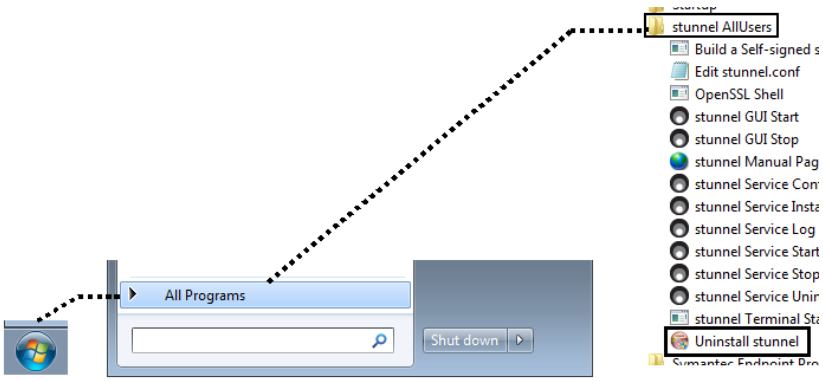
Note:
After the stunnel.exe installer is run, a shortcut icon will display on your desktop. Double-clicking on the icon displays the stunnel log file / command window. You can minimize the command window and continue operating TestStream Management Software.



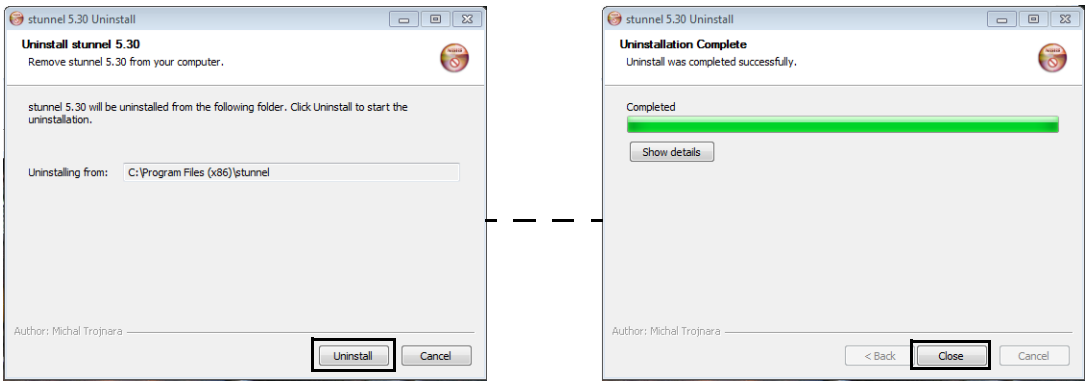
Uninstalling the TLS/SSL Component

Use the following procedure to uninstall (if necessary) the TLS/SSL component on your TestStream Management Software system.

1 From the **Start** icon, select **All Programs**, then scroll down to **stunnel AllUsers > Uninstall stunnel**.



2 From the **Uninstall stunnel** prompt, click **Uninstall**. When the **Uninstallation Complete** notice displays, click **Close**.



Installing and Starting the TestStream Management Client

Note: In redundant TestStream Management Server applications, when using an Internet browser, TestStream Management Software can be accessed by entering either server's IP address. However, if accessing TestStream Management Software using Command Line Interface (refer to Appendix A, Command Line Interface Commands), the IP address of the active server must be used.

In the event of a TestStream Management Server rollover, where the Active server is no longer network accessible, the Standby server now assumes the role of Active server. Access to the TestStream Management Server (from the Internet browser) can now be accomplished by entering the IP address of the new Active (formally Standby) server.

TestStream Management Client can be started from the web page (it uses Java Web Start that requires Java 1.8 or older) or using the TestStream Launcher (it does not require Java installed in the workstation).

Installing the TestStream Launcher

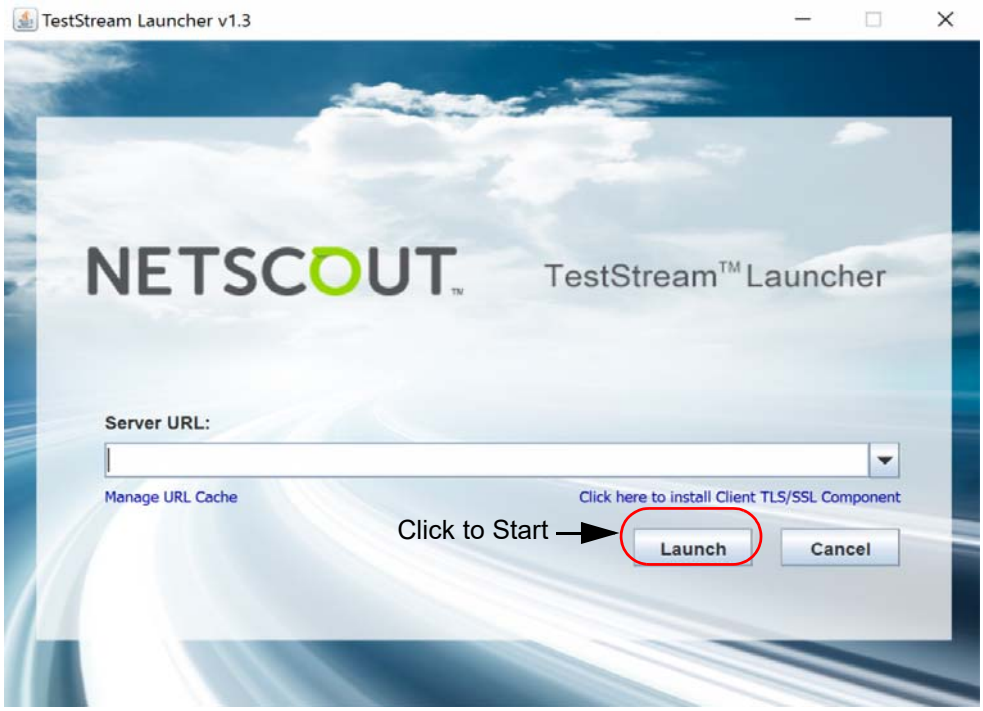
1. Download the *TestStreamLauncher-1.3.msi* file from the MasterCare portal.
2. Go to the location where the *TestStreamLauncher-1.3.msi* file was downloaded. Double click on the file to install the application.

   Note: You only have to install the TestStream Launcher software one time, on your work station. This application can now be used to connect to any switch or server running TestStream 4.10.200 or greater.

3. After the TestStream Launcher application is installed,an application shortcut named “TestStreamLauncher-1.3” will be placed on the workstation’s desktop and in the Start menu, under the TestStream folder.
4. To open the TestStream Management Client application, click on the TestStream Launcher shortcut in the Start menu or double click the TestStream Launcher shortcut on the desktop. The NETSCOUT welcome screen is displayed.

Starting and Logging into the TestStream Management Client

1 From the NETSCOUT welcome screen display, type in the server URL or select a previously used URL from the drop down menu. Then click the **Launch** button to start the TestStream Management Client.



2 Once the TestStream Management Client application is downloaded, the login screen displays.

3 From the login screen, type in the assigned username in the **Username:** field (the username is not case sensitive) and the assigned password in the **Password:** field (the password is case sensitive), then click **Log On**.

4 You will be prompted to enter a new password.

Note: When the user logs in for the first time after being added or after a password reset, the logon command will prompt the user to enter a new password. The logon command will require the user to enter the default password first, then enter the new password and then to confirm the new password.

5 Click **Log On** again. The current status / configuration settings of all of the switches connected to the users TestStream Management Server is now downloaded to the TestStream Management Client.

The TestStream Management Client main screen displays (refer to TestStream Management Main Screen on page 2-15).

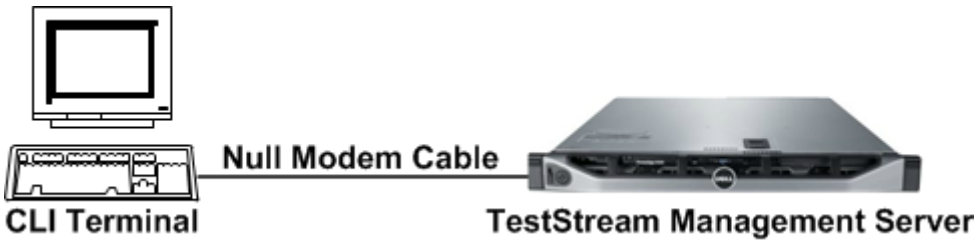
Note: During this login period, the TestStream Management application momentarily freezes all actions occurring on the TestStream Management server, gathers all of the information on the TestStream Management server controlling the switch, and copies the information to the TestStream Management Client. Once the login is successful, the client user now has the switches current up to date information, insuring that the client is fully synchronized with the actions of the switch.

Important: The account is locked after a defined number (refer to Change Security Policy on page 2-31) of consecutive unsuccessful password login attempts. To unlock the account, login to TestStream Management using an account with **administrative** privileges and reset the password (to the default value) of the locked account (refer to Reset a User Password on page 2-31). All failed login attempts and login locking / unlocking are logged in the audit trail.

If not already done, NETSCOUT recommends updating the Username and Password from the default settings (refer to User Accounts on page 2-30 and Change Password on page 2-37).

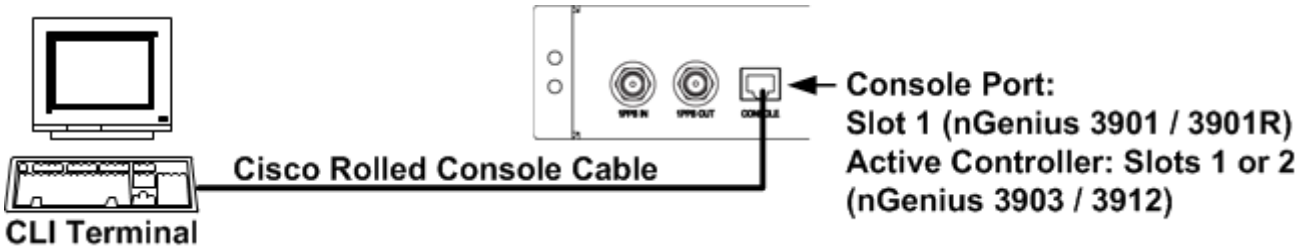
CLI Access to the TestStream Management Server

To operate TestStream Management using Command Line Interface (CLI) commands, connect a Null Modem Cable from a PC/Terminal to the TestStream Management server. From the PC/Terminal set a terminal emulator (e.g., Procomm) to the following settings: 8N1, 115200 baud, local echo off, no flow control.



CLI Access using an nGenius 3900 Series Blade Console Port

To operate TestStream Management Software using Command Line Interface (CLI) commands from an embedded blade, connect a Cisco Rolled Console Cable from a PC/Terminal to the CONSOLE port on the (active controller) blade. From the PC/Terminal, configure a terminal emulator (e.g., Procomm, Putty) to the following settings: 8N1, 115200 baud, local echo off, no flow control.



Refer to Starting a CLI Session on page A-3 for logging into and running a CLI session.

SSH Access Support on TestStream Management

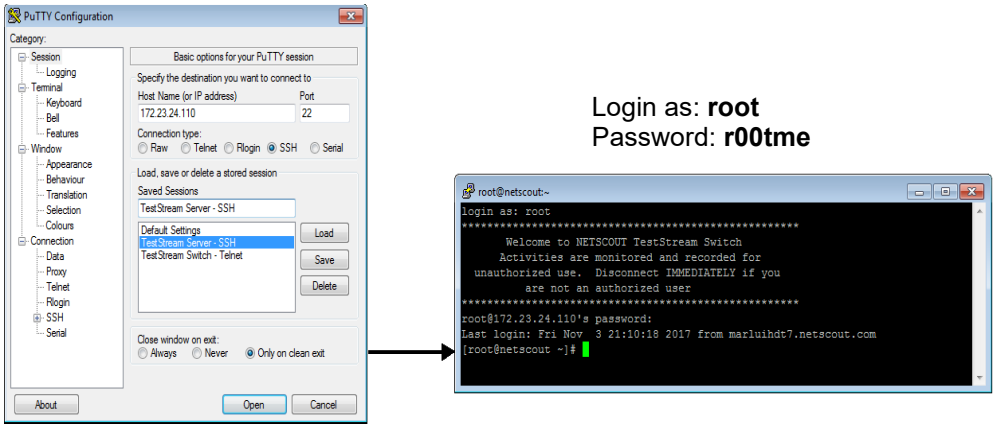
Three methods of SSH access are supported on TestStream Management:

- SSH access to the CLI: Provides an ssh session (configurable through the TestStream Client, **Tools > Configure > Remote Access**, refer to Configure Remote Access on page 4-25) redirecting the input to TestStream CLI telnet which only accepts TestStream CLI commands. To ssh to the CLI using port number 22022 (default), log in with:
  Username = **administrator**, Password = **netscout1**.

  Note: When the user logs in for the first time after being added or after a password reset, the logon command will prompt the user to enter a new password. The logon command will require the user to enter the default password first, then enter the new password and then to confirm the new password.

- Regular SSH for maintenance usage: Provides an ssh session to normal Linux shell commands for maintenance. To ssh using port number 22 (default), log in with:
  Username = **root**, Password = **r00tme**.

  Note: When the user logs in for the first time after being added or after a password reset, the logon command will prompt the user to enter a new password. The logon command will require the user to enter the default password first, then enter the new password and then to confirm the new password.

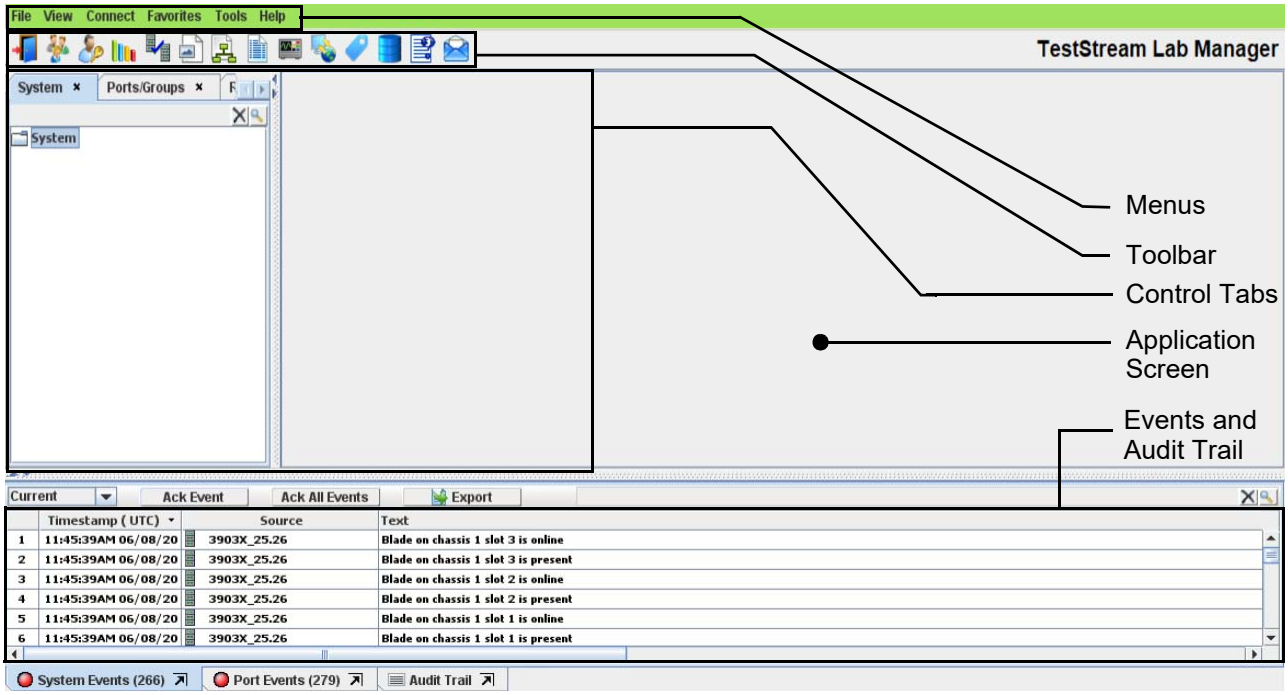


- tsadmin maintenance usage: Provides an ssh session to allow management activities from the Linux shell without having to log in as root. To ssh using port number 22 (default), log in with: Username = **tsadmin**, Password = **t3ststr3@m+lab+automation**

TestStream Management Main Screen

After logging on to the TestStream Management application, the TestStream Management main screen displays. The screen has five main sections:

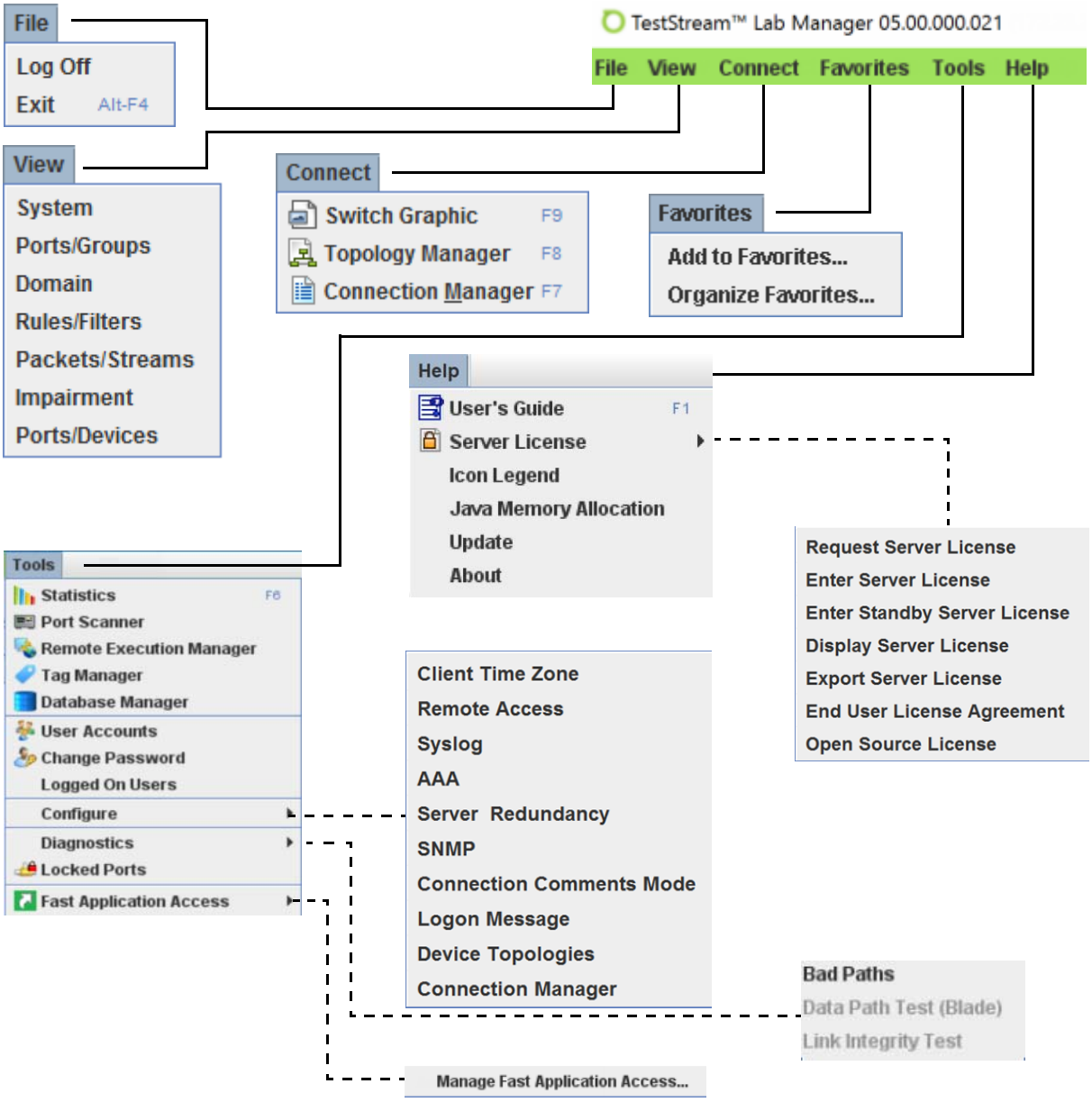
- Menus
- Toolbar
- Control Tabs
- Application Screen
- Events and Audit Trail



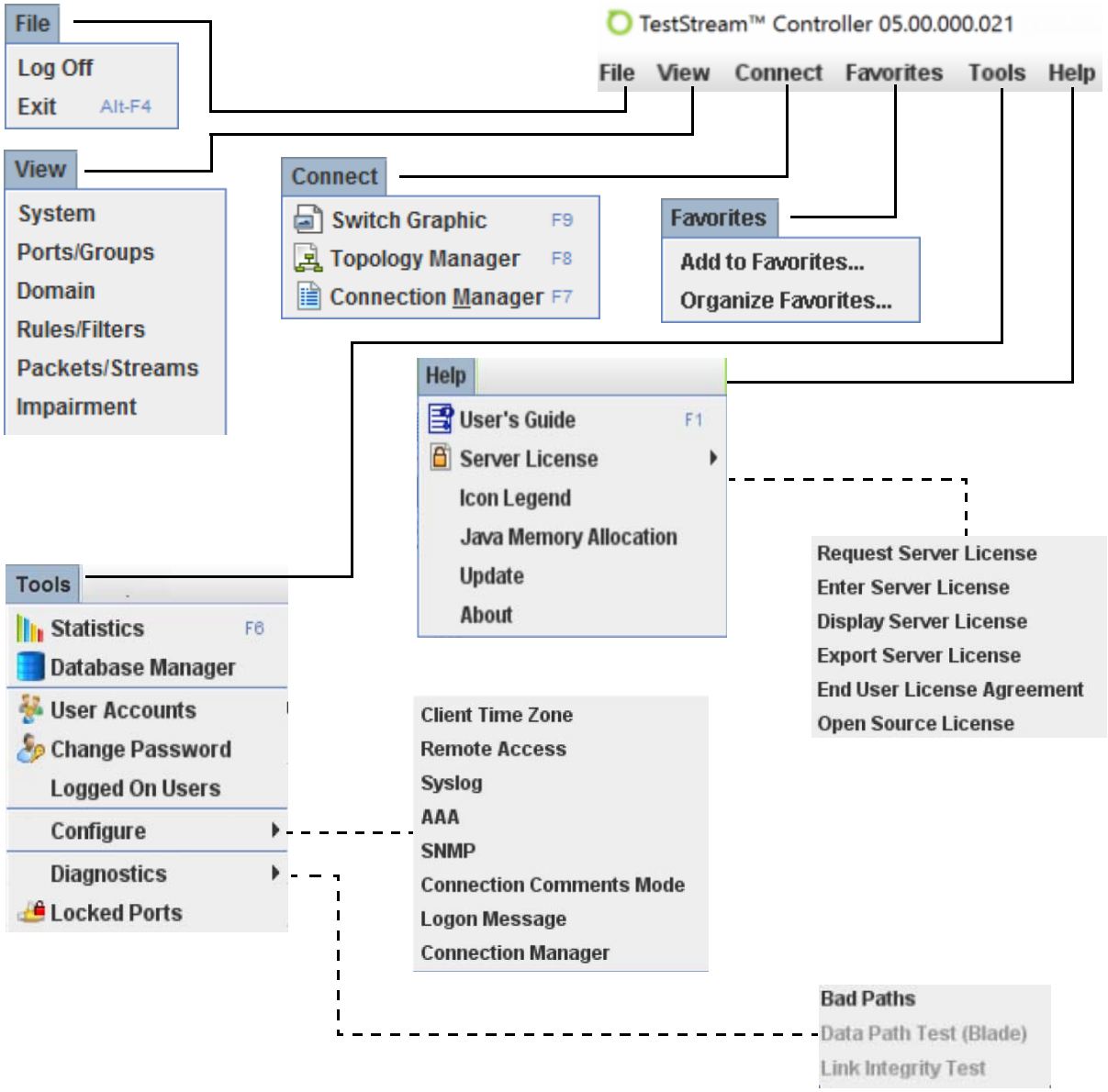
Menus

The menus are comprised of six sections for both TestStream Lab Manager and TestStream Controller.

TestStream Lab Manager menus:



TestStream Contoller menus:



- File - provides selections for TestStream Management user logoff and ending the current TestStream Management Software session.
- View - provides selection of the control tabs (System, Ports/Groups, Domain, Rules/Filters, Packets/Streams, Impairment, and Ports/Devices) refer to Control Tabs on page 2-19. Clicking on a tab name opens the selected tab function screen. Clicking the **X** next to the tab name closes the screen.
- Connect - provides the functions for switch/port interconnections.
- Favorites - used to manage bookmarks / links for launching a TestStream Management application.
- Tools - used to manage user access, configuration, and test functions.
- Help - access to the *TestStream Management Software Administrator Guide* (this document), TestStream Management server Licensing, Icon Legend chart, Java Memory Allocation information, TestStream Management server Updating, and About (TestStream Management server version information).

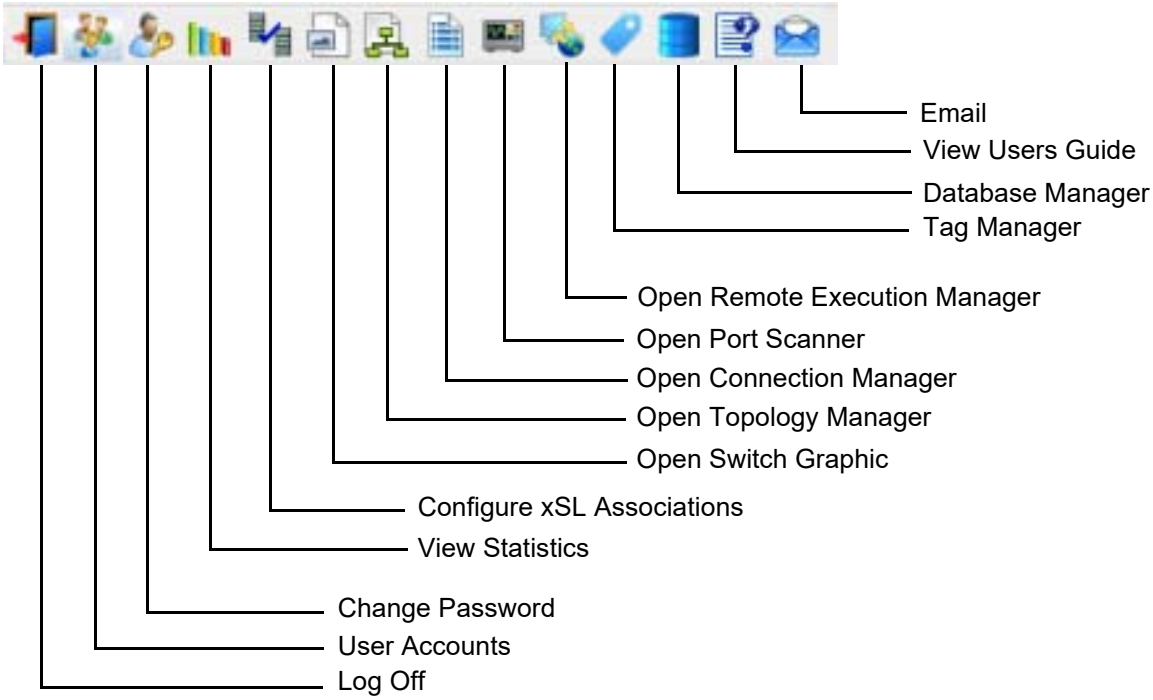
Menu Keyboard Shortcuts

In addition to point and click selection, the following menu items contain keyboard shortcuts:

- File > Exit: **Alt+F4**
- Connect > Switch Graphic: **Alt+F9**
- Connect > Topology Manager: **Alt+F8**
- Connect > Connection Manager: **Alt+F7**
- Tools > Statistics: **Alt+F6**
- Help > User's Guide: **Alt+F1**

Toolbar

The toolbar provides shortcuts for the commonly used TestStream Management functions.

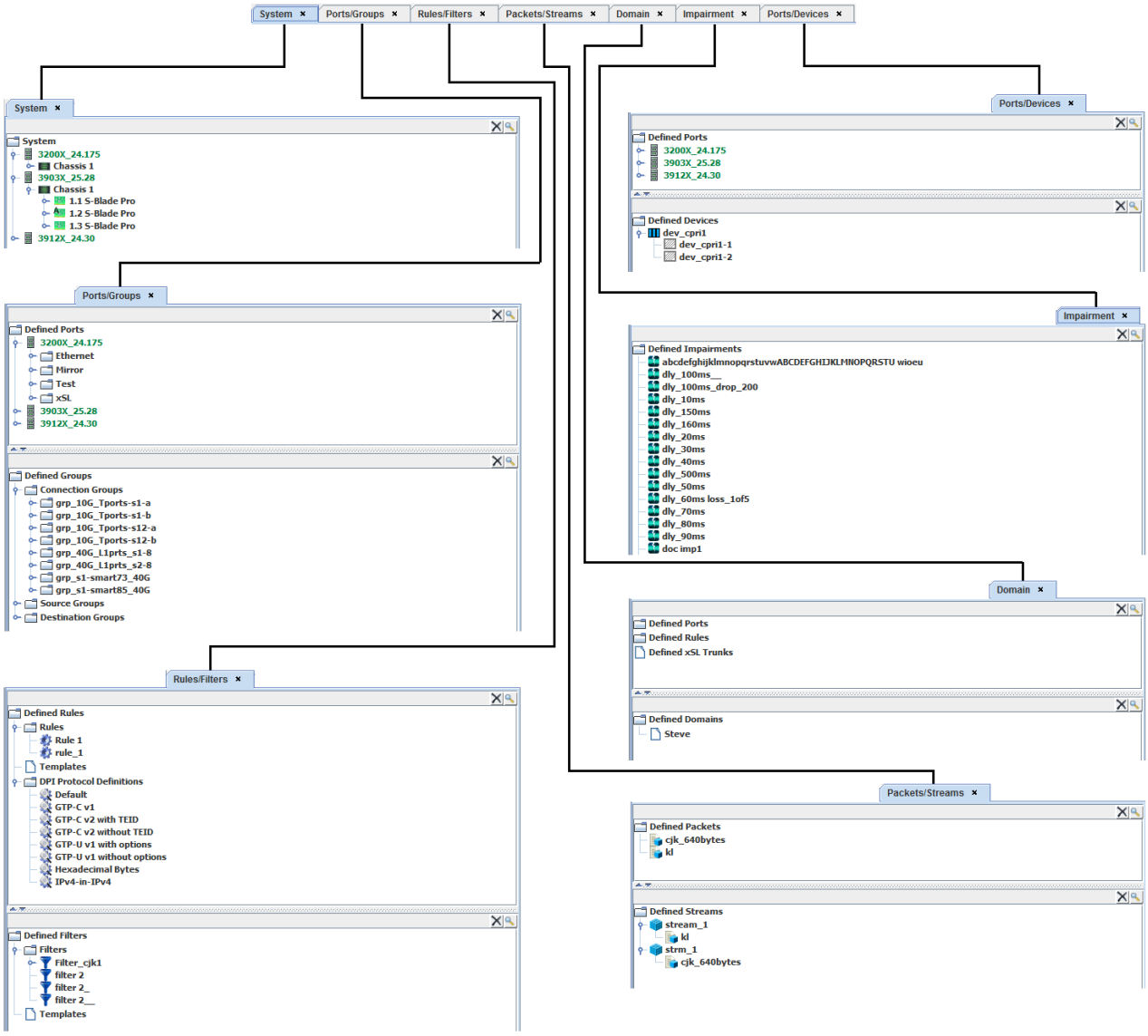


- Log Off TestStream Management (Log Off TestStream Management on page 2-55) - ends the current user session.
- User Accounts (User Accounts on page 2-30) - Add, Edit, Remove, and change Security Levels of assigned users (Administrator level only).
- Change Password (Change Password on page 2-37) - change logon password.
- View Statistics (Statistics on page 4-7) - displays System / Port Statistics and Port Utilization.
- Configure xSL Associations (xSL Trunk Configuration on page 3-105) - accesses the xSL Associations utility.
- Open Switch Graphic (Viewing Switch Details on page 3-13) - displays a graphic representation of a selected switch showing the installed chassis, blades, port status, and control modules.
- Open Topology Manager (Topology Manager on page 6-2) - accesses the Topology Manager.
- Open Connection Manager (Connection Manager on page 6-34)- accesses the Connection Manager.
- Open Port Scanner (Port Scanner (TestStream Lab Manager Only) on page 4-2) - accesses the Port Scanner.
- Open Remote Execution Manager (Remote Execution Manager (TestStream Lab Manager Only) on page 4-17) - accesses the Remote Execution Manager.
- Database Manager (Database Manager on page 4-20) - access to the Database backup functions.
- Tag Manager ( ) - access to user defined tags.

- View User's Guide (User's Guide on page 2-40) - link to the *TestStream Management Software Administrator Guide* (this document) located on My.NETSCOUT.com.
- Email NETSCOUT Customer Support (Email NETSCOUT Customer Support on page 2-39)- contact NETSCOUT's Customer Support in case of difficulty.

Control Tabs

Switch configuration and control is accomplished from the seven control tabs:



- System (System on page 3-1) - provides a physical view of the devices (switch model, chassis, installed blades – types, ports, status of each port (connected, not connected, monitored).
- Ports/Groups (Ports/Groups on page 3-185) - allows viewing of defined ports and groups (if created) in a switch and creation or modifications of groups.
- Rules/Filters (Rules/Filters on page 3-188) - allows custom defining of packet fields.
- Packets/Streams (Packets/Streams on page 3-222) - allows a user to construct individual packets and define one or more packet streams for test generation purposes.
- Domain (Domain on page 3-237) - allows defining a set of accessible ports under a unique user-defined name.
- Impairment (Impairment on page 3-231) - allows constructing individual impairments used to create disruptive packet-based test streams for testing purposes.

- Ports/Devices (Ports/Devices (TestStream Lab Manager Only) on page 3-239) - allows defining / creating devices and adding ports to the created devices. This control tab is for TestStream Lab Manager only and does not appear on the TestStream Controller display.

Note: The positioning of the control tabs are fluid, determined by the order a tab is selected from the View menu (refer to Menus on page 2-16). Clicking the **X** next to the tab name closes the screen.

Application Screen

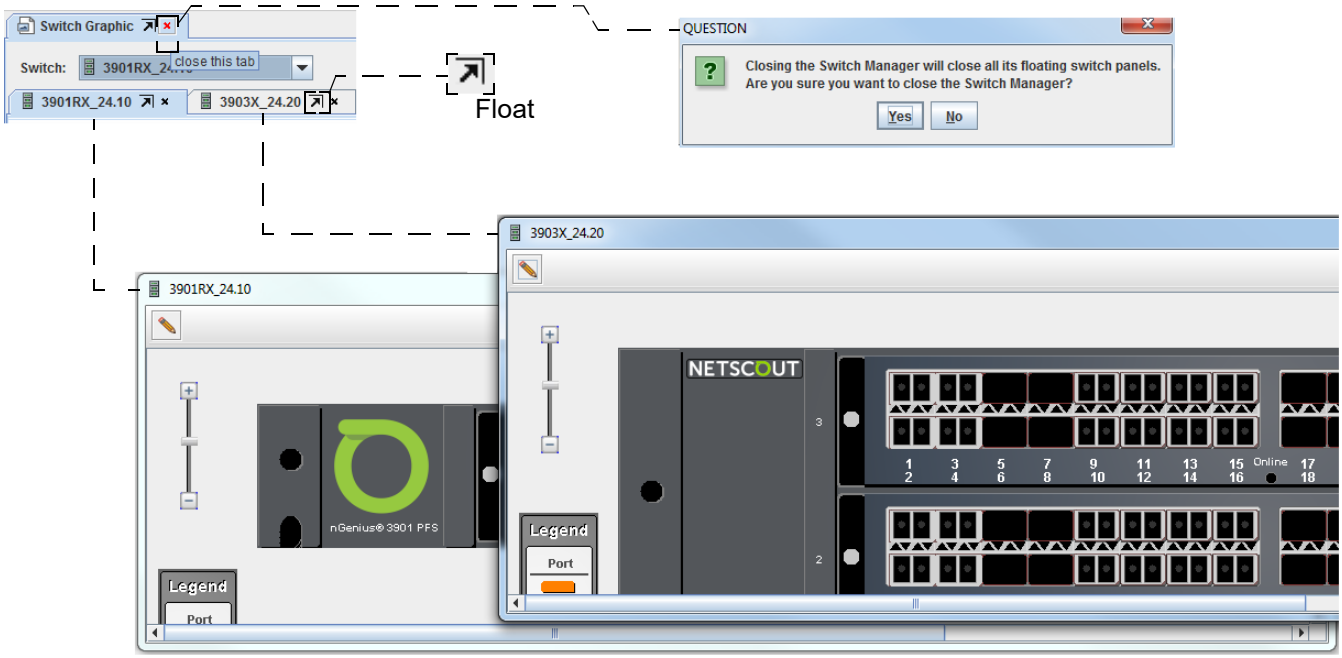
The Application Screen is used to display the following:

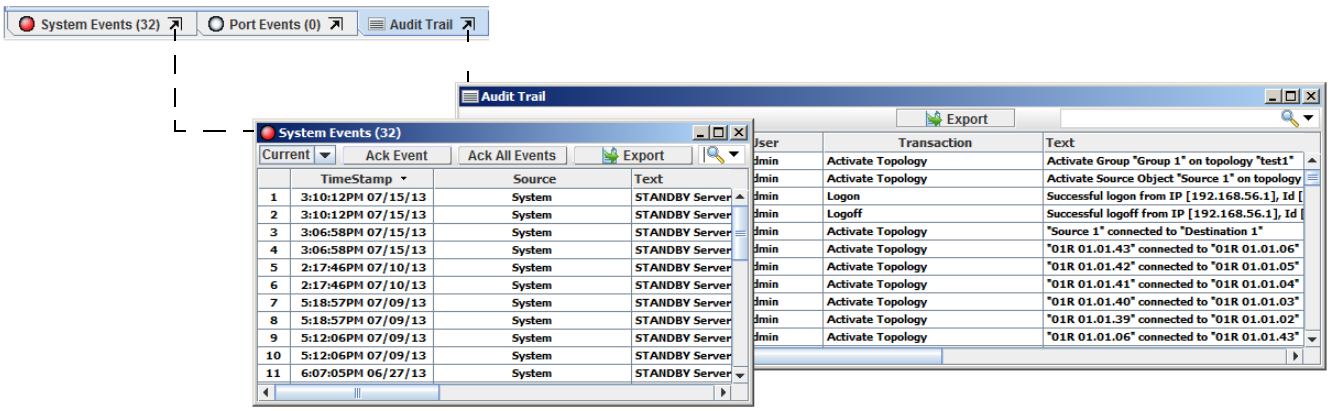
- Switch/Chassis/Blade views for scheduling and control.
- System Statistics to display real time and historical port statistics for switches in the network.
- Connection and Topology Managers to view and control live connections.
- xSL configuration, Scanners, and REM

Floating Windows

To improve visibility and usability, the event (System / Port / Audit Trail) and feature (Switch Graphic / Topology Manager / Connection Manager / Statistics) tabs support a floating window mode. Clicking on the float icon (located at the upper right corner of an event or feature tab) separates (undocks) the selected window from the main TestStream Management screen. The selected window can then be positioned as required for ease of visibility. All floating windows retain the same functions as a docked window.

Closing (docking) a floating window, by clicking on the **X**, returns the window to the main TestStream Management screen. Closing a main screen (e.g., Switch Graphic tab) while having associated floating windows displayed prompts a warning message requesting a confirmation. All floating windows are returned to the main TestStream Management screen upon logout or exit of TestStream Management.


Switch Graphic
Switch:
3901RX_24.10
3903X_24.20
close this tab
Float
QUESTION
Closing the Switch Manager will close all its floating switch panels.
Are you sure you want to close the Switch Manager?
Yes
No
3903X_24.20
3901RX_24.10
NETSCOUT
nGenius® 3901 PFS
Legend
Port
Online


System Events (32)
Port Events (0)
Audit Trail
Audit Trail
Export
Transaction
Text
Activate Topology
Activate Group "Group 1" on topology "test1"
Activate Source Object "Source 1" on topology
Logon
Successful logon from IP [192.168.56.1], Id
Logoff
Successful logoff from IP [192.168.56.1], Id
"Source 1" connected to "Destination 1"
"01R 01.01.43" connected to "01R 01.01.06"
"01R 01.01.42" connected to "01R 01.01.05"
"01R 01.01.41" connected to "01R 01.01.04"
"01R 01.01.40" connected to "01R 01.01.03"
"01R 01.01.39" connected to "01R 01.01.02"
"01R 01.01.06" connected to "01R 01.01.43"
System Events (32)
Current
Ack Event
Ack All Events
Export
TimeStamp
Source
Text
1 3:10:12PM 07/15/13 System STANDBY Server
2 3:10:12PM 07/15/13 System STANDBY Server
3 3:06:58PM 07/15/13 System STANDBY Server
4 3:06:58PM 07/15/13 System STANDBY Server
5 2:17:46PM 07/10/13 System STANDBY Server
6 2:17:46PM 07/10/13 System STANDBY Server
7 5:18:57PM 07/09/13 System STANDBY Server
8 5:18:57PM 07/09/13 System STANDBY Server
9 5:12:06PM 07/09/13 System STANDBY Server
10 5:12:06PM 07/09/13 System STANDBY Server
11 6:07:05PM 06/27/13 System STANDBY Server

Events and Audit Trail

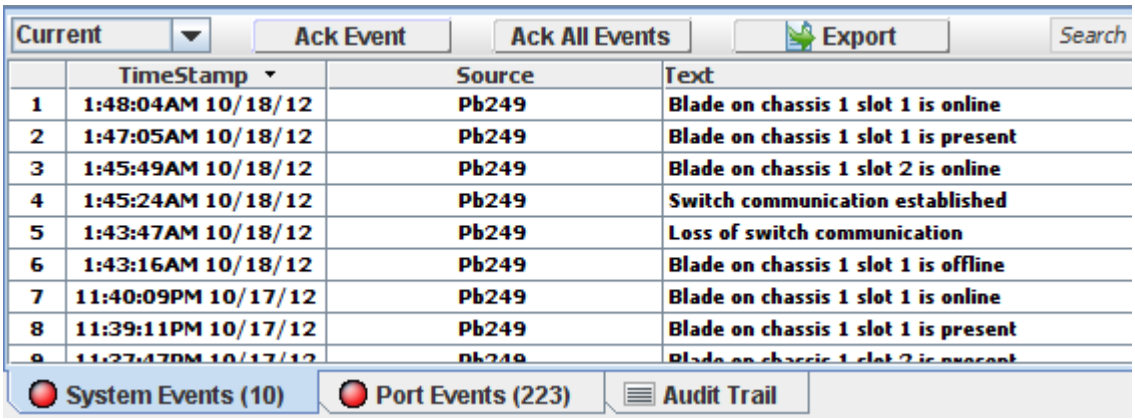
The Events section maintains a log of system and port events, and an audit trail. Current and previous events / audit trails (up to 180 days or 50,000 entries) can be reviewed as required. The user can acknowledge all events or selected events when required. The displayed events can be saved to a CSV format file when required.

Each tab has a right-click accessible popup menu (Filters / Print / Export / Float):

- **Filters** allows sorting and viewing of defined parameters: source, date range (start – end dates).
- **Print** sends data in a table format to a user-defined printer.
- **Export** allows saving the data into an Excel (CSV) file format.

System Events

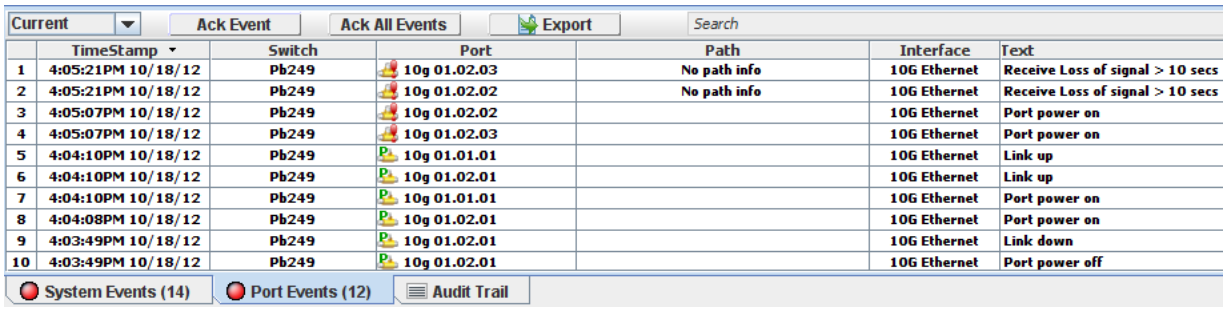
System events display the event time, source, and description of the event.



	TimeStamp	Source	Text
1	1:48:04AM 10/18/12	Pb249	Blade on chassis 1 slot 1 is online
2	1:47:05AM 10/18/12	Pb249	Blade on chassis 1 slot 1 is present
3	1:45:49AM 10/18/12	Pb249	Blade on chassis 1 slot 2 is online
4	1:45:24AM 10/18/12	Pb249	Switch communication established
5	1:43:47AM 10/18/12	Pb249	Loss of switch communication
6	1:43:16AM 10/18/12	Pb249	Blade on chassis 1 slot 1 is offline
7	11:40:09PM 10/17/12	Pb249	Blade on chassis 1 slot 1 is online
8	11:39:11PM 10/17/12	Pb249	Blade on chassis 1 slot 1 is present

Port Events

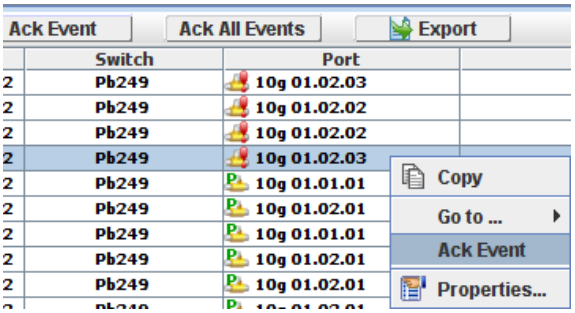
Port events display the event time, switch, port, connection path (to-from), type of port interface, and description of the event.



	TimeStamp	Switch	Port	Path	Interface	Text
1	4:05:21PM 10/18/12	Pb249	10g 01.02.03	No path info	10G Ethernet	Receive Loss of signal > 10 secs
2	4:05:21PM 10/18/12	Pb249	10g 01.02.02	No path info	10G Ethernet	Receive Loss of signal > 10 secs
3	4:05:07PM 10/18/12	Pb249	10g 01.02.02		10G Ethernet	Port power on
4	4:05:07PM 10/18/12	Pb249	10g 01.02.03		10G Ethernet	Port power on
5	4:04:10PM 10/18/12	Pb249	10g 01.01.01		10G Ethernet	Link up
6	4:04:10PM 10/18/12	Pb249	10g 01.02.01		10G Ethernet	Link up
7	4:04:10PM 10/18/12	Pb249	10g 01.01.01		10G Ethernet	Port power on
8	4:04:08PM 10/18/12	Pb249	10g 01.02.01		10G Ethernet	Port power on
9	4:03:49PM 10/18/12	Pb249	10g 01.02.01		10G Ethernet	Link down
10	4:03:49PM 10/18/12	Pb249	10g 01.02.01		10G Ethernet	Port power off

Acknowledging Events

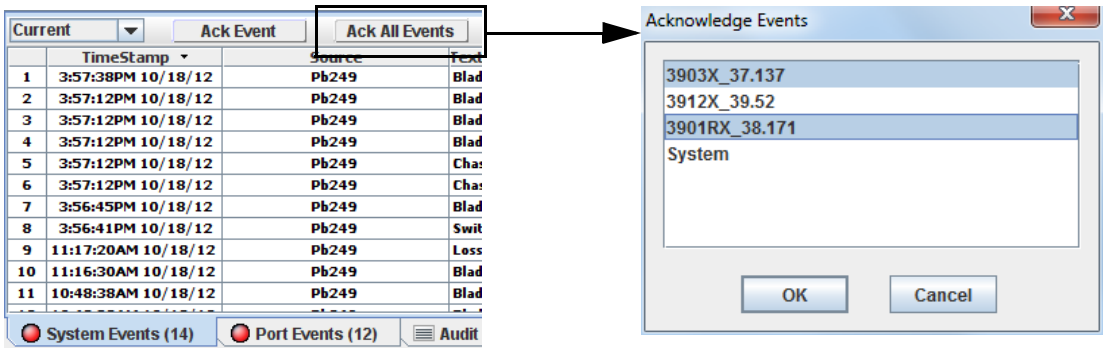
Acknowledging system and port events from the Events/Audit Trail section is accomplished by selecting either the Ack Event / Ack All Events buttons or by a drop down menu and selecting **Ack Event**, allowing the option to select one or more desired switches to acknowledge events.



Acknowledging System/Port Events on Multiple Switches

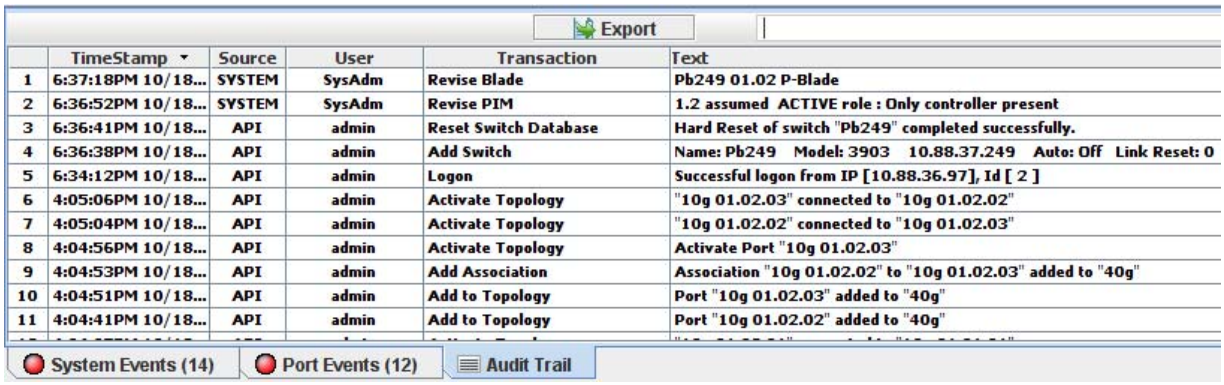
To acknowledge system or port events on one or more switches at a time:

1. From the Events/Audit Trail section, select the System or Port Event tab (where the events are indicated by the number of recorded events) then click on **Ack All Events**. An Acknowledge screen displays.
2. Select the required switches (even if there is only a single switch on your network), then click **OK**. All events on the selected switches are now acknowledged.



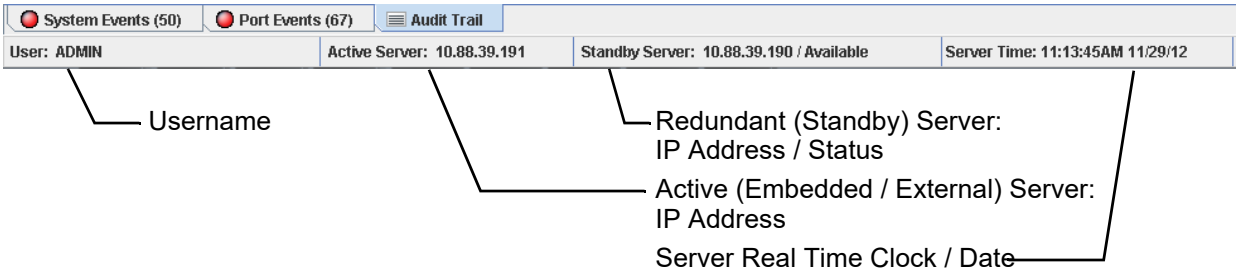
Audit Trail

Maintains a list of all transactions to the TestStream Management server. The audit trail can be exported to a CSV file format when required.



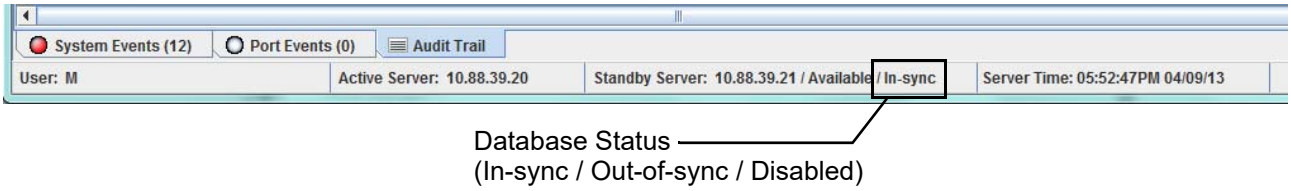
Server Status

An information bar located under the System/Port Events and Audit Trail tabs displays the current logged in User, TestStream Management server(s) status (embedded / external / redundant and IP addresses), and logged in Server Real Time Clock. The Standby Server information displays when redundant server capability is defined (refer to Configure Server Redundancy on page 4-37).



Database Synchronization Status

The information status bar displays the synchronization status of the connectivity database between the active and standby servers.



The status states are:

- **In-sync** - Redundancy is configured and the standby server database is currently identical to the active server
- **Out-of-sync** - Redundancy is configured but currently unavailable (i.e., network or server down)
- **Disabled** - Redundancy is disabled due to upgrade, database restore, roll back, or misconfiguration

CLI Functionally

The **SHO**w **SERV**ers command contains an optional **DET**ails parameter. If DETails is specified, the synchronization state of the standby database is also displayed.

The output for **SHOw SERVERs** command is similar to the following:

```
Online Server:    10.88.38.210    AVAILABLE
Standby Server:   10.88.38.211    AVAILABLE
```

The output for **SHOw SERVERs DETails** command is similar to the following:

```
Online Server:    10.88.38.210    AVAILABLE
Standby Server:   10.88.38.211    AVAILABLE / In-sync
```

Alternative forms for the Standby Server are:

```
Standby Server:   10.88.38.211    AVAILABLE / Out-of-sync
Standby Server:   10.88.38.211    AVAILABLE / Disabled
```

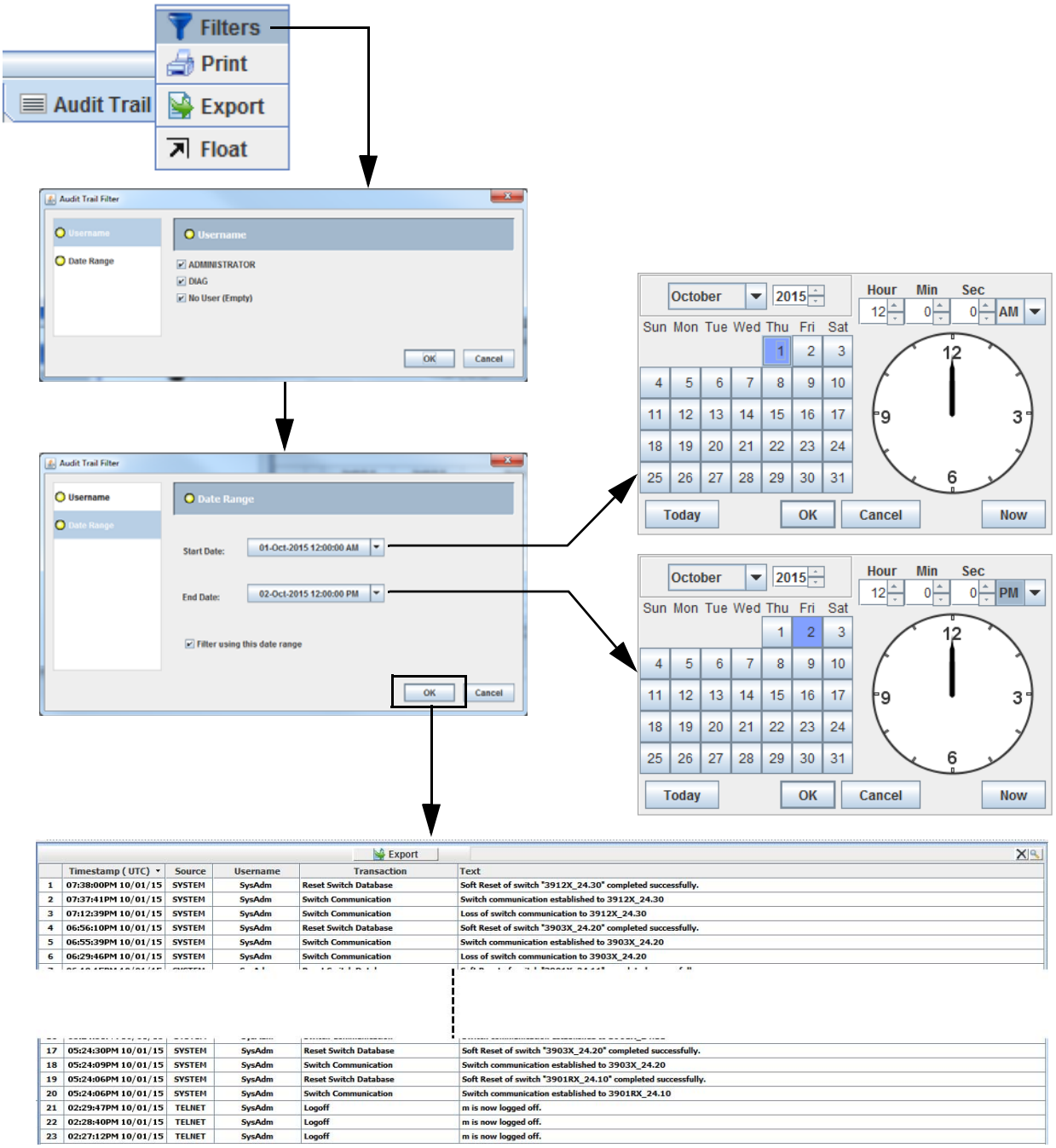
Filter Reports

Collected data (i.e., system - port, audit trails, and test results) can be located and displayed for a defined time period.

As an example, an audit trail report for a switch is required for a 12-hour period on October 1, 2015.

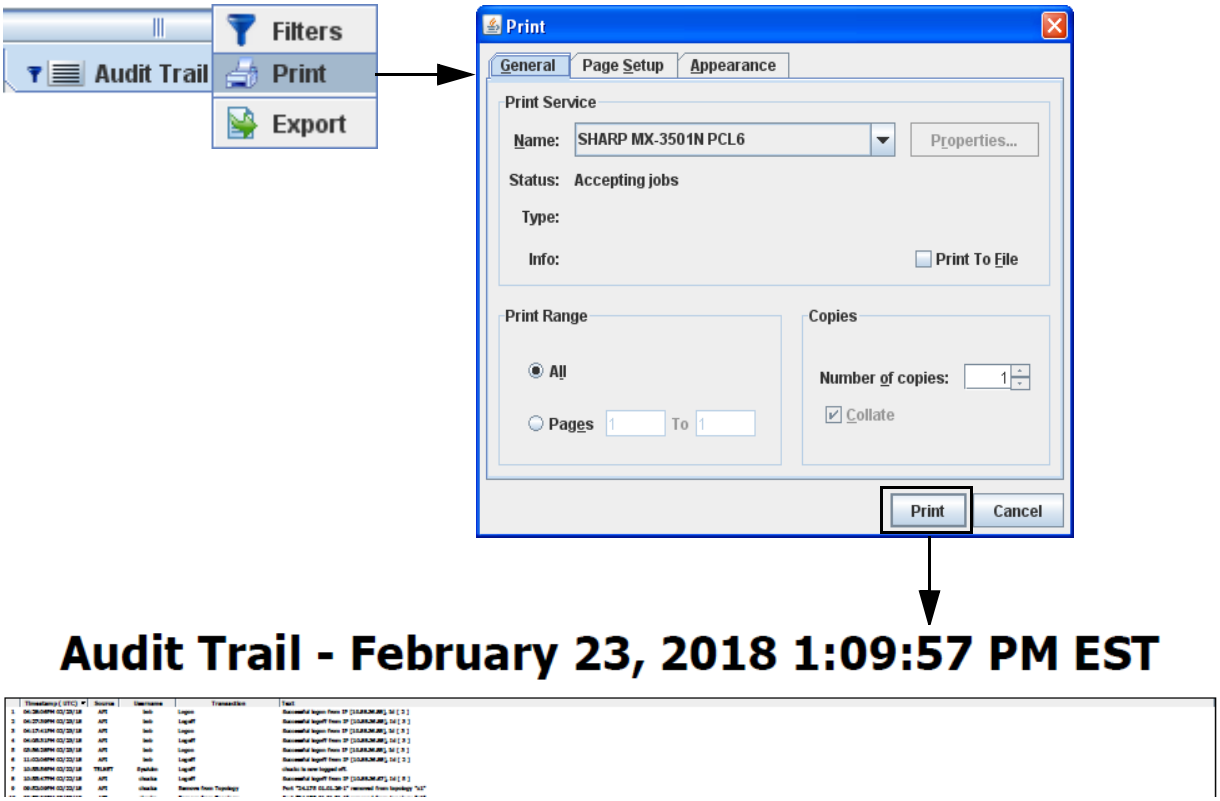
1. From the alarm display section, right-click the Audit Trail tab and select **Filters**. The Audit Trail Filter screen displays.
2. From the User screen, check the required users for the audit report.

3 From the Date Range screen, define the start and end dates of the search. Check the Filter Using this Date Range box. Click **OK**. the results of the audit filter are displayed in the alarm section.



Print Reports

Collected data can be printed in a table format to a user-defined printer.

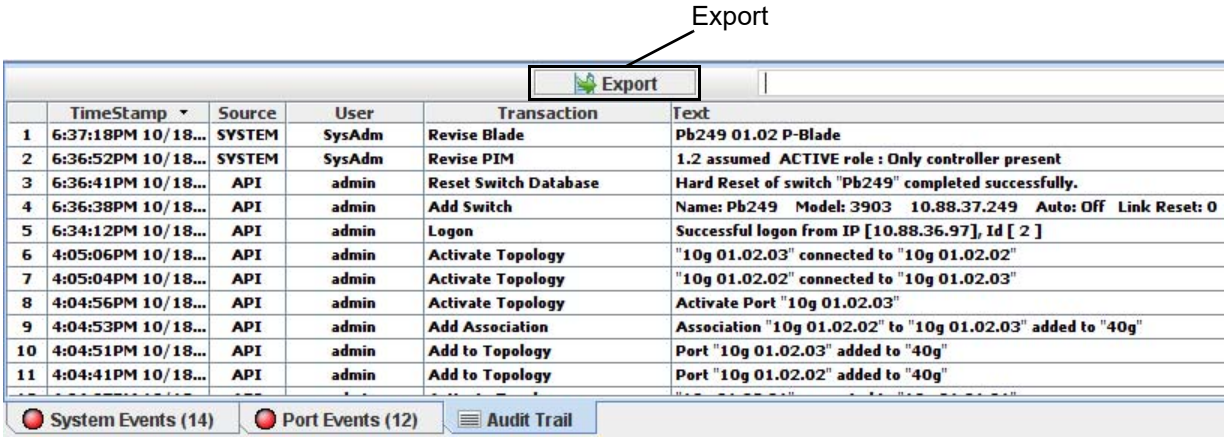


Exporting Reports

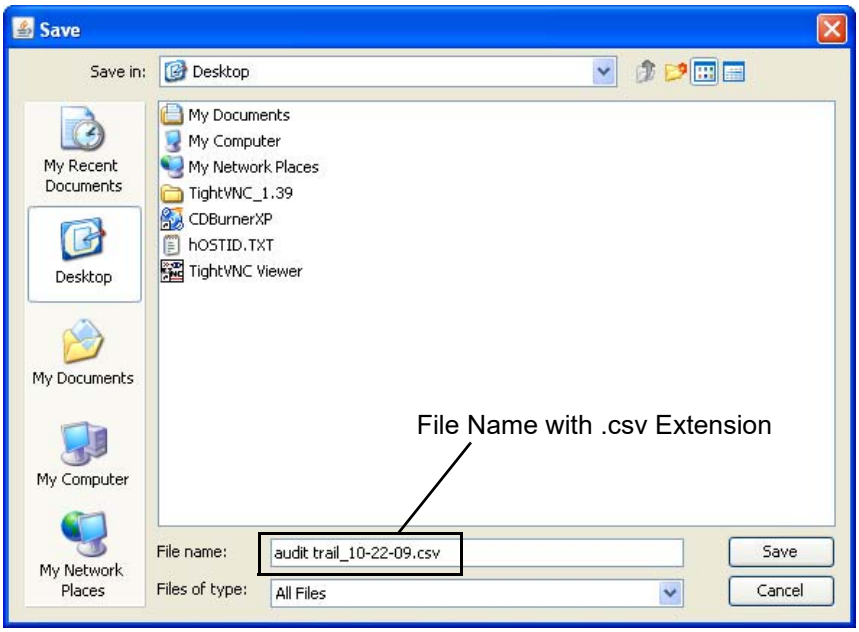
Collected data (i.e., system and port events, audit trails, and test results) can be exported to a CSV file format for use in an Excel spreadsheet or other application.

As an example, an audit trail report for a switch is required for an Excel spreadsheet.

1 From the Alarm section, select **Audit Trail**.



2 Click **Export**, a Save File screen displays. In the File name field, enter the name of the file being exported along with the extension (.csv). Click **Save**.



The file can now be opened in Excel or any other application capable of reading the CSV file format.

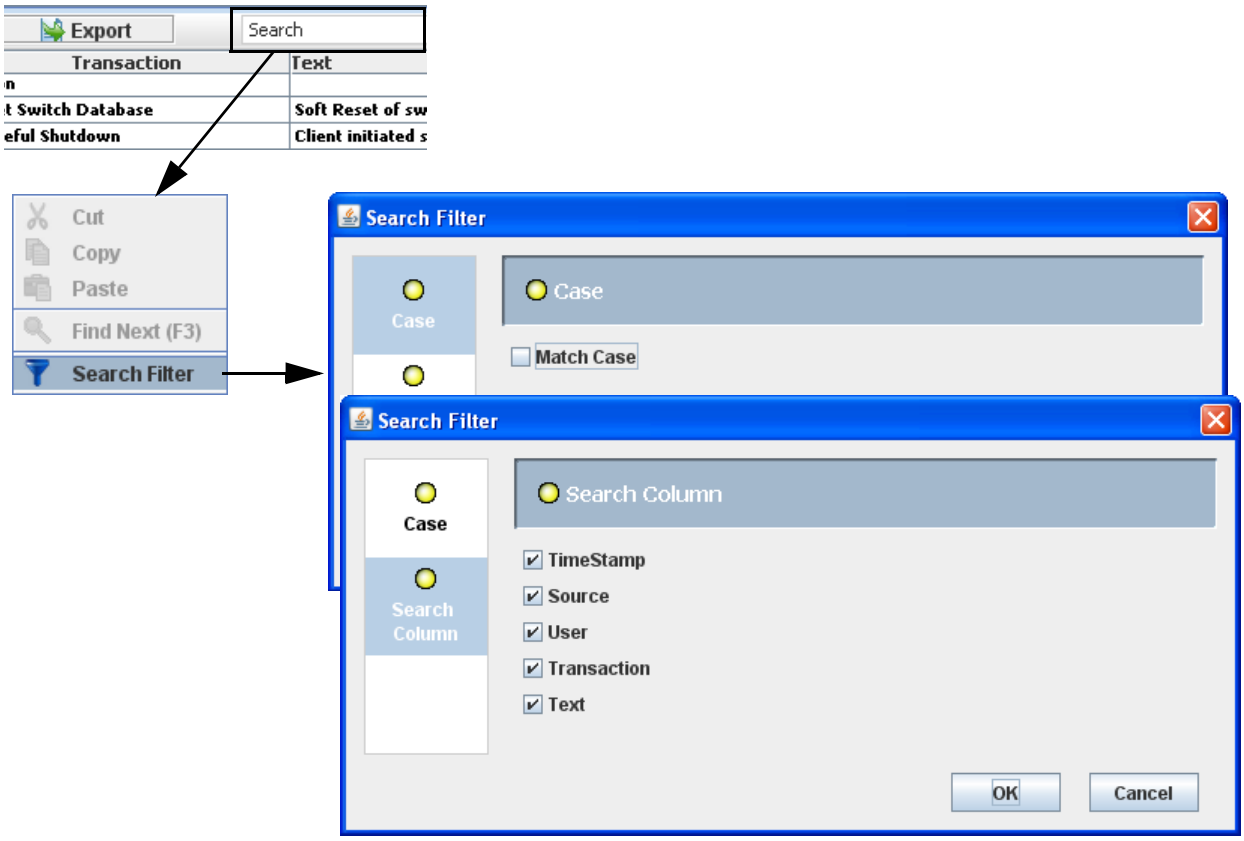
	A	B	C	D	E	F	G	H	I	J	K	L
1	TimeStamp	Source	User	Transaction	Text							
2	11:43:52Am 10/22/09	API001	ADMIN	LOGON								
3	5:27:17Pm 10/21/09	API001	ADMIN	LOGOFF								
4	2:26:56Pm 10/21/09	API001	ADMIN	CON PORT	4G - 1.2.26	4G - 1.2.28			WARNING: Port is already connected			
5	1:07:28Pm 10/21/09	API001	ADMIN	LOGON								
6	5:32:46Pm 10/20/09	API001	ADMIN	LOGOFF								
7	4:03:51Pm 10/20/09	API001	ADMIN	LOGON								
8	3:51:33Pm 10/20/09	API001	ADMIN	LOGOFF								
9	2:59:39Pm 10/20/09	API001	ADMIN	LOGON								
10	1:43:53Pm 10/20/09	API001	ADMIN	LOGOFF								
11	1:38:23Pm 10/20/09	API001	ADMIN	LOGON								
12	12:12:26Pm 10/20/09	API001	ADMIN	LOGOFF								
13	11:59:20Am 10/20/09	API001	ADMIN	LOGON								
14	4:22:14Pm 10/16/09	API001	ADMIN	LOGOFF								
15	3:40:12Pm 10/16/09	API001	ADMIN	LOGON								
16	3:39:46Pm 10/16/09	API001	ADMIN	LOGOFF								
17	2:12:48Pm 10/16/09	API001	ADMIN	LOGOFF								
18	11:30:30Am 10/16/09	API001	ADMIN	LOGON								
19	11:19:33Am 10/16/09	API001	ADMIN	CON PORT	4G - 1.2.26	4G - 1.2.28						
20	11:02:21Am 10/16/09	API001	ADMIN	LOGON								
21	10:58:28Am 10/16/09	API001	ADMIN	LOGOFF								
22	10:57:06Am 10/16/09	API001	ADMIN	CFG PIM	SW2920	Chassis 01 DCE/DCE 12						
23	10:56:30Am 10/16/09	API001	ADMIN	CFG PIM	SW2920	Chassis 01 DCE/DCE 11						
24	10:55:29Am 10/16/09	API001	ADMIN	CFG PIM	SW2920	Chassis 01 UFC-DC32 02						
25	10:55:29Am 10/16/09	API001	ADMIN	CFG PIM	SW2920	Chassis 01 UFC-DC32 01						
26	10:55:03Am 10/16/09	API001	ADMIN	CFG SWI	SW2920	2K Connectivity						
27	10:55:03Am 10/16/09	API001	ADMIN	CFG SWI	SW2920	Fabric-V						
28	10:55:03Am 10/16/09	API001	ADMIN	CFG SWI	SW2920	IP 1.1.1.1						
29	10:55:03Am 10/16/09	API001	ADMIN	CFG SWI	SW2920	2900 SP 2K						
30	10:54:40Am 10/16/09	API001	ADMIN	LOGON								
31	10:54:25Am 10/16/09	TSS		SYS STARTUP								
32	10:53:28Am 10/16/09	TSS		SYS EXIT								
33	10:52:38Am 10/16/09	API001	ADMIN	LOGON								
34	10:51:07Am 10/16/09	TSS		SYS STARTUP								
35	10:45:01Am 10/16/09	TSS		SYS EXIT								
36	8:03:31Am 10/16/09	API001	ADMIN	LOGON								
37	6:09:28Pm 10/15/09	API001	ADMIN	LOGON								
38	4:49:28Pm 10/15/09	API001	ADMIN	LOGON								
39	1:54:30Pm 10/15/09	API001	ADMIN	LOGON								
40	9:25:52Am 10/15/09	TSS		SYS STARTUP								
41												

audit trail_10-22-09

Search / Filter

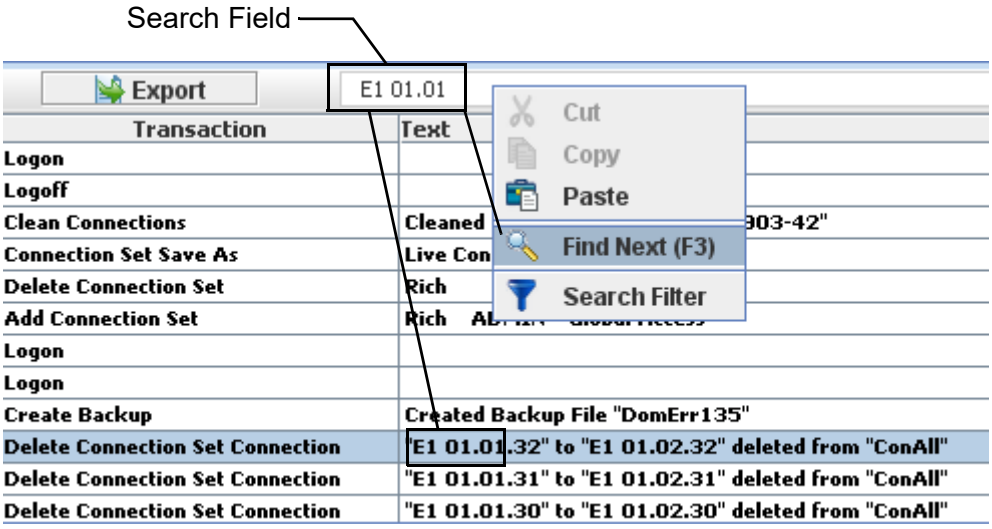
The search function allows the user to define the search parameters for a particular system / port event or audit trail based on selected column fields.

From the Alarm section, select the required system / audit trail tab. Right-click on the ***Search*** field. Select **Search Filter**. The Search Filter screen displays. From the Case and Search Column screens, click to select / unselect the fields required for the search query.



Find Next (F3)

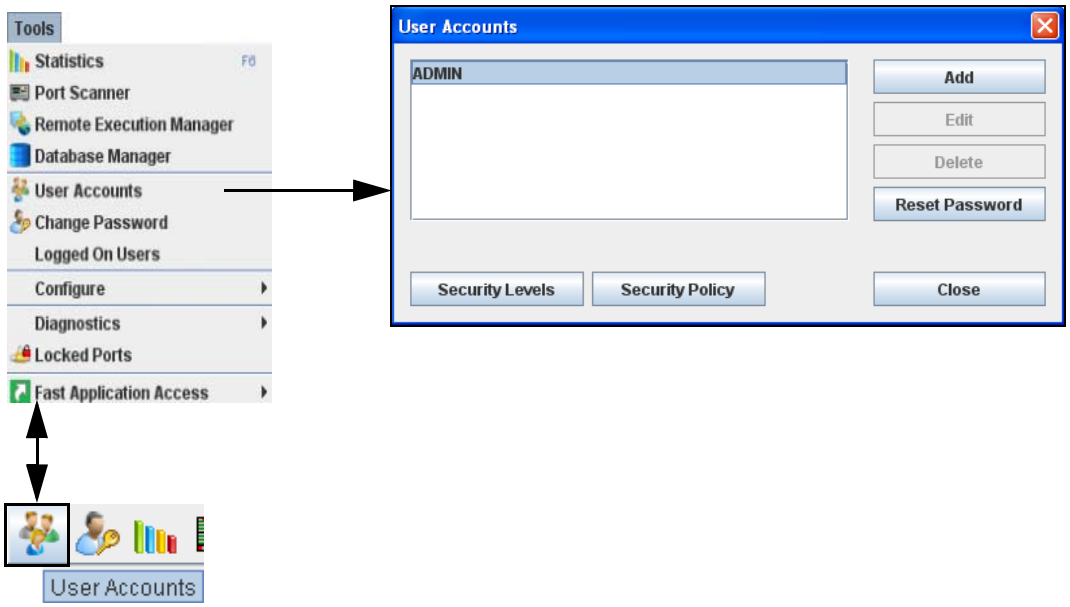
From the Search field, enter a variable name (e.g., logon, E1 01.01) to locate all occurrences starting with the name or part of a name. The first occurrence of the variable will be located. To locate additional occurrences of the same variable name, right-click on the search name and select **Find Next (F3)** or use the **F3** key. Continue using the F3 key to find all occurrences as required.



User Accounts

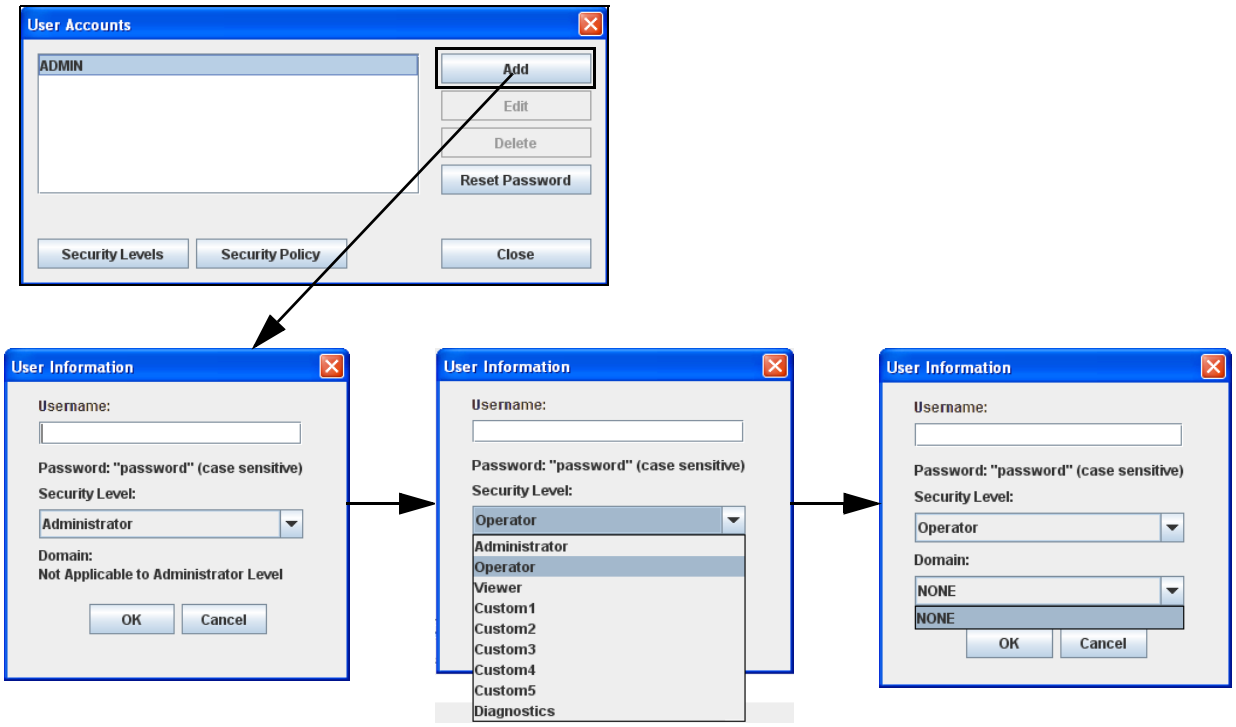
User Accounts, accessible from the Administrator user level, is used to assign, modify, or remove TestStream Management users and change the security levels of assigned users.

To access User Accounts, from the TestStream Management menu, select **Tools > User Accounts**, or from the toolbar, select the **User Accounts** icon.



Add User

1 From the User Accounts screen, click **Add**. The User Information screen displays,.



2 Enter the new Username - 1 to 50 characters, not case sensitive.

> **Note:** The following special characters are allowed when creating / modifying a username in TestStream Management:
> **~ ` ! @ # $ ^ & * - _ + { } [ ] | < > ? , . / : ;**

3 Select the required Security Level (refer to TestStream Management Software Security Levels on page 2-32):

- Administrator – access to all TestStream Management functions and limited diagnostics
- Operator – access to all TestStream Management functions except Switch
- Viewer – no access to TestStream Management control functions; monitor and testing only
- Diagnostics - full access to all TestStream Management diagnostic functions
- Custom – access functions definable

4 Select the Domain level (if required).

> **Note:** Domain levels are user-defined and user-named.
> A user with Administrator security level cannot have a domain.

5 Click **OK**. The user has been created with the default password (password).

6 Click **OK** to save the local settings.

Edit a User Account

From the User Accounts screen, select the user, then click **Edit**. Make changes as required (user name, security level, domain access). Click **OK** to save the updates.

Delete a User

From the User Accounts screen, select the user, then click **Delete**. A confirmation message displays. Click **Yes** to confirm.

Reset a User Password

Resets an assigned users' password to the TestStream Management default. From the User Accounts screen, select the user, then click **Reset Password**. A confirmation message displays. Click **Yes** to confirm.

Change Security Levels

A security level determines the transactions that a user can perform. The Security Level option allows editing available transactions for a previously defined security level, or define a new security level.

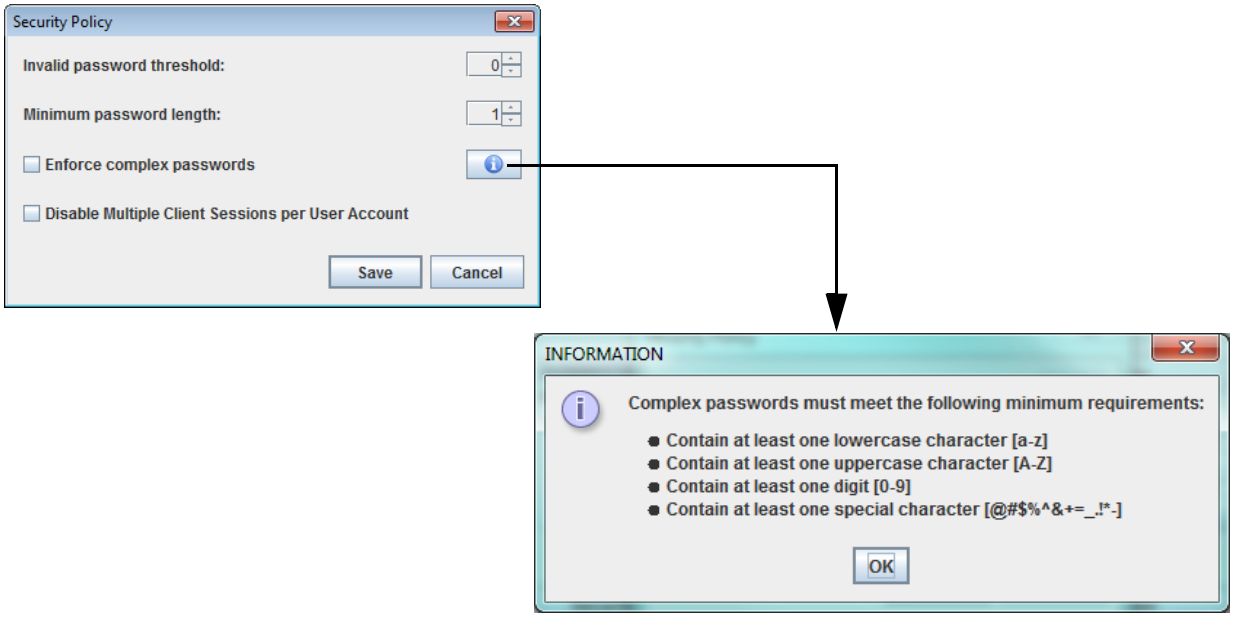
From the User Accounts screen, select the user, then click **Security Levels**. Select the required access level for the user. Make changes as required. Click **Save** to keep the updates.

Change Security Policy

TestStream Management supports a security policy for invalid password thresholds (i.e., the number of times an invalid password can be entered before the user is locked out of TestStream Management) and the minimum password character length.

> **Note:** To prevent any administrators from being completely locked out of the server, any account with administrator rights will be allowed to login through the serial port, even if it is locked. Once logged in through the serial port, the administrator can reset its own password.

From the User Accounts screen, select the user, then click **Security Policy**. The Security Policy screen displays.



Select the required invalid password threshold (default of zero (0) for no limit). Select the minimum password character length (minimum of one (1) character).

Optionally, select the check box to enforce complex passwords (refer to the information screen for the minimum requirements when creating a complex password).

Optionally, select the check box to prevent multiple client sessions being active from a single users account.

Click **Save** to keep the updates.

TestStream Management Software Security Levels

TestStream Management's security levels:

- Administrator – access to all TestStream Management functions and some diagnostics
- Operator – access to all TestStream Management functions except Switch
- Viewer – no access to TestStream Management control functions; monitor and testing only
- Diagnostics - full access to all TestStream Management diagnostic functions

are pre-defined / selected to allow TestStream Management access dependent on the users security setting. An additional level:

- Custom (1 - 5) – access functions definable

allows customized user settings by clicking on (all or part of) a feature. The following shows the pre-defined feature settings available at each security level.

		Security Level				
Feature		Administrator	Operator	Viewer	Diagnostics	Custom
Switch		X			X	
	Add	X			X	
	Revise	X			X	
	Delete	X			X	
	Clean Connections	X			X	

		Security Level				
Feature		Administrator	Operator	Viewer	Diagnostics	Custom
Blade		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Port		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Filter		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Rule		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Group		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
	Add Member	X	X		X	
	Remove Member	X	X		X	
	Move Member	X	X		X	
Packet Definition		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Stream		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
	Add Member	X	X		X	
	Remove Member	X	X		X	
	Move Member	X	X		X	
Stream Generator		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	

		Security Level				
Feature		Administrator	Operator	Viewer	Diagnostics	Custom
Scanner		X	X		X	
	Revise	X	X		X	
	Add Member	X	X		X	
	Remove Member	X	X		X	
	Move Member	X	X		X	
	Activate	X	X		X	
	Deactivate	X	X		X	
Connection		X	X		X	
	Port	X	X		X	
	Test Port	X	X		X	
	Group	X	X		X	
	xSL/PxSL	X	X		X	
Connection Set		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Topology		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Alarm		X	X		X	
	System Acknowledge	X	X		X	
	Port Acknowledge	X	X		X	
Diagnostics		X	X	X	X	
	Current Port Path	X	X	X	X	
Database		X	X		X	
	Backup	X	X		X	
	Restore	X	X		X	
	Manage	X	X		X	
Impairment		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Device		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	

		Security Level				
Feature		Administrator	Operator	Viewer	Diagnostics	Custom
Device Port		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Reservation		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Remote Server		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Remote Execution Profile		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Reservation Remote Execution		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	
Fast Application Access		X	X		X	
	Add	X	X		X	
	Revise	X	X		X	
	Delete	X	X		X	

Administrator-Specific Functions

The TestStream Management functions not selectable from the security table that are available only at the Administrator Level include:

- Blade - Shutdown, Restart, Reboot
- Domains
- Unlock All Ports
- SFM – Move Connections, Shutdown, Restart, Reboot
- Force-off Logged On Users
- Create Clone Port
- Configure Server Redundancy
- Configure SNMP
- Configure Syslog
- Configure Remote Access
- Configure AAA
- Configure Users
- Update/Rollback
- Configure Connections Comments Mode
- Configure Logon Message
- Enter License Key
- Enter Standby License Key
- Device Topologies

Note: The following user options listed under Security are not supported from TestStream Management:
Group > Move Member
Diagnostics > Data Generator
Diagnostics > Data Path Test (Port)
Diagnostics > Data Path Test (Blade)
Diagnostics > Display Bad Path
Diagnostics > Mark Bad Path
Diagnostics > UnMark Bad Path
Diagnostics > Link Integrity Test
Diagnostics > Port Flapping
Diagnostics > PIM Test
Diagnostics > Midplane Test
Diagnostics > Cable Characterization Test
Diagnostics > Cable Installation Test
Diagnostics > Status

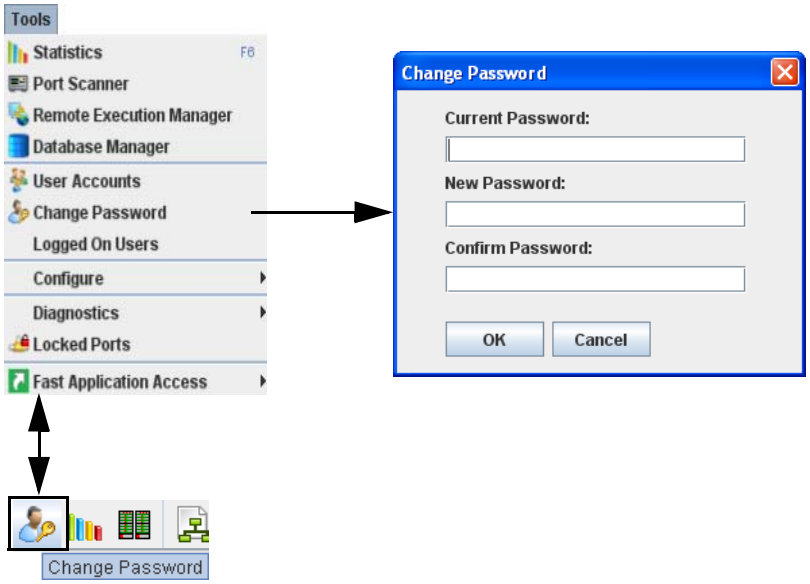
Change Password

When a new user account is created, a default password is assigned to the account. This password should be changed to a new value.

Note: After a new user account is created and the user logs in for the first time, a **Set Password** pop up window will display requesting that the new user change their password. Enter the new password, then confirm the new password and click **OK**.

Changing the Password from the TestStream Management GUI

1 Select **Tools > Change Password**, or from the toolbar, select the **Change Password** icon. The Change Password screen displays.



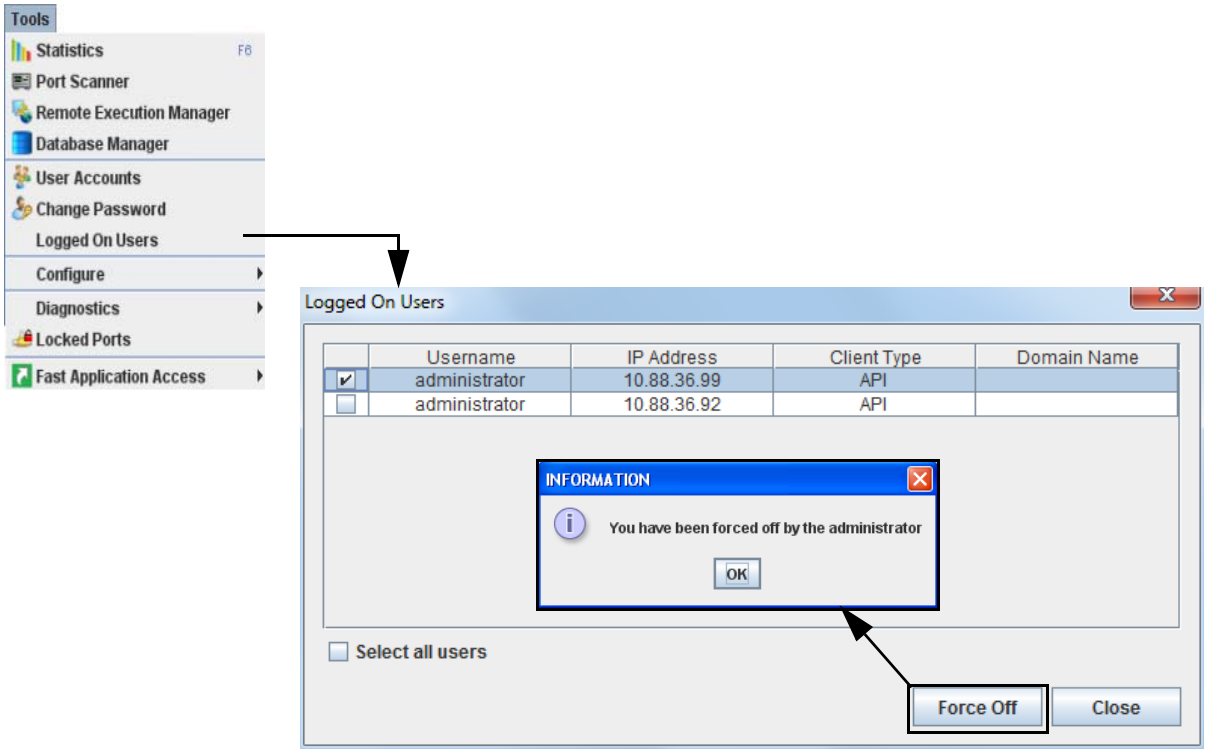
2 Enter the currently used password, then enter the new password (case sensitive, up to 95 characters long - all characters allowed for regular passwords).
For complex passwords, one of these special characters must be included:
@ # $ % ^ & + = _ . ! * -

3 Re-enter the new password for confirmation. Click **OK**.

Logged On Users

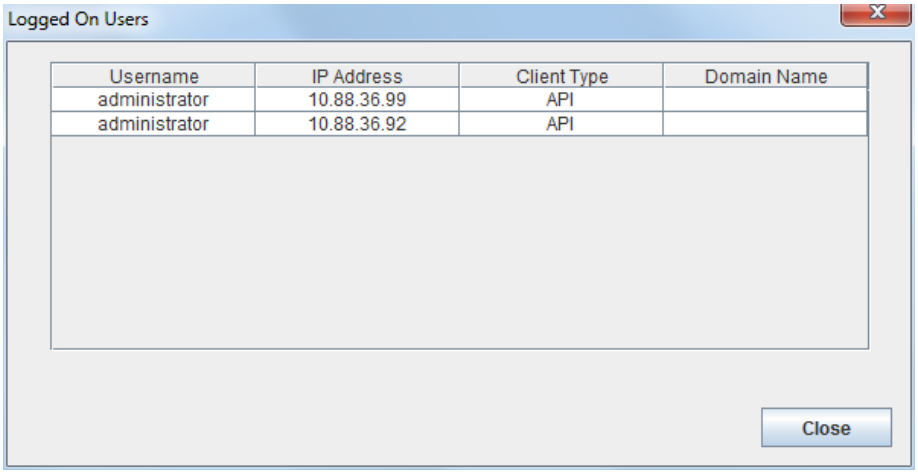
When updating the TestStream Management software, all users must be logged off from TestStream Management. This feature is used, from the administrative level, to remotely log off any users prior to performing a software update.

1 From the administrative level, select **Tools > Logged On Users**. The Logged On Users screen displays. All currently logged on users (other than the administrative user running Logged On Users) are identified.



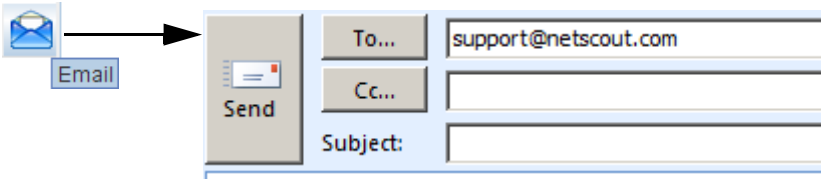
2 Select either separately, or click **Select all users** then click **Force Off** to end the users TestStream Management sessions.

Non-administrative users can display the list of logged users, but cannot perform a remote log-off.



Email NETSCOUT Customer Support

To send an email to NETSCOUT's Customer Support, click the **Email** icon. A message screen with NETSCOUT's service request email address displays. Enter the message text as required, then click **Send**.



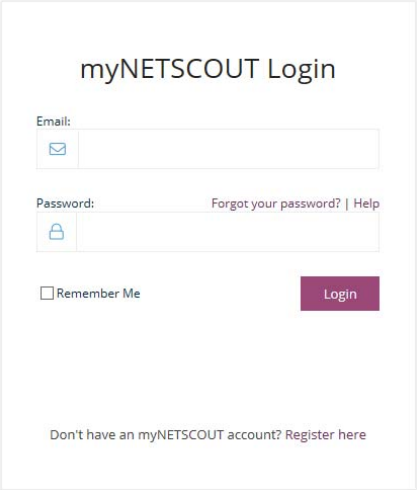
Help Menu

User's Guide

Note: Adobe Acrobat™ Reader 8.0 or later is required to read this manual. The latest version of Acrobat Reader is available for download from the Adobe web site at www.adobe.com.

Select **Help > User's Guide**, or the **View Users Guide** icon in the toolbar, or from the keyboard **Alt+F1** to access the *TestStream Management Software 5.1.0 Administrator Guide* (this document, in PDF format) from *My.NETSCOUT.com*.

Note: A *My.NETSCOUT* user account is required to access the *TestStream Management Software Administrator Guide.* Enter your assigned account username and password - if you do not have a *My.NETSCOUT* account you can create one from the *My.NETSCOUT.com* login screen (click **Register** and follow the User Registration instructions).

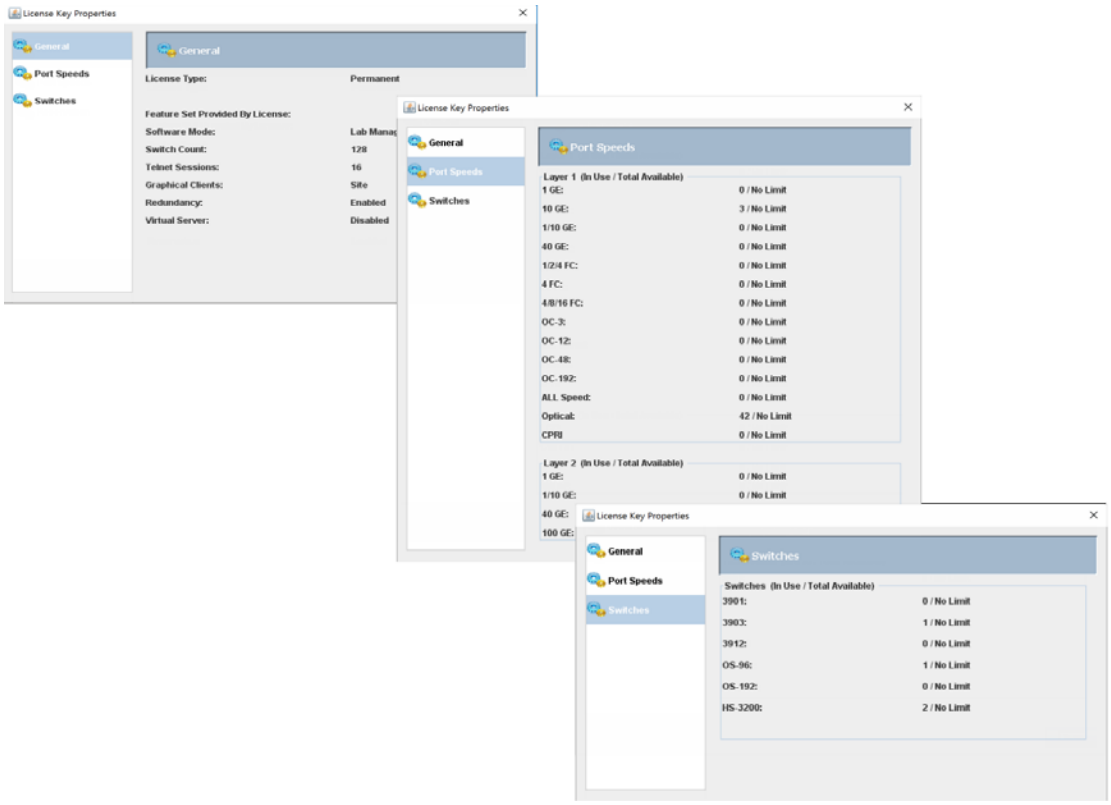


Your Internet browser (e.g., Internet Explorer, Firefox, Chrome, etc.) used to run TestStream Management Software must support the ability of opening PDF files natively from within the browser. In the event that your browser does not support opening PDF files, you can directly access the Administrator Guide from *My.NETSCOUT.com* using Adobe Acrobat Reader by entering the URL of the Administrator Guide:

https://my.netscout.com/mcp/Documents/TS_Mgmt_v520_AG_733-1614.pdf

Display Server License

To view the current status of the TestStream Management license, select **Help > Server License > Display Server License**. The License Key Properties window displays. The General tab shows the license features of the switch. Selecting Port Speeds displays license-specific supported interfaces for both Layer 1 and Layer 2. Selecting Reservation displays the number of switches enabled per switch type.



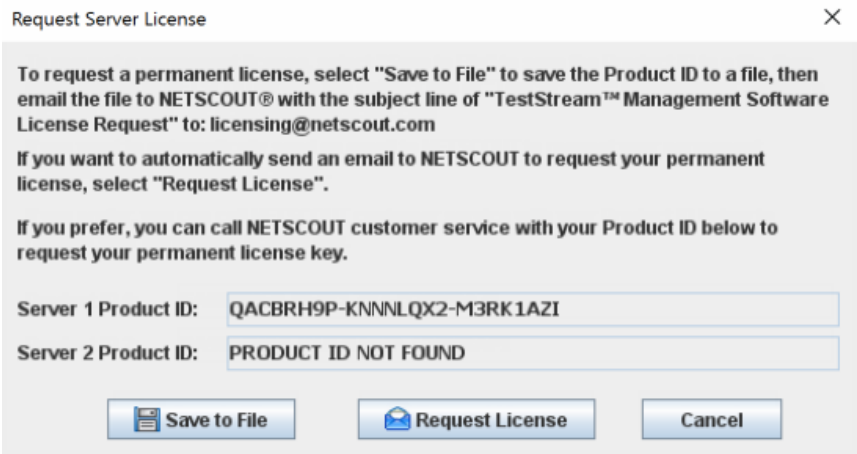
TestStream Management License Usage Guidelines

Note: The TestStream Management Server license allows a maximum of 32 nGenius 3900 series switches networked to the TestStream Management Server.

- Separate TestStream Management licenses are required for each primary and secondary TestStream Management Server - nGenius 3900 series switches networked to the TestStream Management Server share the same license.
- A separate TestStream Management license is required for standalone nGenius 3900 series switches.
- Connections are defined by the maximum per-connection speed:
  - A license for a 100 Gb/s connection could be used to make one 100 Gb/s, one 10 Gb/s or even one 1 Gb/s connection.
  - A license for a 40 Gb/s connection could be used to make one 40 Gb/s, one 10 Gb/s or even one 1 Gb/s connection.
  - A license for a 10 Gb/s connection can be used to make one 10 Gb/s connection or one 1 Gb/s connection.
- Combining connection licenses is not allowed: You cannot bond four 10 Gb/s connections into one 40 Gb/s, or bond ten 1 Gb/s connections into a 10 Gb/s connection.
- Sixteen 1/10 Gb/s connections can be used for sixteen connections of either 1 Gb/s or 10 Gb/s but cannot be combined into 40 Gb/s connections.
- Creating 40 Gb/s connections requires a license with one or more 40 Gb/s connections defined in the license.

Request Server License

Customer-ordered licensed-specific feature upgrades require a new permanent license key. Select **Help > Server License > Request Server License**. The Request Server License window displays.

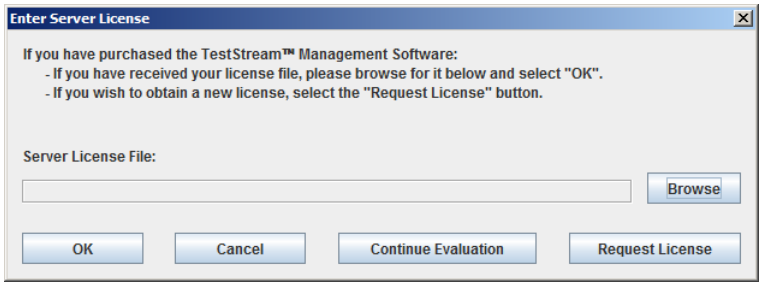


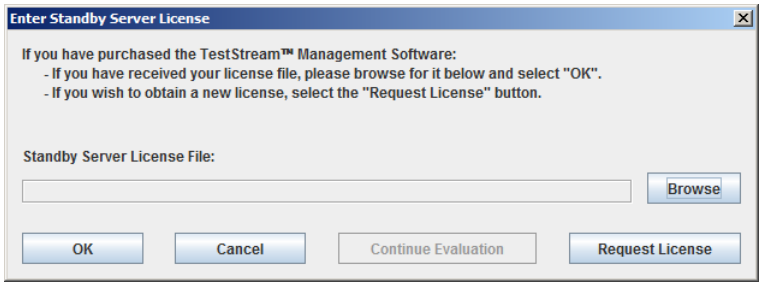
- **Product ID 1** refers to the Primary server.
- **Product ID 2** refers to the Standby server.

Select the **Save to File** button to save the Product ID to a file, then send the file to NETSCOUT at **licensing@netscout.com** using the subject line **TestStream Management Software License Request**.
- or -
Automatically send a request to NETSCOUT by clicking the **Request License** button.
- or -
Call NETSCOUT customer service to request a server license. Have the TestStream Management Product ID available when calling.

Enter Server License / Enter Standby Server License

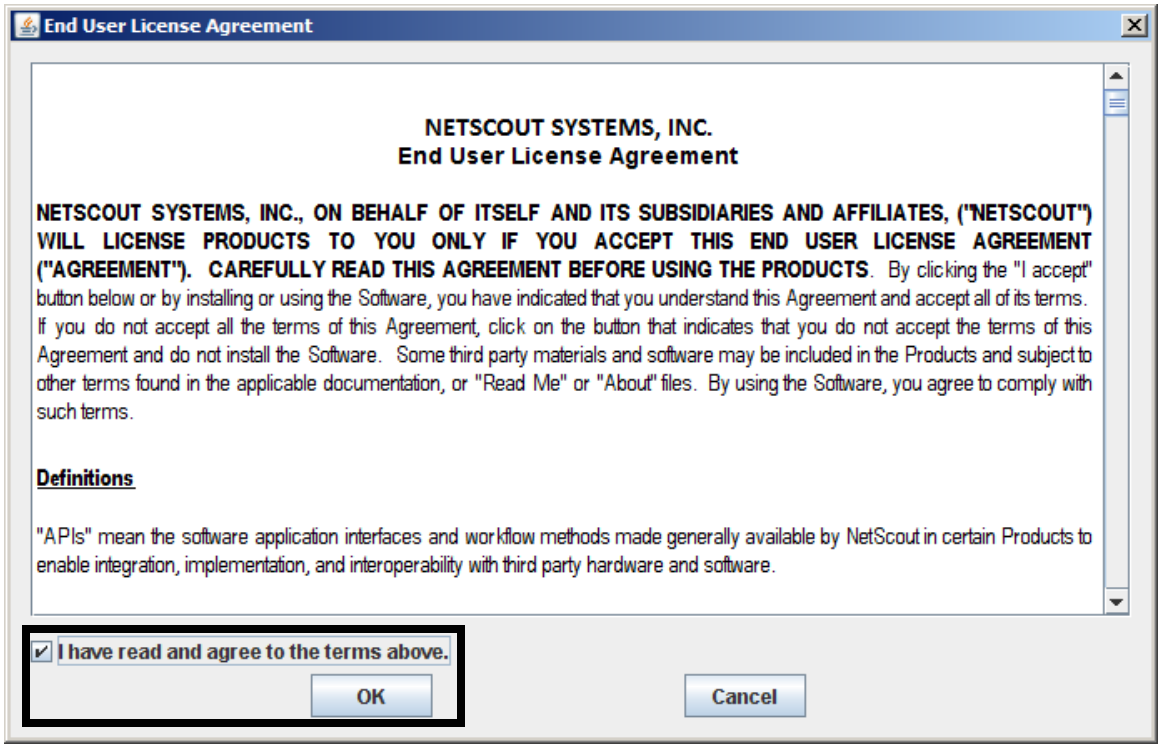
After receiving your permanent TestStream Management server licenses for the primary and/or standby servers, activate the licenses. From the administrative level, select **Help > Server License > Enter Server License** or **Enter Standby Server License**. The Enter Server License / Enter Standby Server License window displays.





Click on **Browse** to locate the received license file. Select the ***.mlf*** file, click **Open** to place the license file into the Server License File field, then click **OK**. The End User License Agreement screen displays.

Read the EULA carefully. If in agreement, click the software terms agreement box, then **OK**.



TestStream Management EULA

To view NETSCOUT's End User License Agreement (EULA), select **Help >Server License > End User License Agreement**. The EULA document displays.

NETSCOUT

NETSCOUT SYSTEMS, INC.
End User License Agreement

NETSCOUT SYSTEMS, INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES, ("NETSCOUT") WILL LICENSE PRODUCTS TO YOU ONLY IF YOU ACCEPT THIS END USER LICENSE AGREEMENT ("AGREEMENT"). CAREFULLY READ THIS AGREEMENT BEFORE USING THE PRODUCTS. By clicking the "I accept" button below or by installing or using the Software, you have indicated that you

NETSCOUT in certain Products to enable integration, implementation, and interoperability with third party hardware and software.

"Documentation" means any installation guides, reference guides, operation manuals and release notes provided with the Product in printed, electronic, or online form.

"Enterprise" means an entity that has been assigned a Maintenance account number. In the event an entity has multiple Maintenance account numbers, each Maintenance account is a separate Enterprise and requires a separate Enterprise License.

TestStream Management Open Source License

To view the TestStream Management Open Source License, select **Help >Server License > Open Source License**. The Open Source License document displays.

NETSCOUT™

Offer to Provide Source Code of Certain Software

NETSCOUT TestStream™ Management Software contains copyrighted software that is licensed under the General Public License (GPL, under the Lesser General Public License version, and/or other Free Open Source Software Licenses). Such software in this product is distributed without any warranty to the extent permitted by the applicable law. Copies of these licenses are included in NETSCOUT TestStream Management Software.

Icon Legend Chart

Select **Help > Icon Legend** to display a chart of the various connection status indicators used in TestStream Management. Click the **X** to close the chart.

General

- Switch - Designates a configured switch
- Chassis - Designates a configured switch chassis
- Blade - Designates a configured chassis blade
- Undefined Port - Indicates that a port is not configured with interface properties
- Defined SFP Port - SFP port is configured with interface properties
- Defined QSFP Port - QSFP port is configured with interface properties
- Defined CXP, CFP, or QSFP28 Port - CXP, CFP, or QSFP28 port is configured with interface properties
- Group - Set of defined ports
- Filter - Designates a defined filter
- Rule - Designates a defined rule
- DPI Protocol - Designates a defined DPI protocol
- xSL Trunk - Designates group of xSLs defined as a continuous pipe
- Active Controller - Designates the current active controller / blade in a 3900 switch
- Packet - Designates a defined packet
- Stream - Designates a defined stream containing one or more defined packets
- Stream Generator - Designates a defined stream generator containing a defined stream

- Device - Designates a configured device
- Undefined Device Port - Designates a not configured device port
- Defined Device Port - Designates a configured device port
- Mapped Device Port - Designates a device port containing an assigned TestStream port.
- (S) Standard Topology - Topology used for switch ports.
- (D) Device Topology - Topology used for device ports..

Status Indicators

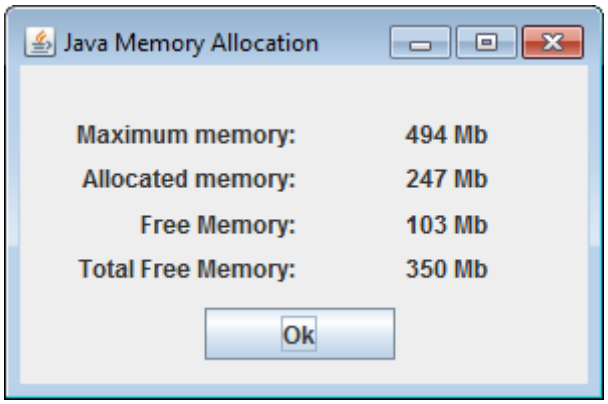
- Connected - Defined port-to-port path is established
- Powered On - Indicates port is powered on; connected port check mark supersedes the powered on green dot
- Always Powered Off - A port is powered down even when in an active connection
- xSL Associated - Defined xSL associated ports are connected
- Rx/Tx Connected - Receiver (Rx) and Transmitter (Tx) port pairs are connected
- Alarmed - An alarm exists on the port
- Locked - Defined port that is accessible by a particular user; no other user can use / modify the port
- Unavailable - Port that has been reassigned to the backplane in Extended Mode
- Monitored - Indicates that a normal port is connected to and is monitored by a test/tap port
- Conflict - SFP is installed into a port but not matching port configuration
- Not in Domain - A port is not in this users domain, no access to port; this icon overrides other condition icons
- Maintenance (Switch)- Indicates that the Clean Connections utility is in use on a selected switch
- Shutdown (Switch)- Indicates shutdown of a switch
- Version Mismatch - Software version of TestStream Management on embedded switches does not match operating version installed on TestStream Management Server
- Partial Connection - Displays during activation/deactivation of destination group ports, indicating that some of the destination ports in a group are connected to a source port
- Time Stamping - Displays when the Enable Nanostamp option is selected on a defined port
- Packet Slicing - Displays when the Packet Slicing option is selected on a defined port
- LBF (Load Balancing Failover) - Indicates when a port is in a Load Balancing Failover / Failback condition
- Degraded - An xSL trunk is experiencing traffic above its high threshold value setting
- Failed - An xSL trunk is dropping traffic due to congestion drops
- Disabled - An HS-3200 port is set to disabled; the port maintains the functionally of a defined port, except that it cannot be connected to or perform statistics collections
- Impairment Delay - Indicates packet latency delay on a PCE port
- Impairment Loss - Indicates packet loss on a PCE port

Port types

- M - Mirror Port
- T - Test Port
- X - xSL Port
- C - Clone Port
- P- PCE Port
- I - iSL Port

Java Memory Allocation

To check the memory available on the TestStream Management workstation, select **Help > Java Memory Allocation**. The Java Memory Allocation screen displays. Click **OK** to close the screen.



Updating TestStream Management Servers

Important: When updating to a later version of TestStream Management Server, external servers are updated first, followed by selecting the individual switches to update (refer to Updating nGenius 3900 Series Switches on page 2-53).

Note: Updating the TestStream Management Servers does not update the managed switches connected to the servers. Refer to Updating nGenius 3900 Series Switches on page 2-53 to update the TestStream Management Software version on the nGenius 3900 series switches.

Important: NETSCOUT recommends backing up the TestStream Management configuration database prior to performing an upgrade procedure (refer to Backup on page 4-21).

Important: For redundant TestStream Management Servers, prior to performing an update, verify that both the active and standby servers are operational. If one of the servers are non-operational or inaccessible, the software updating process will not be performed.

To upgrade/restore the TestStream Management Servers to a different version of the TestStream Management Server program, select **Help > Update**. The Update Server Wizard screen displays.

Downloading and Verifying the Upgrade/Installation Package

1. Download the TestStream_5.2.0.x.zip and TestStream_5.2.0.x.sha256 files from the MasterCare portal.
2. Verify the sha256 checksum.
   - **a** In Linux, from the same directory where the 2 downloaded files are located, run: sha256sum -c TestStream_5.2.0.x.sha256
   - **b** In Windows 10, open a command prompt window, change directory to where the two downloaded files are located, run: certutil -hashfile TestStream_5.2.0.x.zip SHA256
     - Compare the output with the contents of the file TestStream_5.2.0.x.sha256

New Version Update

Updating to a new version of TestStream Management will take several minutes to complete.

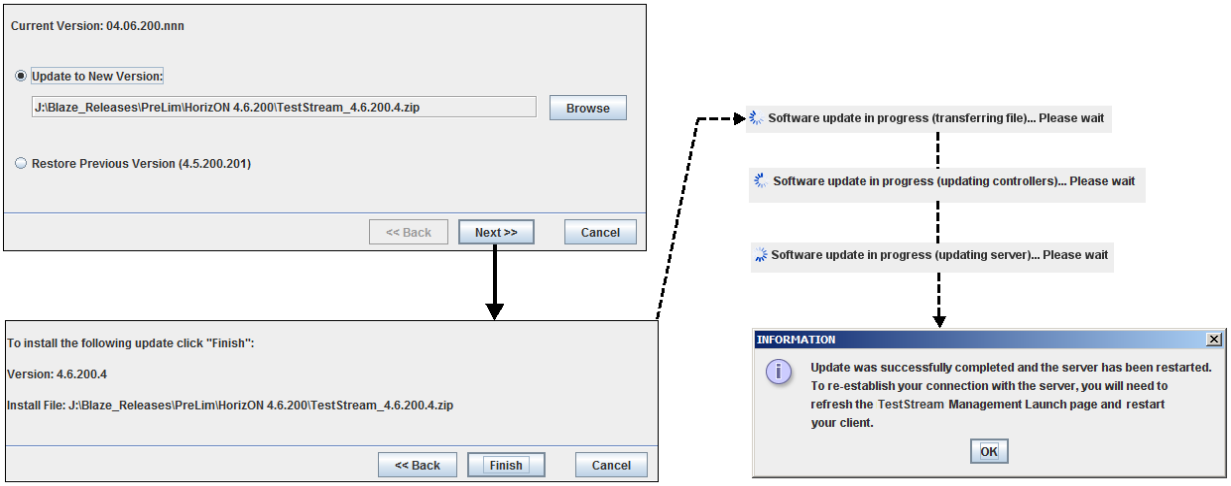
Prior to installing the update, verify that all other TestStream Management users on the server are logged OFF (refer to Logged On Users on page 2-38).

Note: The server must be at 5.0.0 or 5.1.0 in order to upgrade to 5.2.0.

It is possible to upgrade the TestStream Management Server from version 5.0.0/5.1.0 to version 5.2.0 without upgrading any of the switches being controlled by that server.

Important: Connectivity interruptions for several minutes may occur during the update process.

1 Select **Update to New Version** then click the **Browse** button to open a search window to locate the TestStream Management Server Update file. Select the TestStream Management update file to load then click **Next**.



2 A confirmation screen displays the selected file to load. Click **Finish**.
An information message is displayed, along with upgrade status information in the Audit Trail, informing that the update was successfully completed.

3 Click **OK**, TestStream Management logs off. Restart and login to TestStream Management.

Note: After performing a software upgrade on redundant external servers, the user may need to wait up to 30 minutes before completing a successful login to the server(s). With co-located redundant servers, typical login wait time is 5 minutes or less. Geo-diverse server logins can take longer (up to 30 minutes), depending on the latency existing between the two servers.

Important: After logging onto TestStream Management, perform a Reconcile Port Connectivity (refer to Reconcile Port Connectivity on page 3-156) on each nGenius switch connected to the TestStream Management server to resynchronize the connectivity database.

Restore Previous Version

Important: External server downgrade to the previous version of TestStream Management requires all connected switches to be downgraded to the previous version prior to the external server downgrade.

Important: Prior to performing the restore procedure, please contact NETSCOUT Customer Support (refer to Contacting NETSCOUT Customer Support on page 1-2).

Note: Refer to Clearing the Java Cache on page 2-51 if installing a previous version of TestStream Management.

Restoring a previous version of TestStream Management will take several minutes to complete.

Important: Connectivity interruptions for several minutes may occur during the restore process.

Note: The user can restore an embedded switch from version 5.2.0 to version 5.0.0/5.1.0.

The user can restore one or more externally managed switches from version 5.2.0 to version 5.0.0/5.1.0.

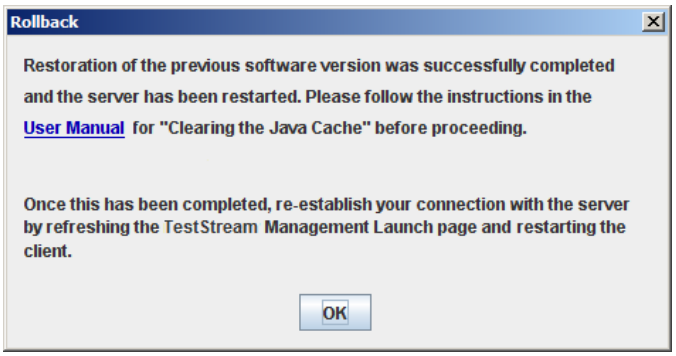
The user can restore an external server from version 5.2.0 to version 5.0.0/5.1.0 if all of its managed switches are running an equal or lesser version.

The user may not restore any switch or external server that is configured to use a feature not implemented in the previous software version of TestStream. The feature must be disabled before attempting the restore operation.

The user may not perform a restore operation on any system (embedded switch, external server, or externally managed switch) unless that system was previously upgraded from 5.0.0/5.1.0.

1 Select **Restore Previous Version** to downgrade to the last version of TestStream Management installed on the system. Click **Next**.

2 A confirmation screen displays the version being installed. Click **Finish**.
A message is displayed informing that the restoration of the previous software version was successfully completed, the TestStream Management server is restarted, and a reminder to clear the Java Cache (refer to Clearing the Java Cache on page 2-51) prior to restarting TestStream Management.



3 Click **OK**, TestStream Management logs off. After the Java Cache is cleared, restart and login to TestStream Management.

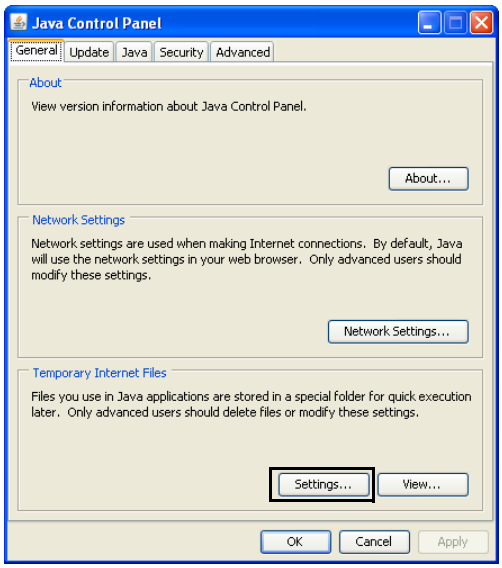
Important: After logging onto TestStream Management, perform a Reconcile Port Connectivity (refer to Reconcile Port Connectivity on page 3-156) on each nGenius switch connected to the TestStream Management server to resynchronize the connectivity database.

Clearing the Java Cache

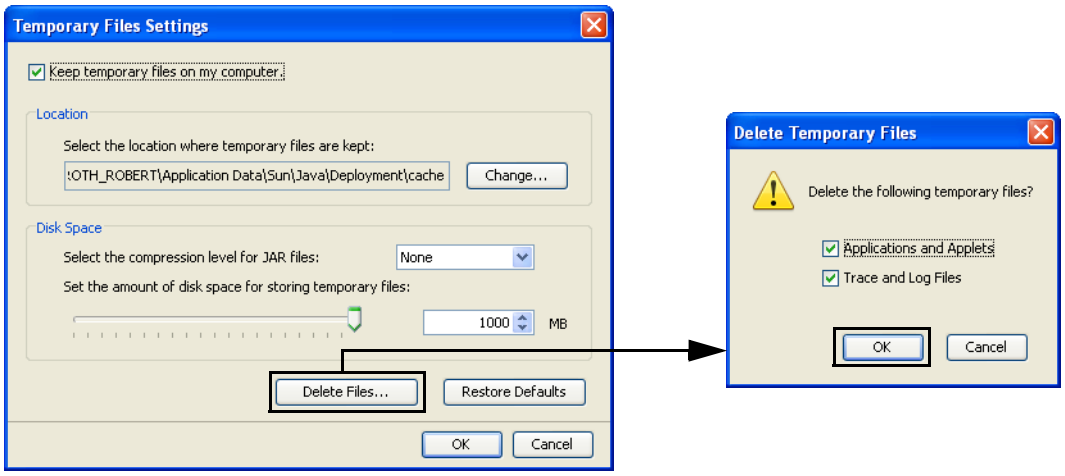
If installing a previous version of TestStream Management, the Java cache must be cleared after performing the downgrade and prior to restarting TestStream Management.

Java Control Panel

1 From the Windows desktop, select **Start > Settings > Control Panel**. From the Control Panel, double-click the **Java** icon. The Java Control Panel displays.



2 Click **Settings** from Temporary Internet Files. The Temporary Internet Files screen displays.

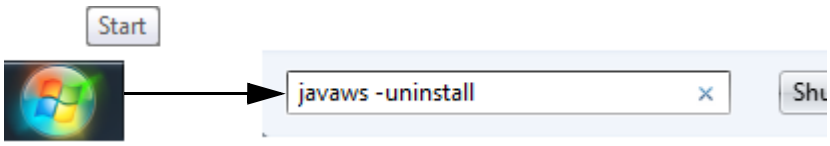


3 Click **Delete Files**. Select all of the boxes, click **OK**.

4 Click **OK** to close Temporary Internet Files, then **OK** to close the Java Control Panel.

Windows Command Line

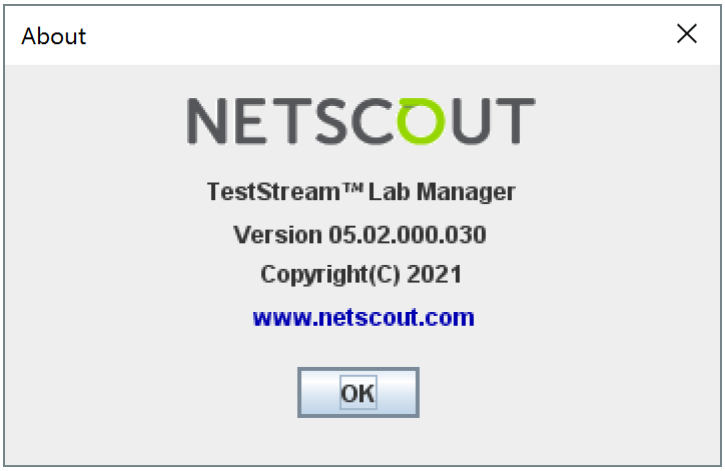
From the Windows Desktop, select **Start**. Enter the command **`javaws -uninstall`** in the command line field then <enter>. This will remove all applications from the cache.



About TestStream Management

To view the current operating version and software build of TestStream Management, select **Help > About**.

The About screen displays. Click **OK** to close the screen.



Updating nGenius 3900 Series Switches

To update nGenius 3900 series switches to the same software version of the external TestStream Management Server, right click on the required switch(es) and select **Update** from the drop down menu. The Update Switch Wizard screen displays.

Important: NETSCOUT recommends backing up the TestStream Management configuration database prior to performing an upgrade procedure (refer to Backup on page 4-21).

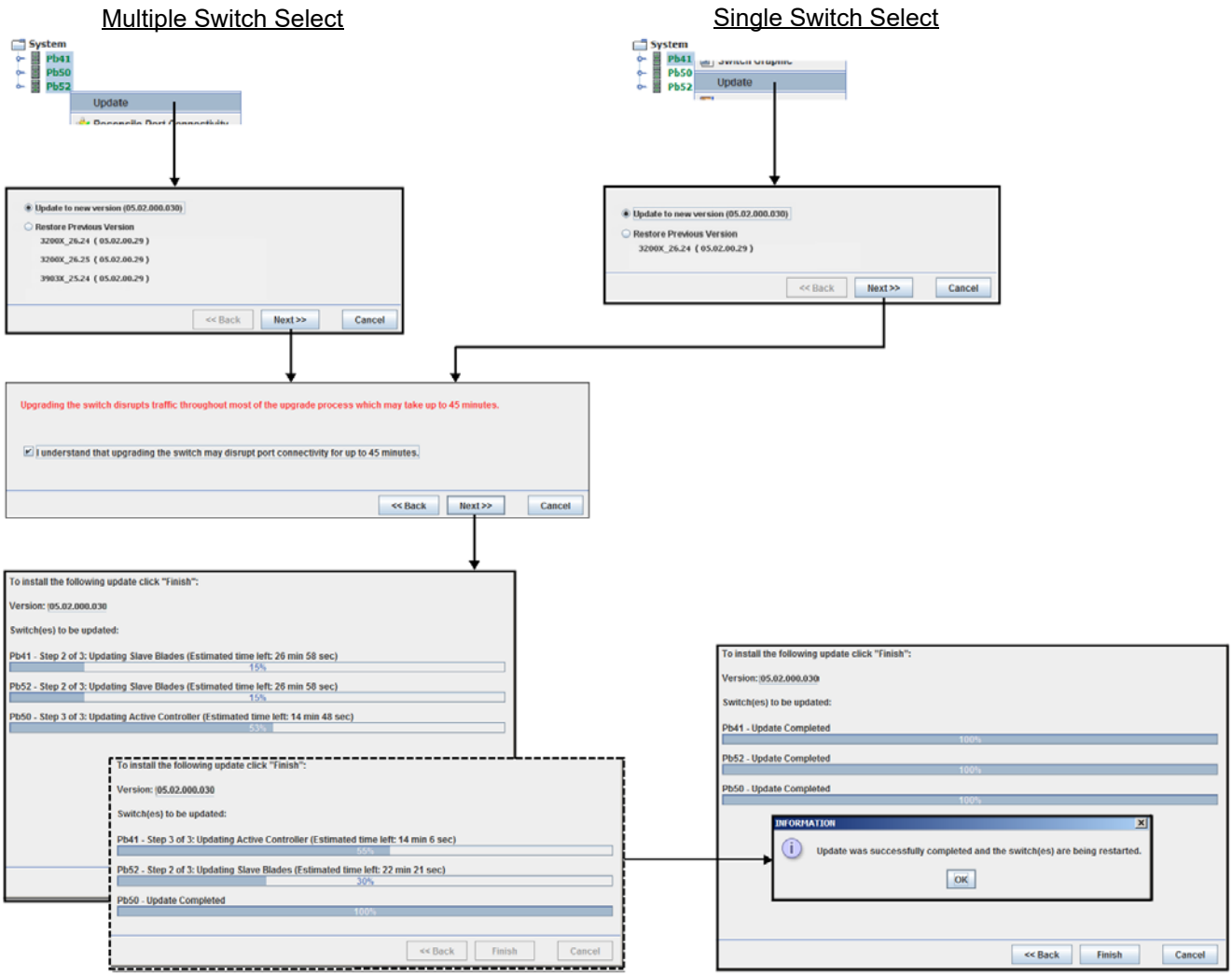
New Version Update

Note: Updating to a new version of TestStream Management will take several minutes to complete.

Prior to installing the update, verify that all other TestStream Management users on the switch(es) are logged OFF (refer to Logged On Users on page 2-38).

Important: Connectivity interruptions for several minutes may occur during the update process.

1 Select **Update to New Version** (default) then click **Next**.



2 A message displays informing you that the upgrade will disrupt traffic up to 45 minutes during the upgrade process. Click on the check box to acknowledge, then click **Next**.

3 Progress bars show the status (percent completed / estimated time remaining) of each switch being updated. Once all of the switches are updated, an information message is displayed, along with upgrade status information in the Audit Trail, informing that the update was successfully completed and the switch(es) were restarted.

4 Click **OK** to end the update session.

Important: After the update, perform a Reconcile Port Connectivity (refer to Reconcile Port Connectivity on page 3-156) on the nGenius switch to resynchronize the connectivity database.

Restore Previous Version

Note: Selecting Restore Previous Version rolls back the switch to its previous version (not the TestStream Server's previous version) of TestStream Management.

Important: Connectivity interruptions for several minutes may occur during the restore process.

1 Select **Restore Previous Version** to downgrade (restore) to the last version of TestStream Management installed on the switch(es). Click **Next**.

2 Progress bars show the status (percent completed / estimated time remaining) of each switch being restored. Once all of the selected switches are restored, an information message is displayed informing that the restoration of the previous software version was successfully completed and the switch(es) were restarted.

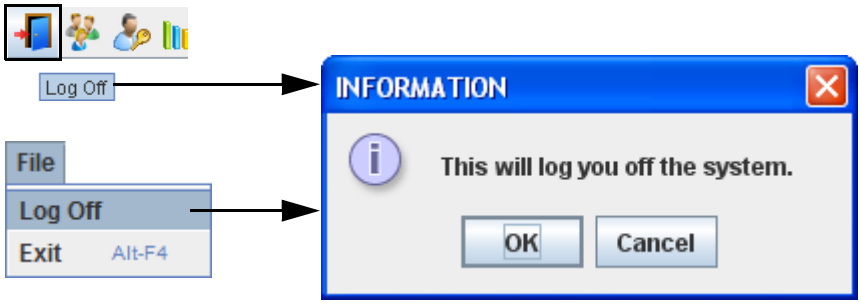
3 Click **OK** to end the restore session.

Important: After the version restore, perform a Reconcile Port Connectivity (refer to Reconcile Port Connectivity on page 3-156) on the nGenius switch to resynchronize the connectivity database.

Log Off TestStream Management

To end the current user's TestStream Management session:

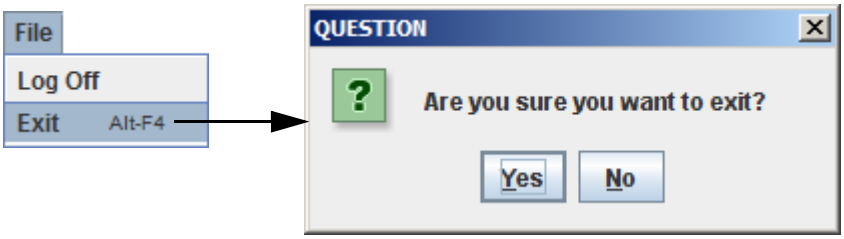
From the toolbar, click the **Log Off** icon or select **File > Log Off**. Click **OK** from the Information screen. The TestStream Management logon screen displays allowing a new user logon to start.



Exit from TestStream Management

To automatically end the current user's TestStream Management session and close the Internet browser window:

From the toolbar, select **File > Exit** or from the keyboard **Alt+F4**. Click **Yes** to confirm. The user is automatically logged off and the Internet browser window is closed.



Chapter 3
Configuration and Control

This chapter covers the TestStream Management configuration and control features.

Seven control and configuration tabs:

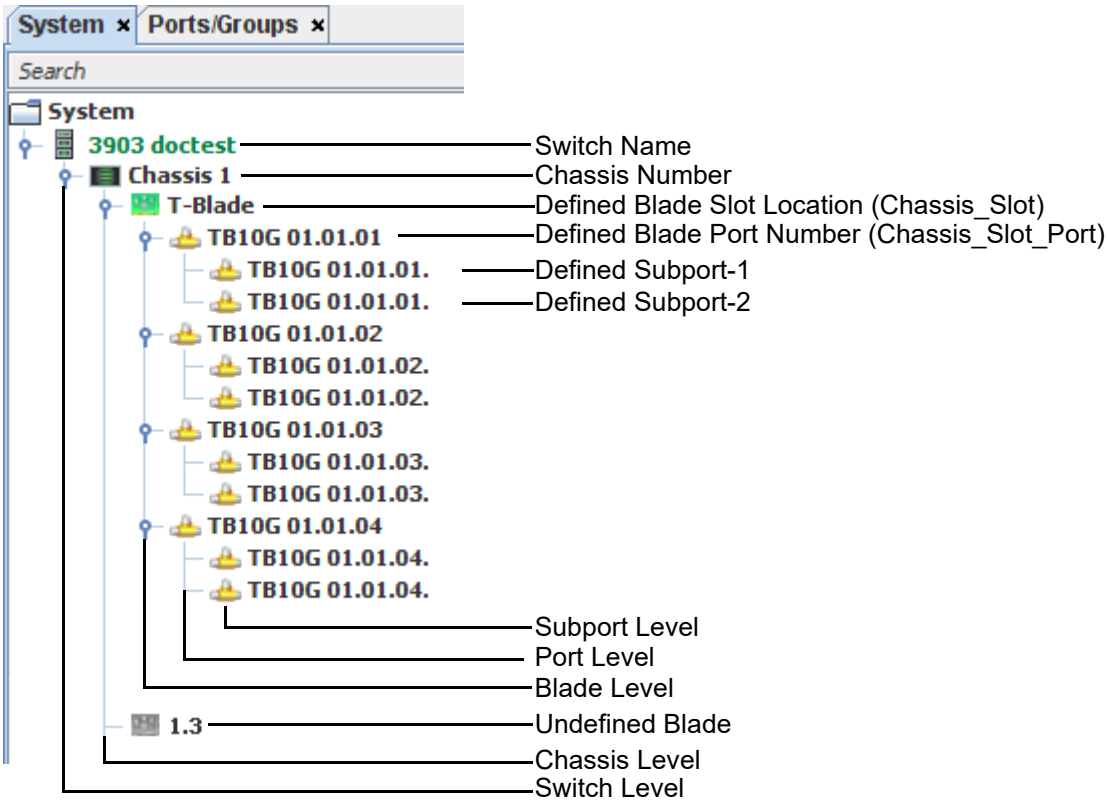
- System on page 3-1
- Ports/Groups on page 3-185
- Rules/Filters on page 3-188
- Packets/Streams on page 3-222
- Impairment on page 3-231
- Domain on page 3-237
- Ports/Devices (TestStream Lab Manager Only) on page 3-239

are used for adding switches and blades, defining and connecting ports and creating user defined port groups, defining packet rules and filters, construct individual packets, create custom packet impairments, creating user-specific domains, and defining devices and their ports.

System

System is used for processes associated with the switch (e.g., adding blades, defining ports).

Selecting the System tab provides a physical view of the switches contained in the users network (switch model, chassis, installed blades – types, ports, status of each port / subport (connected, not connected, monitored).

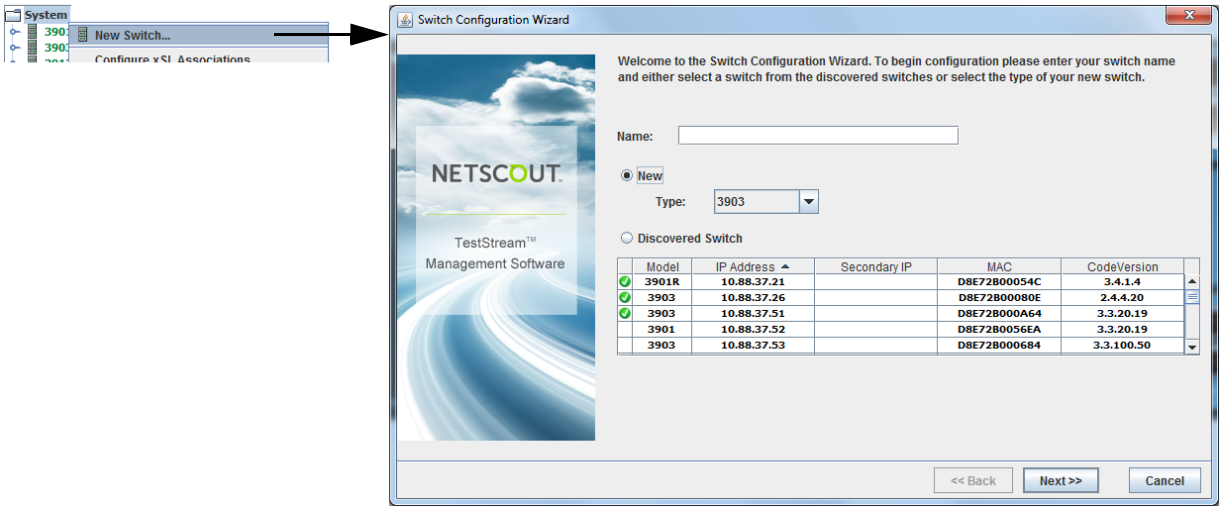


Adding a Switch

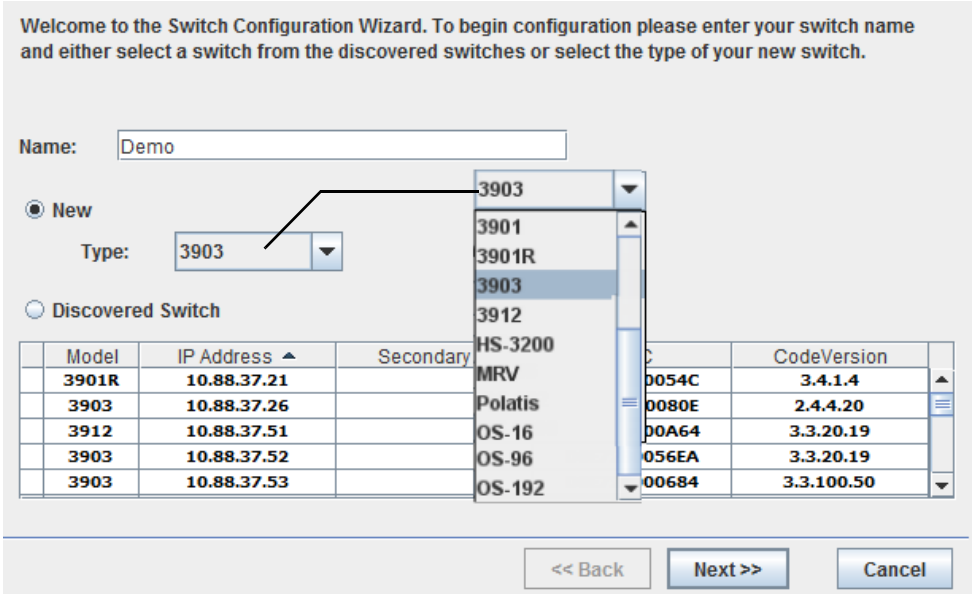
1 Select the System folder, right click and select **New Switch**. The Switch Configuration Wizard displays. The wizard polls and displays all discovered switches on the network. A green check mark indicates switches accessible for configuration. Select either a discovered switch or click **New** and add a new switch.

Important: Do not add an nGenius 3900 switch containing a later version of TestStream Management Software to a TestStream Management server containing an earlier version of TestStream Management Software.

Note: Only switches that are in the same subnet are discoverable, all other switches must be manually added.



1 Enter a switch name, click **New**, and select the switch type from the drop down menu. Click **Next**.



2 On the next screen, enter the Switch IP Addresses:

The Primary Switch IP Address is the IP address used by the active controller. This is the only IP address required to manage the nGenius 3900 switch.

The Secondary Switch IP Address is the IP address used by the standby controller. This is not used to manage the nGenius 3900 switch and can be left blank. An IP address can be assigned for diagnostic support if required.

Note: If the Secondary Switch IP Address is not provided, the corresponding Ethernet port is not disabled.

Optionally, enter a port prefix name to be used to identify the ports.

Important: The port prefix name cannot be made up of four (4) dotted numbers (nn.nn.nn.nn - e.g.,10.88.99.11).

Optionally, enter individual (not the same name) designations for SFP Subports 1 and 2.

Note: Subport 1 is defined as the receiving input signal (e.g., source, input, Rx) Subport 2 is defined as acquiring the signal from a source port (e.g., destination, output, Tx).

SFP Protocol Preference - select the primary SFP interface (Ethernet is default) to be used in the switch.

Note: SFP Protocol Preference - This feature only applies to S-Blades; ignore this option for all other blades.

SSH Inactivity Timer - allows setting the active time (default of 30 minutes) a user can remote access a switch from the Console port via SSH (refer to CLI Access using an nGenius 3900 Series Blade Console Port on page 2-13). Once the defined time expires, the user is automatically logged off.

Note: SSH Inactivity Timer - This feature option is not supported in the HS-3200 switch.

TLS/SSL Communications - select to enable the TLS/SSL component (refer to Installing the TestStream Client TLS/SSL Component on page 2-7) from the 3900 switch to the external TestStream Management server.

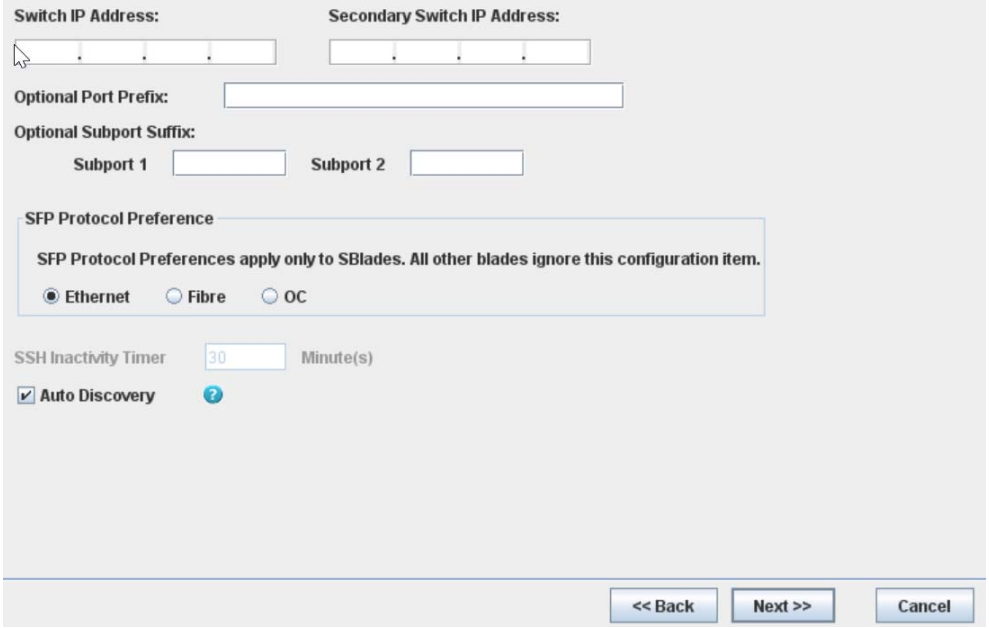
Note: STLS/SSL Communications - This feature option is not supported in the HS-3200 switch.

Auto Discovery (selected by default) - enables TestStream Management to locate all blades and installed SFPs, and based on the SFP protocol preference selected, automatically configure the blade ports to match the installed SFP characteristics (e.g., Ethernet, Fibre, OC). Un-selecting this feature allows the user to manually configure a blade and associated ports (refer to Adding a Blade to a Chassis on page 3-56 and Configuring Blade Ports on page 3-57) after the switch is defined.

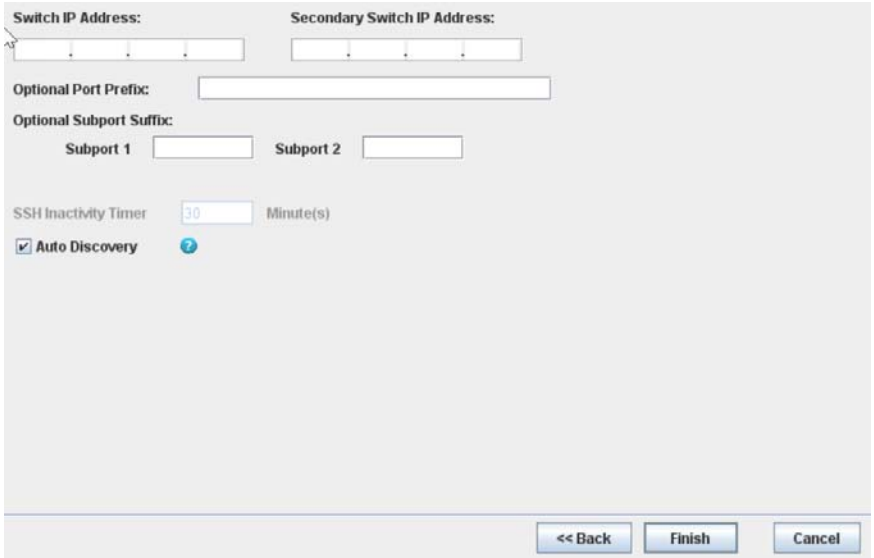
Note: To update the SFP database of a switch that previously was set to Auto Discovery Disabled but now has Auto Discovery Enabled, right-click on the switch and select **Ack System Events** (refer to Acknowledge System/Port Events from the Switch Level on page 3-165). The updated SFP information is now received and re-populates the blades.

For 3901 / 3901R /3903 / 3912 switches, click **Next**.
For OS-16 / 96 / 192 Optical Switches, click **Finish**.
For HS-3200 / HS-6400 switches, click **Next**.
For MRV switches, click **Next**.
For Polatis switches, click **Finish**.

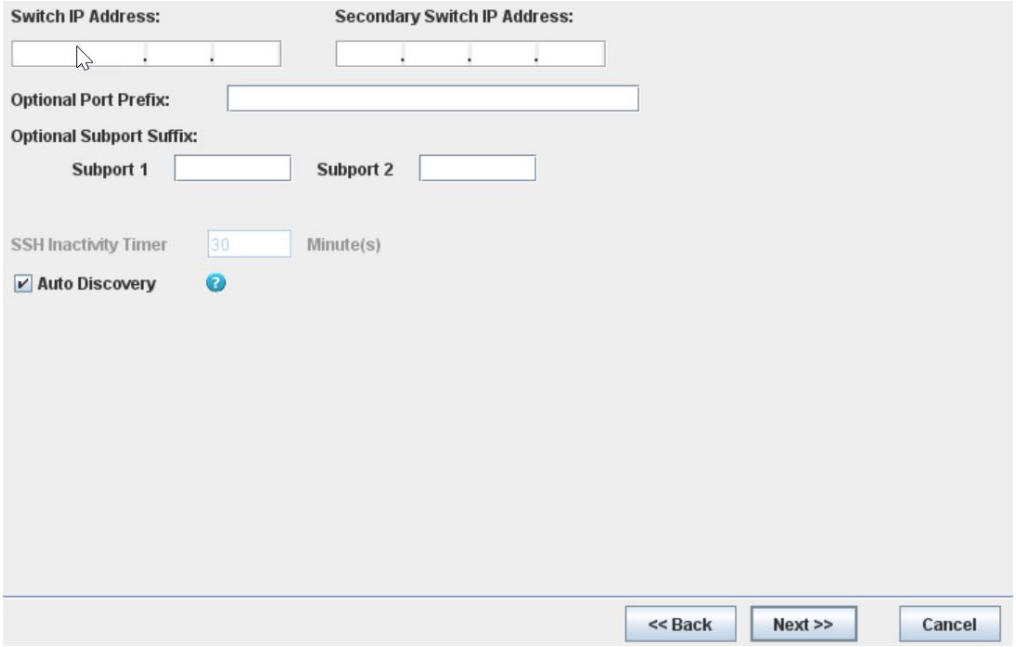
3901 / 3901R / 3903 / 3912



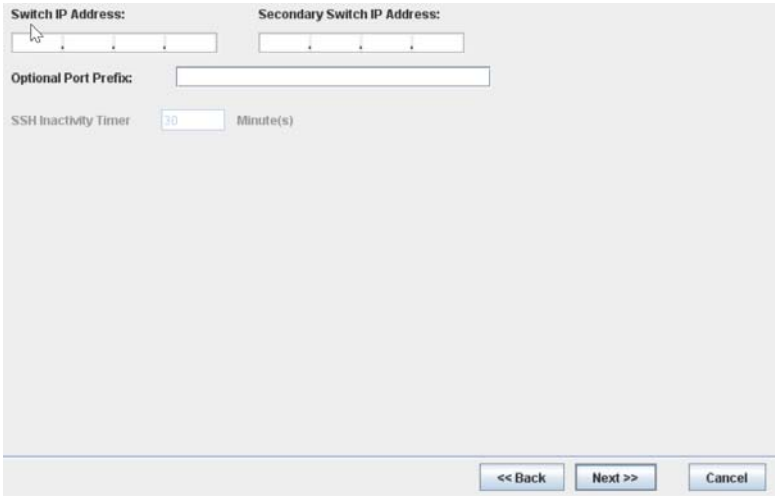
OS-16 / 96 / 192



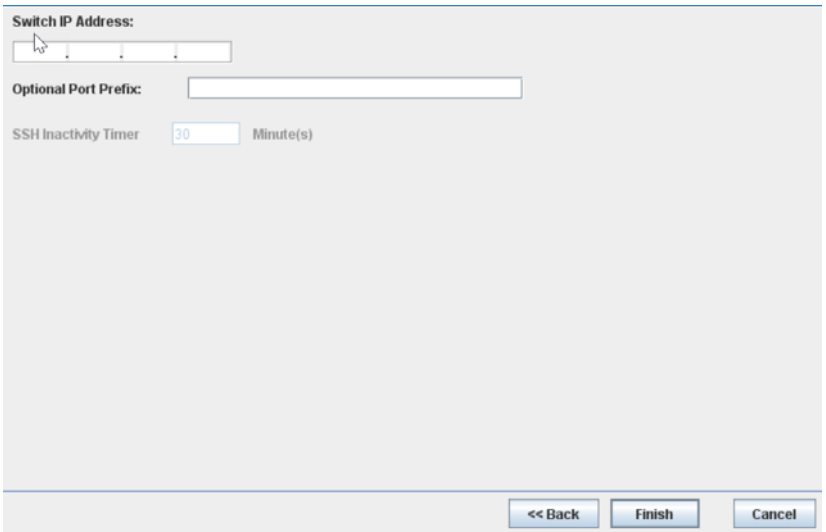
HS-3200 / HS-6400



MRV Switch



Polatis Switch



Note: SCPI top level branch MMemory is used for commands for storing and loading switch configurations. Multiple commands may be sent per line. These should be separated by ; (semicolon).

Listing Files:
:mmem:cat?
store_add1,store_only1

Renaming Files:
:mmem:cat?
store_add1,store_only1
:mmem:move "store_only1","store_only01"
:mmem:cat?
store_add1,store_only01

Deleting Files:
:mmem:cat?
store_add1,store_only01
:mmem:del "store_add1"
:mmem:cat?
store_only01

Storing and Loading Files
:OXC:SWIT:CONN:STAT?
(@11,12),(@204,203)
:mmem:stor:oxc (@1:384),"store_add1",ADD
:mmem:cat?
store_add1

:mmem:cat?
store_add1
:OXC:SWIT:CONN:STAT?
(@13,14),(@206,205)
:mmem:load:oxc "store_add1"
:OXC:SWIT:CONN:STAT?
(@13,14),(@206,205)

3 On this screen, select any of the optional Switch Parameters:

Default Link Propagation (S/S Pro-Blade, HS-3200): Set the delay to either Enabled (default) or Disabled. This setting defines the detection of Loss of Signal (LOS) from one end of a connection to the other end when the transmitter is turned off.

Note: When moving the pointer's cursor over a connected S/S-Blade Pro port, from either the system / port tree or the blade graphic view, the Link Propagation status of the port is included in the tool tip window (e.g., Connected Link Prop Disabled or Connected Link Prop Enabled).

Note: The following feature options are not supported in the HS-3200 switch: S-Blade Pro Mode, S-Blade Pro QSFP Preferences, Enable VN-Tag Detection Mode, Enable Cisco FabricPath header stripping, and Local Console.

Default S-Blade Pro Mode: Allows S-BLADE Pro blades to operate in either:

- **Normal Mode** - Optimized for Layer 1 switching, allowing all ports and bridge links to be available for connections. Connecting traditional Layer 1 ports to Smart Layer 1 ports require use of the Smart Bridge. Each 1/10GbE connection requires a single link, while a 40GbE connection requires 4 links.
  - or -
- **Utilization Mode** - Used to measure utilization on selected ports, reserving half of the bridge links for statistics collection. In this mode, the 6 Smart Layer 1 ports are still available for connections. In addition, 8 Smart Bridge links are available for connecting traditional Layer 1 ports to Smart Layer 1 ports.

Default S-Blade Pro QSFP mode: Select one of the following:

- **40G QSFP** - Configures a single 40G port for each QSFP discovered.
- **10G QSFP (4/10G)** - Configures four (4) 10G ports for each QSFP discovered.

SFM Pro External Fabric Mode (3903 system; refer to SFM Pro External Fabric Mode on page 3-93**):** Allows connecting a 3903 and 3912 switch together, creating a shared backplane to form a (logical) 15-slot switch. Selecting the check box for this 3903 system allows assigning the 3903 to a 3912 for External Fabric Mode. In addition, the S-Blade Pro QSFP Mode defaults to **10G QSFP** (10Gb is required for chassis expansion) and the S-Blade Pro Mode defaults to **Normal** (required for chassis expansion).

SFM Pro External Fabric Mode (3912 system; refer to SFM Pro External Fabric Mode on page 3-93**):** Allows connecting a 3903 and 3912 switch together, creating a shared backplane to form a (logical) 15-slot switch. Select the check box and enter the name of the corresponding 3903 system being connected to the 3912. In addition, the S-Blade Pro QSFP Mode defaults to **10G QSFP** (10Gb is required for chassis expansion) and the S-Blade Pro Mode defaults to **Normal** (required for chassis expansion).

Enable S-Blade Pro Extended Fabric Mode (3903 systems):
Allows using the Smart backplane ports to make Layer-1 ports off-board connections for 10GbE using S-Blade Pro blades.

Enable VN-Tag Detection Mode: Provides filtering and load balancing of the fields encapsulated in VN-Tagged frames and stripping of the VN-Tags (refer to Port Properties - VN-Tag Stripping on page 3-139).
If VN-Tag Detection Mode is enabled, if the source and destination ports are on different blades, the VN-Tags will always be removed.
If VN-Tag Detection Mode is not enabled, VN-Tagged frames will pass through the system with VN-Tags intact.

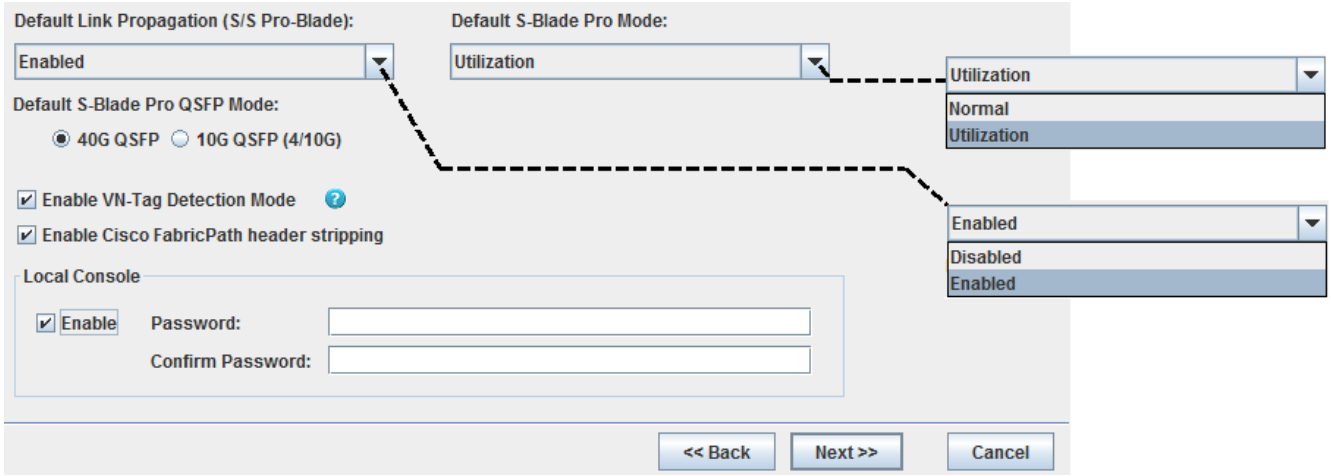
Enable Cisco FabricPath header stripping: Allows configuring Cisco FabricPath (CFP) stripping on the nGenius 3900 series switch (refer to Cisco FabricPath Header Stripping on page 3-12).

Local Console: Select **Enable** to allow access to the local TestStream Management External Server console port for maintenance activities in the event Ethernet / network connections are lost. Enter a user password then re-enter the password for confirmation.

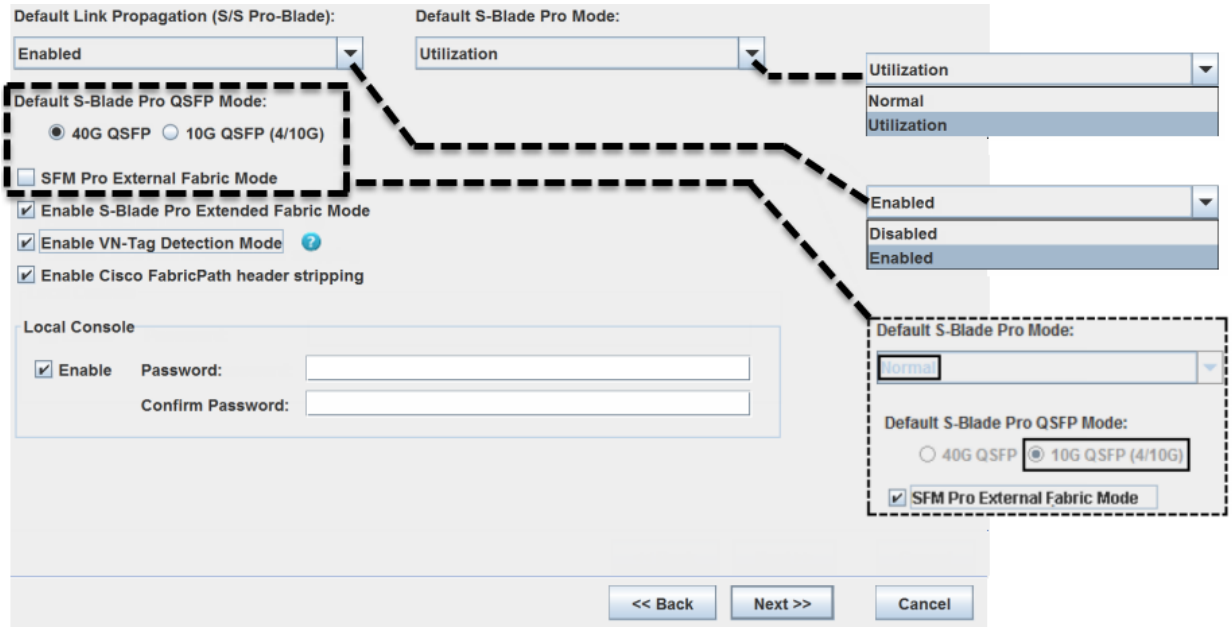
Note: I Commands Available Through the Console Port of the Active Controller in a Switch:
HELP
EXIT
DIAGStat {SWItch|CHAssis|BLAde|PRTNum} [name]
LOGOFF
LOGon
RETrieve INVentory
REVise SWItch IP [options]
SHOw CONnected PORts [PAGE] [number]
SHOw SWItch IP
SHOw PRTNum INFO {*|portname} [PAGE] [number]
SHUTdown {SWItch|BLAde|SFM} [REBOot|RESTart] [name]

4 For 3901 / 3901R / 3903 / 3912 switches, click **Next**.
For HS-3200 switches, click **Finish**.

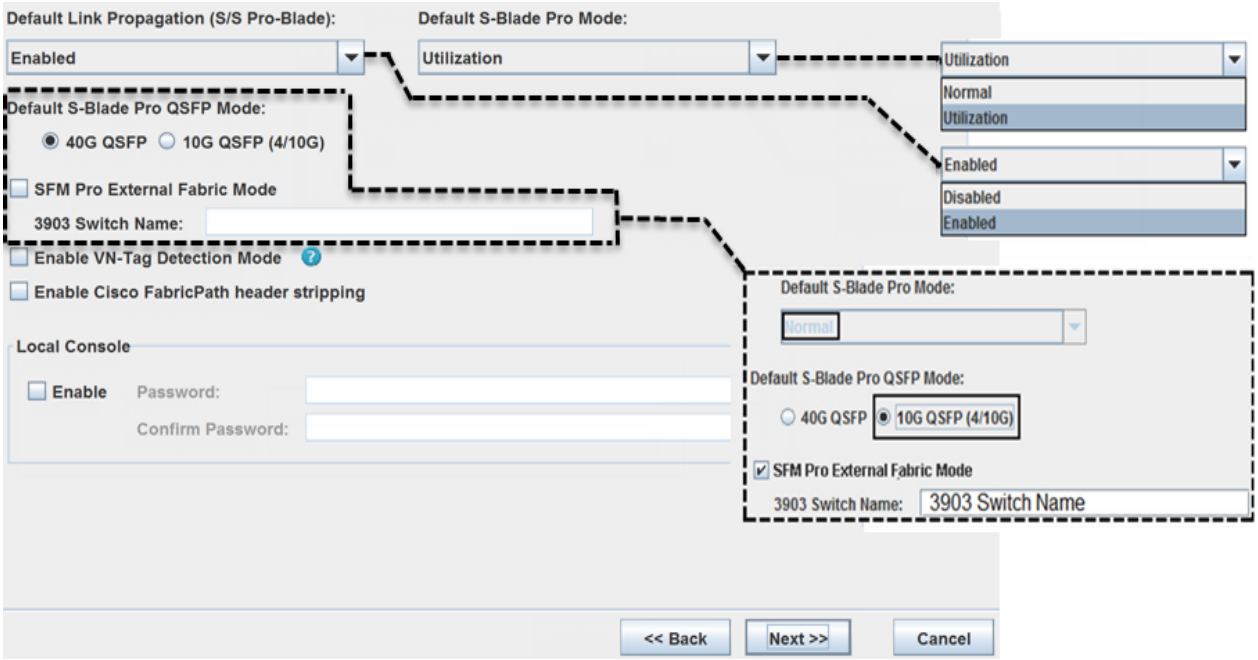
3901 / 3901R



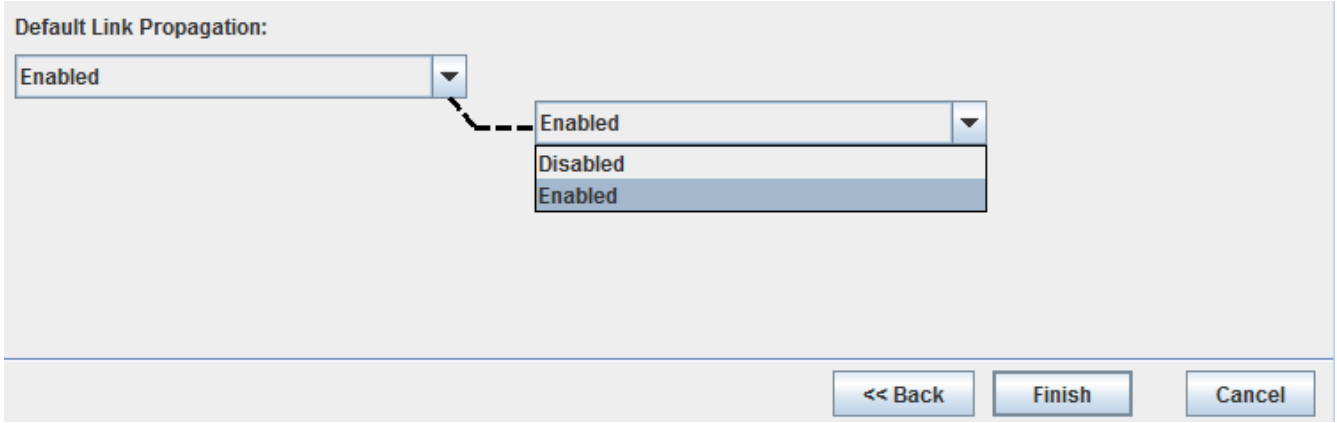
3903


Default Link Propagation (S/S Pro-Blade):
Enabled
Default S-Blade Pro Mode:
Utilization
Utilization
Normal
Utilization
Default S-Blade Pro QSFP Mode:
40G QSFP
10G QSFP (4/10G)
SFM Pro External Fabric Mode
Enable S-Blade Pro Extended Fabric Mode
Enable VN-Tag Detection Mode
Enable Cisco FabricPath header stripping
Enabled
Disabled
Enabled
Local Console
Enable
Password:
Confirm Password:
Default S-Blade Pro Mode:
Normal
Default S-Blade Pro QSFP Mode:
40G QSFP
10G QSFP (4/10G)
SFM Pro External Fabric Mode
<< Back
Next >>
Cancel

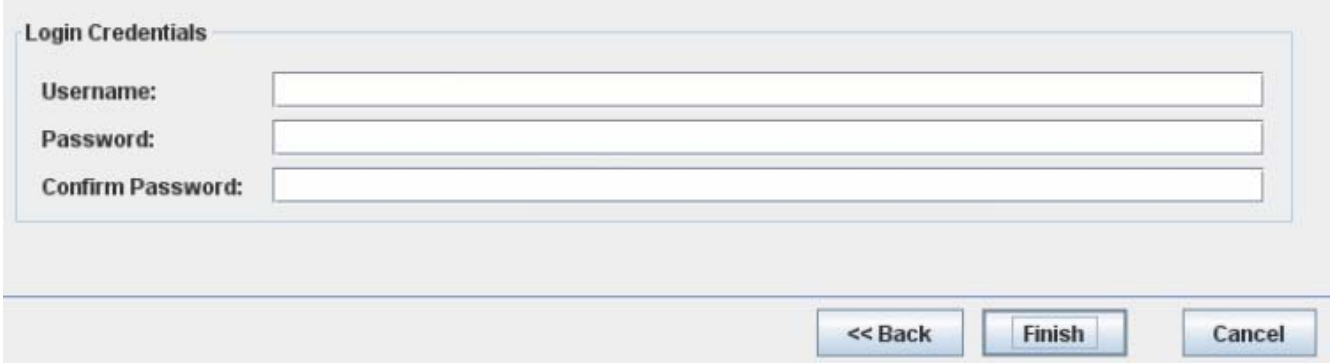
3912


Default Link Propagation (S/S Pro-Blade):
Enabled
Default S-Blade Pro Mode:
Utilization
Utilization
Normal
Utilization
Default S-Blade Pro QSFP Mode:
40G QSFP
10G QSFP (4/10G)
SFM Pro External Fabric Mode
3903 Switch Name:
Enabled
Disabled
Enabled
Enable VN-Tag Detection Mode
Enable Cisco FabricPath header stripping
Default S-Blade Pro Mode:
Normal
Local Console
Enable
Password:
Confirm Password:
Default S-Blade Pro QSFP Mode:
40G QSFP
10G QSFP (4/10G)
SFM Pro External Fabric Mode
3903 Switch Name:
3903 Switch Name
<< Back
Next >>
Cancel

HS-3200 / HS-6400



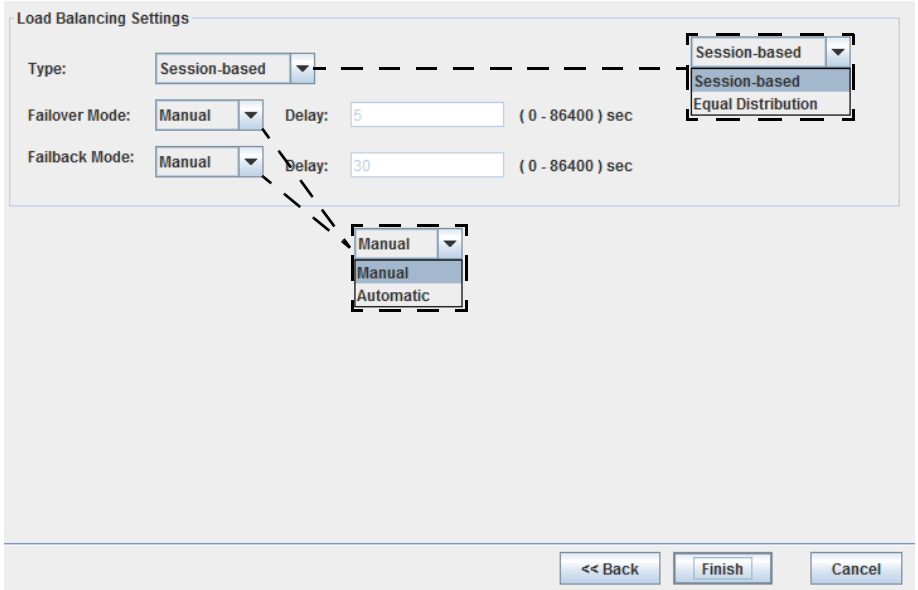
MRV



5 On the next screen, set the **Load Balancing Settings** (refer to Load Balancing Failover / Failback on page 3-172) on the switch.

Set the Load Balancing Type to either Equal Distribution or Session-Based (default). This setting defines the method used to distribute output traffic to multiple destinations:

- **Equal Distribution** – distributes packets evenly across all ports within the Load Balancing Group. The equal balancing helps reduce the risk of over-subscription on any given port.
- **Session-Based** – distributes packets to ports based on their session.
- **Failover Mode**: Select either Automatic or Manual (default) mode. Enter the delay timer value (in seconds, range = 0 to 86400 (24 hours), default is 5 seconds).
- **Failback Mode**: Select either Automatic or Manual (default) mode. Enter the delay timer value (in seconds, range = 0 to 86400 (24 hours), default is 30 seconds).



6 Click **Finish**. The new switch now displays on the switch level.

Cisco FabricPath Header Stripping

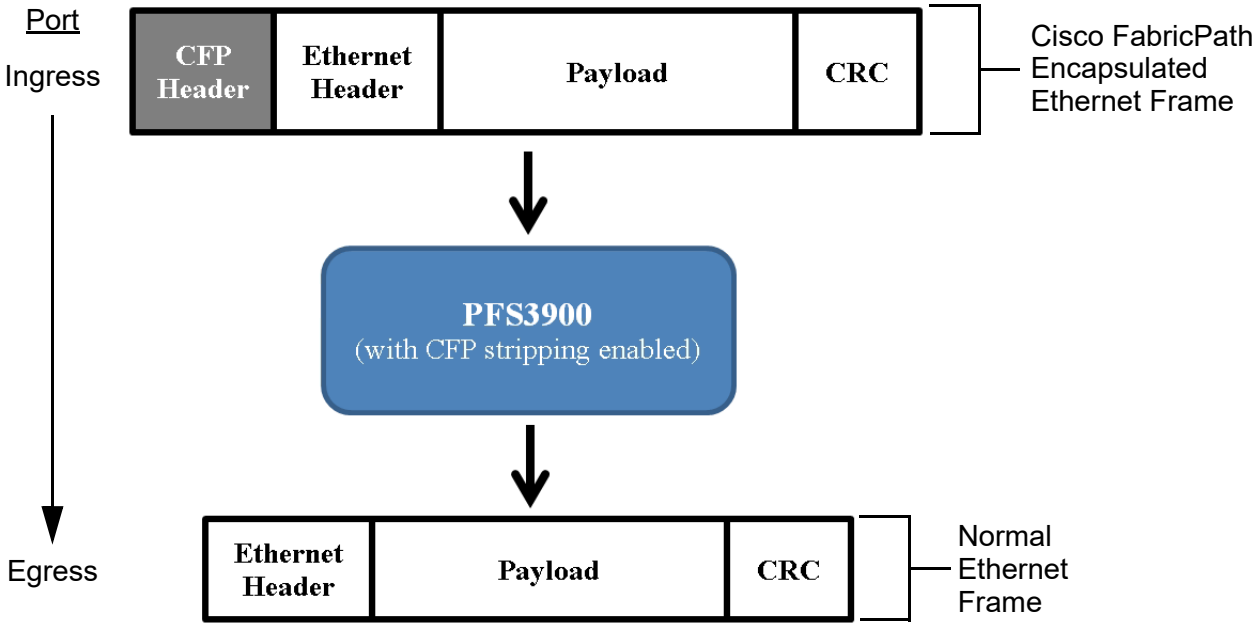
Customers deploying Cisco FabricPath within their Data Centers creates a challenge to monitor services across these links using existing monitoring tools that don't understand FabricPath-encapsulated frames. In order to monitor these links customers require a method to unencapsulate FabricPath traffic before forwarding to their existing tools. The T-Blade has the capability to detect FabricPath-encapsulated frames and strip the FabricPath header from those frames prior to forwarding them to external monitoring equipment.

Cisco FabricPath combines the simplicity of Layer 2 switching with the scalability and resilience of Layer 3 routing. FabricPath removes the need for Spanning Tree (STP), allowing the creation of highly scalable Layer 2 Ethernet networks that have numerous active and forwarding links. In this switching system, traffic is spread across all available paths, thus significantly increasing available bandwidth. In addition, FabricPath enables VLANs to be extended across Data Centers allowing any application to be supported on any server anywhere, thereby increasing flexibility of deployment and simplifying operations.

CFP header stripping is a switch-wide configuration parameter that affects the behavior of all ports on the switch. When CFP stripping is enabled (either through the TestStream Management GUI or CLI command), the T-Blade detects CFP encapsulated frames on all ingress ports, and strip the CFP headers from frames forwarded on all egress ports.

Note:
For clone ports (including PCE ports), the CFP header is stripped in the Egress (Tx) port.

In order to correctly process CFP traffic passing between switches connected via xSLs, both switches must have CFP header stripping enabled.



CFP Stripping Mode CLI Command

The following CLI command is used for configuring CFP Stripping Mode:

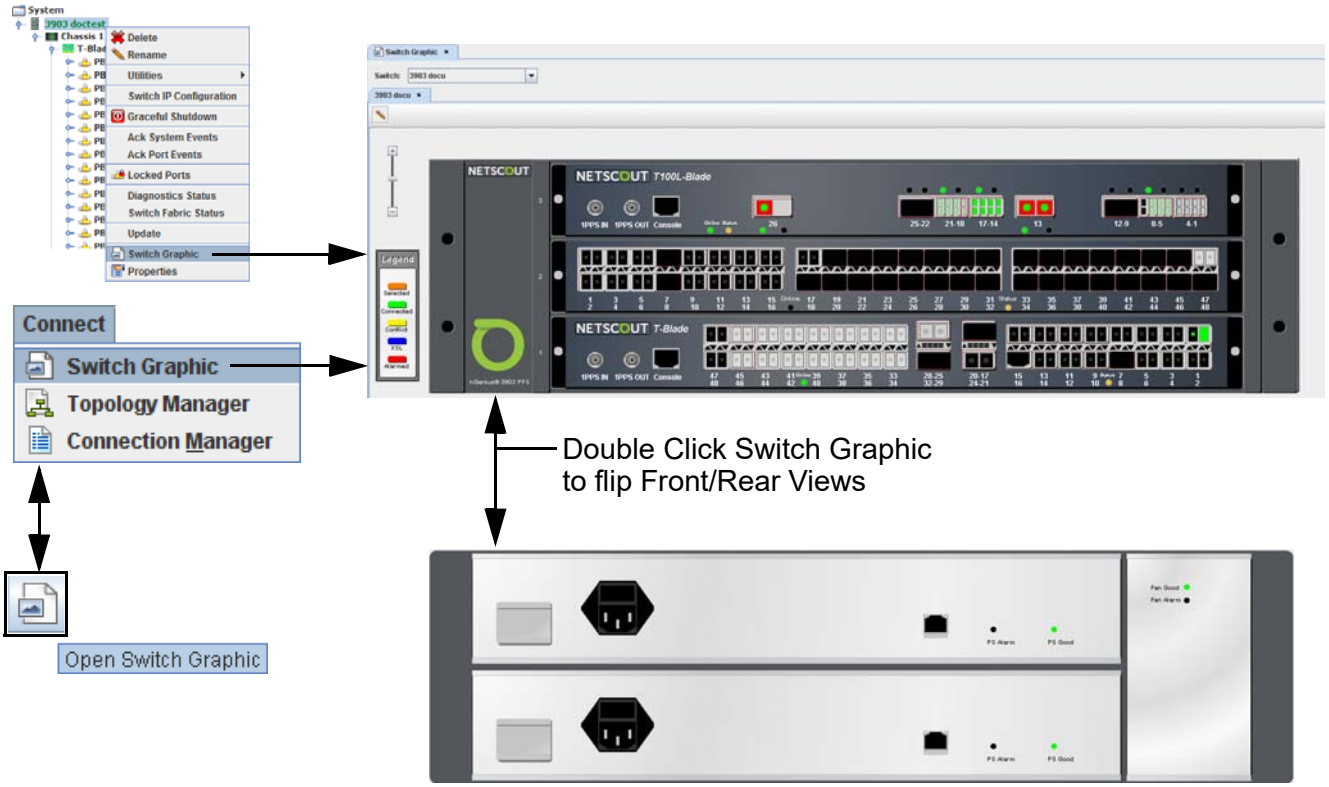
REVise **SWI**tch *switchname* **CFP** {**ENA**bled|**DIS**abled}

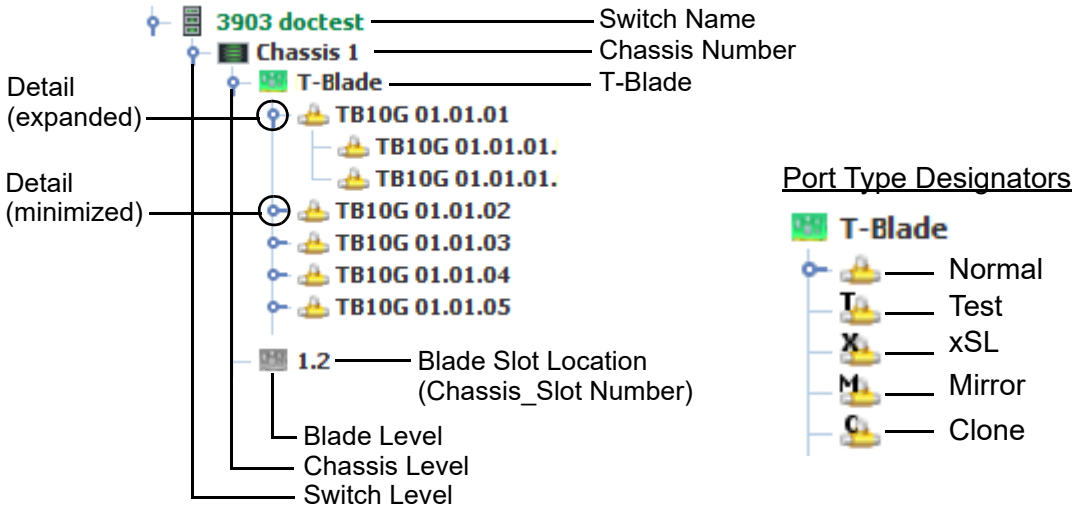
Example:
rev swi MySwitch cfp ena

Viewing Switch Details

Right clicking on a switch and selecting **Switch Graphic**, selecting **Connect > Switch Graphic**, or from the toolbar, selecting the **Open Switch Graphic** icon, or from the keyboard **Alt+F9** displays a close up detail of the chassis showing installed blades and system components of the selected switch. Moving the pointer's cursor over the front switch graphic displays information on the switch (switch name, blade number, port information / status). From this view, blades and ports can be defined.

Note: Switch Graphic does not support MRV and Polatis switches.

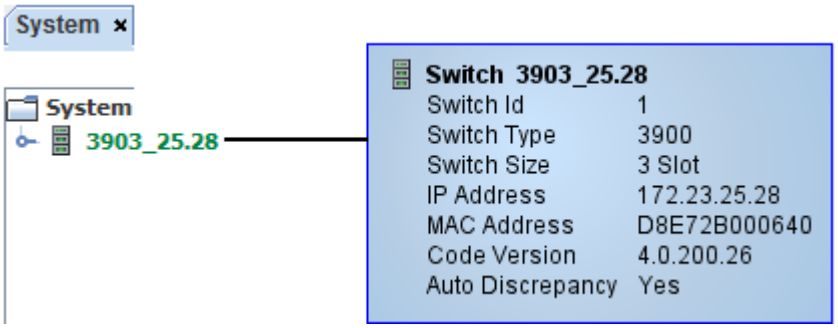




System Tab

From the Switch level, moving the pointer's cursor over a listed switch displays additional information including:

- Switch Name (assigned switch name)
- Switch ID (position switch is listed in switch tree)
- Switch Type / Series (default = 3900)
- Switch Size (number of blade slots available in system: 3901 - 1 slot, 3903 - 3 slots, 3912 - 12 slots)
- IP Address (IPv4 address)
- MAC Address (assigned internal chassis address)
- Code Version (TestStream Management software version)
- Auto Discrepancy (active = Yes, not active = No)



nGenius 3901 / 3901R / 3903 / 3912 Front Views

Selecting a switch chassis displays a close up detail of the nGenius 3900 switches chassis showing installed blades and ports. Positioning the pointer's cursor near a blade displays an information block describing the blade in detail. Positioning the pointer's cursor on a port displays further information on the port itself. Refer to Blade Port Legends on page 3-52 for the different port states (colors / images) displayed on the Switch Graphic screen. A system or port error condition on a blade is indicated with a red triangle on the right side of the blade.

Defined ports are displayed with the interface connector style used with the particular SFP module.

Double-click on the chassis body (not the blades) in the switch graphic display screen to alternate between front and rear chassis views.

3912 AC Power Supplies

The 3912 front view also displays the power supply status indicators, and connectors for power and Ethernet. In the event of AC input power loss to a power supply, a red **X** is displayed over the affected AC input connector.

nGenius 3901 / 3901R / 3903 / 3912 Rear Views

AC Power Supplies (nGenius 3901 / 3901R / 3903)

The rear chassis view displays the AC power supplies, fan modules (nGenius 3901R and 3903), status indicators (nGenius 3901R and 3903), and interconnections for power and Ethernet (nGenius 3901, 3901R, and 3903). The status indicators for power and fan are active, showing the actual status of the nGenius 3900 series switch components. In the event of a component failure, the appropriate failure indicator will display. In the event of AC input power loss to a power supply, the PS ALARM indicator lights yellow and a red **X** is displayed over the affected AC input connector. In a fan failure, the FAN ALARM indicator lights yellow and a red **X** is displayed over the fan module.

DC Power Supplies (nGenius 3901R)

The rear chassis view displays the DC power supplies, fan module, status indicators, and interconnections for DC input power. The status indicators for power and fan are active, showing the actual status of the nGenius 3901R switch components. In the event of a component failure, the appropriate failure indicator will display. In the event of DC input power loss to a power supply, the BATT ALARM indicator lights yellow and a red **X** is displayed over the affected DC input connector. In a fan failure, the FAN ALARM indicator lights yellow and a red **X** is displayed over the fan module.

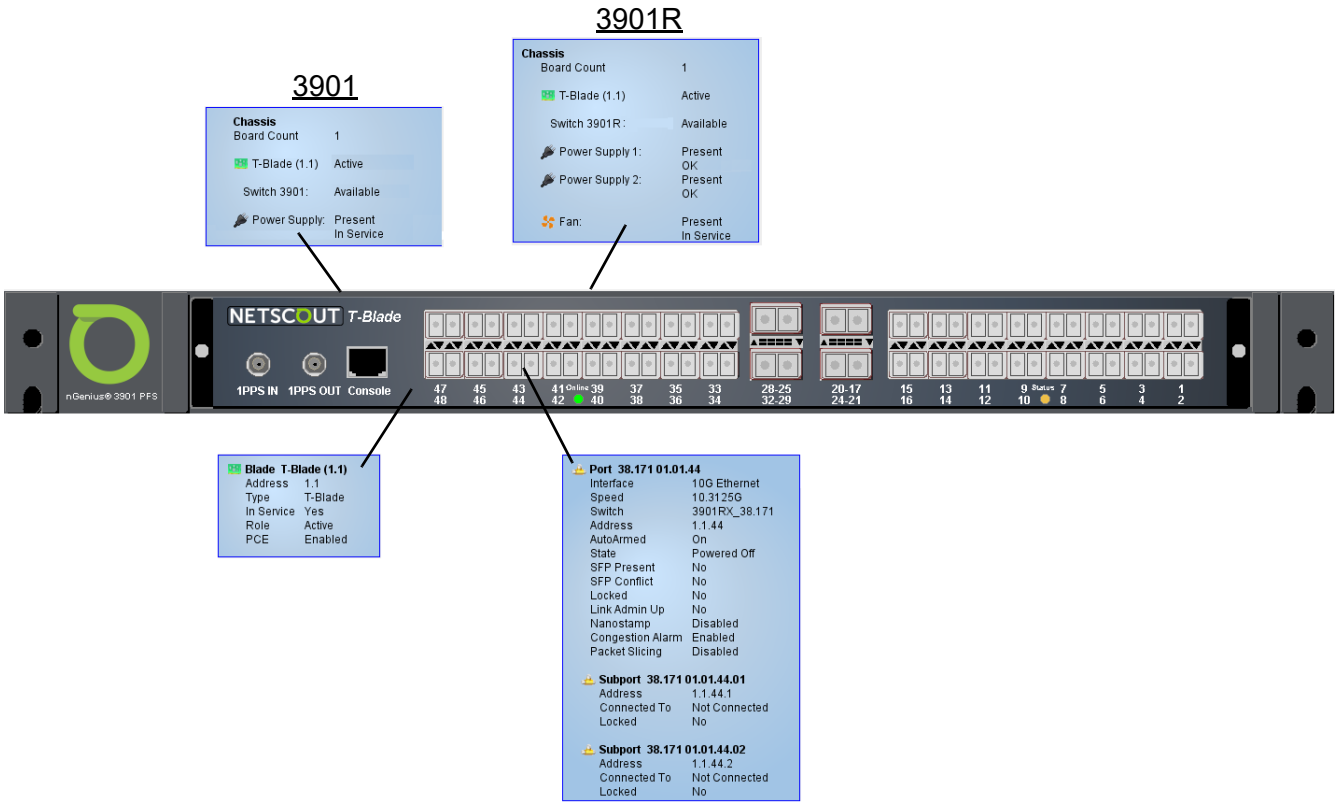
DC Power Supplies (nGenius 3903)

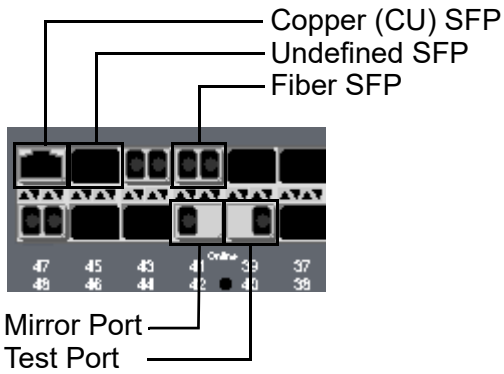
The rear chassis view displays the DC power supplies (nGenius 3903), fan module, status indicators, and interconnections for DC input power, 1PPS, and Ethernet. The status indicators for power and fan are active, showing the actual status of the nGenius 3900 series switch components. In the event of a component failure, the appropriate failure indicator will display. In the event of DC input power loss to a power supply, the BATT ALARM and PS ALARM indicators light yellow and a red **X** is displayed over the affected DC input connector. In a fan failure, the FAN ALARM indicator lights yellow and a red **X** is displayed over the fan module.

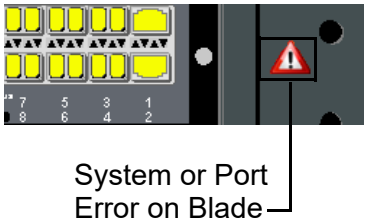
3912 Rear View

The rear chassis view displays the fan modules, switch fabric modules (SFM), and status indicators. In a fan failure, the FAN ALARM indicator lights yellow and a red **X** is displayed over the fan module. If an SFM fails, the STATUS indicator lights yellow and a red **X** is displayed over the SFM module. In addition, positioning the pointer's cursor near an SFM displays an information block describing the operational status of the module.

nGenius 3901 / 3901R Switch Front View

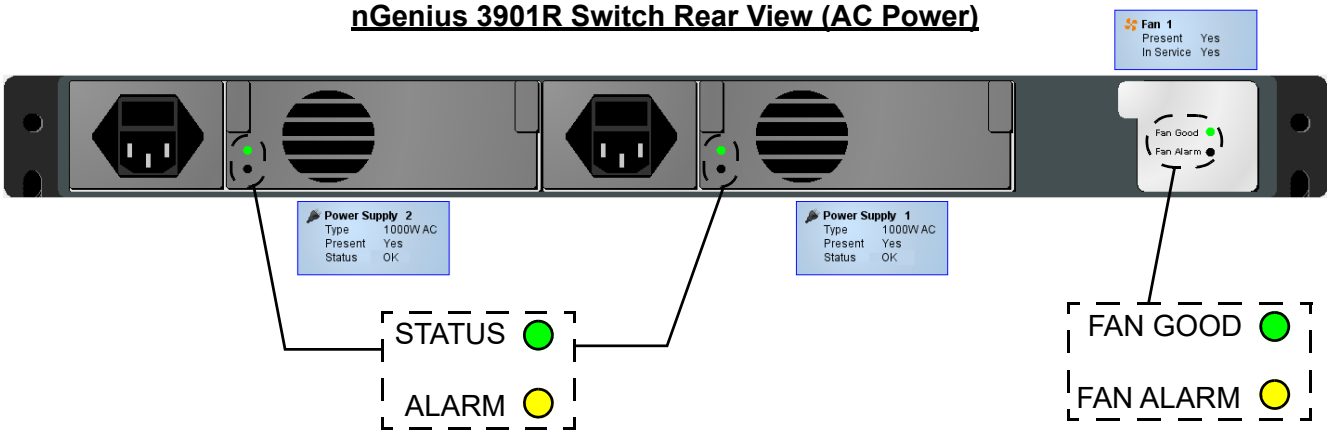




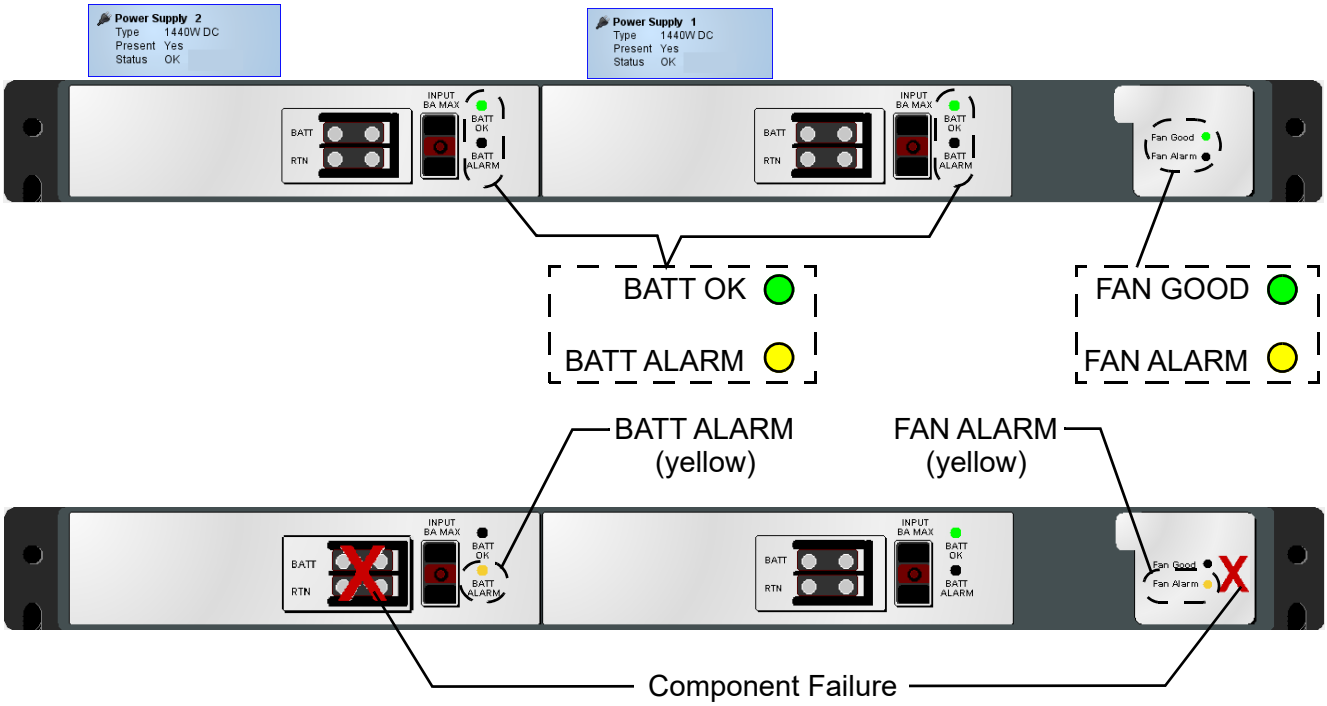


nGenius 3901 Switch Rear View

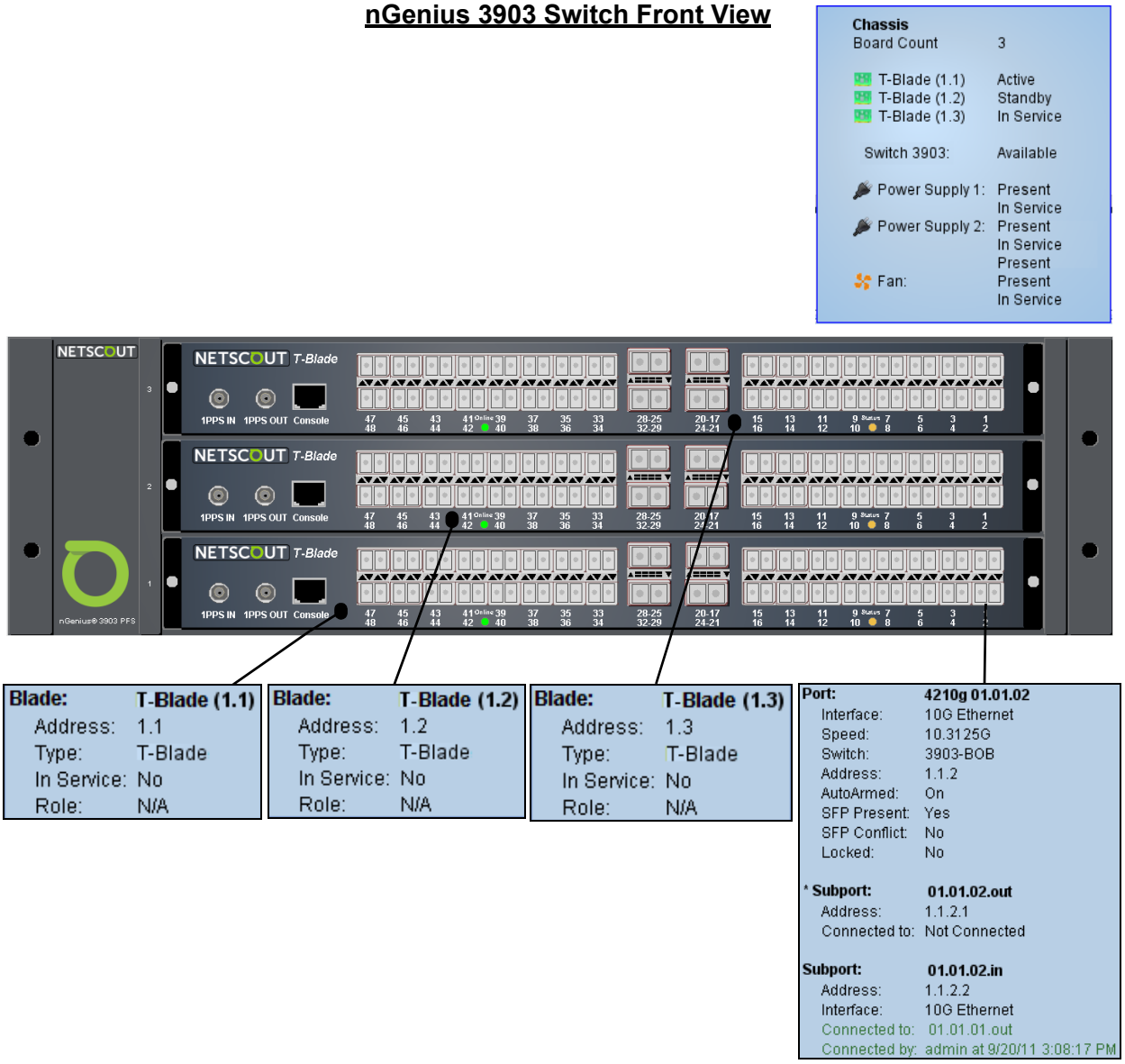
nGenius 3901R Switch Rear View (AC Power)



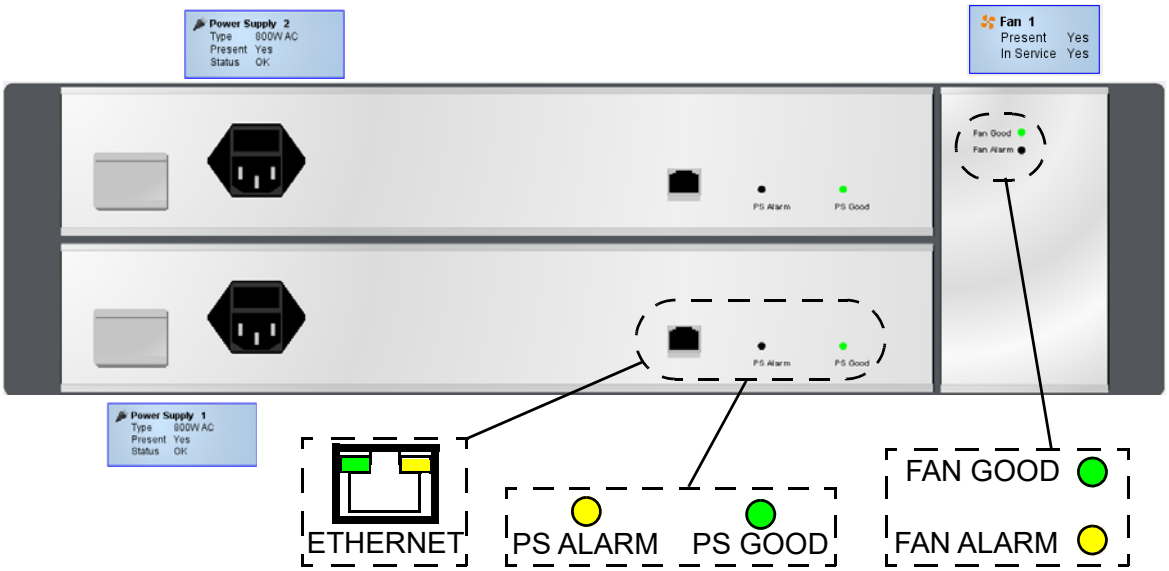
nGenius 3901R Switch Rear View (DC Power)

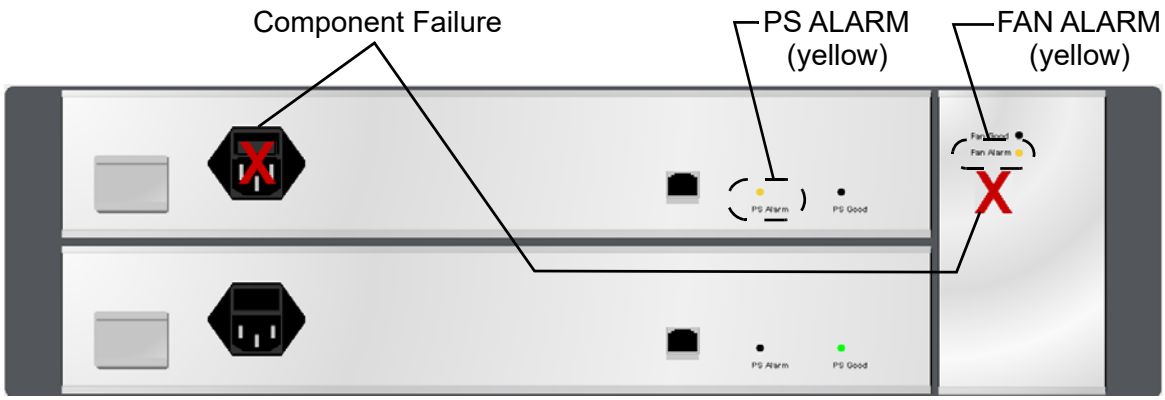


nGenius 3903 Switch Front View

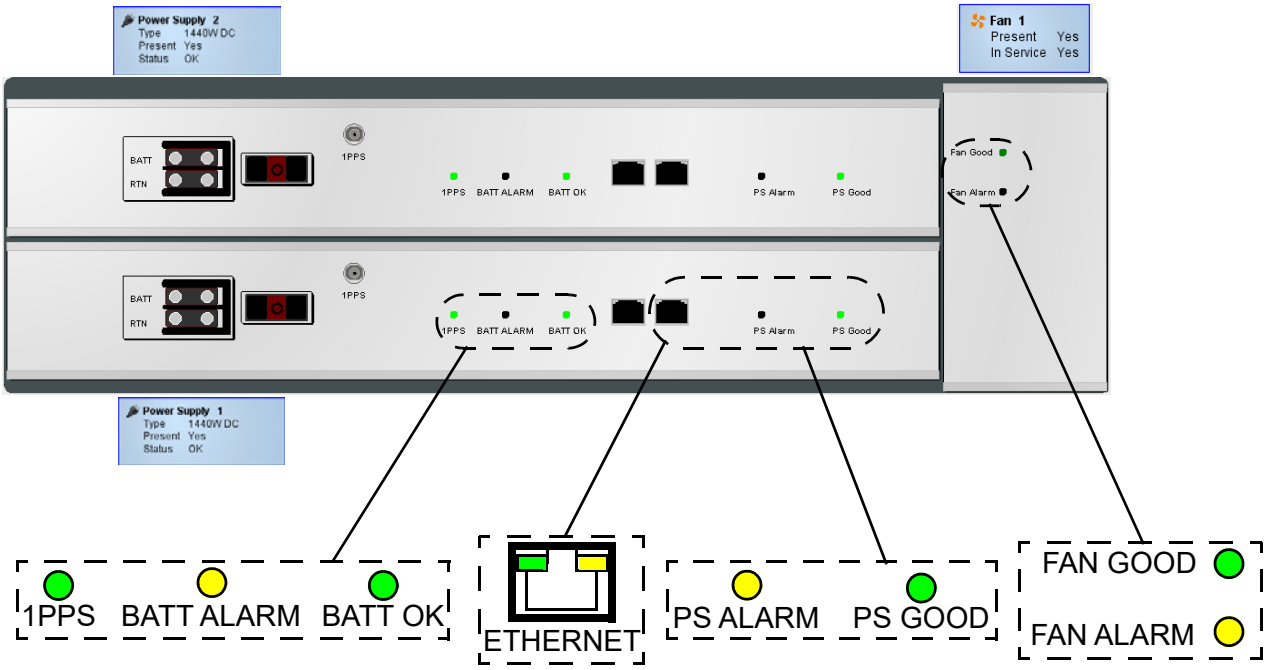


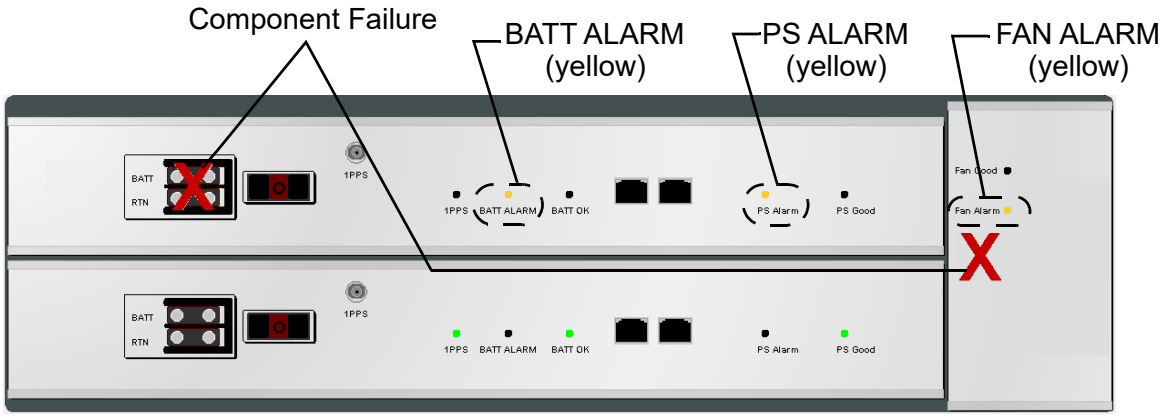
nGenius 3903 Switch Rear View (AC Power)



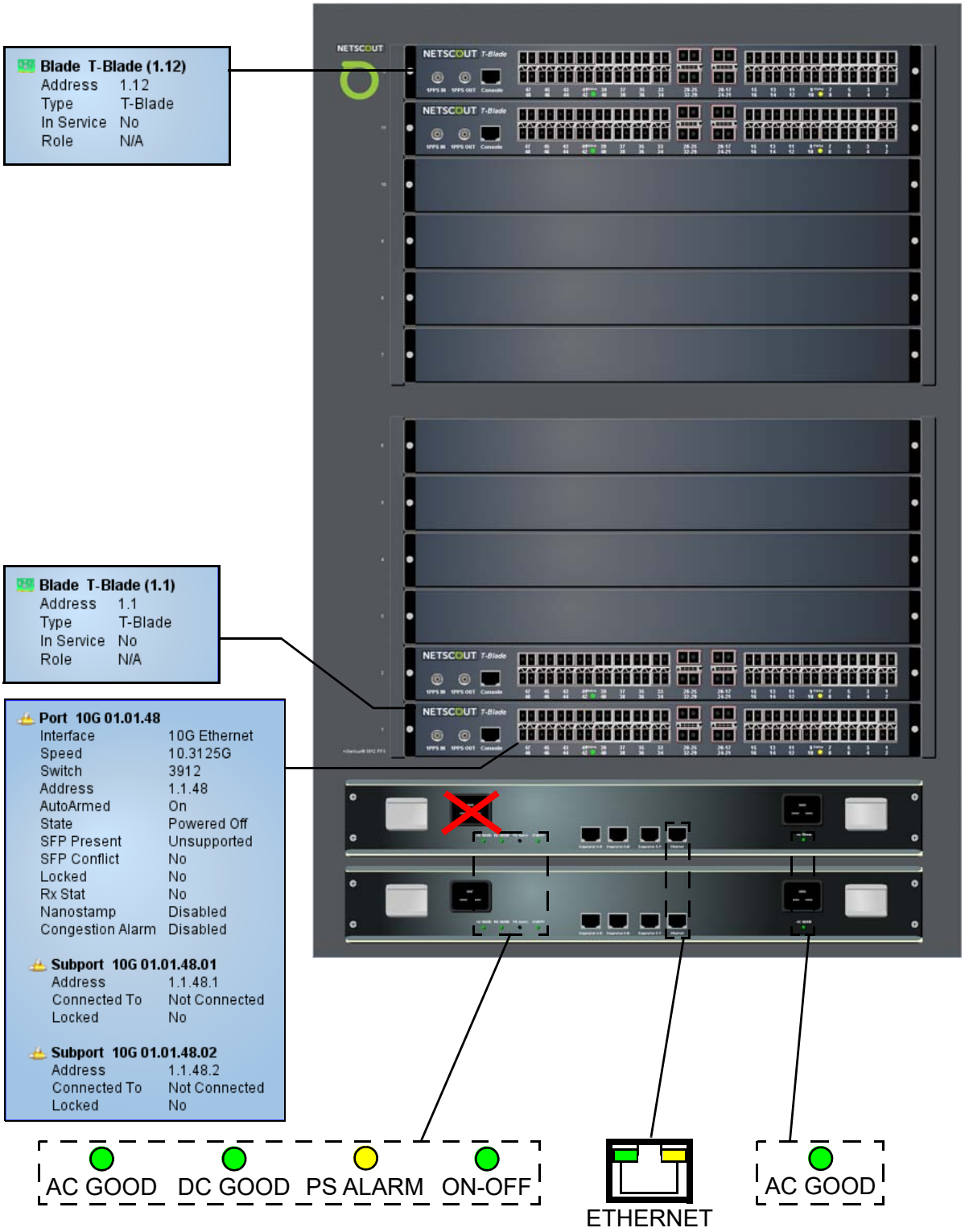


nGenius 3903 Switch Rear View (DC Power)

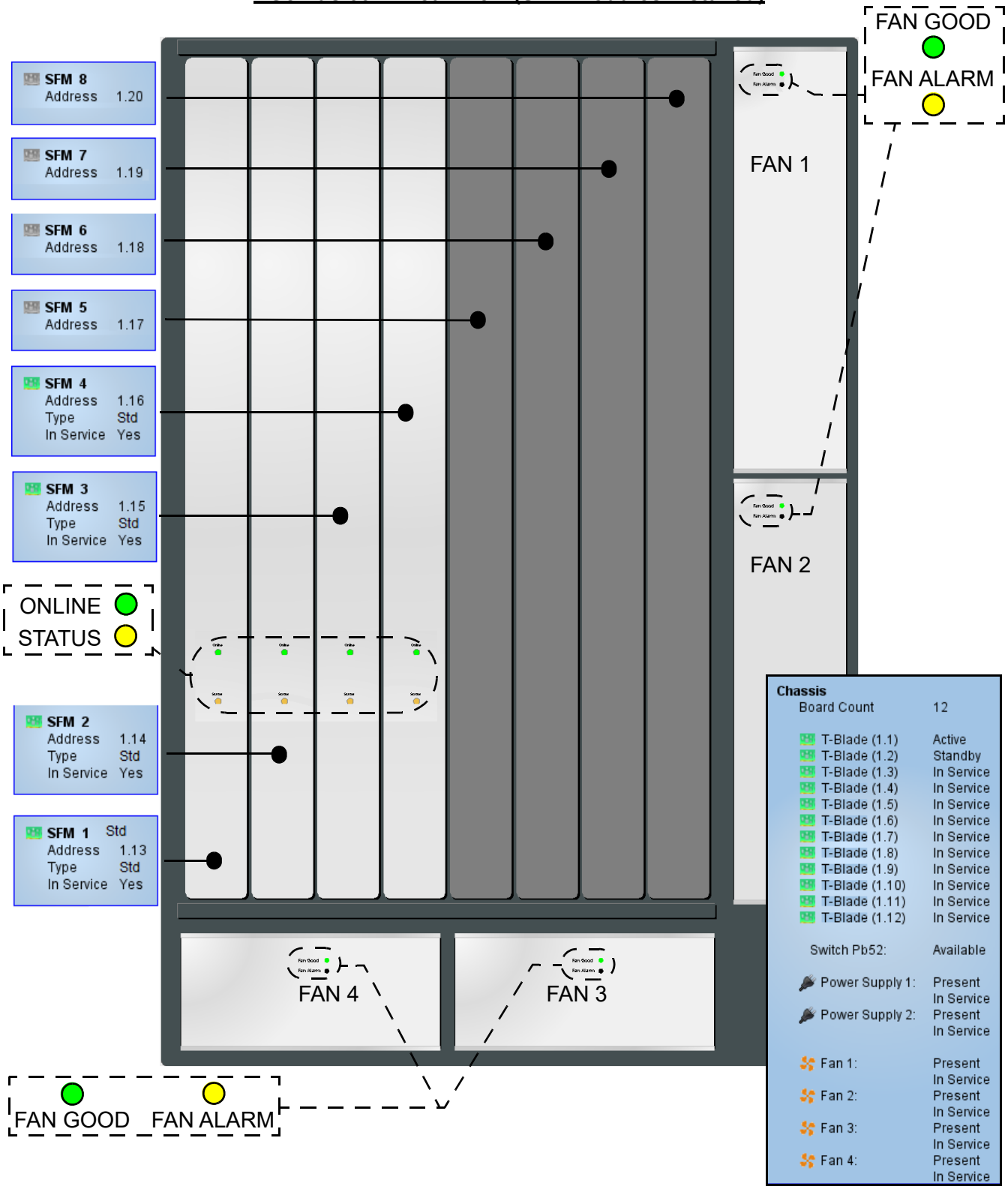




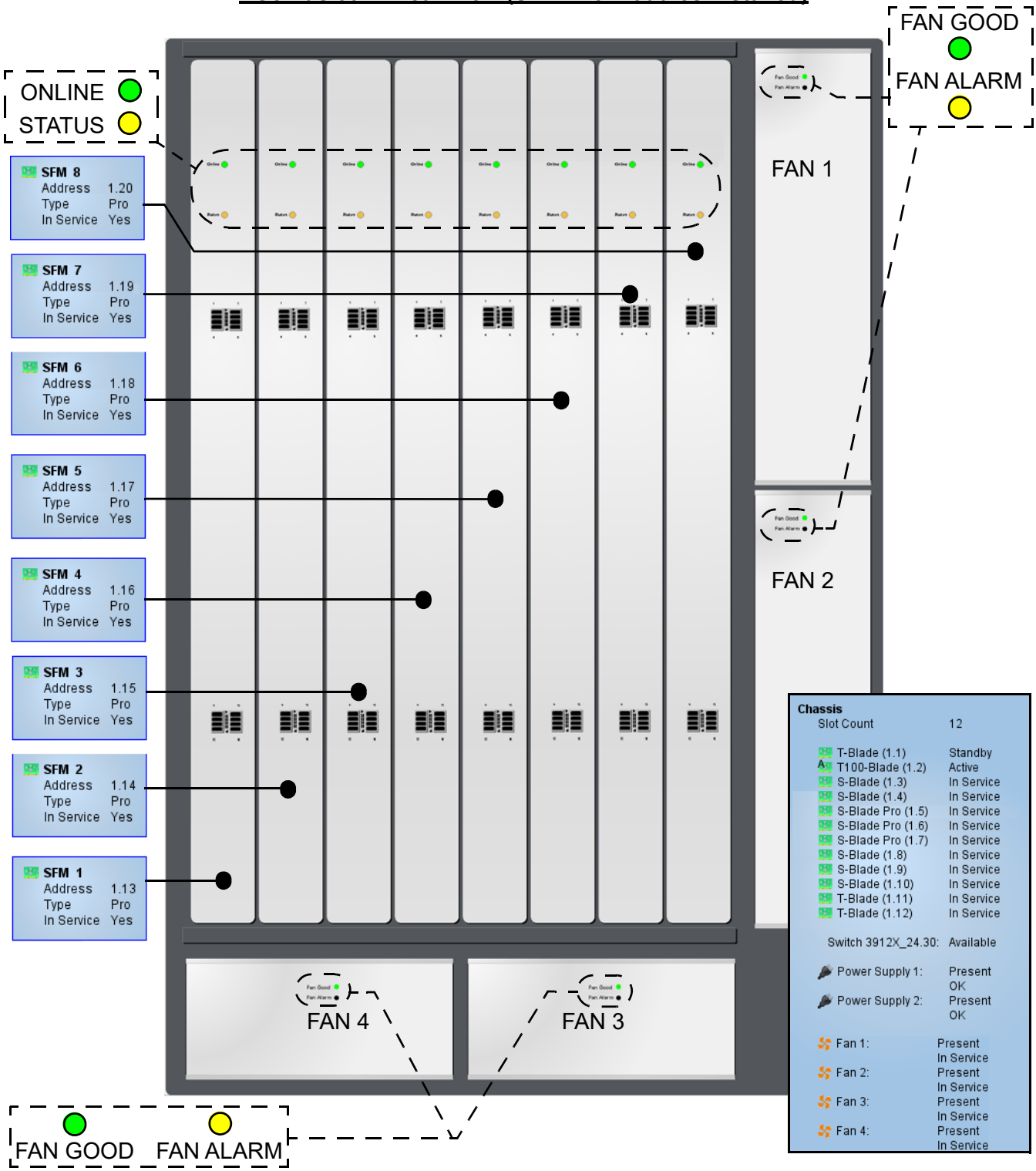
nGenius 3912 with T-Blades



nGenius 3912 Rear View (SFM Modules Installed)



nGenius 3912 Rear View (SFM Pro Modules Installed)



OS-16 / OS-96 / OS-192 Front Views

Selecting a switch chassis displays a close up detail of the optical switch chassis.

OS-16: The OS-16 is shown as a defined logical O-Blade (1.1) showing the defined optical ports. Positioning the pointer's cursor in the location of port numbers 1.1 through 1.16 displays an information block describing the O-Blade in detail. Positioning the pointer's cursor on a port displays further information on the port itself. Refer to Blade Port Legends on page 3-52 for the different port states (colors / images) displayed on the Switch Graphic screen. A system or port error condition on an O-Blade is indicated with a red triangle on the right side of the blade.

OS-96: The OS-96 is shown as a defined logical O-Blade (1.1) showing the defined optical ports. Positioning the pointer's cursor in the location of port numbers 1.1 through 1.96 displays an information block describing the O-Blade in detail. Positioning the pointer's cursor on a port displays further information on the port itself. Refer to Blade Port Legends on page 3-52 for the different port states (colors / images) displayed on the Switch Graphic screen. A system or port error condition on an O-Blade is indicated with a red triangle on the right side of the blade.

OS-192: The OS-192 is shown as two defined logical O-Blades (1.1 and 1.2) showing the defined optical ports. Positioning the pointer's cursor in the location of port numbers 1.1 through 1.96 displays an information block describing O-Blade (1.1) in detail. Positioning the pointer's cursor in the location of port numbers 2.1 through 2.96 displays an information block describing O-Blade (1.2) in detail. Positioning the pointer's cursor on a port displays further information on the port itself. Refer to Blade Port Legends on page 3-52 for the different port states (colors / images) displayed on the Switch Graphic screen. A system or port error condition on an O-Blade is indicated with a red triangle on the right side of the blade.

Defined ports are displayed with the interface connector style used with the LC connector.

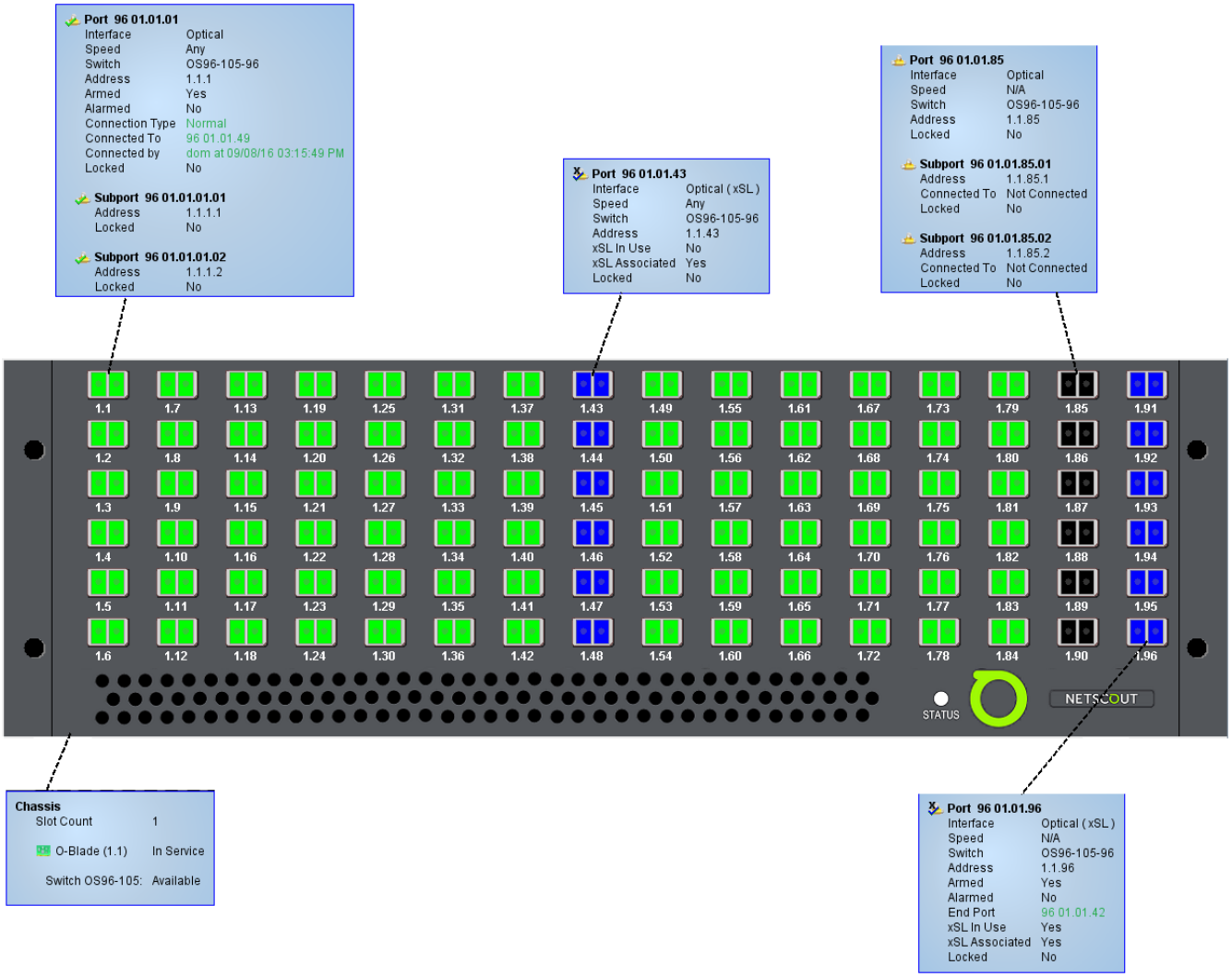
Double - click on the edge of the chassis body in the switch graphic display screen to alternate between front and rear chassis views.

Note: OS-16 / OS-96 / OS-192 Rear Views

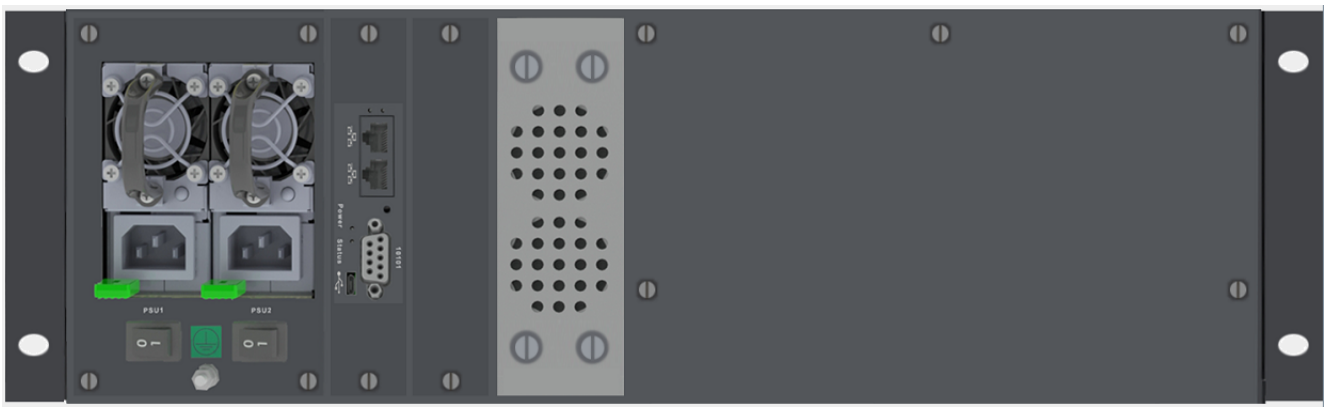
Clicking the Rear View arrow icon from the OS-96 or OS-192 front view displays a static rear view graphic of the OS-96 / OS-192 power supplies, network interface module and cooling fan module. TestStream does not support operational status details concerning the power supplies, network interface or the fan module.

The OS-16 rear view graphic is not supported.

OS-96 Optical Switch: Front View

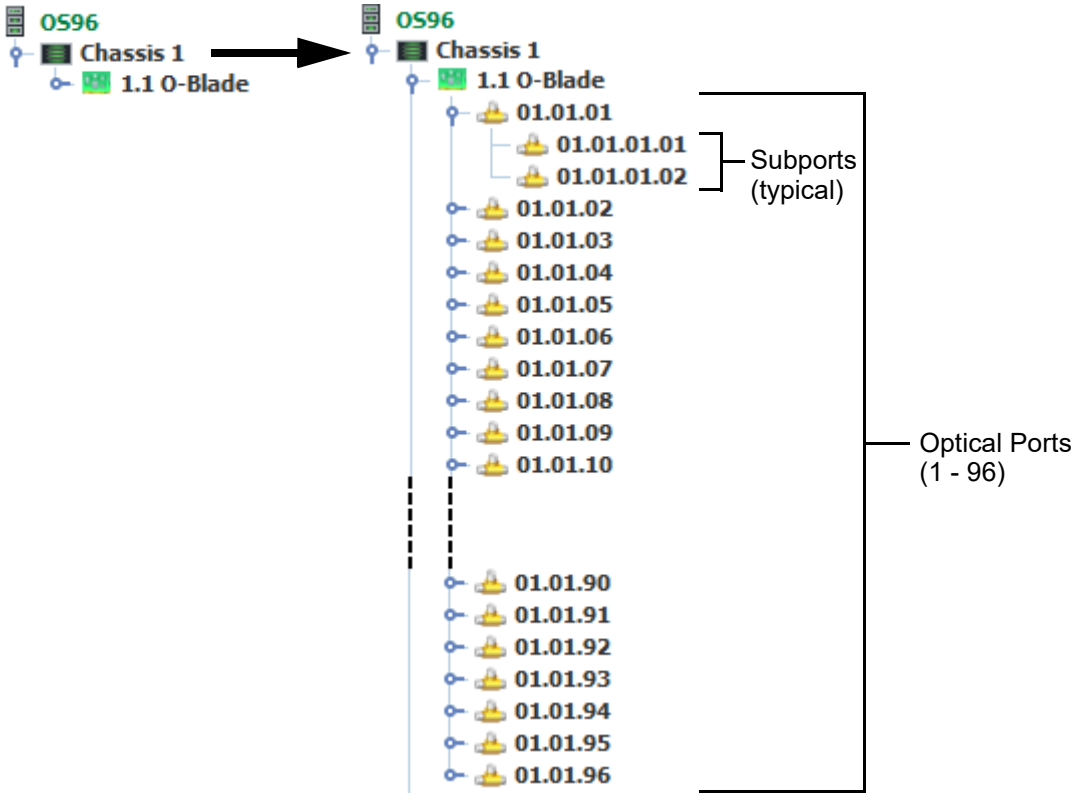


OS-96 Optical Switch: Rear View

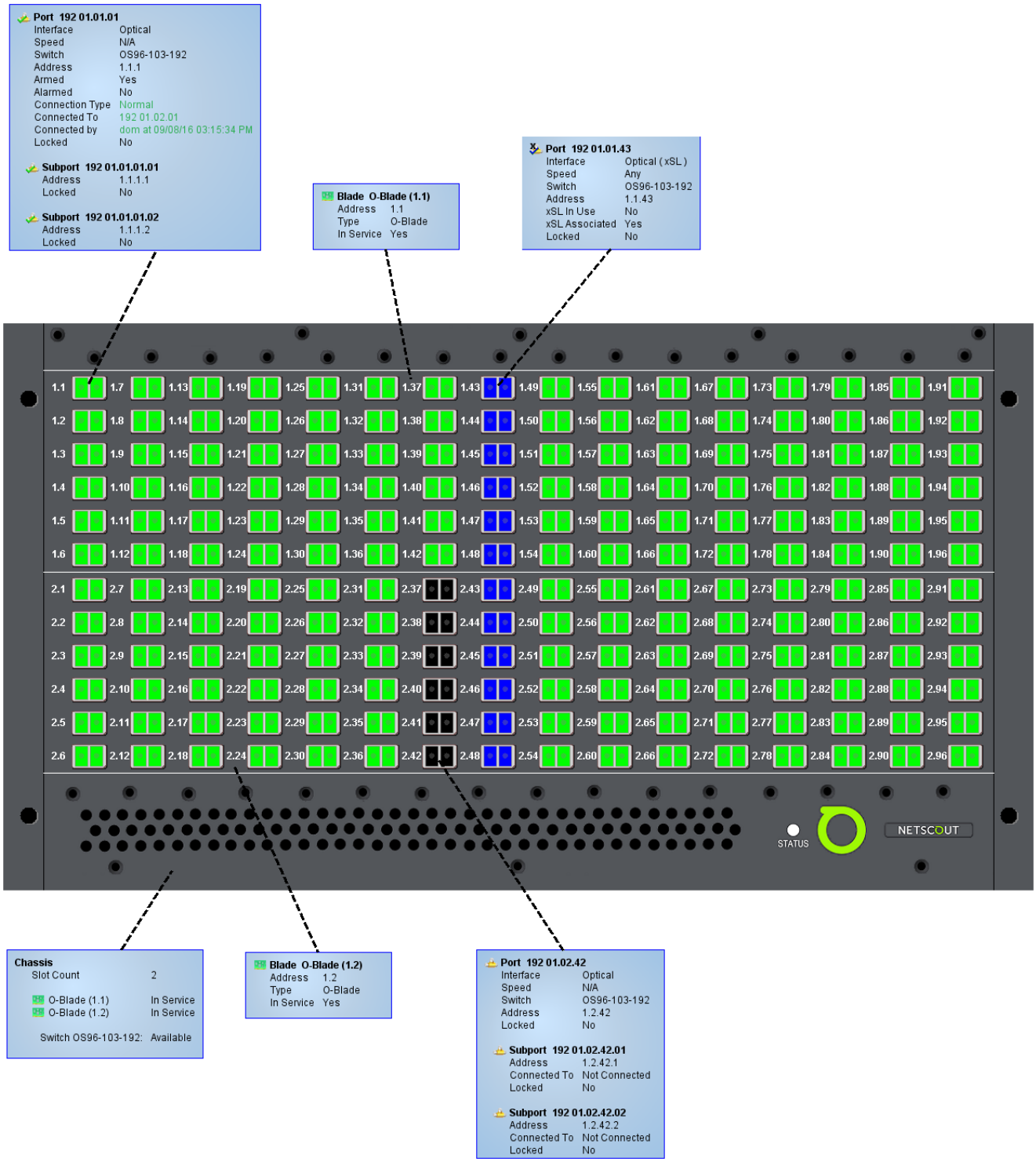


OS-96 System Tree

The OS-96 is depicted as an individual O-Blade containing 96 duplex / 192 simplex optical ports.



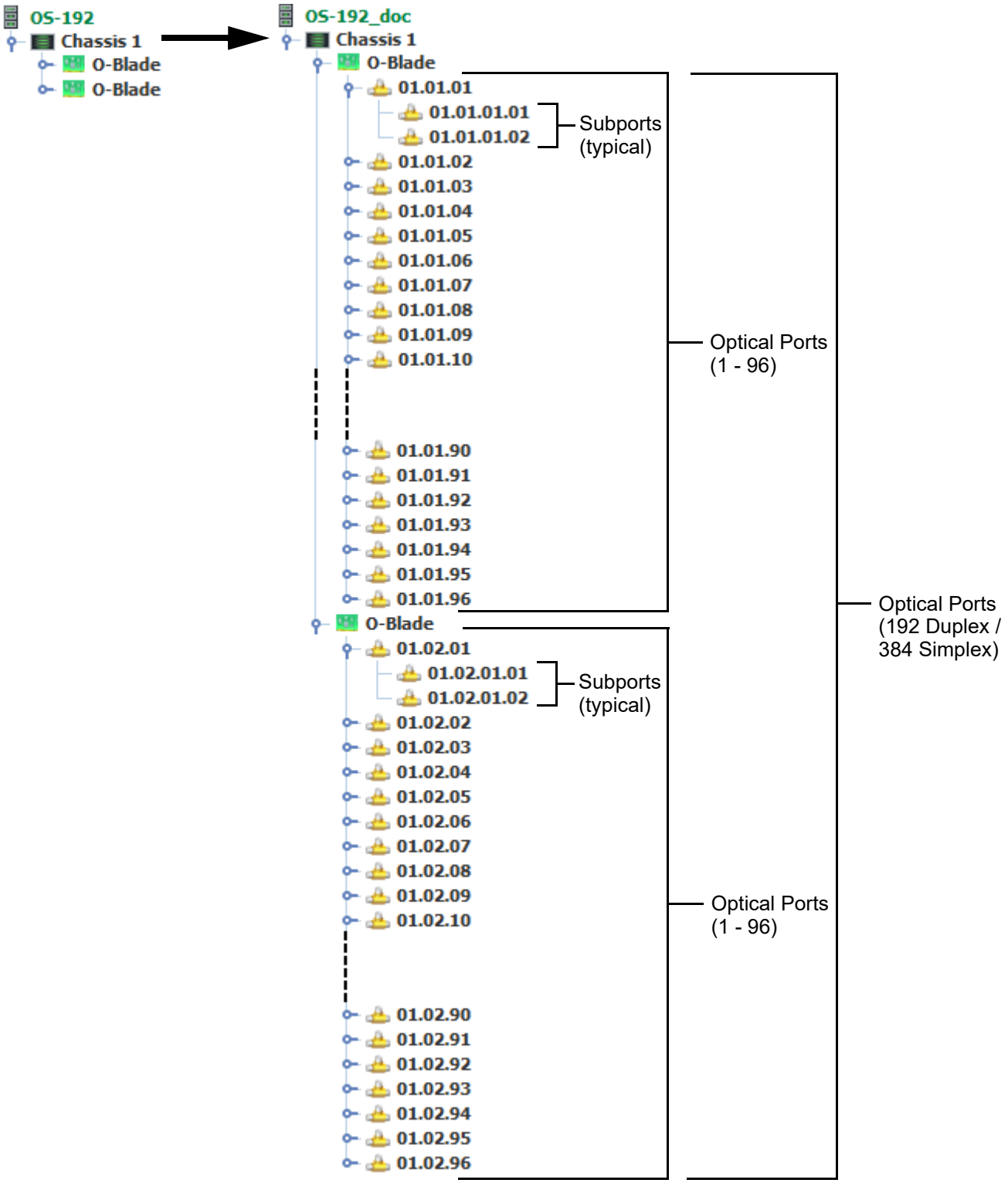
OS-192 Optical Switch: Front View



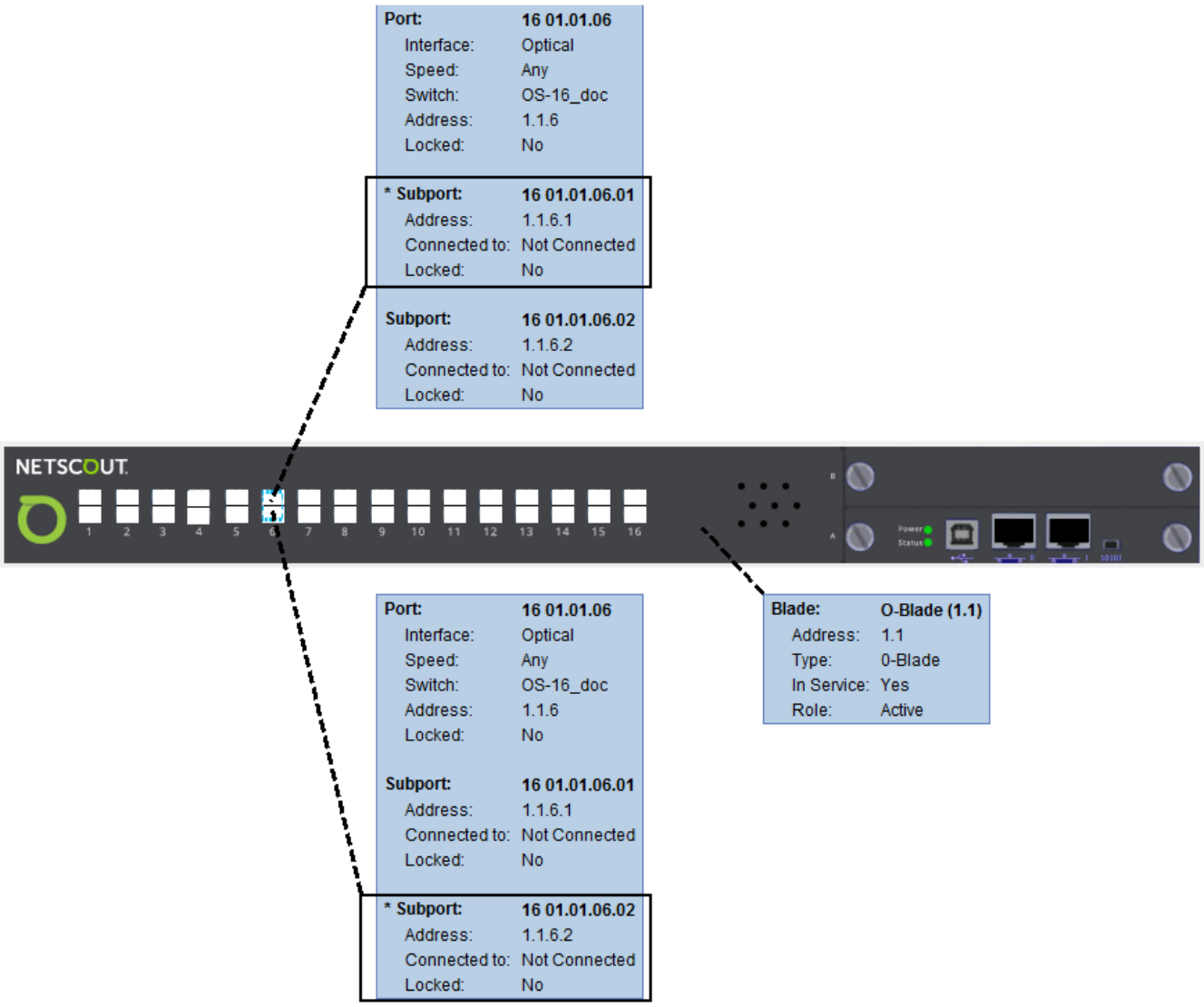
OS-192 Optical Switch: Rear View

OS-192 System Tree

The OS-192 is depicted as two individual O-Blades each containing 96 duplex / 192 simplex optical ports for a total of 192 duplex / 364 simplex connections.

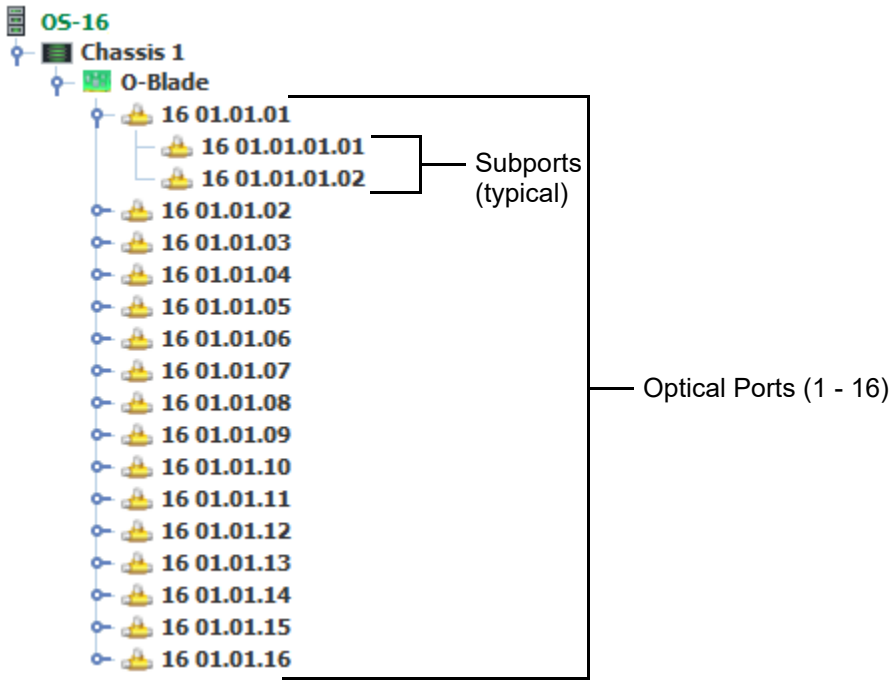


OS-16 Optical Switch: Front View



OS-16 System Tree

The OS-16 is depicted as a single O-Blade containing 16 duplex / 32 simplex optical ports.



HS-3200 Front and Rear Views

Selecting an HS-3200 switch chassis displays a close up detail of the HS-3200 switch chassis.

HS-3200 Front View

Selecting an HS-3200 switch displays a close up front view detail of the chassis showing the ports and system / fan / power supplies status indicators. Positioning the pointer's cursor over the chassis displays an information block describing the switch (blade) in detail. Positioning the pointer's cursor on a port displays further information on the port itself. Refer to Blade Port Legends on page 3-52 for the different port states (colors / images) displayed on the Switch Graphic screen. A system or port error condition on a blade is indicated with a red triangle on the right side of the blade.

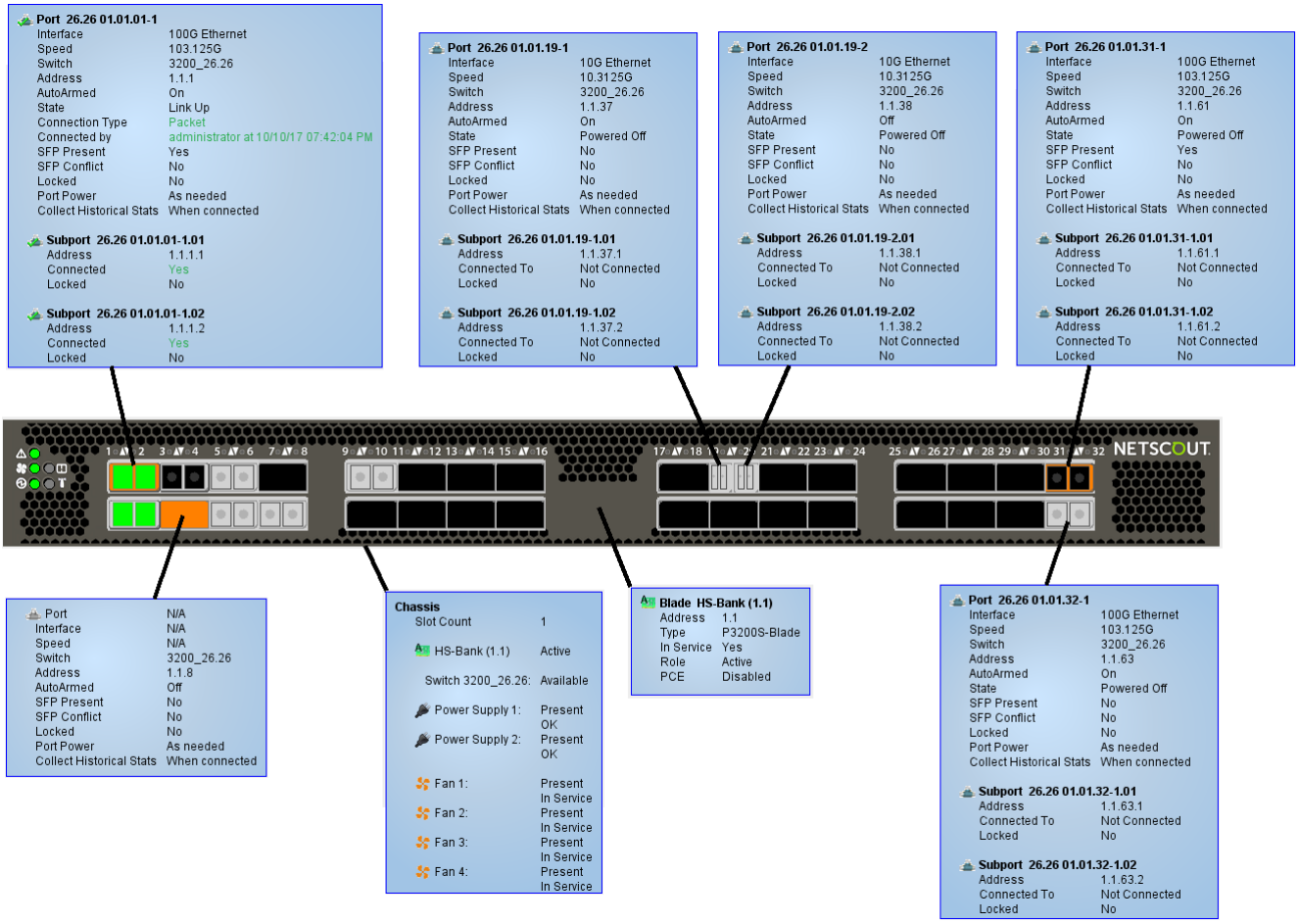
Defined ports are displayed with the interface connector style used with the LC connector.

Double - click on the edge of the chassis body in the switch graphic display screen to alternate between front and rear chassis views.

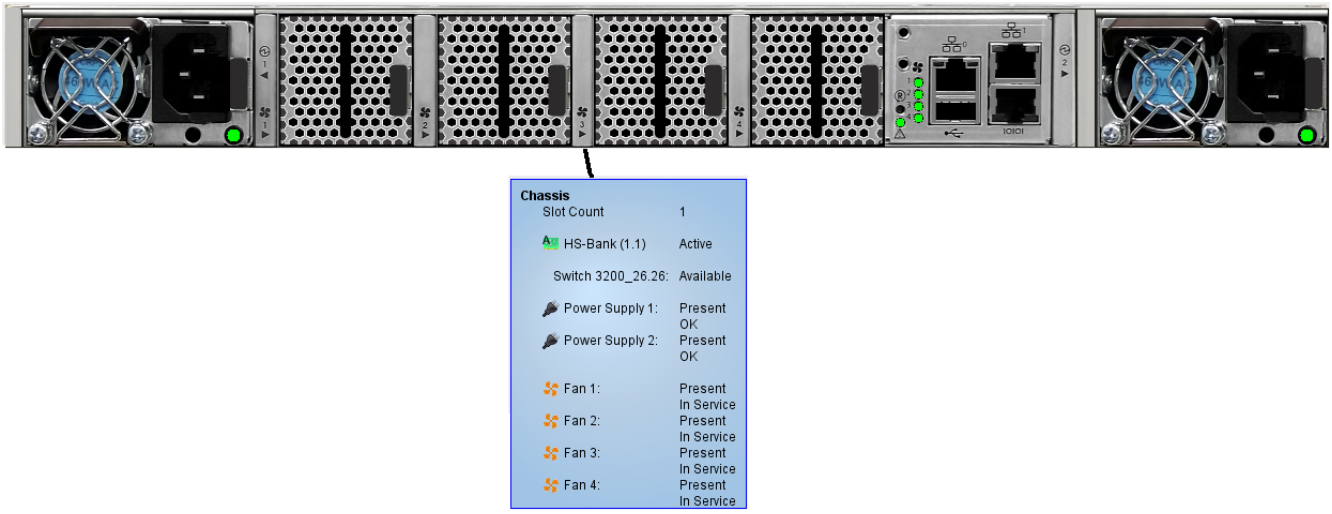
HS-3200 Rear View

The rear chassis view displays the two power supply modules, four fan modules, and system / fan / power supplies status indicators. In a power supply failure, the corresponding power supply status indicator changes from green to amber. In a fan failure, the corresponding fan status indicator changes from green to red. In addition, positioning the pointer's cursor over the chassis displays an information block describing the operational status of the switch chassis in detail.

HS-3200 Switch: Front View

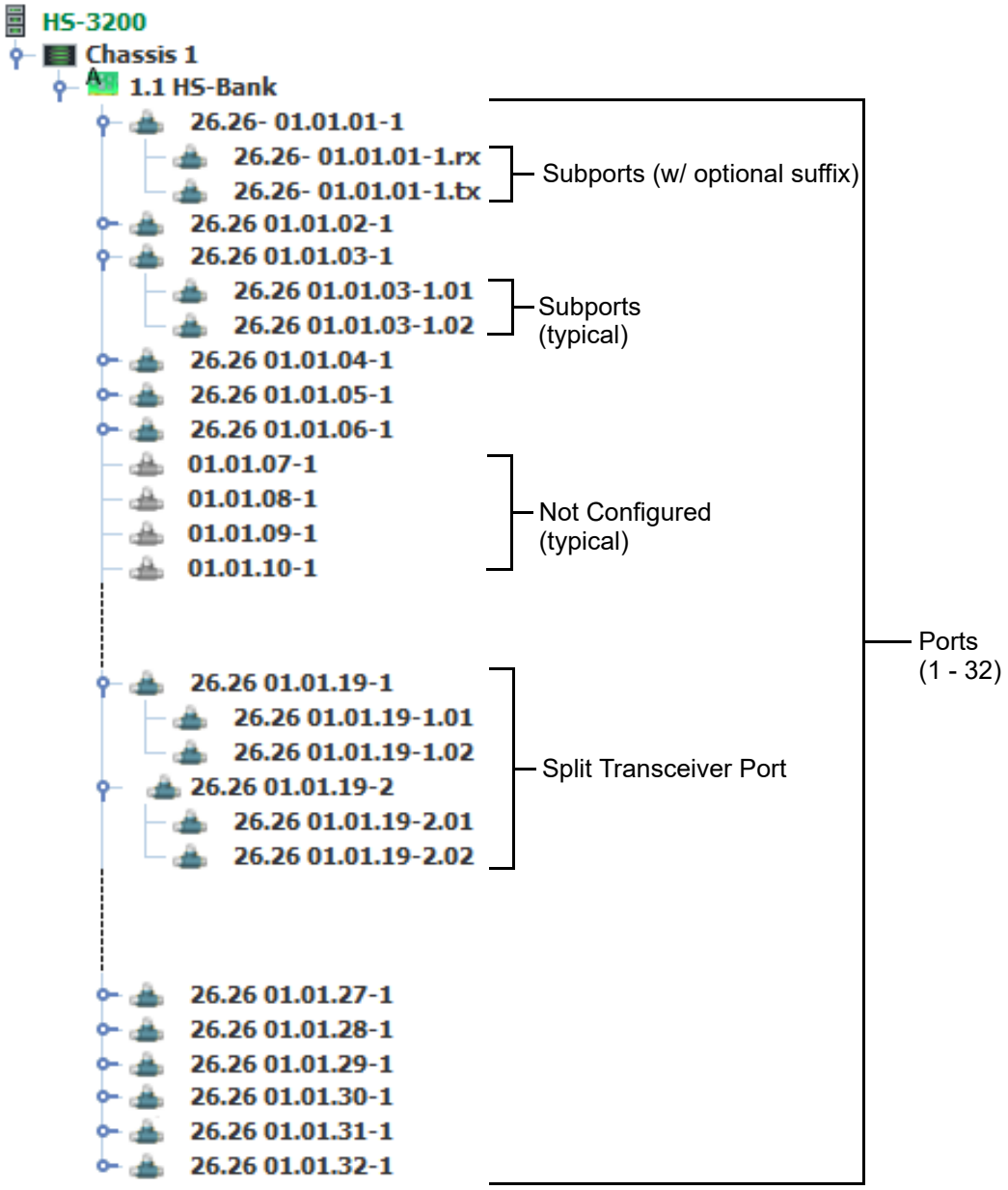


HS-3200 Switch: Rear View



HS-3200 System Tree

The HS-3200 is depicted as an blade containing 32 duplex / 64 duplex ports.



Enabled / Disabled Ports

The 100 GbE top row / odd-numbered ports on the HS-3200 can be split into 2 50GbE ports, or to 2 or 4 25GbE ports, using a breakout cable.

Splitting a 100GbE QSFP28 port into 4 separate 25GbE ports (using a breakout cable) disables the 100GbE port (on the even-numbered row) below it.

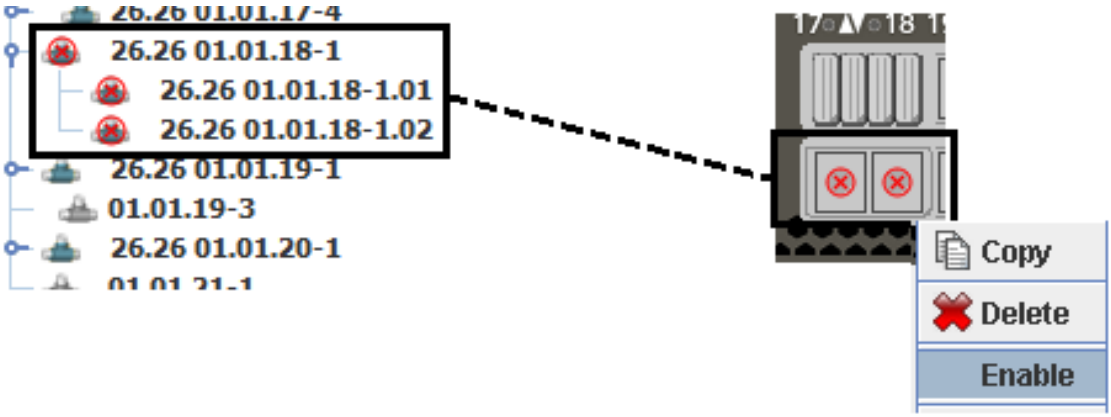
If a top port is set to x4 mode (refer to HS-3200/HS-6400 on page 3-81, Screen 2), the bottom port (directly under the top port) is checked for the following conditions:

- If the bottom port is not defined, the top port will be configured and enabled.
- If the bottom port is defined but locked, not in domain, or powered on, the top port will be configured and disabled. Otherwise it will be enabled and the bottom port will be disabled.

When a top port is changed from a x4 configuration, the bottom port is automatically enabled if it had previously been disabled.

Disabled ports are identified in the system tree and the switch graphic by a red circled **x**. A disabled port has all the functionality of a defined port, except it will not allow connections to be made or statistics collection on that port performed.

Right clicking on a disabled port and selecting **Enable** from the menu allows enabling the port. If the "top port" is enabled, it will be disabled, unless the "top port" is locked, not in domain, or powered on.



HS-6400 Front and Rear Views

Selecting an HS-6400 switch chassis displays a close up detail of the HS-6400 switch chassis.

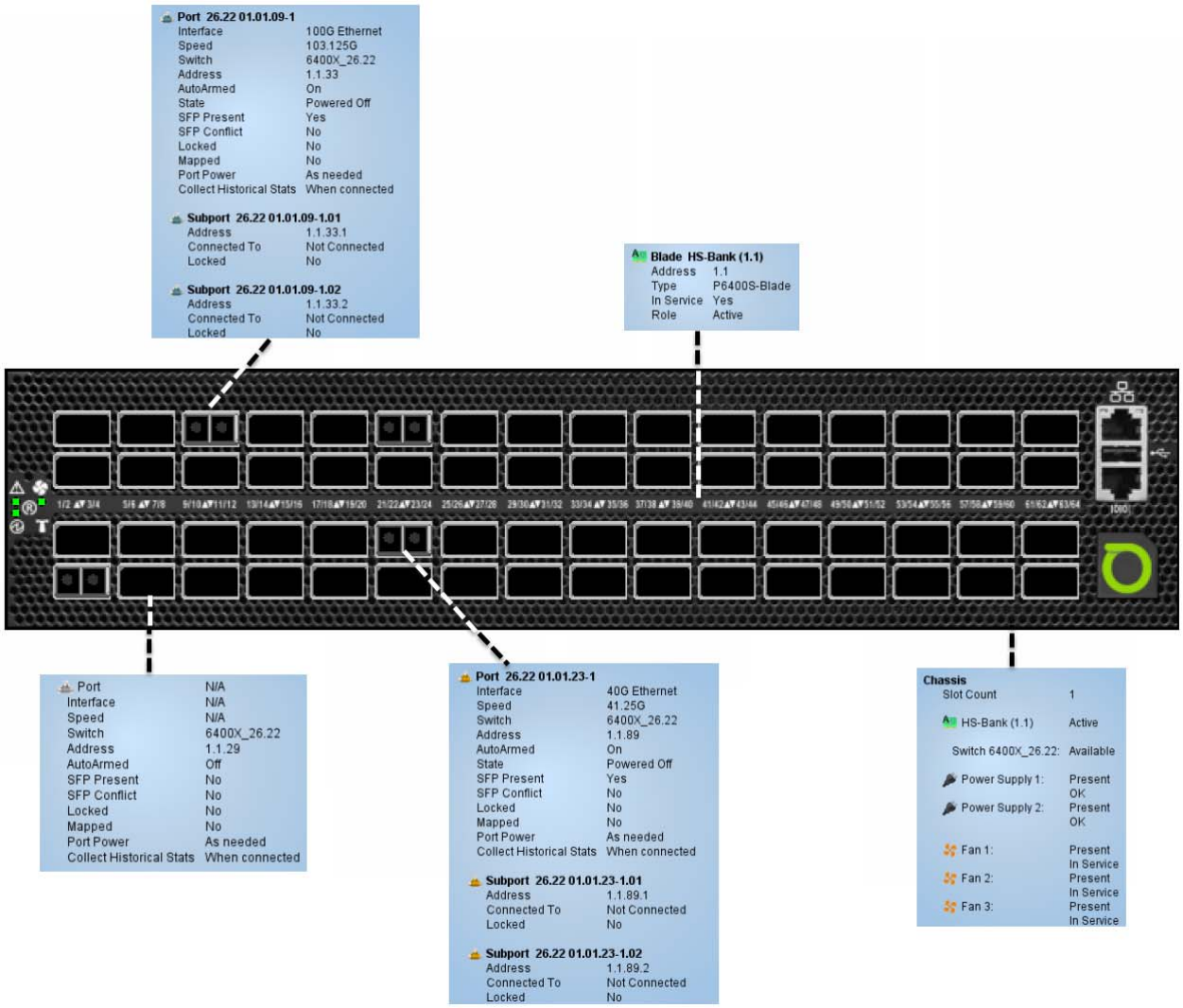
HS-6400 Front View

Selecting an HS-6400 switch displays a close up front view detail of the chassis showing the ports and system / fan / power supplies status indicators. Positioning the pointer's cursor over the chassis displays an information block describing the switch (blade) in detail. Positioning the pointer's cursor on a port displays further information on the port itself. Refer to Blade Port Legends on page 3-52 for the different port states (colors / images) displayed on the Switch Graphic screen. A system or port error condition on a blade is indicated with a red triangle on the right side of the blade.

Defined ports are displayed with the interface connector style used with the LC connector.

Double - click on the edge of the chassis body in the switch graphic display screen to alternate between front and rear chassis views.

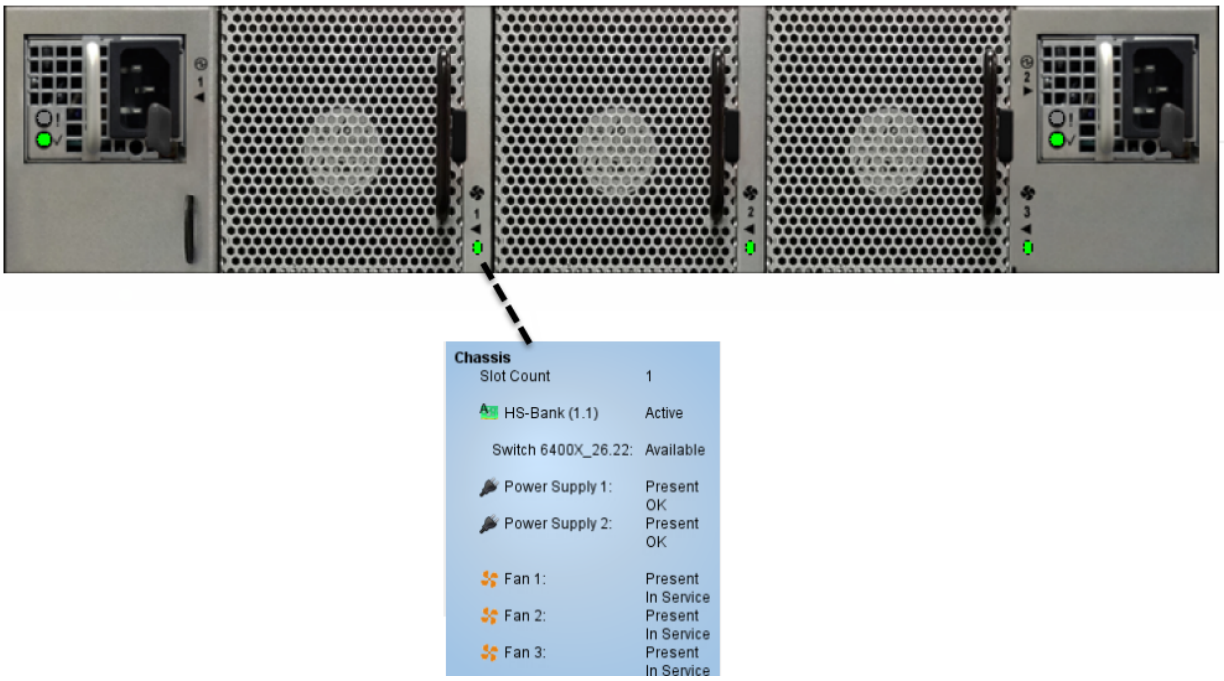
HS-6400 Switch: Front View



HS-6400 Rear View

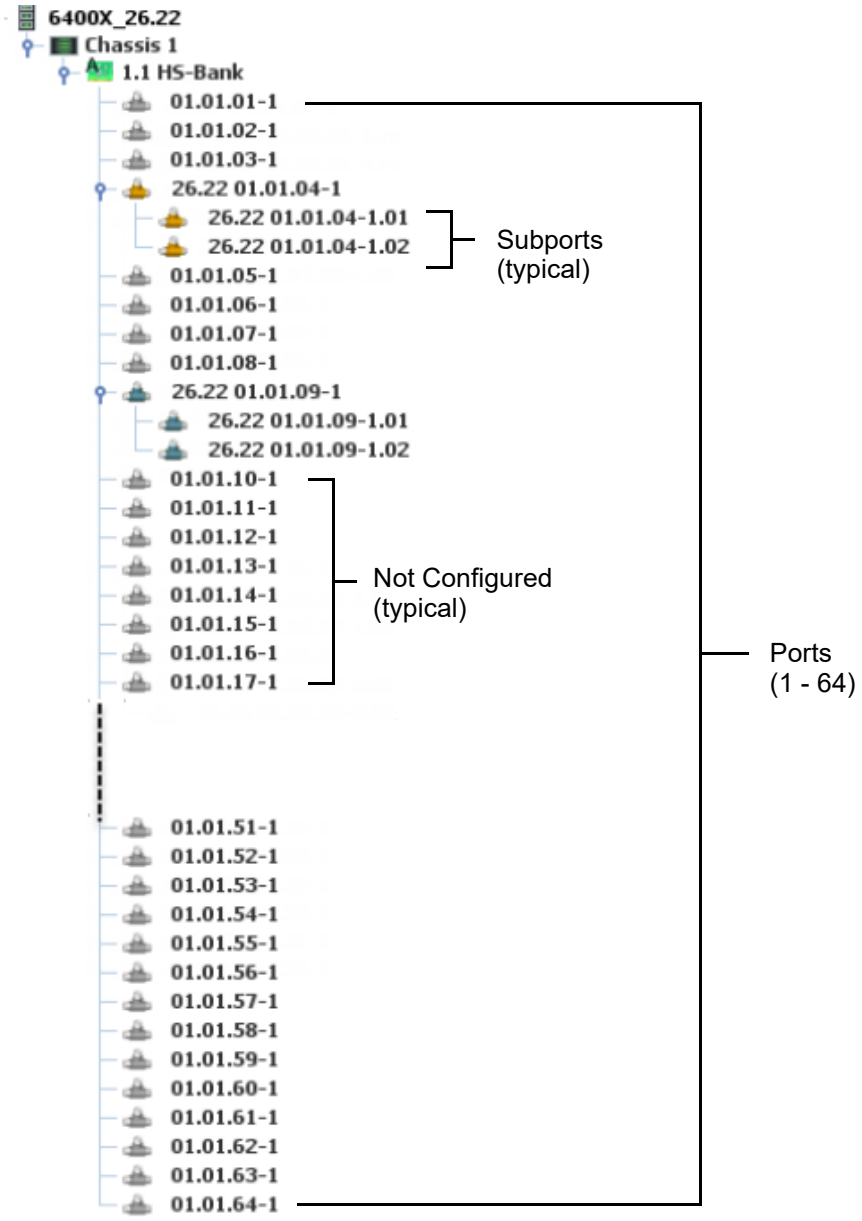
The rear chassis view displays the two power supply modules, three fan modules, and system / fan / power supplies status indicators. In a power supply failure, the corresponding power supply status indicator changes from green to amber. In a fan failure, the corresponding fan status indicator changes from green to red. In addition, positioning the pointer's cursor over the chassis displays an information block describing the operational status of the switch chassis in detail.

HS-6400 Switch: Rear View



HS-6400 System Tree

The HS-6400 is depicted as an blade containing 32 duplex / 64 duplex ports.

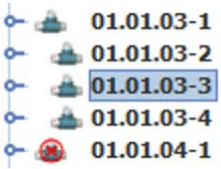


Port Configurations

All (64) QSFP28 front ports are independently configurable as either 1x100Gig, 2x50Gig, 1x40G, 2x25G or 2x10G (some of these lower speeds will require the use of appropriate breakout cables).

Two more interfaces are supported: 4x25G and 4x10G. These interfaces are only available on odd ports and when selected, the corresponding even port (odd port number +1) will be disabled. When using 2x25G, 2x10G, 4x25G, 4x10G, 2x50G, primary and partner ports must have the same speed. Speed changes must be configured using the primary port.

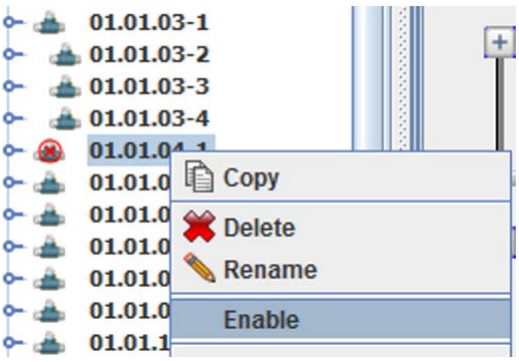
The even numbered port is disabled when the corresponding odd numbered port interface is 4x25/10G.



When an odd port has been configured as 4x25G/10G the corresponding even numbered ports (odd port +1, primary and partner ports) will be disabled. Users shall be able to re-enable the even numbered ports and when that happens the corresponding odd ports (primary and all its partner ports) will be disabled.

Disabled ports are identified in the system tree and the switch graphic by a red circled **x**. A disabled port has all the functionality of a defined port, except it will not allow connections to be made or statistics collection on that port performed.

Right clicking on a disabled port and selecting **Enable** from the menu allows enabling the port. If an even numbered port is enabled, then the corresponding odd numbered port (primary and partner ports) will be disabled.



The primary port interface can be changed from 2x25G/10G to 4x25G/10G without having to delete the partner port first. If the partner port is deleted, when going from 2x25G/10G to 4x25G/10G that port will remain undefined.

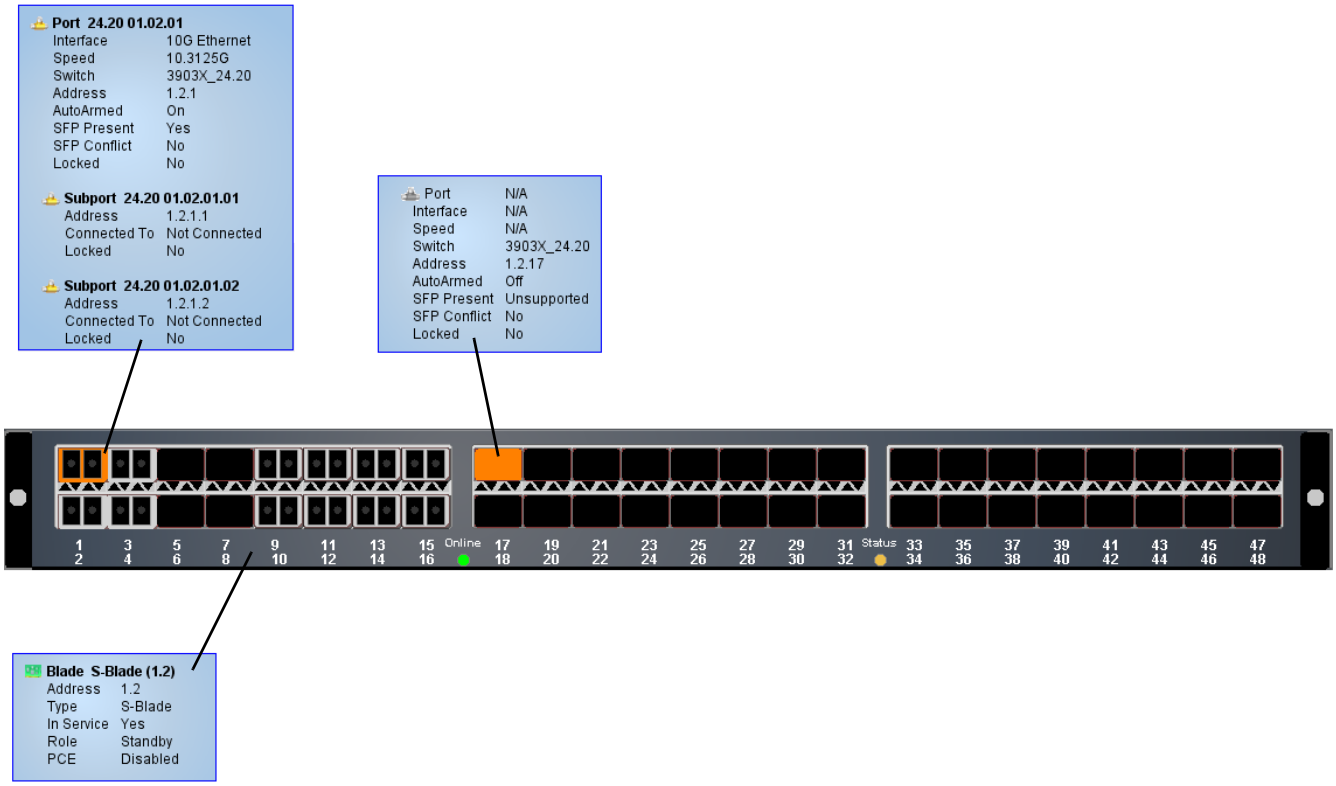
To change the primary port interface from 4x25G/10G to 2x25G/10G, the even numbered partner ports must be deleted first. If all the partner ports are deleted first, when changing the port interface from 4x25G/20G to 2x25G/10G, the partner port will be undefined (displayed as not configured or showing a gray port icon)

To delete a port, the partner ports must be deleted first. A primary port cannot be deleted if one or more partner ports are defined.

Selecting multiple ports for configuration in the GUI will allow changing their interfaces, but the server will reject invalid configurations.

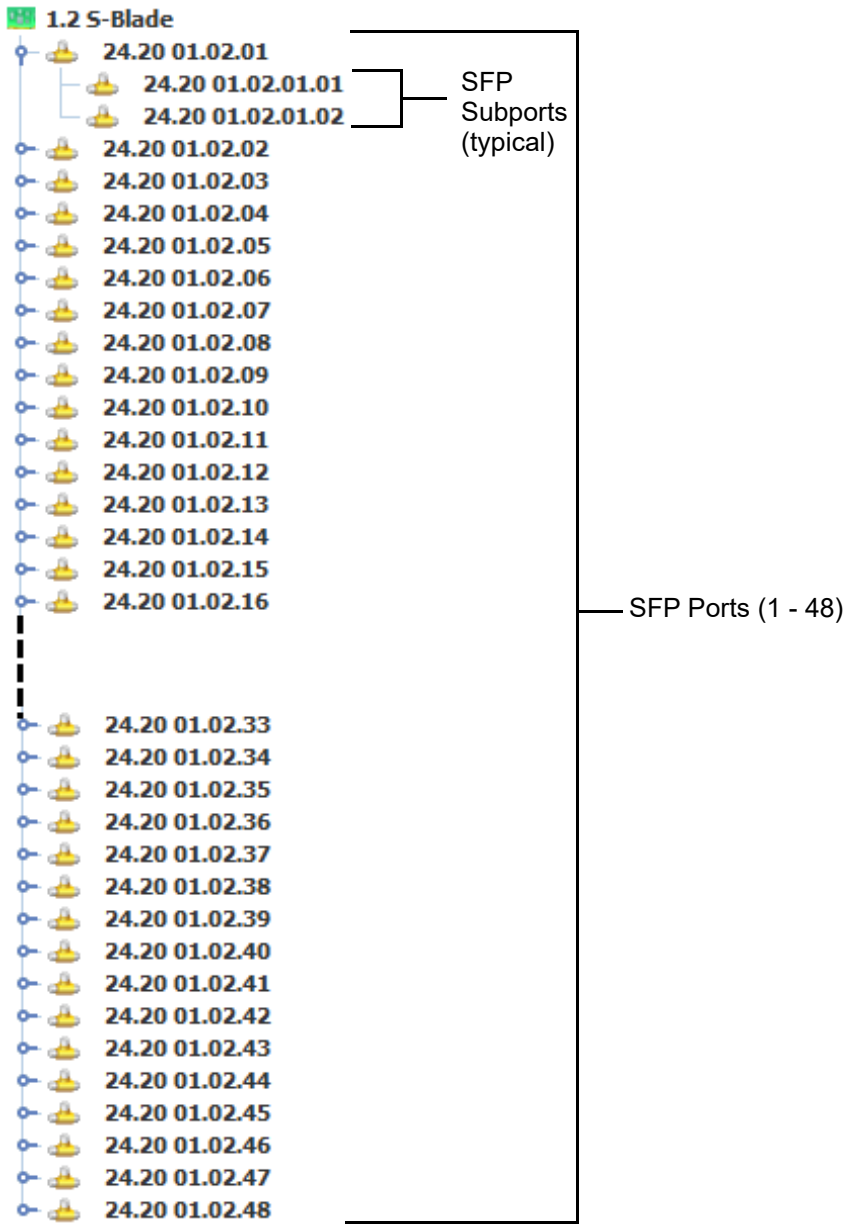
S-Blade Graphic

Installed S-Blades are displayed by right clicking on a switch and selecting **Switch Graphic**, selecting **Connect > Switch Graphic**, or from the toolbar, selecting the **Open Switch Graphic** icon, or from the keyboard **Alt+F9**. Moving the pointer's cursor over the front switch graphic displays information on the switch name, blade number, port information / status). Refer to Blade Port Legends on page 3-52 for descriptions of the different port states (colors / images) displayed on the blade.



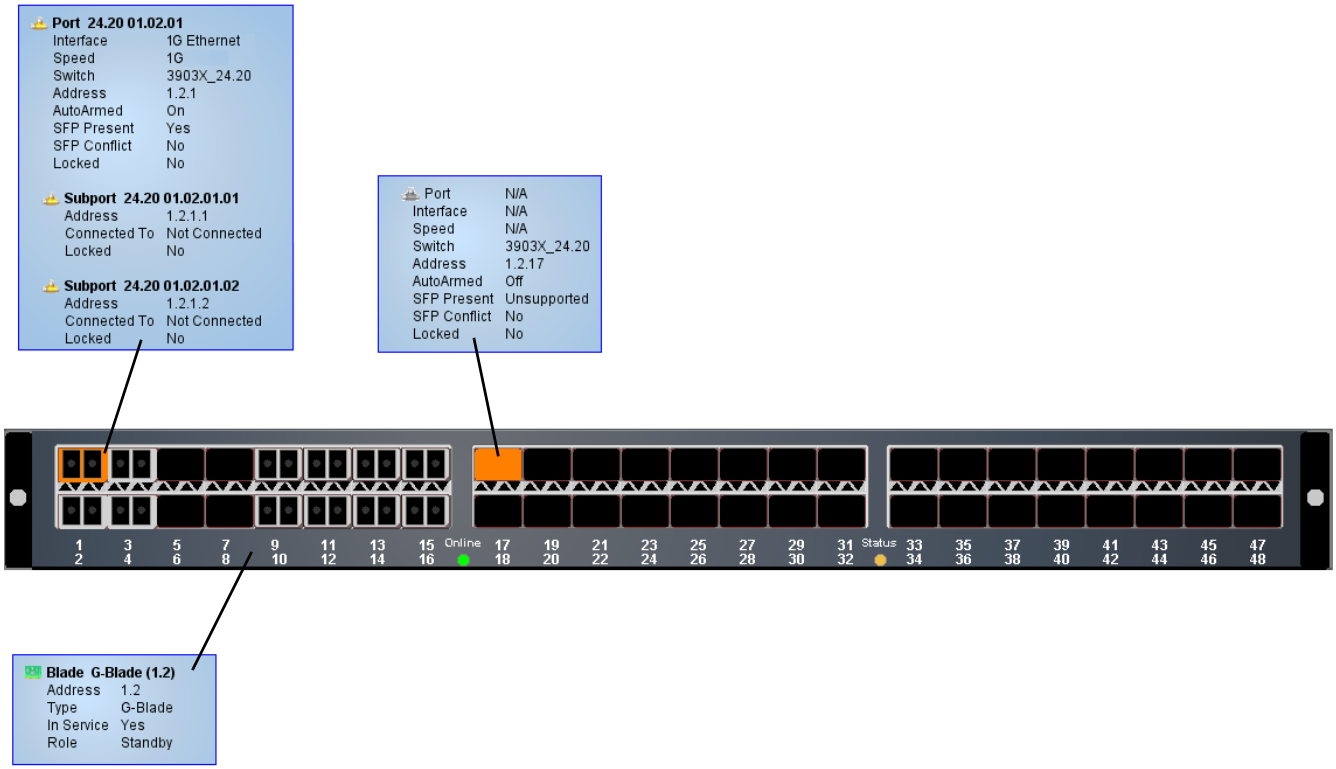
S-Blade System Tree

For the S-Blade, Ports 1 through 48 are displayed as SFP ports.



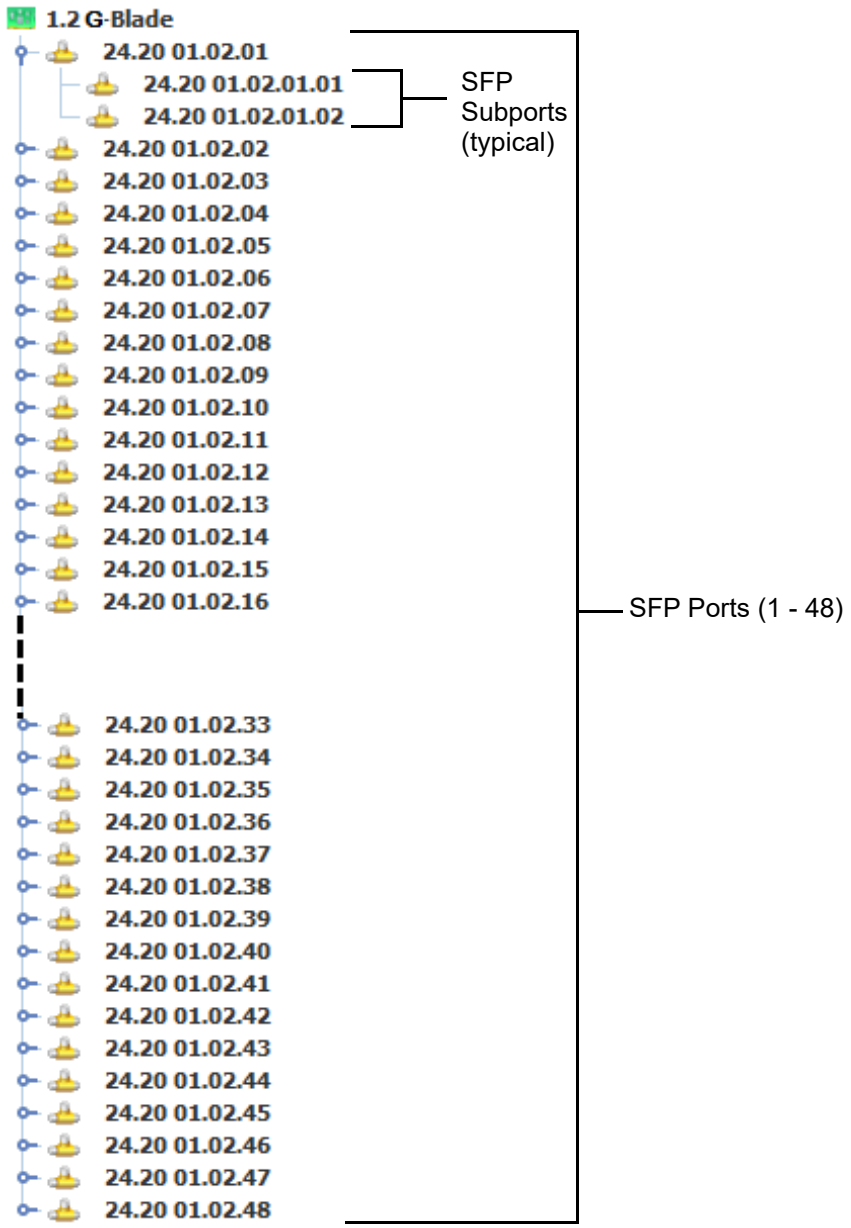
G-Blade Graphic

Installed G-Blades are displayed by right clicking on a switch and selecting **Switch Graphic**, selecting **Connect > Switch Graphic**, or from the toolbar, selecting the **Open Switch Graphic** icon, or from the keyboard **Alt+F9**. Moving the pointer's cursor over the front switch graphic displays information on the switch name, blade number, port information / status). Refer to Blade Port Legends on page 3-52 for descriptions of the different port states (colors / images) displayed on the blade.



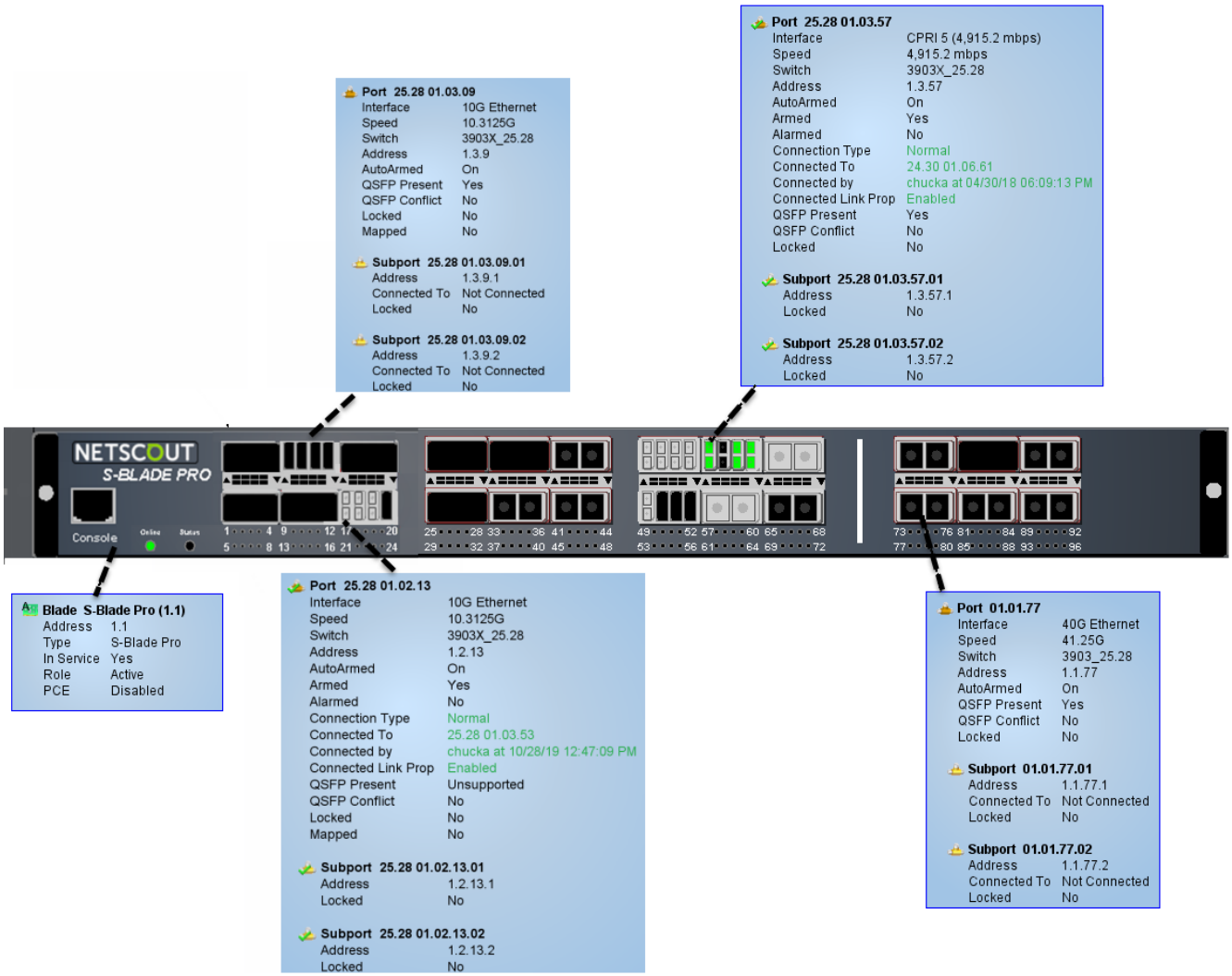
G-Blade System Tree

For the G-Blade, Ports 1 through 48 are displayed as SFP ports.



S-Blade Pro Graphic

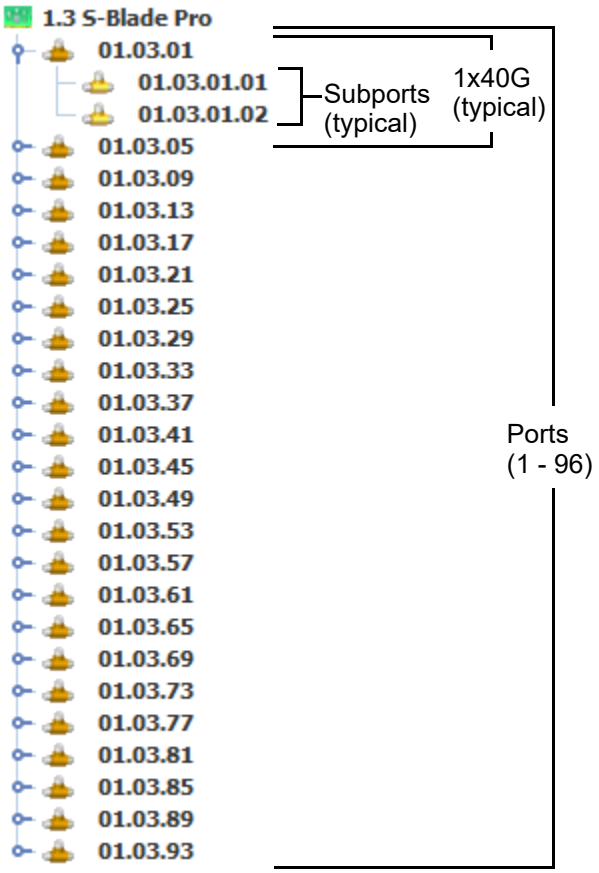
Installed S-Blade Pro blades are displayed by right clicking on a switch and selecting **Switch Graphic**, selecting **Connect > Switch Graphic**, or from the toolbar, selecting the **Open Switch Graphic** icon, or from the keyboard **Alt+F9**. Moving the pointer's cursor over the front switch graphic displays information on the switch name, blade number, port information / status). Refer to Blade Port Legends on page 3-52 for descriptions of the different port states (colors / images) displayed on the blade.



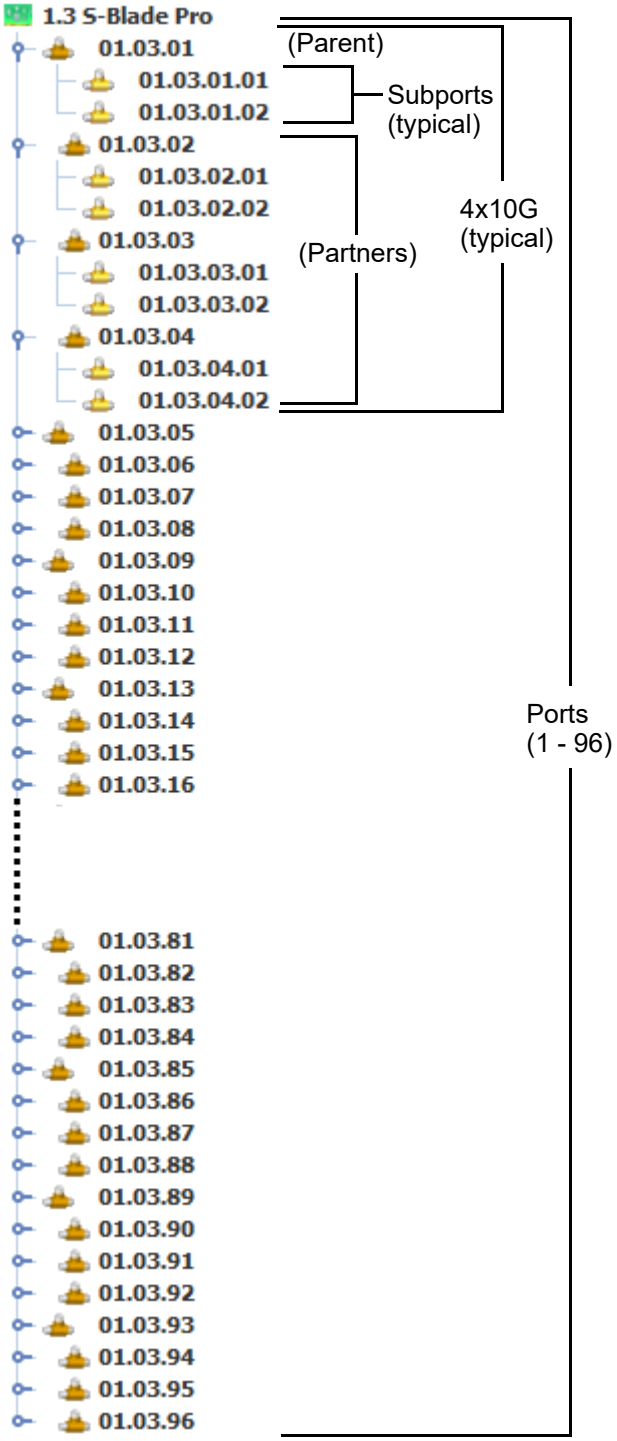
S-Blade Pro System Tree

For the S-Blade Pro, QSFP ports 1 through 96 are displayed as 4x40Gb, 4x1/10Gb and QSFP to 4xSFP Coupler ports. Refer to S-Blade, G-Blade, S-Blade Pro, S-Blade 64, T-Blade, HS-3200, and HS-6400 Port Icons on page 3-51 for icon types used in the system tree.

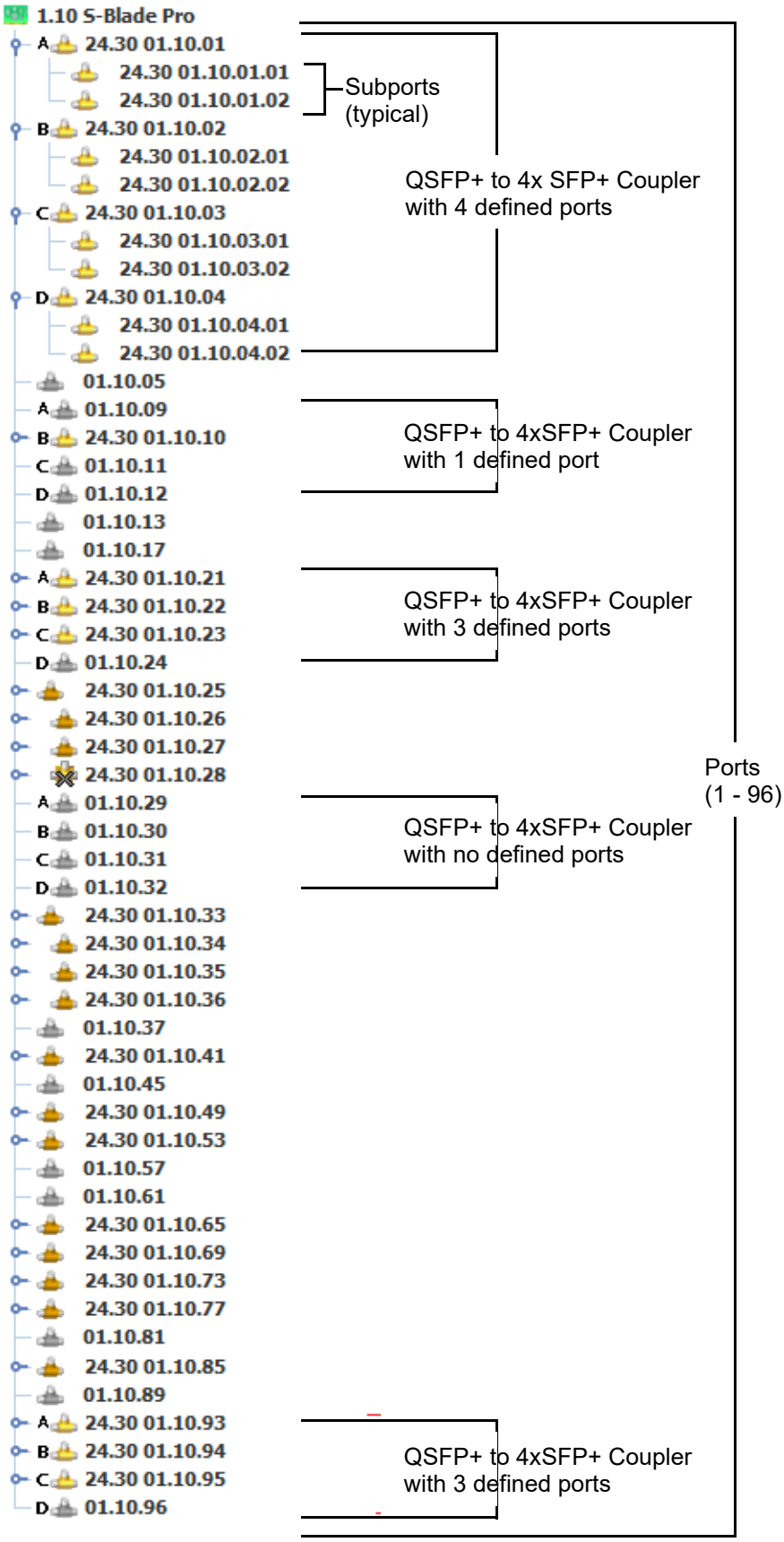
40 GbE Ports



1/10 GbE Ports

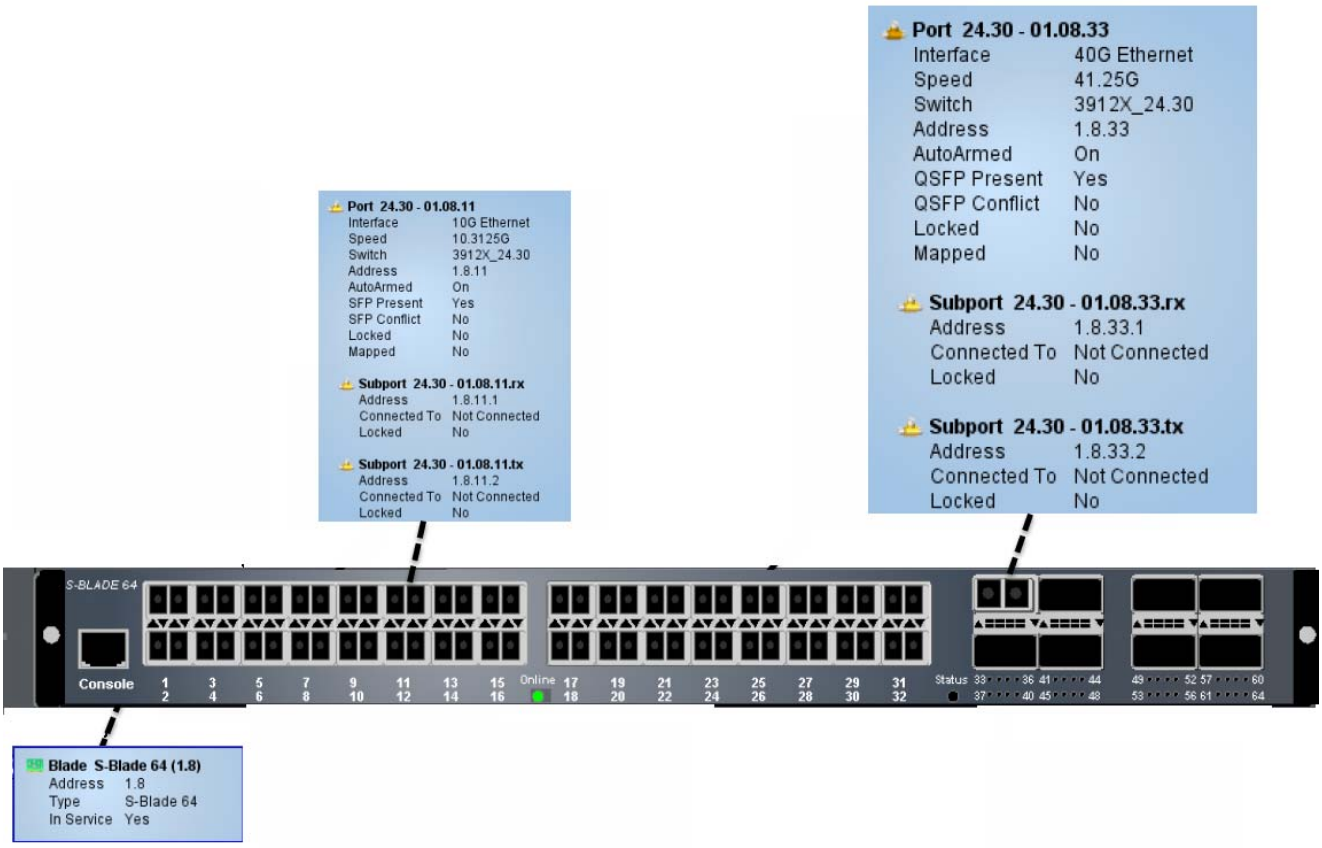


QSFP+ to 4xSFP+ Coupler



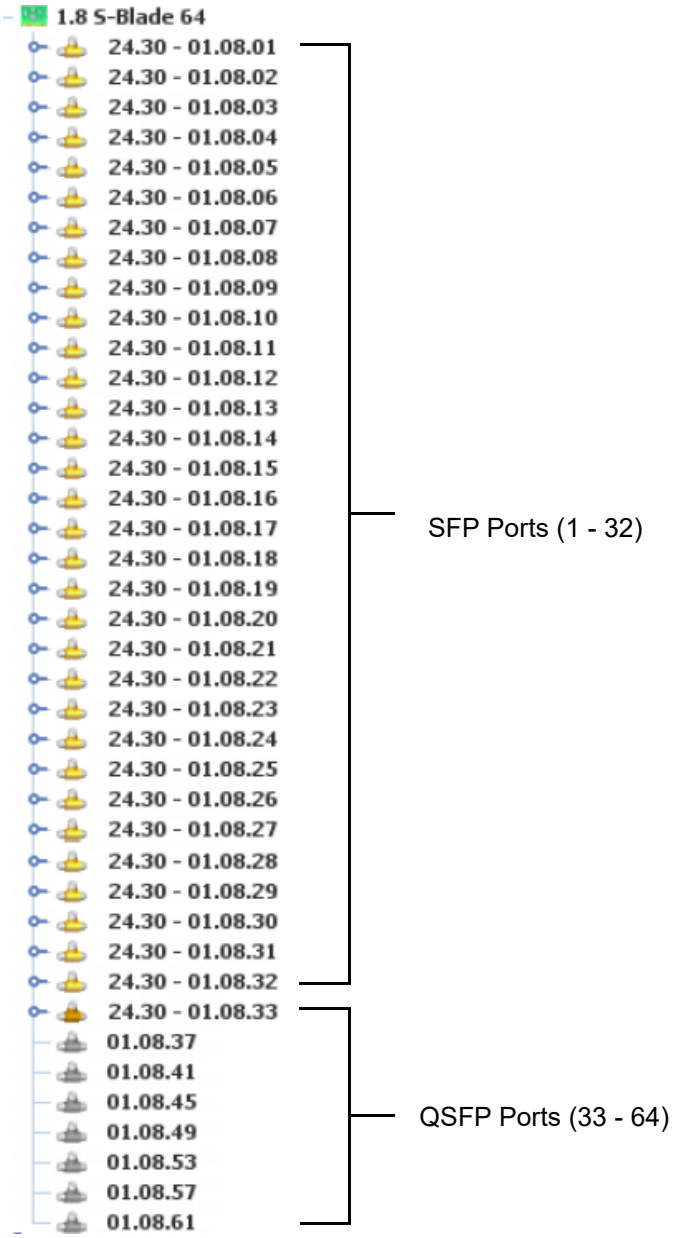
S-Blade 64 Graphic

Installed S-Blade 64 blades are displayed by right clicking on a switch and selecting **Switch Graphic**, selecting **Connect > Switch Graphic**, or from the toolbar, selecting the **Open Switch Graphic** icon, or from the keyboard **Alt+F9**. Moving the pointer's cursor over the front switch graphic displays information on the switch name, blade number, port information / status). Refer to Blade Port Legends on page 3-52 for descriptions of the different port states (colors / images) displayed on the blade.



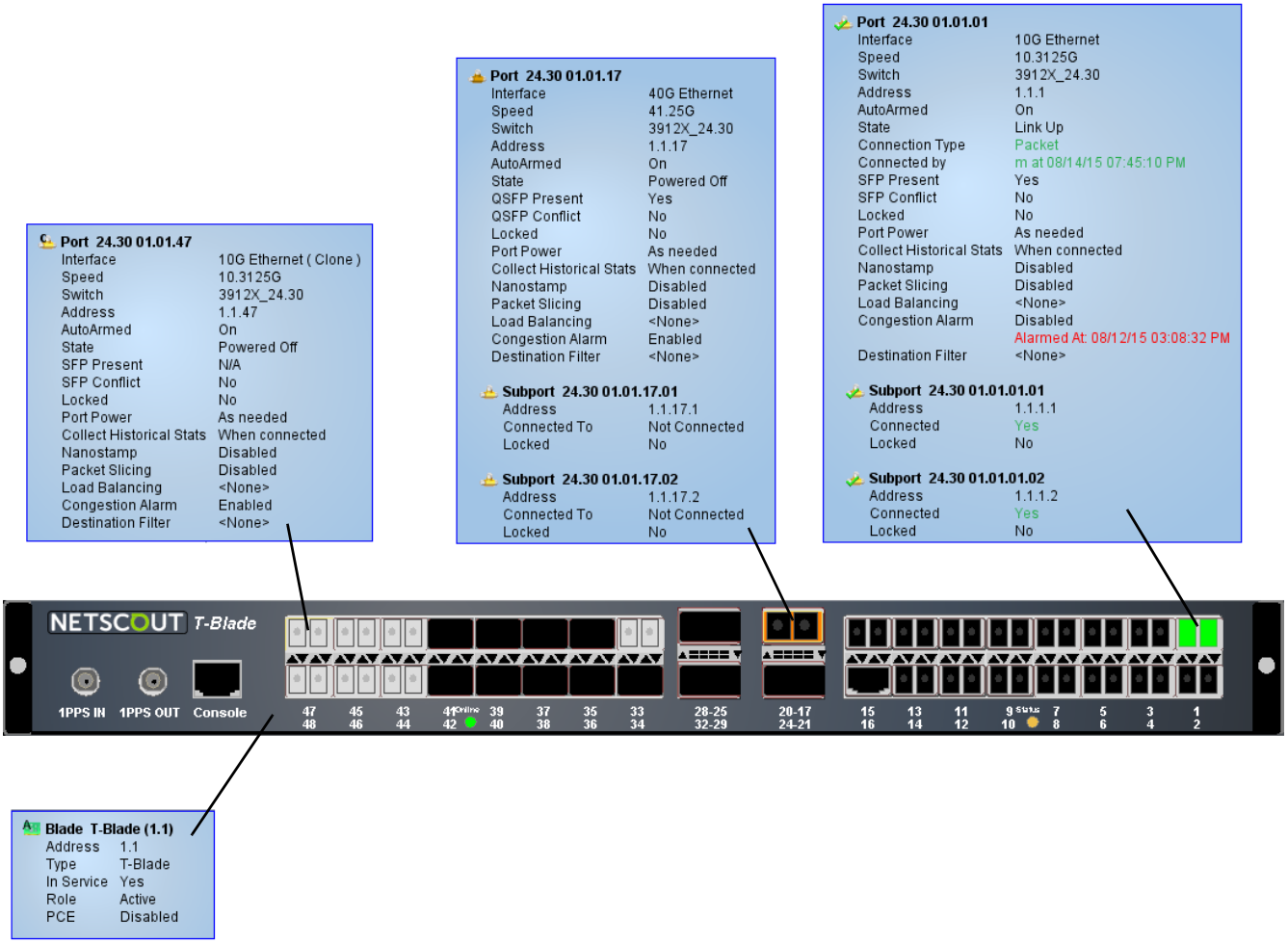
S-Blade 64 System Tree

For the S-Blade 64, QSFP ports 17 through 32 are displayed as 4x10Gb ports. Refer to S-Blade, G-Blade, S-Blade Pro, S-Blade 64, T-Blade, HS-3200, and HS-6400 Port Icons on page 3-51 for icon types used in the system tree.



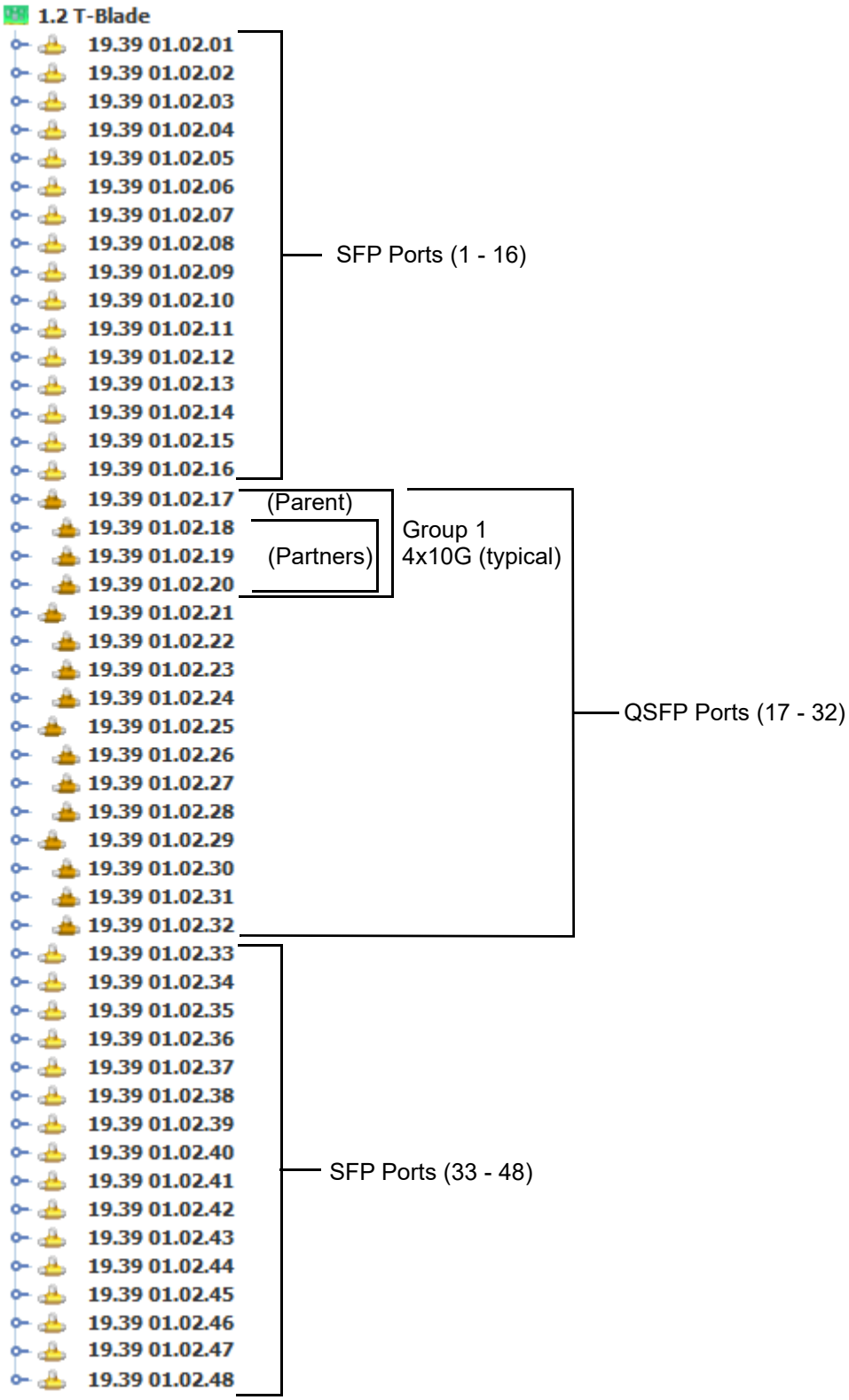
T-Blade Graphic

Installed T-Blades are displayed by right clicking on a switch and selecting **Switch Graphic**, selecting **Connect > Switch Graphic**, or from the toolbar, selecting the **Open Switch Graphic** icon, or from the keyboard **Alt+F9**. Moving the pointer's cursor over the front switch graphic displays information on the switch name, blade number, port information / status). Refer to Blade Port Legends on page 3-52 for descriptions of the different port states (colors / images) displayed on the blade.



T-Blade System Tree

For the T-Blade, QSFP ports 17 through 32 are displayed as 4x10Gb ports. Refer to S-Blade, G-Blade, S-Blade Pro, S-Blade 64, T-Blade, HS-3200, and HS-6400 Port Icons on page 3-51 for icon types used in the system tree.



S-Blade, G-Blade, S-Blade Pro, S-Blade 64, T-Blade, HS-3200, and HS-6400 Port Icons

To differentiate between SFP, QFSP, and QSFP28 ports in the S-Blade, G-Blade, S-Blade Pro, S-Blade 64, T-Blades, HS-3200, and the HS-6400, the following icons are used in the system tree:

 —— SFP Port (S-Blade, G-Blade, T-Blade,
S-Blade Pro with QSFP+ to 4xSFP+ Coupler, S-Blade 64)

 —— QSFP Port (S-Blade Pro, S-Blade 64, T-Blade)

 —— QSFP / QSFP28 Ports (HS-3200, HS-6400)

Blade Port Legends

The following lists the different port states (colors / images) displayed on the Switch Graphic screen.

Transceiver Type	Port Image	Description
GigE - CU (Copper)		Defined / No Transceiver Present (Gray Fill)
		Defined / Transceiver Present (Black Fill)
		Alarmed (Red Fill)
		Conflict (Yellow Fill
		Connected (Green Fill)
		xSL (Blue Fill)
1/10G Fiber / 10G DAC		Defined / No Transceiver Present (Black Outline)
		Alarmed / No Transceiver Present (Red Outline)
		Conflict / No Transceiver Present (Yellow Outline)
		Connected / No Transceiver Present (Green Outline)
		xSL / No Transceiver Present (Blue Outline)
		Defined / Transceiver Present (Black Fill)
		Alarmed / Transceiver Present (Red Fill)
		Simplex (Mirror or Test) / Transceiver Present / Alarmed / Powered On and Linked-up (Half Gray / Half Red / Green Dot)
		Conflict / Transceiver Present (Yellow Fill)
		Connected / Transceiver Present (Green Fill)
		xSL / Transceiver Present (Blue Fill)
		Simplex (Mirror or Test) / Transceiver Present / Powered On and Linked-up (Half Gray / Half Black / Green Dot)
		Powered On and Linked-up (Green Dots)

Transceiver Type	Port Image	Description
100G / 40G Fiber / DAC		Defined / No Transceiver Present (Black Outline)
		Alarmed / No Transceiver Present (Red Outline)
		Conflict / No Transceiver Present (Yellow Outline)
		Connected / No Transceiver Present (Green Outline)
		xSL / No Transceiver Present (Blue Outline)
		No Transceiver Present (Green Dots)
		Defined / Transceiver Present (Black Fill)
		Alarmed / Transceiver Present (Red Fill)
		Conflict / Transceiver Present (Yellow Fill)
		Connected / Transceiver Present (Green Fill)
		xSL / Transceiver Present (Blue Fill)
Optical: • OS-16 Switch		Defined / Not Connected (Black Fill)
		Alarmed (Red Fill)
		Connected (Green Fill)
Optical: • OS-96 Switch • OS-192 Switch		Defined / Not Connected (Black Fill)
		Alarmed (Red Fill)
		Connected (Green Fill)
		xSL (Blue Fill)

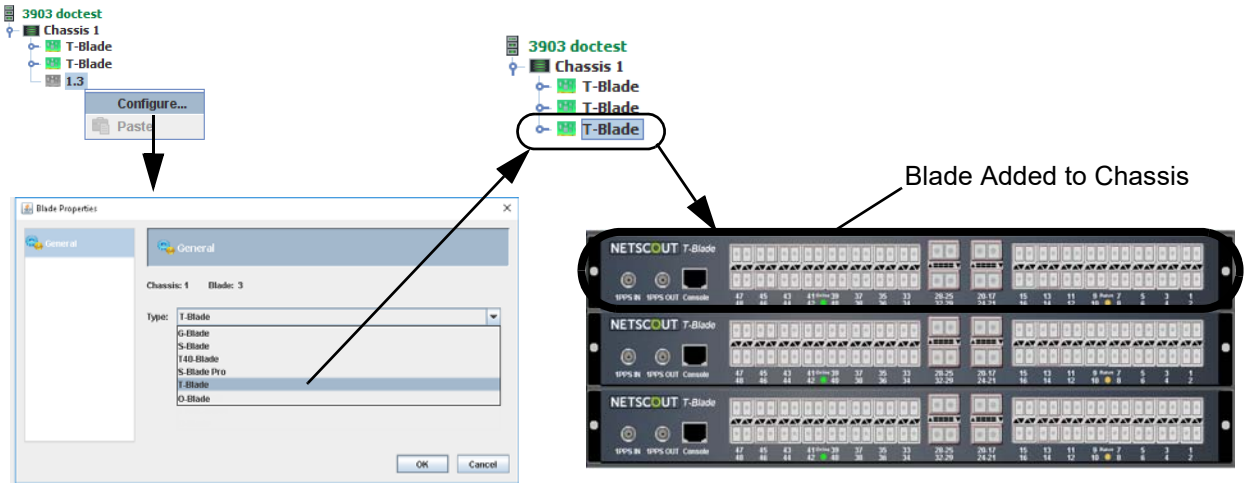
Transceiver Type	Port Image	Description
50G / 40G / 25G Breakout Cable / 100G Fiber QSFP		Defined / No Transceiver Present (Black Outline)
		Alarmed / No Transceiver Present (Red Outline)
		Conflict / No Transceiver Present (Yellow Outline)
		Connected / No Transceiver Present (Green Outline)
		xSL / No Transceiver Present (Blue Outline)
		No Transceiver Present (Green Dots)
		Defined / Transceiver Present (Black Fill)
		Alarmed / Transceiver Present (Red Fill)
		Conflict / Transceiver Present (Yellow Fill)
		Connected / Transceiver Present (Green Fill)
		xSL / Transceiver Present (Blue Fill)
		xSL / Transceiver Present / Powered On and Linked-up (Blue Fill with Green Dots)

Transceiver Type	Port Image	Description
100Base-FX/LX		Defined / No Transceiver Present (Black Outline)
		Alarmed / No Transceiver Present (Red Outline)
		Conflict / No Transceiver Present (Yellow Outline)
		Connected / No Transceiver Present (Green Outline)
		xSL / No Transceiver Present (Blue Outline)
		Defined / Transceiver Present (Black Fill)
		Alarmed / Transceiver Present (Red Fill)
		Simplex (Mirror or Test) / Transceiver Present / Alarmed / Powered On and Linked-up (Half Gray / Half Red / Green Dot)
		Conflict / Transceiver Present (Yellow Fill)
		Connected / Transceiver Present (Green Fill)
		xSL / Transceiver Present (Blue Fill)
		Simplex (Mirror or Test) / Transceiver Present / Powered On and Linked-up (Half Gray / Half Black / Green Dot)
		Powered On and Linked-up (Green Dots)
QSFP+ to 4xSFP+ Coupler (copper/optical)		Coupler inserted and SFP coupler ports are not defined
		SFP coupler port defined, but not present
		SFP coupler port defined, present and not connected
		SFP coupler port defined, present, connected and link is up (link up for copper only)
		SFP coupler port defined, present, connected and alarmed

Adding a Blade to a Chassis

Note: Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) must be disabled to allow manual configuration/addition of a blade via the TestStream Management GUI.

1. From the Switch > Chassis > Blade level, select an undefined blade slot, right click, and select **Configure**. The Blade Properties screen displays.
2. From the Type: drop down list, select the blade type (e.g., T-Blade) for the slot location.
3. Click **OK**. The new blade now displays in the listing and a representation of the blade is shown on the chassis graphic in the slot selected.
4. Continue populating the other chassis slots with the required blades as necessary.



Blade Type Mismatch

When a blade is replaced or a blade type for a slot has been pre-configured and a blade is inserted, if the inserted blade type does not match the configured blade type, a blade type mismatch alarm will be generated. Replace the blade with one matching the expected blade type or update the current blade type.

Note: Changing the configured blade type will delete all the configuration present for that blade.

Removing a Blade from a Chassis

To remove a blade from the switch, right-click on the blade from the system tree and select **Delete** on the drop-down menu.

Note: Prior to selecting Delete, verify that the auto-discrepancy detection feature for the switch is off (not selected) and the blade is physically removed from the switch. If the blade is still present in the switch, an error message displays:

Configuring Blade Ports

G-Blades

1 From the Switch > Chassis > Blade > Port level, select a port, right click and select **Configure**. The Port Configuration Wizard displays.

Screen 1

2 Enter the name of the new port in the **Name:** field.

Optionally, enter designations for SFP / QSFP Subport 1 (e.g., tx) and Subport 2 (e.g., rx). Click **Next**.

Note: If Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) is not disabled (to allow manual configuration/addition of a blade via the nGenius TestStream Management GUI), a port name is automatically created in the Name field with the Subport Suffix fields filled in. These fields can be altered as required during port configuration.

---

3 Click **Next**.

Screen 2

4 Select the Interface type (Gig-E, Gig-E CU or 100M Fib) from the drop down menu.

5 Optionally, set the Link Propagation delay to either Default (pre-selected) or to Disabled or Enabled. This setting defines the detection of Loss of Signal (LOS) from one end of a connection to the other end when the transmitter is turned off.

6 Select the Port Type required (Normal, Test, xSL, or Mirror; refer to Port Types on page 3-85).

If Interface Type **GIG-E** is selected, an Auto-Negotiation option selection block displays. Selecting **Auto-Negotiation** enables auto-negotiation on the port.

If Port Type **Test** is selected, a Force Test Port Link Up option selection block displays. Select **Force Test Port Link Up** to enable the test port to come up and stay up even when there is no signal being received from the attached device; also prevents any Link Down events from being reported when the attached device goes down.

7 Click **Next**.

Screen 3

8 Accept the AutoArm / Alarm default settings. To activate trigger alarms, select the **Receive Loss of Signal** checkbox and select from the dropdown listing the required LOS (1, 2, 5, 10, or 30 seconds) time (refer to Receive Loss of Signal on page 3-101).

9 Optionally, select the checkbox for Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power).

10 Click **Next**.

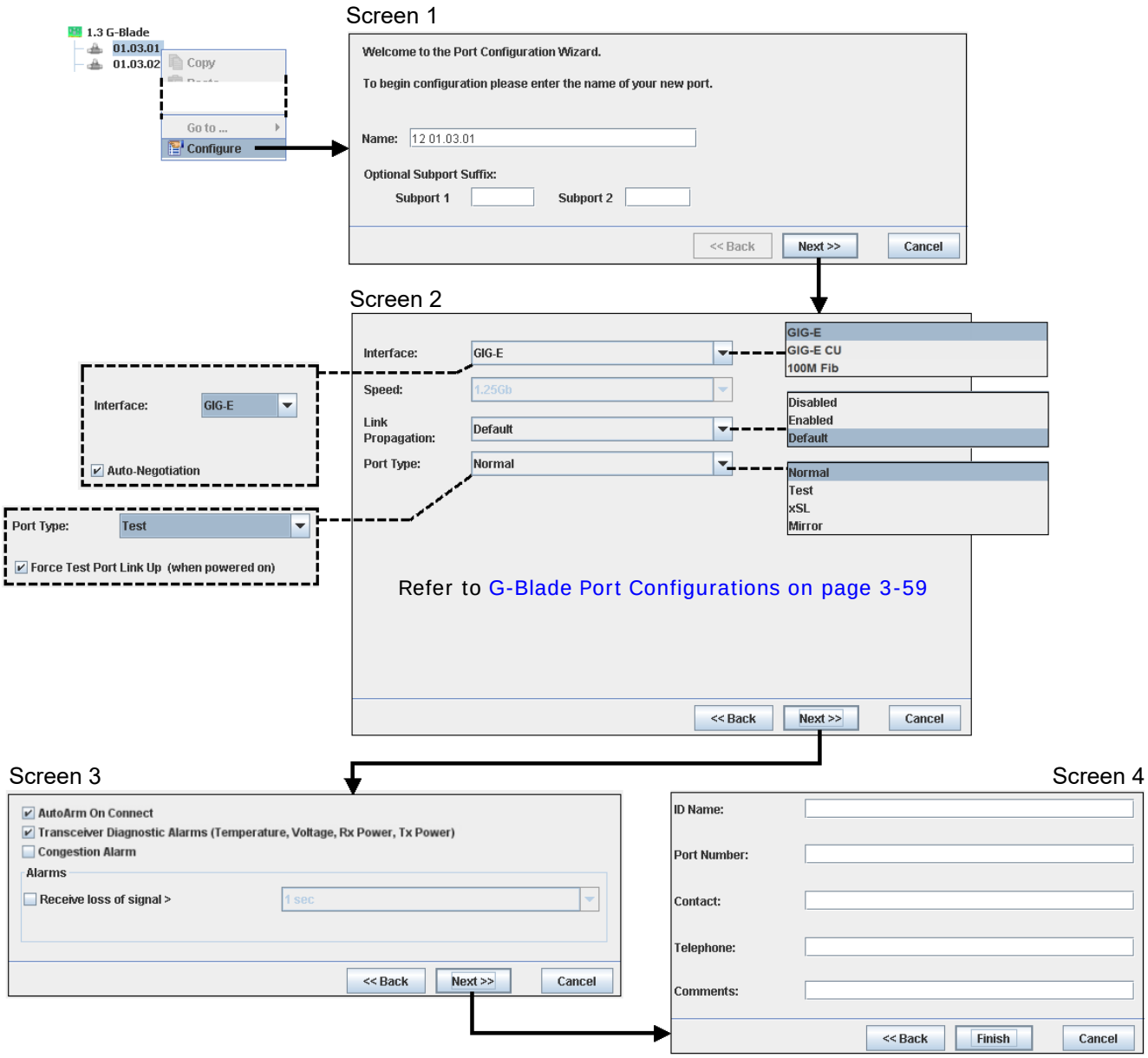
Screen 4

11 Make any additions to the information screen as necessary. Click **Finish**. The configured port now displays on the port level.

12 Continue configuring additional ports on the blade as required.

Note: To configure multiple ports with the same configuration settings, refer to Configuring Multiple Ports on a Blade on page 3-100.

Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.


Screen 1
1.3 G-Blade
01.03.01
01.03.02
Copy
Go to ...
Configure
Welcome to the Port Configuration Wizard.
To begin configuration please enter the name of your new port.
Name: 12 01.03.01
Optional Subport Suffix:
Subport 1
Subport 2
<< Back
Next >>
Cancel
Screen 2
Interface: GIG-E
Speed: 1.25Gb
Link Propagation: Default
Port Type: Normal
GIG-E
GIG-E CU
100M Fib
Disabled
Enabled
Default
Normal
Test
xSL
Mirror
Refer to G-Blade Port Configurations on page 3-59
Interface: GIG-E
Auto-Negotiation
Port Type: Test
Force Test Port Link Up (when powered on)
Screen 3
AutoArm On Connect
Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power)
Congestion Alarm
Alarms
Receive loss of signal >
1 sec
Screen 4
ID Name:
Port Number:
Contact:
Telephone:
Comments:
Finish

G-Blade Port Configurations

The following table shows the allowed port configurations / options for each interface / port type.

Interface	Port Type	AutoArm	Transceiver	Receive LOS
Gig-E	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
Gig-E CU	Normal	X (default)	X (default)	
	Test (Force Test Link selected)	X (default)	X (default)	
	Test (Force Test Link not selected)	X (default)	X (default)	
	xSL	X (default)	X (default)	
	Mirror		X (default)	
100M Fib	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
		X = option available X (default) = option available and selected by default		

S-Blades

1 From the Switch > Chassis > Blade > Port level, select a port, right click and select **Configure**. The Port Configuration Wizard displays.

Screen 1

2 Enter the name of the new port in the **Name:** field.

Optionally, enter designations for SFP / QSFP Subport 1 (e.g., tx) and Subport 2 (e.g., rx). Click **Next**.

Note: If Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) is not disabled (to allow manual configuration/addition of a blade via the nGenius TestStream Management GUI), a port name is automatically created in the Name field with the Subport Suffix fields filled in. These fields can be altered as required during port configuration.

---

3 Click **Next**.

Screen 2

4 Select the Interface type from the drop down menu.

5 Optionally, set the Link Propagation delay to either Default (pre-selected) or to Disabled or Enabled. This setting defines the detection of Loss of Signal (LOS) from one end of a connection to the other end when the transmitter is turned off.

6 Select the Port Type required (Normal, Test, xSL, or Mirror; refer to Port Types on page 3-85).

If Port Type **Test** is selected, a Force Test Port Link Up option selection block displays. Select **Force Test Port Link Up** to enable the test port to come up and stay up even when there is no signal being received from the attached device; also prevents any Link Down events from being reported when the attached device goes down.

7 Click **Next**.

Screen 3

8 Accept the AutoArm / Alarm default settings. To activate trigger alarms, select the **Receive Loss of Signal** checkbox and select from the dropdown listing the required LOS (1, 2, 5, 10, or 30 seconds) time (refer to Receive Loss of Signal on page 3-101).

9 Optionally, select the checkbox for Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power).

10 Click **Next**.

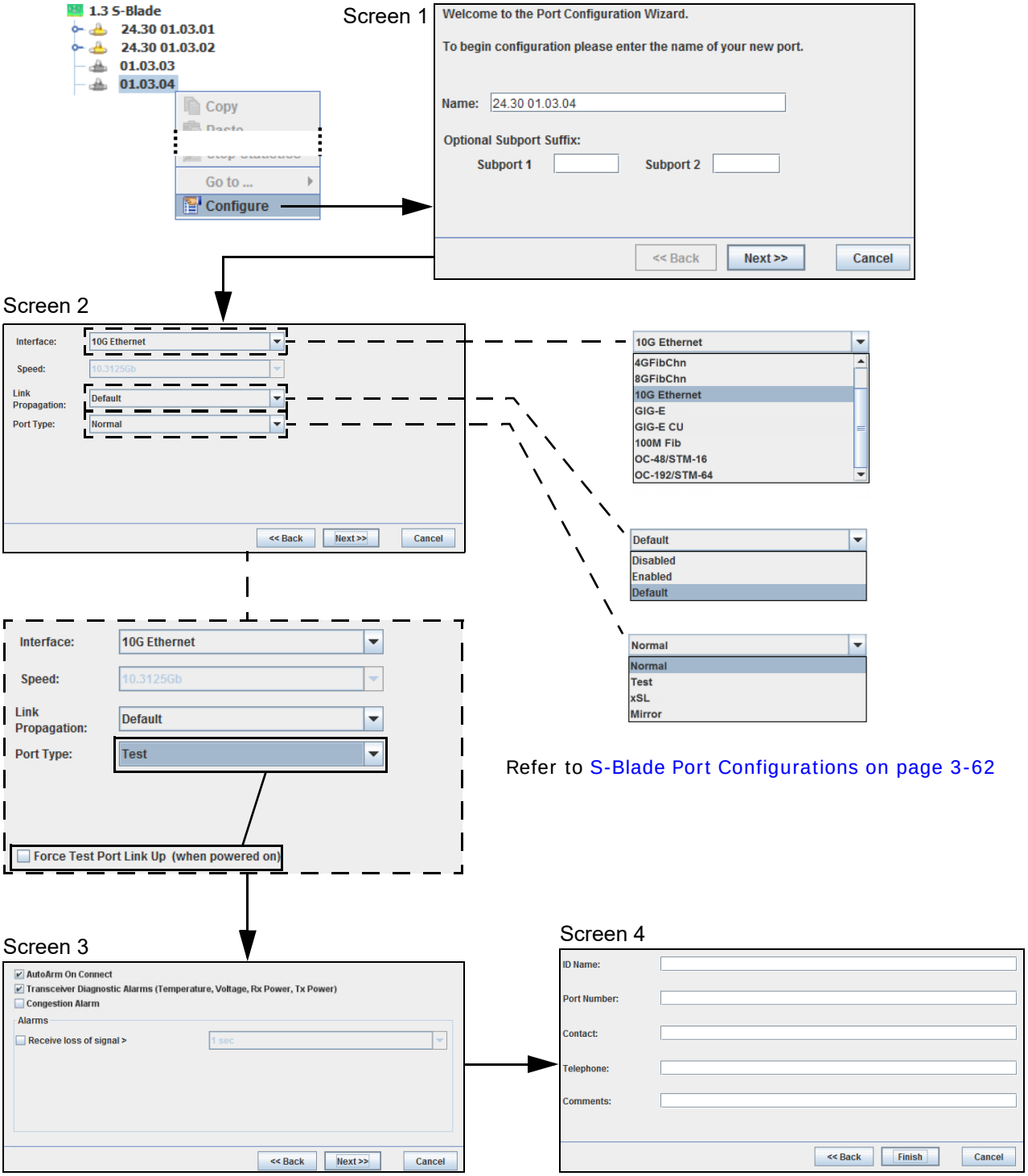
Screen 4

11 Make any additions to the information screen as necessary. Click **Finish**. The configured port now displays on the port level.

12 Continue configuring additional ports on the blade as required.

Note: To configure multiple ports with the same configuration settings, refer to Configuring Multiple Ports on a Blade on page 3-100.

Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.



Refer to S-Blade Port Configurations on page 3-62

S-Blade Port Configurations

The following table shows the allowed port configurations / options for each interface / port type.

Interface	Port Type	AutoArm	Transceiver	Receive LOS
1/2/4/8 FibChn	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
10G Ethernet	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
Gig-E	Normal		X (default)	X
	Test (Force Test Link selected)		X (default)	X
	Test (Force Test Link not selected)		X (default)	X
	xSL		X (default)	X
	Mirror		X (default)	X
Gig-E CU	Normal	X (default)	X (default)	
	Test (Force Test Link selected)	X (default)	X (default)	
	Test (Force Test Link not selected)	X (default)	X (default)	
	xSL	X (default)	X (default)	
	Mirror		X (default)	
100M Fib	Normal		X (default)	X
	Test (Force Test Link selected)		X (default)	X
	Test (Force Test Link not selected)		X (default)	X
	xSL		X (default)	X
	Mirror		X (default)	X
OC-3/STM-1	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
OC-12/STM-4	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X

Interface	Port Type	AutoArm	Transceiver	Receive LOS
OC-48/STM-16	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
OC-192/STM-64	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
		X = option available X (default) = option available and selected by default		

S-Blade Pro

1 From the Switch > Chassis > Blade > Port level, select a port, right click and select **Configure**. The Port Configuration Wizard displays.

Screen 1

2 Enter the name of the new port in the **Name:** field.

Optionally, enter designations for QSFP Subport 1 (e.g., tx) and Subport 2 (e.g., rx). Click **Next**.

Note: If Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) is not disabled (to allow manual configuration/addition of a blade via the nGenius TestStream Management GUI), a port name is automatically created in the Name field with the Subport Suffix fields filled in. These fields can be altered as required during port configuration.

Screen 2

3 Select the QSFP type from the drop down menu.
- Standard
- QSFP to 4xSFP Coupler

4 Select the Interface type from the drop down menu.
QSFP Layer-1 Ports (ports 1 - 72):
- 1/10/40G Ethernet
- 2/4/8G Fiber Channel
- CPRI 9/CPRI 8/CPRI 7/CPRI 6/CPRI 5/CPRI 4/CPRI 3/CPRI 2/CPRI 1 (refer to CPRI Interface on page 3-87)
- 10G CU (requires a QSFP+ to SFP+ adapter)
- 3G/6G/12G SAS

- or -

QSFP Smart Ports (ports 73 - 96):
- 10/40G Ethernet

5 Optionally, set the Link Propagation delay to either Default (pre-selected) or to Disabled or Enabled. This setting defines the detection of Loss of Signal (LOS) from one end of a connection to the other end when the transmitter is turned off.

6 Select the Port Type required (Normal, Test, xSL, or Mirror; refer to Port Types on page 3-85).

If Interface Type **GIG-E** is selected, an Auto-Negotiation option selection block displays. Selecting **Auto-Negotiation** enables auto-negotiation on the port.

If Port Type **Test** is selected, a Force Test Port Link Up option selection block displays. Select **Force Test Port Link Up** to enable the test port to come up and stay up even when there is no signal being received from the attached device; also prevents any Link Down events from being reported when the attached device goes down.

7 Click **Next**.

Screen 3

8 Accept the AutoArm / Alarm default settings. To activate trigger alarms, select the **Receive Loss of Signal** checkbox and select from the dropdown listing the required LOS (1, 2, 5, 10, or 30 seconds) time (refer to Receive Loss of Signal on page 3-101).

Optionally, select the checkbox for Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power).

9 Click **Next**.

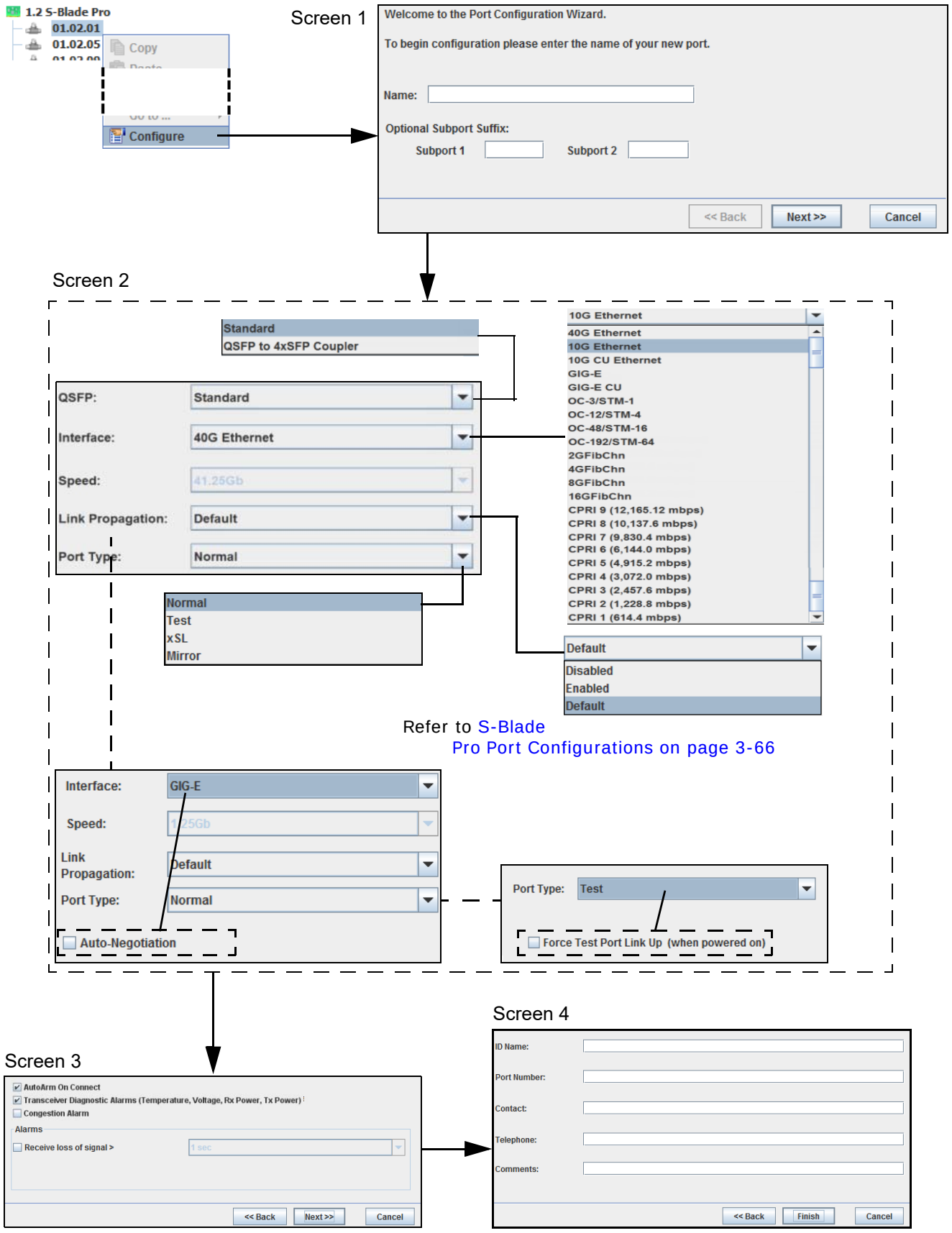
Screen 4

10 Make any additions to the information screen as necessary. Click **Finish**. The configured port now displays on the port level.

11 Continue configuring additional ports on the blade as required.

Note: To configure multiple ports with the same configuration settings, refer to Configuring Multiple Ports on a Blade on page 3-100.

Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.


1.2 S-Blade Pro
01.02.01
01.02.05
Copy
Configure
Screen 1
Welcome to the Port Configuration Wizard.
To begin configuration please enter the name of your new port.
Name:
Optional Subport Suffix:
Subport 1
Subport 2
<< Back
Next >>
Cancel
Screen 2
Standard
QSFP to 4xSFP Coupler
QSFP:
Standard
Interface:
40G Ethernet
Speed:
41.25Gb
Link Propagation:
Default
Port Type:
Normal
Normal
Test
xSL
Mirror
10G Ethernet
40G Ethernet
10G Ethernet
10G CU Ethernet
GIG-E
GIG-E CU
OC-3/STM-1
OC-12/STM-4
OC-48/STM-16
OC-192/STM-64
2GFibChn
4GFibChn
8GFibChn
16GFibChn
CPRI 9 (12,165.12 mbps)
CPRI 8 (10,137.6 mbps)
CPRI 7 (9,830.4 mbps)
CPRI 6 (6,144.0 mbps)
CPRI 5 (4,915.2 mbps)
CPRI 4 (3,072.0 mbps)
CPRI 3 (2,457.6 mbps)
CPRI 2 (1,228.8 mbps)
CPRI 1 (614.4 mbps)
Default
Disabled
Enabled
Default
Refer to S-Blade
Pro Port Configurations on page 3-66
Interface:
GIG-E
Speed:
1.25Gb
Link Propagation:
Default
Port Type:
Normal
Auto-Negotiation
Port Type:
Test
Force Test Port Link Up (when powered on)
Screen 3
AutoArm On Connect
Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power)
Congestion Alarm
Alarms
Receive loss of signal >
1 sec
<< Back
Next >>
Cancel
Screen 4
ID Name:
Port Number:
Contact:
Telephone:
Comments:
<< Back
Finish
Cancel

S-Blade Pro Port Configurations

The following table shows the allowed port configurations / options for each interface / port type.

Interface	Port Type	AutoArm	Transceiver	Receive LOS
40G Ethernet (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
40G Ethernet (ports 73 - 96)	Normal		X (default)	X
	Test (Force Test Link selected)		X (default)	X
	Test (Force Test Link not selected)		X (default)	X
	xSL		X (default)	X
	Mirror		X (default)	X
10G Ethernet 10G CU Ethernet (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
10G Ethernet 10G CU Ethernet (ports 73 - 96)	Normal		X (default)	X
	Test (Force Test Link selected)		X (default)	X
	Test (Force Test Link not selected)		X (default)	X
	xSL		X (default)	X
	Mirror		X (default)	X
2G/4G/8G/16G FibChn (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
Gig-E (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
CPRI9 - CPRI1 (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X

Interface	Port Type	AutoArm	Transceiver	Receive LOS
OC-3/12/48/192 (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
QFSP+to 4xSFP+ Coupler	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
3G/6G/12G SAS (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
OTU1/OTU2/OTU2E (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
		X = option available X (default) = option available and selected by default		

S-Blade Pro (iSL Ports)

iSL ports are only available on S-Blade Pros installed in 3903 systems configured with SFM Pro External Fabric mode enabled (refer to SFM Pro External Fabric Mode on page 3-93).

1 From the Switch > Chassis > Blade > Port level, select a port, right click and select **Configure**. The Port Configuration Wizard displays.

Screen 1

2 Enter the name of the new port in the **Name:** field.

Optionally, enter designations for QSFP Subport 1 (e.g., tx) and Subport 2 (e.g., rx). Click **Next**.

Note: If Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) is not disabled (to allow manual configuration/addition of a blade via the nGenius TestStream Management GUI), a port name is automatically created in the Name field with the Subport Suffix fields filled in. These fields can be altered as required during port configuration.

Screen 2

3 Select the QSFP type from the drop down menu.
- Standard
- QSFP to 4xSFP Coupler

4 Select the Interface type from the drop down menu.
QSFP Layer-1 Ports (ports 1 - 72):
- 1/10G Ethernet (default is 10G)

5 Optionally, set the Link Propagation delay to either Default (pre-selected) or to Disabled or Enabled. This setting defines the detection of Loss of Signal (LOS) from one end of a connection to the other end when the transmitter is turned off.

6 Port Type is pre-selected to **iSL**.

If Interface Type **GIG-E** is selected, an Auto-Negotiation option selection block displays. Selecting **Auto-Negotiation** enables auto-negotiation on the port.

7 Click **Next**.

Screen 3

8 Accept the AutoArm / Alarm default settings. To activate trigger alarms, select the **Receive Loss of Signal** checkbox and select from the dropdown listing the required LOS (1, 2, 5, 10, or 30 seconds) time (refer to Receive Loss of Signal on page 3-101).

Optionally, select the checkbox for Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power).

9 Click **Next**.

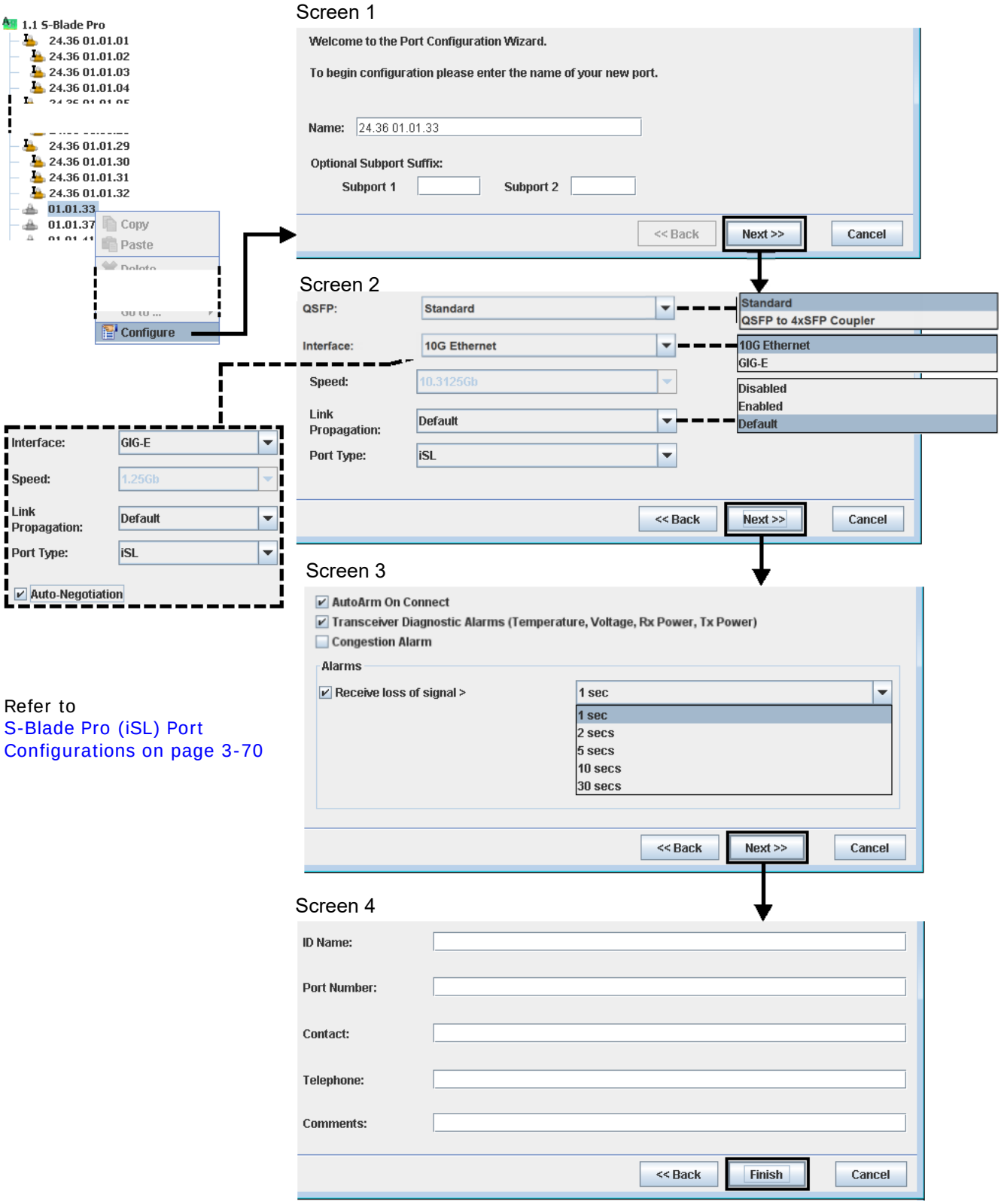
Screen 4

10 Make any additions to the information screen as necessary. Click **Finish**. The configured port now displays on the port level.

11 Continue configuring additional ports on the blade as required.

Note: To configure multiple ports with the same configuration settings, refer to Configuring Multiple Ports on a Blade on page 3-100.

Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.



Refer to
S-Blade Pro (iSL) Port Configurations on page 3-70

S-Blade Pro (iSL) Port Configurations

The following table shows the allowed port configurations / options for the iSL ports.

Interface	Port Type	AutoArm	Transceiver	Receive LOS
10G Ethernet (ports 1 - 72)	iSL	X (default)	X (default)	
Gig-E (ports 1 - 72)	iSL	X (default)	X (default)	
		X = option available X (default) = option available and selected by default		

S-Blade 64

1 From the Switch > Chassis > Blade > Port level, select a port, right click and select **Configure**. The Port Configuration Wizard displays.

Screen 1

2 Enter the name of the new port in the **Name:** field.

Optionally, enter designations for QSFP Subport 1 (e.g., tx) and Subport 2 (e.g., rx). Click **Next**.

Note: If Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) is not disabled (to allow manual configuration/addition of a blade via the nGenius TestStream Management GUI), a port name is automatically created in the Name field with the Subport Suffix fields filled in. These fields can be altered as required during port configuration.

Screen 2

3 Select the QSFP type from the drop down menu.
- Standard
- QSFP to 4xSFP Coupler

4 Select the Interface type from the drop down menu.
QSFP Layer-1 Ports (ports 1 - 72):
- 1/10/40G Ethernet
- 2/4/8G Fiber Channel
- CPRI 9/CPRI 8/CPRI 7/CPRI 6/CPRI 5/CPRI 4/CPRI 3/CPRI 2/CPRI 1 (refer to CPRI Interface on page 3-87)
- 10G CU (requires a QSFP+ to SFP+ adapter)
- 3G/6G/12G SAS

- or -

QSFP Smart Ports (ports 73 - 96):
- 10/40G Ethernet

5 Optionally, set the Link Propagation delay to either Default (pre-selected) or to Disabled or Enabled. This setting defines the detection of Loss of Signal (LOS) from one end of a connection to the other end when the transmitter is turned off.

6 Select the Port Type required (Normal, Test, xSL, or Mirror; refer to Port Types on page 3-85).

If Interface Type **GIG-E** is selected, an Auto-Negotiation option selection block displays. Selecting **Auto-Negotiation** enables auto-negotiation on the port.

If Port Type **Test** is selected, a Force Test Port Link Up option selection block displays. Select **Force Test Port Link Up** to enable the test port to come up and stay up even when there is no signal being received from the attached device; also prevents any Link Down events from being reported when the attached device goes down.

7 Click **Next**.

Screen 3

8 Accept the AutoArm / Alarm default settings. To activate trigger alarms, select the **Receive Loss of Signal** checkbox and select from the dropdown listing the required LOS (1, 2, 5, 10, or 30 seconds) time (refer to Receive Loss of Signal on page 3-101).

   Optionally, select the checkbox for Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power).

9 Click **Next**.

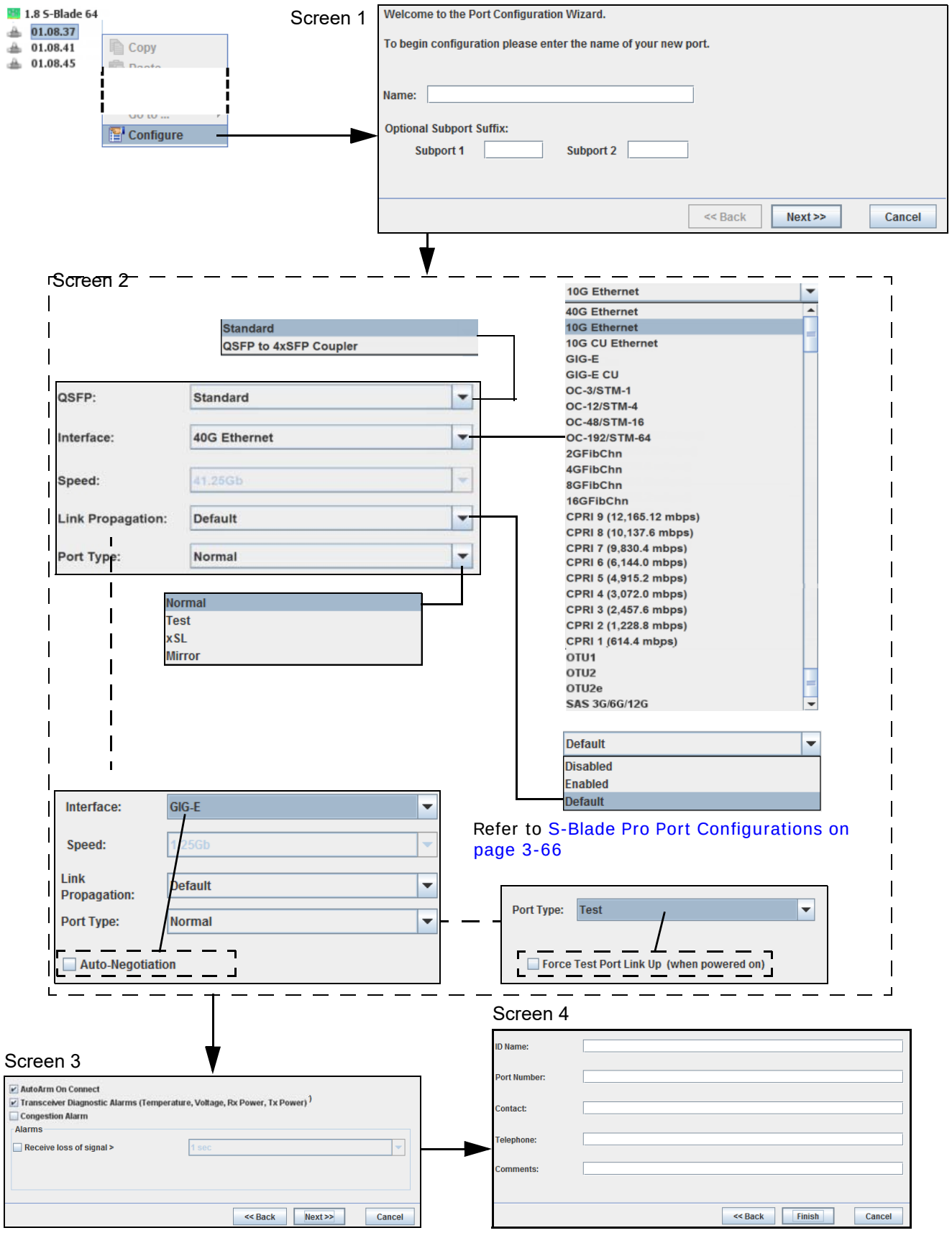
Screen 4

10 Make any additions to the information screen as necessary. Click **Finish**. The configured port now displays on the port level.

11 Continue configuring additional ports on the blade as required.

Note: To configure multiple ports with the same configuration settings, refer to Configuring Multiple Ports on a Blade on page 3-100.

Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.


1.8 S-Blade 64
01.08.37
01.08.41
01.08.45
Copy
Configure
Screen 1
Welcome to the Port Configuration Wizard.
To begin configuration please enter the name of your new port.
Name:
Optional Subport Suffix:
Subport 1
Subport 2
<< Back
Next >>
Cancel
Screen 2
Standard
QSFP to 4xSFP Coupler
QSFP:
Standard
Interface:
40G Ethernet
Speed:
41.25Gb
Link Propagation:
Default
Port Type:
Normal
Normal
Test
xSL
Mirror
10G Ethernet
40G Ethernet
10G Ethernet
10G CU Ethernet
GIG-E
GIG-E CU
OC-3/STM-1
OC-12/STM-4
OC-48/STM-16
OC-192/STM-64
2GFibChn
4GFibChn
8GFibChn
16GFibChn
CPRI 9 (12,165.12 mbps)
CPRI 8 (10,137.6 mbps)
CPRI 7 (9,830.4 mbps)
CPRI 6 (6,144.0 mbps)
CPRI 5 (4,915.2 mbps)
CPRI 4 (3,072.0 mbps)
CPRI 3 (2,457.6 mbps)
CPRI 2 (1,228.8 mbps)
CPRI 1 (614.4 mbps)
OTU1
OTU2
OTU2e
SAS 3G/6G/12G
Default
Disabled
Enabled
Default
Interface:
GIG-E
Speed:
1.25Gb
Link Propagation:
Default
Port Type:
Normal
Auto-Negotiation
Port Type:
Test
Force Test Port Link Up (when powered on)
Refer to S-Blade Pro Port Configurations on page 3-66
Screen 3
AutoArm On Connect
Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power)
Congestion Alarm
Alarms
Receive loss of signal >
1 sec
<< Back
Next >>
Cancel
Screen 4
ID Name:
Port Number:
Contact:
Telephone:
Comments:
<< Back
Finish
Cancel

S-Blade 64 Port Configurations

The following table shows the allowed port configurations / options for each interface / port type.

Interface	Port Type	AutoArm	Transceiver	Receive LOS
40G Ethernet (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
40G Ethernet (ports 73 - 96)	Normal		X (default)	X
	Test (Force Test Link selected)		X (default)	X
	Test (Force Test Link not selected)		X (default)	X
	xSL		X (default)	X
	Mirror		X (default)	X
10G Ethernet 10G CU Ethernet (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
10G Ethernet 10G CU Ethernet (ports 73 - 96)	Normal		X (default)	X
	Test (Force Test Link selected)		X (default)	X
	Test (Force Test Link not selected)		X (default)	X
	xSL		X (default)	X
	Mirror		X (default)	X
2G/4G/8G/16G FibChn (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
Gig-E (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
CPRI9 - CPRI1 (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X

Interface	Port Type	AutoArm	Transceiver	Receive LOS
OC-3/12/48/192 (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
QFSP+to 4xSFP+ Coupler	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
3G/6G/12G SAS (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
OTU1/OTU2/OTU2E (ports 1 - 72)	Normal	X (default)	X (default)	X
	Test (Force Test Link selected)	X (default)	X (default)	X
	Test (Force Test Link not selected)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X
	Mirror		X (default)	X
		X = option available X (default) = option available and selected by default		

T-Blades

1 Click on the detail icon of the blade to display the associated ports.

2 On the selected blade from the port level, select a port, right click and select **Configure**. The Port Configuration Wizard displays.

Screen 1

3 Enter the name of the new port in the **Name:** field.

Optionally, enter designations for SFP / QSFP Subport 1 (e.g., tx) and Subport 2 (e.g., rx). Click **Next**.

Note: If Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) is not disabled (to allow manual configuration/addition of a blade via the nGenius TestStream Management GUI), a port name is automatically created in the Name field with the Subport Suffix fields filled in. These fields can be altered as required during port configuration.

Screen 2

4 Select the Interface type:
SFPs - 10G Ethernet, GIG-E, or GIG-E CU (ports 1 - 16, 33 - 48)
- or -
QSFPs - 40G Ethernet, 10G Ethernet, GIG-E, or GIG-E CU (ports 17, 21, 25, 29) from the drop down menu.

Note: QSFP ports can also be set to 4x10G or 4x1G (dependent on transceiver).

---

5 Select the Port Type required (Normal, Test, xSL, Mirror, or Clone; refer to Port Types on page 3-85).

Note: Clone ports can only be selected / defined by an Administrator-level user.

If Interface Type **GIG-E** is selected, an Auto-Negotiation option selection block displays. Selecting **Auto-Negotiation** enables auto-negotiation on the port.

If Port Type **Test** is selected, a Force Test Port Link Up option selection block displays. Select **Force Test Port Link Up** to enable the test port to come up and stay up even when there is no signal being received from the attached device; also prevents any Link Down events from being reported when the attached device goes down.

If Port Type **Clone** is selected, an Enable External Transmit Data option selection block displays. Selecting **Enable External Transmit Data** allows traffic that is internally looped through the Clone port to also be transmitted externally from this port.

6 Select the Port Power setting - sets the port's power configuration:

- On As Needed (default): the port is powered up if it is in an active connection / connected to another port, is collecting real time or historical statistics, monitoring threshold alarms, or when the port is configured as an xSL port. Otherwise the port is powered off.
- Always On: the port is powered on.
- Always Off: the port is powered off regardless of any condition that would normally power it on.

Note: When powered on, the port's link state depends upon whether it receives a signal from the equipment where its connected unless it is a Clone port (which will always be in a link up state when powered on) or a Test port configured with Force Test Port Link Up.

---

7 Select the Collect Historical Statistics setting - sets the port's Historical Statistics configuration:

- When Connected: historical statistics are collected on both subports when the port is in an active connection / connected to another port.
- Always Collect: the port is powered on (unless configured for Power Always Off) and historical statistics are collected for subport 1 (packets inbound to the port).
- Never Collect: historical statistics are not collected regardless of whether the port is connected to another port.

8 Click **Next**.

Screen 3

9 Accept the AutoArm / Alarm default settings. To activate trigger alarms, select the **Receive Loss of Signal** checkbox and select from the dropdown listing the required LOS (1, 2, 5, 10, or 30 seconds) time (refer to Receive Loss of Signal on page 3-101).

Optionally, select the checkbox for Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power).

Optionally, select the checkbox to activate Congestion Alarms. This will provide an alarm to users when packets are dropped due to over-subscription.

10 Click **Next**.

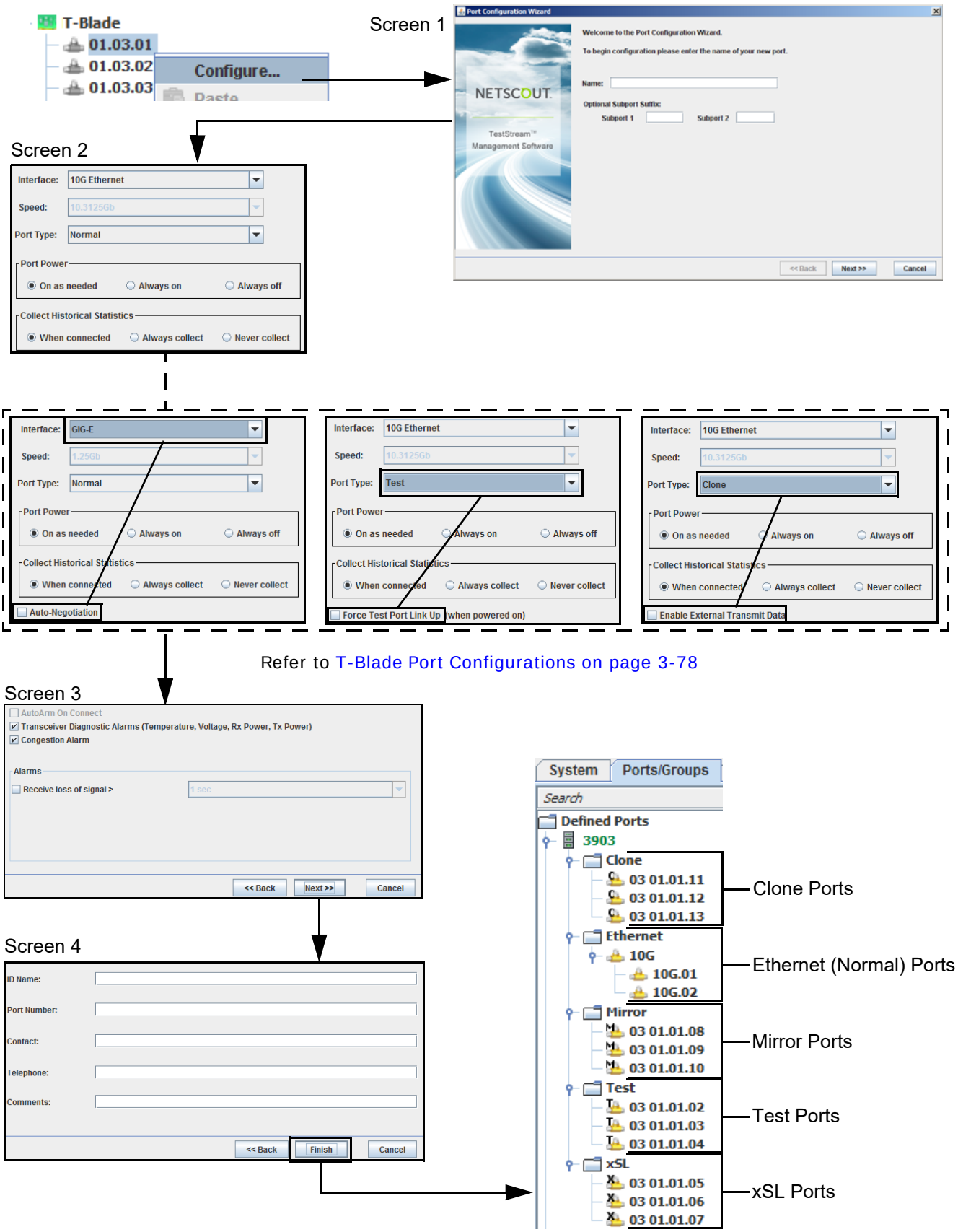
Screen 4

11 Make any additions to the information screen as necessary. Click **Finish**. The configured port now displays on the port level.

12 Continue configuring additional ports on the blade as required.

Note: To configure multiple ports with the same configuration settings, refer to Configuring Multiple Ports on a Blade on page 3-100.

Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.


T-Blade
01.03.01
01.03.02
01.03.03
Configure...
Paste
Screen 1
Port Configuration Wizard
Welcome to the Port Configuration Wizard.
To begin configuration please enter the name of your new port.
Name:
Optional Subport Suffix:
Subport 1
Subport 2
NETSCOUT
TestStream™ Management Software
<< Back
Next >>
Cancel
Screen 2
Interface: 10G Ethernet
Speed: 10.3125Gb
Port Type: Normal
Port Power
On as needed
Always on
Always off
Collect Historical Statistics
When connected
Always collect
Never collect
Interface: GIG-E
Speed: 1.25Gb
Port Type: Normal
Auto-Negotiation
Interface: 10G Ethernet
Speed: 10.3125Gb
Port Type: Test
Force Test Port Link Up (when powered on)
Interface: 10G Ethernet
Speed: 10.3125Gb
Port Type: Clone
Enable External Transmit Data
Refer to T-Blade Port Configurations on page 3-78
Screen 3
AutoArm On Connect
Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power)
Congestion Alarm
Alarms
Receive loss of signal >
1 sec
<< Back
Next >>
Cancel
Screen 4
ID Name:
Port Number:
Contact:
Telephone:
Comments:
<< Back
Finish
Cancel
System
Ports/Groups
Search
Defined Ports
3903
Clone
03 01.01.11
03 01.01.12
03 01.01.13
Clone Ports
Ethernet
10G
10G.01
10G.02
Ethernet (Normal) Ports
Mirror
03 01.01.08
03 01.01.09
03 01.01.10
Mirror Ports
Test
03 01.01.02
03 01.01.03
03 01.01.04
Test Ports
xSL
03 01.01.05
03 01.01.06
03 01.01.07
xSL Ports

T-Blade Port Configurations

The following table shows the allowed port configurations / options for each interface / port type.

Interface	Port Type	AutoArm	Transceiver	Congestion Alarm	Receive LOS
40G Ethernet	Normal		X (default)	X (default)	X
	Test (Force Test Link selected)		X (default)	X (default)	X
	Test (Force Test Link not selected)		X (default)	X (default)	X
	xSL		X (default)	X (default)	X
	Mirror		X (default)		X
	Clone (Enable External Transmit Data selected)		X (default)	X (default)	X
	Clone (Enable External Transmit Data not selected)			X (default)	
10G Ethernet	Normal		X (default)	X (default)	X
	Test (Force Test Link selected)		X (default)	X (default)	X
	Test (Force Test Link not selected)		X (default)	X (default)	X
	xSL		X (default)	X (default)	X
	Mirror		X (default)		X
	Clone (Enable External Transmit Data selected)		X (default)	X (default)	X
	Clone (Enable External Transmit Data not selected)			X (default)	
Gig-E (Auto-Negotiation selected - default)	Normal		X (default)	X (default)	X
	Test (Force Test Link selected)		X (default)	X (default)	X
	Test (Force Test Link not selected)		X (default)	X (default)	X
	xSL		X (default)	X (default)	X
	Mirror		X (default)		X
	Clone (Enable External Transmit Data selected)			X (default)	
	Clone (Enable External Transmit Data not selected)			X (default)	
Gig-E CU	Normal		X (default)	X (default)	
	Test (Force Test Link selected)		X (default)	X (default)	
	Test (Force Test Link not selected)		X (default)	X (default)	
	xSL		X (default)	X (default)	
	Mirror		X (default)		
	Clone (Enable External Transmit Data selected)		X (default)	X (default)	
	Clone (Enable External Transmit Data not selected)			X (default)	

X = option available

X (default) = option available and selected by default

OS-16 / OS-96 / OS-192

1 From the Switch > Chassis > Blade > Port level, select a port, right click and select **Configure**. The Port Configuration Wizard displays.

Screen 1

2 Enter the name of the new port in the **Name:** field.

Optionally, enter designations for Subport 1 (e.g., tx) and Subport 2 (e.g., rx). Click **Next**.

Note: If Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) is not disabled (to allow manual configuration/addition of a blade via the nGenius TestStream Management GUI), a port name is automatically created in the Name field with the Subport Suffix fields filled in. These fields can be altered as required during port configuration.

---

3 Click **Next**.

Screen 2

4 Select the Interface type (Optical = default) from the drop down menu.

5 Select the Port Type required (Normal or xSL).

6 Click **Next**.

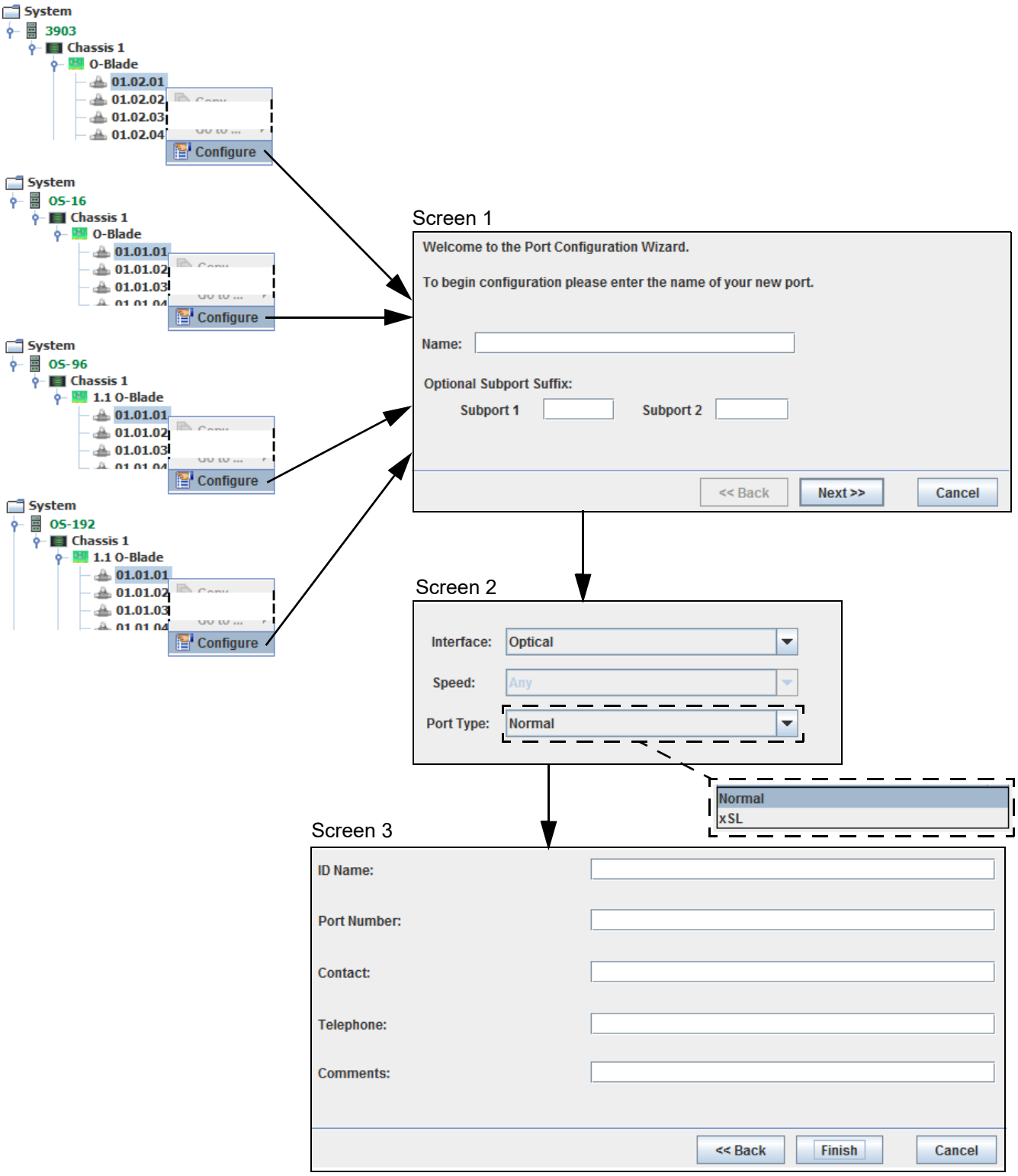
Screen 3

7 Make any additions to the information screen as necessary. Click **Finish**. The configured port now displays on the port level.

8 Continue configuring additional ports on the blade as required.

Note: To configure multiple ports with the same configuration settings, refer to Configuring Multiple Ports on a Blade on page 3-100.

Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.


System
3903
Chassis 1
O-Blade
01.02.01
01.02.02
01.02.03
01.02.04
Configure
System
OS-16
Chassis 1
O-Blade
01.01.01
01.01.02
01.01.03
Configure
System
OS-96
Chassis 1
1.1 O-Blade
01.01.01
01.01.02
01.01.03
Configure
System
OS-192
Chassis 1
1.1 O-Blade
01.01.01
01.01.02
01.01.03
Configure
Screen 1
Welcome to the Port Configuration Wizard.
To begin configuration please enter the name of your new port.
Name:
Optional Subport Suffix:
Subport 1
Subport 2
<< Back
Next >>
Cancel
Screen 2
Interface:
Optical
Speed:
Any
Port Type:
Normal
Normal
xSL
Screen 3
ID Name:
Port Number:
Contact:
Telephone:
Comments:
<< Back
Finish
Cancel

HS-3200/HS-6400

1 From the Switch > Chassis > Blade > Port level, select a port, right click and select **Configure**. The Port Configuration Wizard displays.

Screen 1

2 Enter the name of the new port in the **Name:** field.

Optionally, enter designations for QSFP Subport 1 (e.g., tx) and Subport 2 (e.g., rx). Click **Next**.

Note: If Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) is not disabled (to allow manual configuration/addition of a blade via the nGenius TestStream Management GUI), a port name is automatically created in the Name field with the Subport Suffix fields filled in. These fields can be altered as required during port configuration.

Screen 2

3 Select the Interface type:
QSFP28 - 100G Ethernet, 50G Ethernet, or 25G Ethernet
QSFP - 40G Ethernet or 10G Ethernet
from the drop down menu.
An additional drop down menu allows the user to select the number of connectivity lines per Odd-numbered port:

- 100G - 1 line
- 50G - 2 lines
- 40G - 1 line
- 25G - 2 or 4 lines
- 10G - 2 or 4 lines

4 Select the Port Type required (refer to Port Types on page 3-85):
Normal, Test, xSL, or Mirror

5 Select the Port Power setting - sets the port's power configuration:

- On As Needed (default): the port is powered up if it is in an active connection / connected to another port, is collecting real time or historical statistics, monitoring threshold alarms, or when the port is configured as an xSL port. Otherwise the port is powered off.
- Always On: the port is powered on.
- Always Off: the port is powered off regardless of any condition that would normally power it on.

Note: When powered on, the port's link state depends upon whether it receives a signal from the equipment where its connected or a Test port configured with Force Test Port Link Up.

---

6 Select the Collect Historical Statistics setting - sets the port's Historical Statistics configuration:

- When Connected: historical statistics are collected on both subports when the port is in an active connection / connected to another port.
- Always Collect: the port is powered on (unless configured for Power Always Off) and historical statistics are collected for subport 1 (packets inbound to the port).
- Never Collect: historical statistics are not collected regardless of whether the port is connected to another port.

7 Click **Next**.

Screen 3

8 Accept the AutoArm / Alarm default settings. To activate trigger alarms, select the **Receive Loss of Signal** checkbox and select from the dropdown listing the required LOS (1, 2, 5, 10, or 30 seconds) time (refer to Receive Loss of Signal on page 3-101).

   Optionally, select the checkbox for Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power).

   Optionally, select the checkbox to activate Congestion Alarms. This will provide an alarm to users when packets are dropped due to over-subscription.

9 Click **Next**.

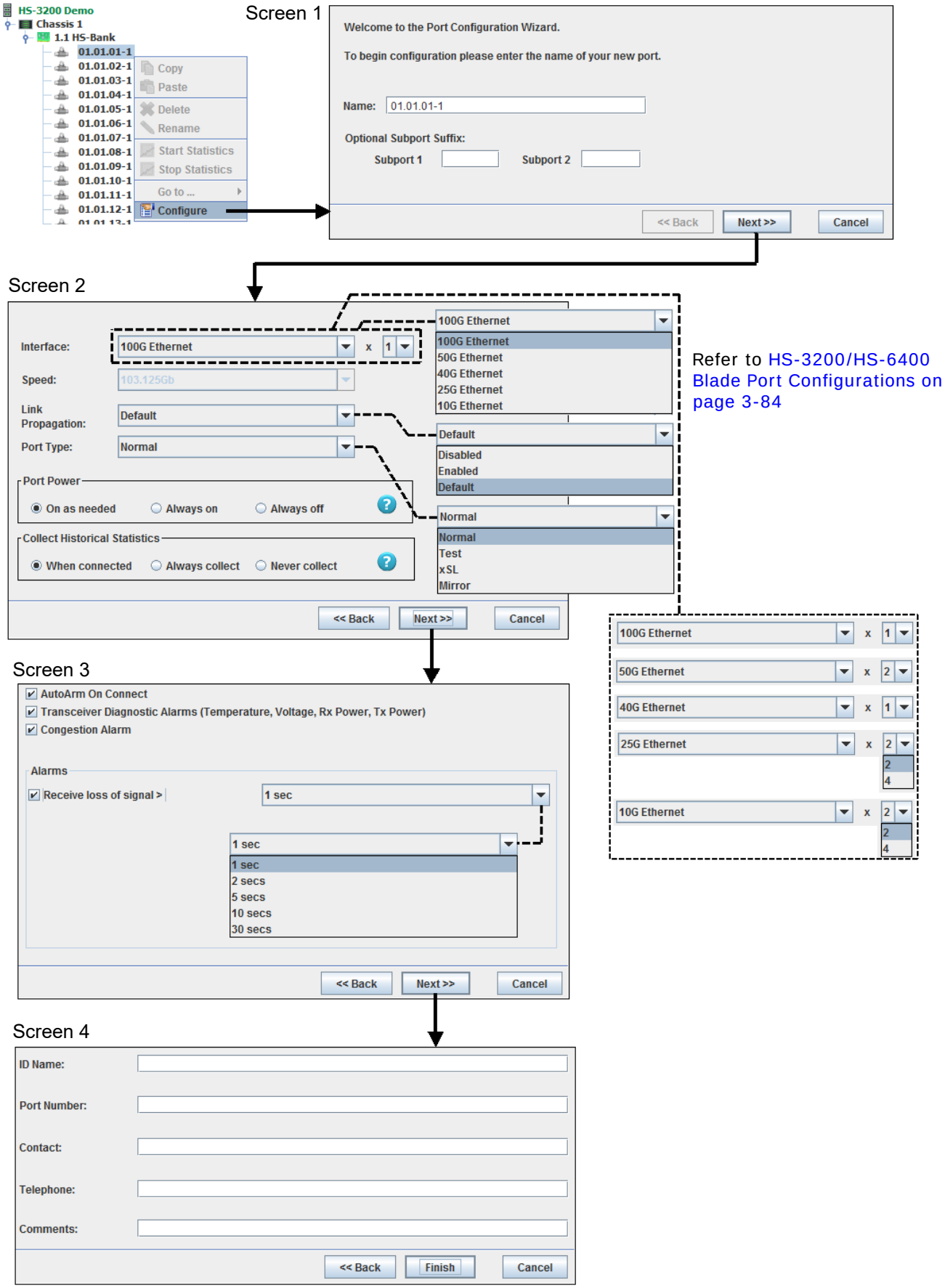
Screen 4

10 Make any additions to the information screen as necessary. Click **Finish**. The configured port now displays on the port level.

11 Continue configuring additional ports on the blade as required.

Note: To configure multiple ports with the same configuration settings, refer to Configuring Multiple Ports on a Blade on page 3-100.

Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.


HS-3200 Demo
Chassis 1
1.1 HS-Bank
01.01.01-1
01.01.02-1
01.01.03-1
01.01.04-1
01.01.05-1
01.01.06-1
01.01.07-1
01.01.08-1
01.01.09-1
01.01.10-1
01.01.11-1
01.01.12-1
Copy
Paste
Delete
Rename
Start Statistics
Stop Statistics
Go to ...
Configure
Screen 1
Welcome to the Port Configuration Wizard.
To begin configuration please enter the name of your new port.
Name: 01.01.01-1
Optional Subport Suffix:
Subport 1
Subport 2
<< Back
Next >>
Cancel
Screen 2
Interface: 100G Ethernet x 1
Speed: 103.125Gb
Link Propagation: Default
Port Type: Normal
Port Power
On as needed
Always on
Always off
Collect Historical Statistics
When connected
Always collect
Never collect
100G Ethernet
50G Ethernet
40G Ethernet
25G Ethernet
10G Ethernet
Disabled
Enabled
Default
Normal
Test
xSL
Mirror
Refer to HS-3200/HS-6400 Blade Port Configurations on page 3-84
Screen 3
AutoArm On Connect
Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power)
Congestion Alarm
Alarms
Receive loss of signal >
1 sec
2 secs
5 secs
10 secs
30 secs
Screen 4
ID Name:
Port Number:
Contact:
Telephone:
Comments:
Finish

HS-3200/HS-6400 Blade Port Configurations

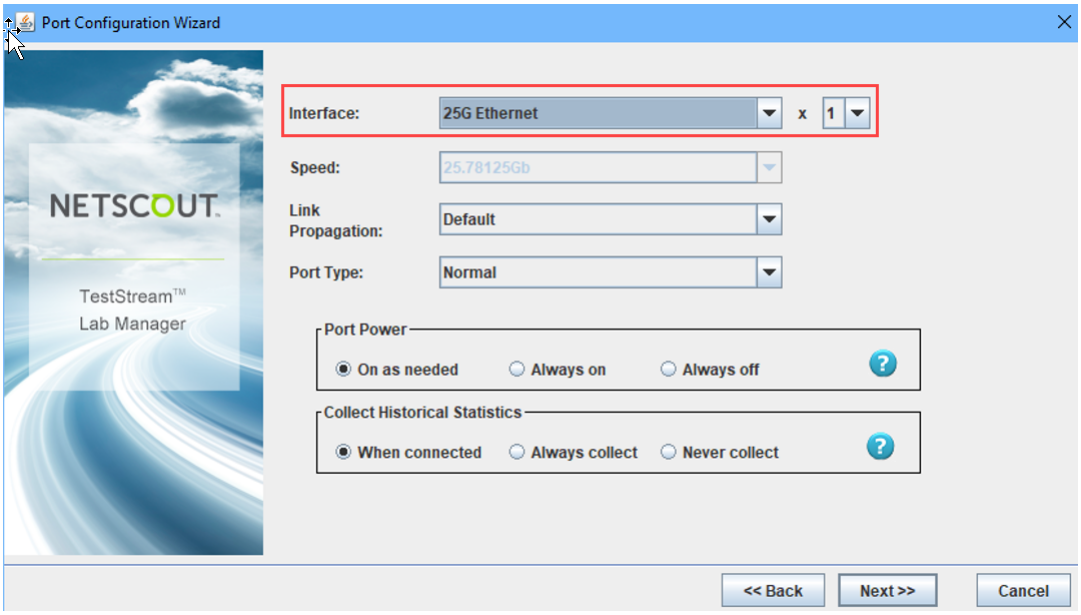
The following table shows the allowed port configurations / options for each interface / port type.

Interface	Port Type	AutoArm	Transceiver	Congestion Alarm	Receive LOS
100G Ethernet	Normal	X (default)	X (default)	X (default)	X
	Test	X (default)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X (default)	X
	Mirror	X (default)	X (default)	X (default)	X
50G Ethernet	Normal	X (default)	X (default)	X (default)	X
	Test	X (default)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X (default)	X
	Mirror		X (default)		X
40G Ethernet	Normal	X (default)	X (default)	X (default)	X
	Test	X (default)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X (default)	X
	Mirror		X (default)		X
25G Ethernet	Normal	X (default)	X (default)	X (default)	X
	Test	X (default)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X (default)	X
	Mirror		X (default)		X
10G Ethernet	Normal	X (default)	X (default)	X (default)	X
	Test	X (default)	X (default)	X (default)	X
	xSL	X (default)	X (default)	X (default)	X
	Mirror		X (default)		X
		X = option available X (default) = option available and selected by default			

QSFP28 to SFP28 adapter

The HS-3200 and HS-6400 support a new QSFP28 to SFP28 adapter. This adapter allows for the use of SFP28 transceivers in QSFP28 ports.

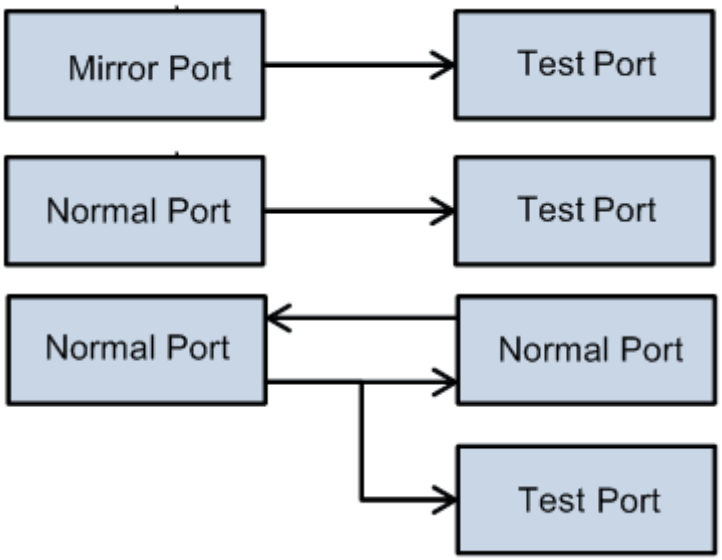
To configure a port for 25G ETH with an adapter, set the interface to **25G Ethernet** and the number of ports to **x1**.



Port Types

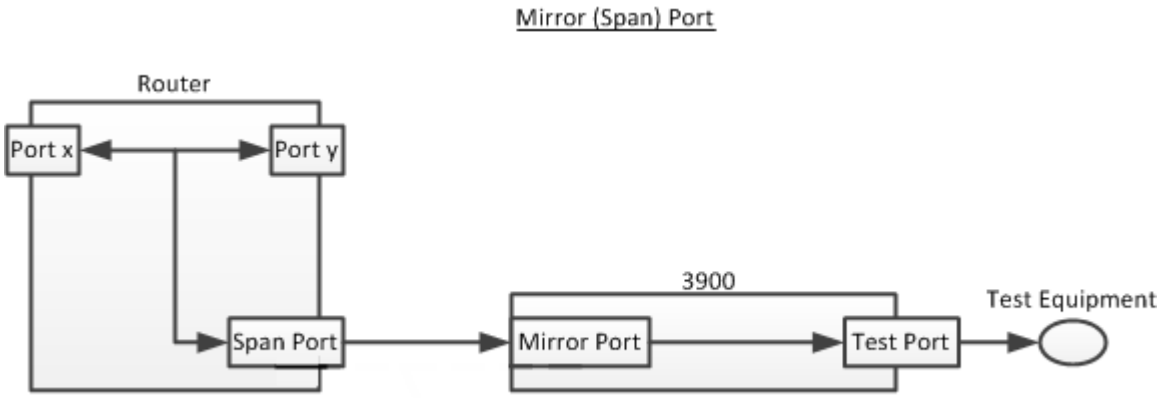
Test Ports

Test ports provide a non-obtrusive way to access and monitor the data flowing across a connected path; commonly used for network intrusion detection systems, network probes, packet sniffers, and other monitoring and collection devices and software requiring access to a network segment.



Mirror Ports

Mirror ports are used on a network switch to actively send a copy of selected / filtered network packets seen on one switch port to one or more Test ports. The filtering feature allows confining the monitoring to selected frames. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system. Mirror ports can only be connected to a Test port, creating a one-way path with the copied data going from the Mirror port to the Test port.

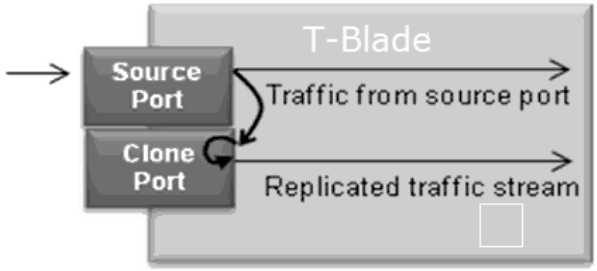


Clone Ports

Note:
Clone Ports are only applicable to T-Blades.

Clone ports can only be selected / defined by an Administrator-level user.

Selecting clone ports provides the capability for any normal port to be placed in a mode which takes traffic received internally from a source, and internally loops it back creating a copy of the traffic stream for filtering and connections. If an SFP is physically installed on that port, the SFPs transmitter is disabled; however, under Port Properties, you can optionally select Enable External Transmit Data.



The clone port function provides a way to apply additional independent processing to a source port traffic stream. Typical examples are:

- Applying filters to a source port stream without impacting the functionally of the port for additional users.
- Applying packet modifiers (when packets are modified, all downstream ports receive the modified packet) - by using a clone port to modify the packets, the original stream is still available in the cloned port.

Once configured as a clone port, the port cannot be used as a regular port; the user has to link it to another port by creating an association from the cloned port to the clone port (refer to Clone Ports on page 6-15). When this association is made and activated, the clone port is linked to the cloned port and is available for connections.

CPRI Interface

S-Blade Pro Layer-1 ports (1 - 72) support the Common Public Radio Interface (CPRI) protocol. The following CPRI interface options can be selected when configuring an S-Blade Pro port:

CPRI Option	Bit Rate
CPRI 1	614.4 Mbit/s
CPRI 2	1,228.8 Mbit/s
CPRI 3	2,457.6 Mbit/s
CPRI 4	3,072.0 Mbit/s
CPRI 5	4,915.2 Mbit/s
CPRI 6	6,144.0 Mbit/s
CPRI 7	9,830.4 Mbit/s
CPRI 8	10,137.6 Mbit/s
CPRI 9	12,165.12 Mbit/s

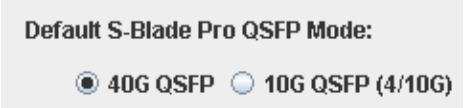
Interface Usage

Each of the CPRI interfaces utilize only one lane of a QSFP+ interface.

Unconfigured Layer 1 ports (i.e., 1, 5, 9, ... 65, 69) can be configured to any of the CPRI option interfaces. A configured port is broken up into 4 ports using the same selected CPRI interface (using 1 main port with 3 partner ports). Each lane can then be independently configured to any interface type (CPRI 1 - 9, 10GbE, GIG-E, 2GFibChan, 4GFibChan, 8GFibChan or 16FibChan).

Transceiver Usage

When a QSFP+ transceiver is inserted into a cage corresponding to an unconfigured main port, its speed defaults to 40G or 4x10G depending on the following Switch Properties Parameter setting:



The port speed can then be changed as required.

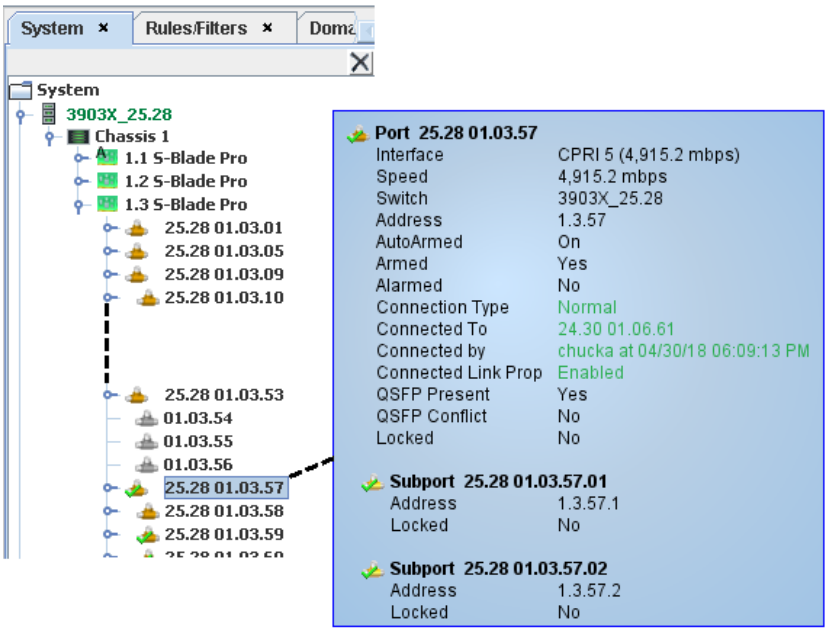
If the default mode is 40GbE, when changing the port interface to any of the CPRI option interfaces the port is broken up into 4 ports using the same selected CPRI interface (using 1 main port with 3 partner ports). Each lane can then be independently configured to any interface type (CPRI 1 - 9, 10GbE, GIG-E, 2GFibChan, 4GFibChan, 8GFibChan or 16FibChan).

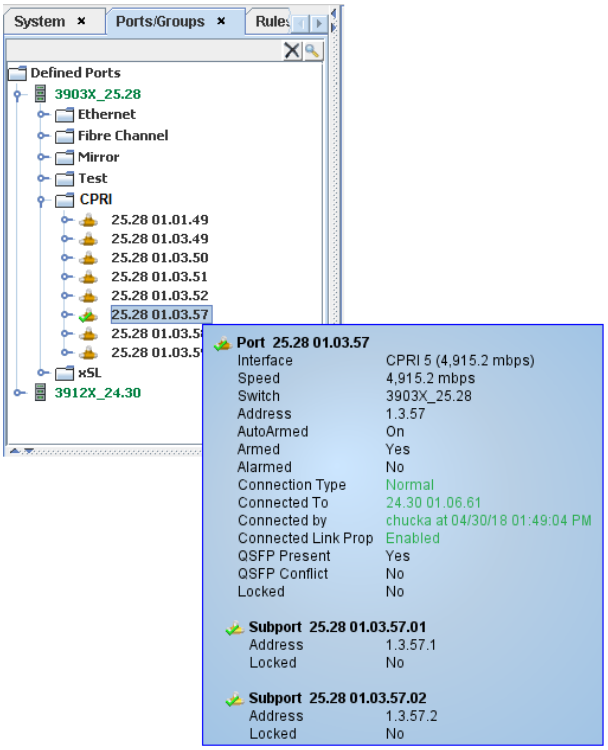
If the default mode is 10GbE, each lane can be independently configured to any interface type (CPRI 1 - 9, 10GbE, GIG-E, 2GFibChan, 4GFibChan, 8GFibChan or 16FibChan).

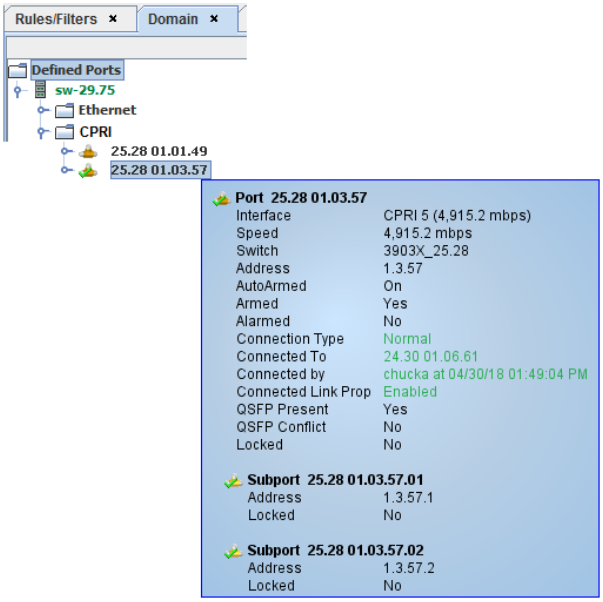
Note: When changing a main port interface back to 40GbE, make sure the partner ports are not configured (the partner ports / configurations must be deleted if configured).

Viewing Port Information

CPRI interface information on a selected port can be obtained from the Switch Graphic (refer to S-Blade Pro Graphic on page 3-44), System, Ports/Groups, and Domain tab selections.



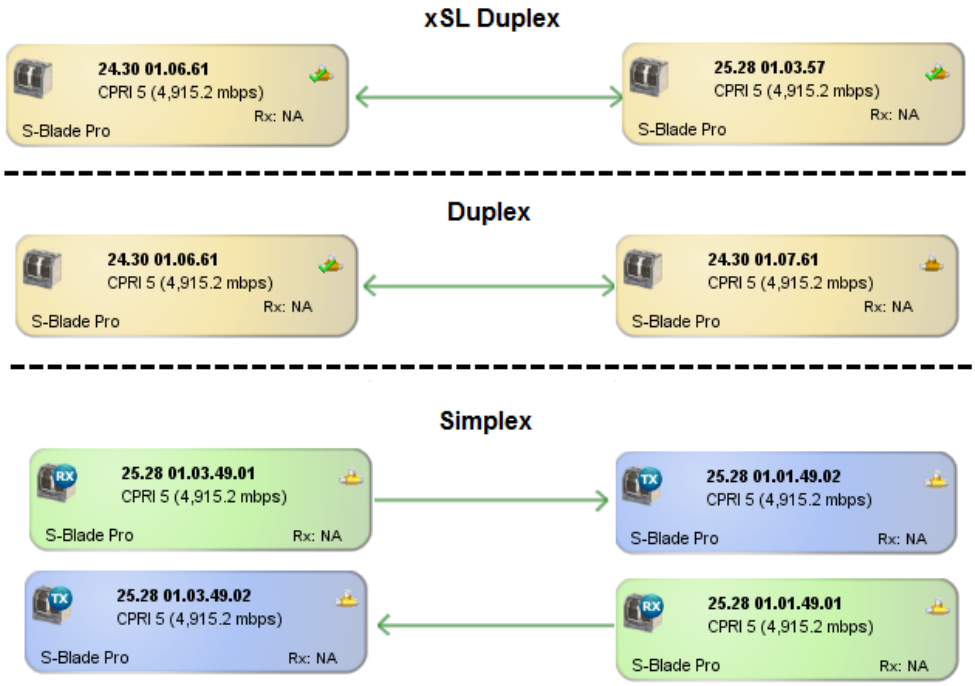




CPRI Port Connections

When making port connections, the connected ports must have the same CPRI interface (e.g., CPRI 9 to CPRI 9, CPRI 5 to CPRI 5, CPRI 1 to CPRI 1).

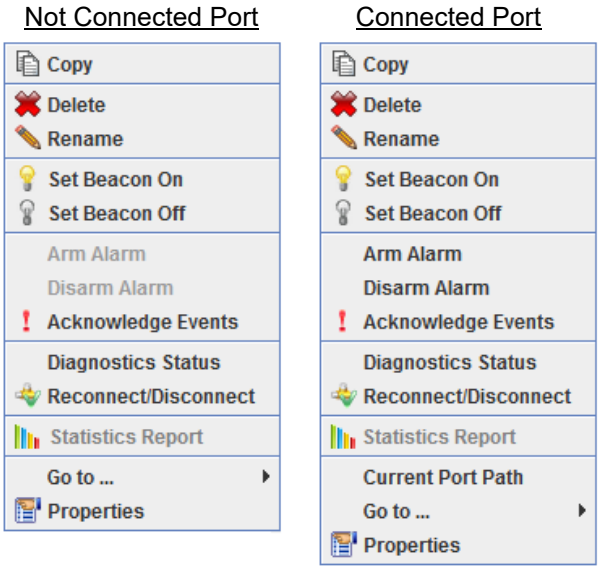
CPRI connected ports can be either duplex, simplex, or xSL.



Note:
S-Blade Pro Extended Fabric Mode does not support CPRI interfaces.
CPRI interface ports do not support impairments.
CPRI interface ports cannot be used in scanners.

CPRI Port Sub-menus

Right-clicking on a CPRI port displays the standard S-Blade Pro port sub-menu (refer to Blade Port Menus on page 3-154) with the following exception: Statistics Report is not available / supported on CPRI ports.



Statistics Restrictions

When using the System Statistics (refer to Statistics on page 4-7) feature in TestStream, the following restrictions concerning CPRI ports must be observed:

- CPRI ports cannot be selected and dragged/dropped into the Port Real Time Statistics table (refer to Port Real Time Statistics on page 4-8).
- CPRI ports cannot be selected and dragged/dropped into the Port Historical Statistics table (refer to Port Historical Statistics on page 4-12).

QSFP+ to 4xSFP+ Coupler

A "QSFP+ to 4xSFP+ Coupler" has on one end a male QSFP+ connector and on the other end 4 SFP+ receptacles (cages). Each lane from the QSFP+ side has a corresponding SFP+ receptacle which supports any compliant SFP+ transceiver module. The SFP+ receptacles are labeled ‘A’, ‘B’, ‘C’ and ‘D’ (corresponding to the QSFP+ lanes 1 through 4).

Note: As of the current release, only QSFP+ ports on the S-Blade Pro support the ‘QSFP+ to 4xSFP+ Coupler’. The power budget available is up to 5 watts per QSFP+ port.

In the following sections the "QSFP+ to 4xSFP+ Coupler" will be referred as coupler.

Port Configuration

An option named ‘QSFP’ is available for QSFP+ ports supporting this feature. This option has two possible values: ‘Standard’ and ‘QSFP to 4xSFP Coupler’. When ‘QSFP to 4xSFP Coupler’ is selected, the system will replace the QSFP+ port with 4 SFP+ ports: one main or parent port (the ‘A’ port) and three partner ports (the ‘B’, ‘C’ and ‘D’ ports). Each SFP+ port can be configured to any of the supported SFP+ interfaces.

Note: The ‘QSFP’ mode can only be viewed or modified using the main or parent port (labeled ‘A’).

To convert the ‘QSFP’ option back to ‘Standard’ make sure all the partner ports are undefined and then using the main or parent port, set its ‘QSFP’ option to ‘Standard’. Note that this is possible only if there is no ‘QSFP+ to 4xSFP+ Coupler’ inserted in the port.

When all four SFP+ ports are deleted and the coupler is removed, the ‘QSFP’ option will revert back to ‘Standard’.

Coupler Insertion

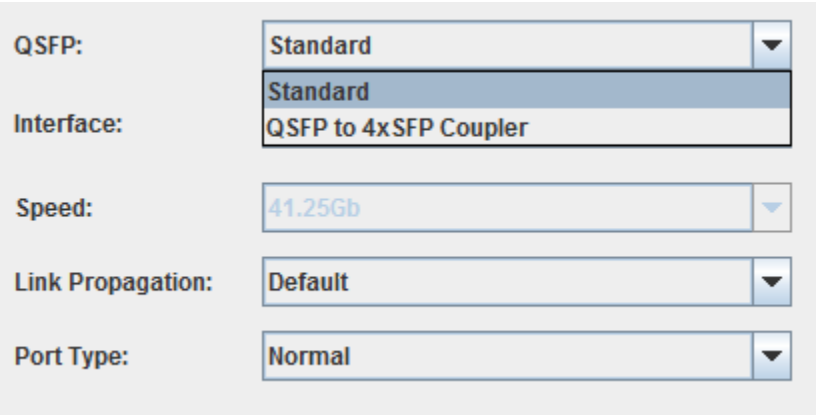
If auto-discovery is enabled, when coupler is inserted into a QSFP+ port corresponding to an un-configured main port, the port ‘QSFP’ option is set to ‘QSFP to 4xSFP Coupler’. The System Tree replaces the undefined QSFP+ port with 4 undefined labeled SFP+ ports.

If an SFP+ module is inserted in any of the receptacles it will be auto discovered and its corresponding SFP port will be configured accordingly.

If auto-discovery is disabled and a coupler is inserted, the ‘QSFP’ option can be manually configured. At the time the configuration is updated, the ‘QSFP’ option will only support the ‘QSFP to 4xSFP Coupler’ value and the ‘Interface’ option will have to match any installed SFP+ transceiver.

GUI

The ‘Port Configuration Wizard’ window allows the configuration of the ‘QSFP’ option. If the ‘QSFP’ option is set to ‘QSFP+ to 4xSFP+ Coupler’, the ‘Interface’ field will only display SFP+ compatible interfaces.



The main or parent port will have a defined interface (as selected at the time the ‘QSFP’ option was set) and the 3 secondary ports will have undefined interfaces.

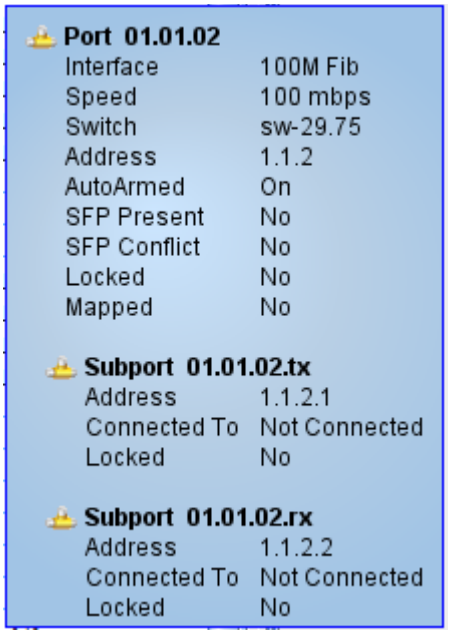
The ‘General’ tab of the Port Properties window of the main or parent port displays the ‘QSFP’ option.

CLI

The command ‘**ADD TO** switchname [**TE**st|**MIR**ror|**XS**1|**CL**one] **POR**t cc.bb.pp portname …’ supports a new option: [STAndard|QSFp4sfp]. For the full command syntax please see Appendix A.

Viewing Port Information

'QSFP' option information on a selected port can be obtained from the Switch Graphic (refer to S-Blade Pro Graphic on page 3-38), System, Ports/Groups, and Domain tab selections. Once the mouse pointer is placed on top of a port icon, the port tool tip is displayed. The port tool tip of the main port will display QSFP and SFP information. The port tool tip of the partner ports will display only SFP information.



Port Sub-menus

Right-clicking on a 'QSFP+ to 4xSFP+ Coupler' SFP+ port displays the standard blade sub-menu.

Port Diagnostics Status

Port diagnostics status is available on all the four SFP+ ports. The diagnostics status for the port will display the SFP+ information (complete with diagnostics if applicable) if the SFP+ transceiver is available.

SFP+ Port Features

The SFP+ ports of the 'QSFP+ to 4xSFP+ Coupler' support all the functionality supported by regular SFP+ ports. For example, they can be used in groups, domains, devices, topologies, impairments, and port scanners (only 10G ETH interfaces are supported).

Port mismatch

Mismatch can happen at the QSFP+ or SFP+ level.

At the QSFP+ level, if a regular QSFP+ transceiver is inserted in a QSFP port configured with the 'QSFP' option set to 'QSFP to 4xSFP Coupler', a 'conflict' status indicator (wrench) will be displayed on the main or parent port. The mismatch can be fixed by inserting a coupler or updating the 'QSFP' option (if partner ports are enabled, they must be deleted first).

At the QSFP+ level, if a coupler is inserted in a QSFP+ port configured with the 'QSFP' option set to 'Standard', a new status indicator will be displayed on the main or parent port. The mismatch can be fixed by inserting a regular QSFP+ transceiver or updating the 'QSFP' option (if partner ports are enabled, they must be deleted first).

At the SFP+ level, if an SFP+ transceiver is inserted in the SFP+ port of the coupler and it does not match the configured interface, a wrench will be displayed on the SFP+ port. The mismatch can be fixed by inserting the expected transceiver or updating the SFP+ port interface.

SFM Pro External Fabric Mode

SFM Pro External Fabric Mode consists of a 3912 with 8 SFM Pro blades and a 3903 with 2 S-Blade Pro blades. The SFM Pro user accessible ports are cabled to the 3903 S-Blade Pro L1 ports providing extra fabric paths for the 3912 front ports. Both 1GbE and 10GbE are supported.

Switch Configuration

A pair of 3903 and 3912 switches are configured to be in External Fabric Mode (XFM). Each switch is set into this mode separately (refer to **SFM Pro External Fabric Mode** on page 3-7). The 3912 switch is configured with the switch name of the corresponding 3903.

Note:
Once a switch is in XFM mode, the only way to remove the switch from XFM mode is by deleting the switch.

When in SFM Pro External Fabric Mode, the 3912 is designated as the **front** switch and the 3903 is the **fabric** switch.

XFM mode is setup only at the time a switch is added. This means that the 3903 must be added first and then the 3912, allowing the 3912 to be configured with the 3903 switch name.

A 3903 in XFM mode must have the **Default S-Blade Pro QSFP Mode** set to **10G**.

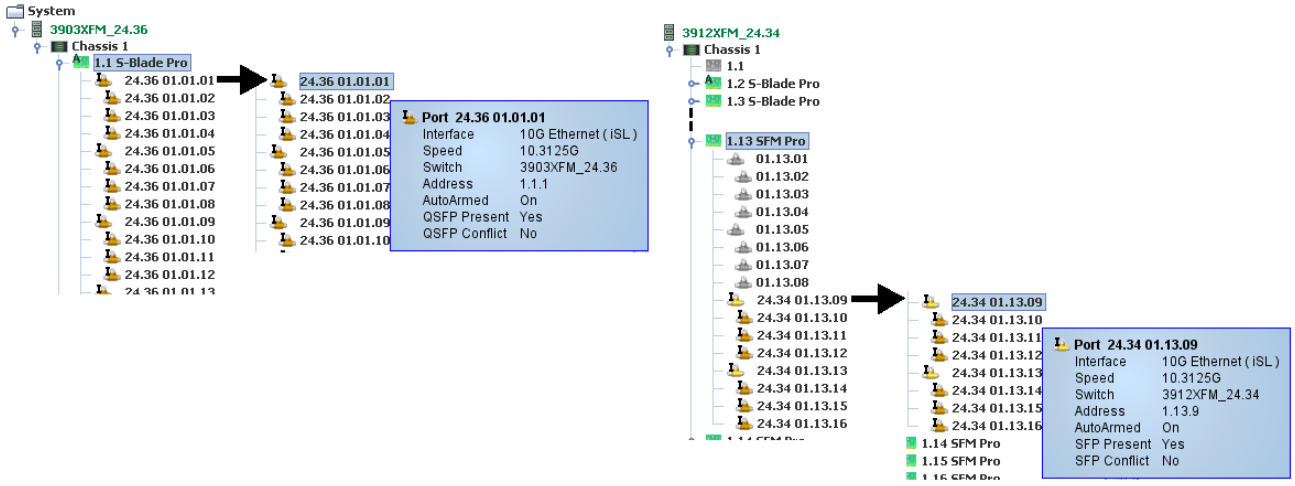
Blade Configuration

The S-Blade Pro blades in the 3912 should be configured with **0** Utilization Lanes under **Bridge Lane Allocation** (refer to Blade Properties > S-Blade Pro on page 3-168). TestStream will not attempt to enforce this configuration to give users the option to use bridge lanes for utilization knowing that it will take away paths available for connections.

The 3903 must be populated with 3 S-Blade Pro blades. With the switch parameters setup as described above, the auto-detected S-Blade Pro blades utilize 0 lanes for utilization as default.

Port Configuration

In the 3903, all of the S-Blade Pro L1 ports are configured as 10GbE ports with type **iSL** (refer to S-Blade Pro (iSL Ports) on page 3-68). In the 3912, all of the SFM-Pro ports are configured as 10GbE ports with type **iSL** (refer to Configuring SFM Pro iSL Ports on page 3-93).



Configuring SFM Pro iSL Ports

iSL ports are only available on SFM Pros installed in 3912 systems configured with SFM Pro External Fabric mode enabled (refer to SFM Pro External Fabric Mode on page 3-93).

1 From the Switch > Chassis > Blade > Port level, select a port, right click and select **Configure**. The Port Configuration Wizard displays.

Screen 1

2 Enter the name of the new port in the **Name:** field.

Optionally, enter designations for QSFP Subport 1 (e.g., tx) and Subport 2 (e.g., rx). Click **Next**.

Note: If Auto Discrepancy Detection (refer to Adding a Switch on page 3-2) is not disabled (to allow manual configuration/addition of a blade via the nGenius TestStream Management GUI), a port name is automatically created in the Name field with the Subport Suffix fields filled in. These fields can be altered as required during port configuration.

Screen 2

3 Select the QSFP type from the drop down menu.
- Standard
- QSFP to 4xSFP Coupler

4 Select the Interface type from the drop down menu.
QSFP Ports (ports 1 - 16):
- GIG-E or 10G Ethernet (default is 10G)

5 Optionally, set the Link Propagation delay to either Default (pre-selected) or to Disabled or Enabled. This setting defines the detection of Loss of Signal (LOS) from one end of a connection to the other end when the transmitter is turned off.

6 Port Type is pre-selected to **iSL**.

If Interface Type **GIG-E** is selected, an Auto-Negotiation option selection block displays. Selecting **Auto-Negotiation** enables auto-negotiation on the port.

7 Click **Next**.

Screen 3

8 Accept the AutoArm / Alarm default settings. To activate trigger alarms, select the **Receive Loss of Signal** checkbox and select from the dropdown listing the required LOS (1, 2, 5, 10, or 30 seconds) time (refer to Receive Loss of Signal on page 3-101).

Optionally, select the checkbox for Transceiver Diagnostic Alarms (Temperature, Voltage, Rx Power, Tx Power).

Optionally, select the checkbox to activate Congestion Alarms. This will provide an alarm to users when packets are dropped due to over-subscription.

9 Click **Next**.

Screen 4

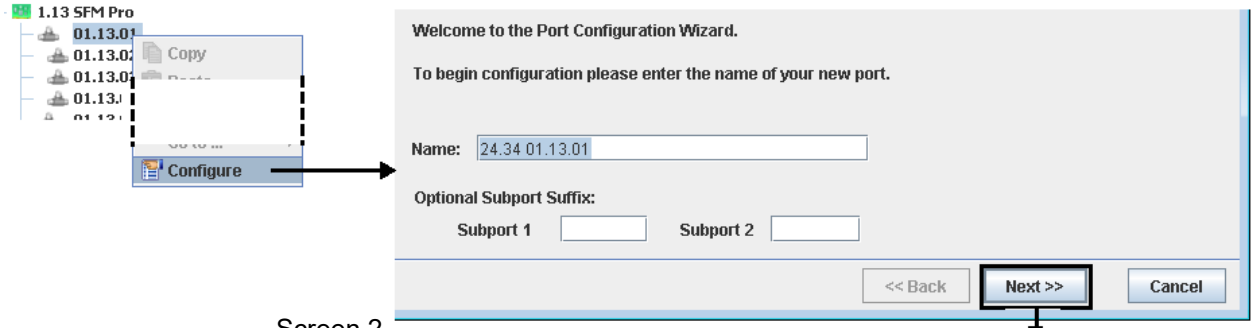
10 Make any additions to the information screen as necessary. Click **Finish**. The configured port now displays on the port level.

11 Continue configuring additional ports on the blade as required.

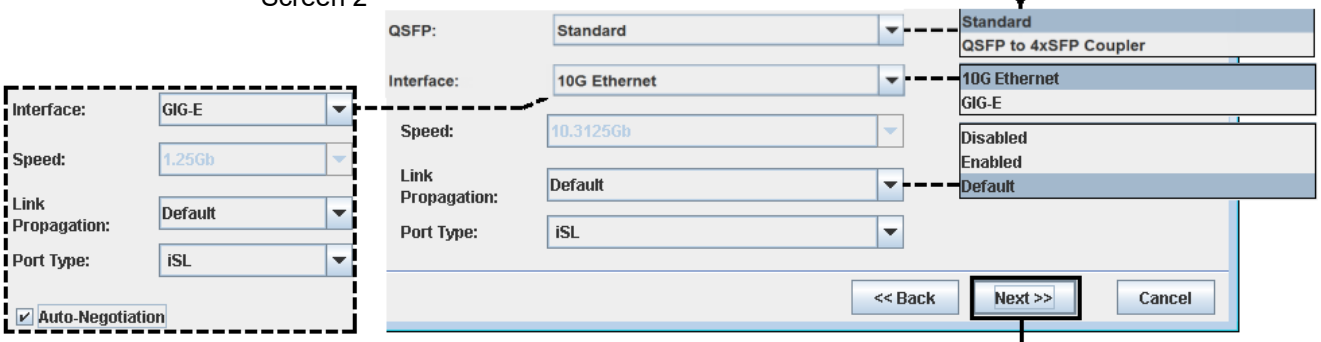
Note: To configure multiple ports with the same configuration settings, refer to Configuring Multiple Ports on a Blade on page 3-100.

Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.

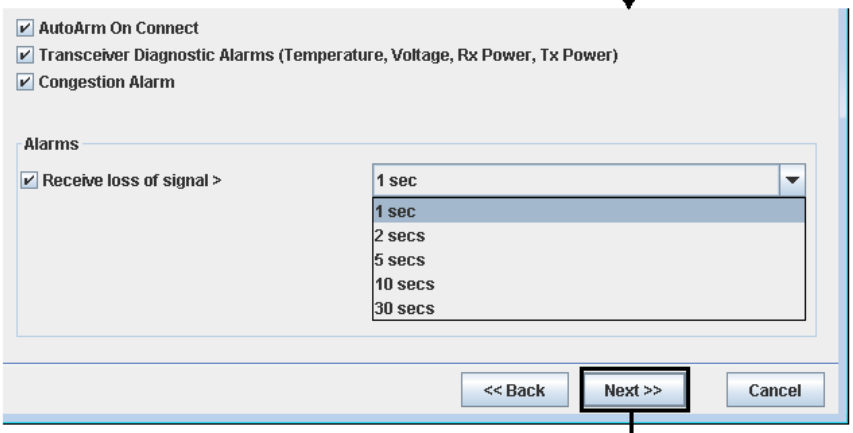
Screen 1



Screen 2

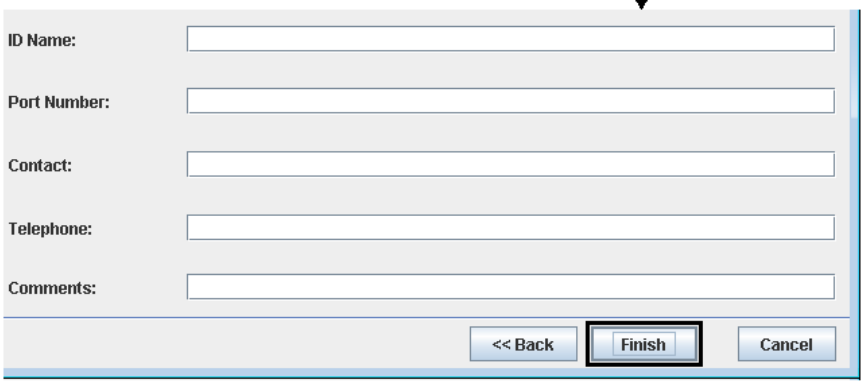


Screen 3



Refer to
SFM Pro (iSL) Port Configurations on page 3-96

Screen 4



SFM Pro (iSL) Port Configurations

The following table shows the allowed port configurations / options for the iSL ports.

Interface	Port Type	AutoArm	Transceiver	Congestion	Receive LOS
10G Ethernet (ports 1 - 72)	iSL	X (default)	X (default)	X (default)	
Gig-E (ports 1 - 72)	iSL	X (default)	X (default)	X (default)	
		X = option available X (default) = option available and selected by default			

iSL Port Usability Rules

- iSL ports are identified by the **I** icon (refer to Icon Legend Chart on page 2-45).
- iSL ports cannot be placed in topology/connection manager. ISL ports cannot be connected by user using CLI commands or the switch graphic.
- iSL ports cannot be added to groups, source groups, or destination groups.
- Device ports cannot be mapped to ISL ports.
- iSL cannot be added to domains.
- iSL cannot be added to probes.
- iSL does not support Port Locking.
- From Port Properties, only General, Alarm, and Optional Information are active. In General, only Link Propagation can be modified (Port Speed and Type cannot be changed).

iSL Port Menu

Right clicking on an iSL port displays the following menu:

- Copy / Paste - Copies the configuration setting of a defined port and assigns the configuration to another port.
- Delete - Remove (undefine) the configuration settings of a port.
- Rename - Change the assigned name of a port.

Important: Port names cannot be made up of four (4) dotted numbers (nn.nn.nn.nn - e.g., 10.88.99.11).

- Set Beacon On / Off - Activates green and yellow pair of LED indicators on the blade to visually locate a blade port in a chassis for maintenance or troubleshooting.
- Arm / Disarm Alarm - Activate / deactivate port alarms

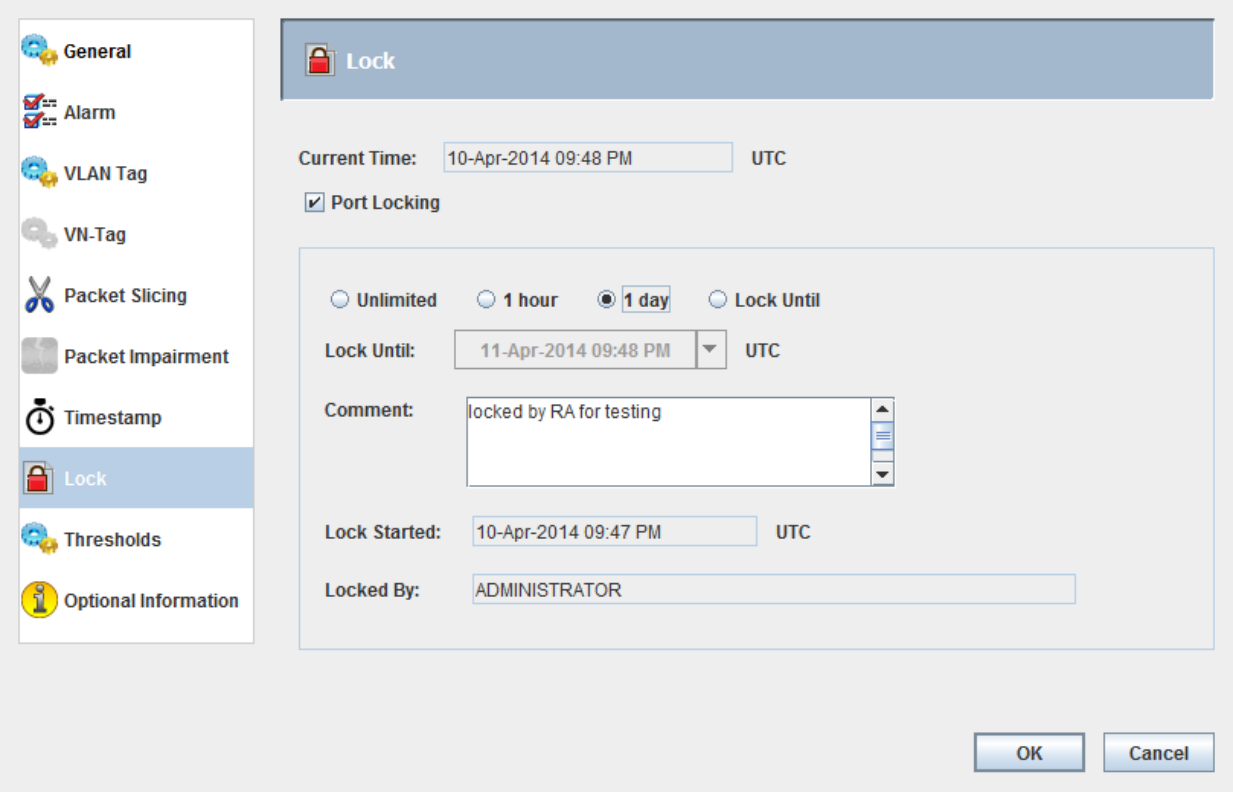
- Acknowledge Events - Acknowledge all port events on the specified port
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.
- Current Port Path - Refer to Current Port Path on page 7-14.
- Properties - Refer to Port Properties on page 3-170.

Port Lock Settings

Port locking allows users exclusive usage of a single port / subport or multiple ports / subports for an assigned time period. Only the owner of the locked port(s) can do anything (e.g., revise / delete / connect / disconnect) with the port; all other users can open the port properties of the port(s) but in a read-only mode (no changes can be made to the port fields).

Note: A user with administrator privileges can override a locked port of another user.

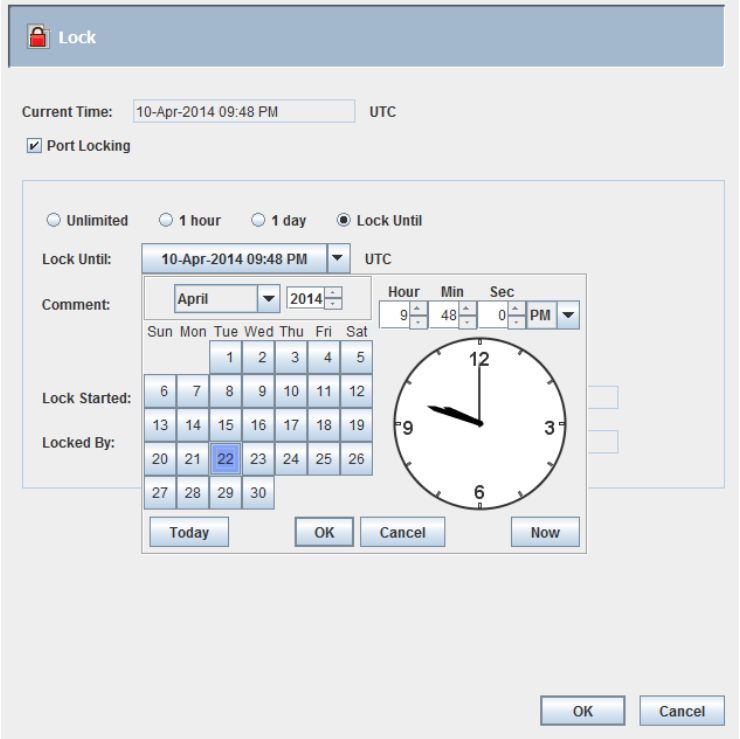
1 Select the required configured port(s), right-click and select **Properties**. The Port Properties window displays. Click on **Lock Settings** to display the setup screen.



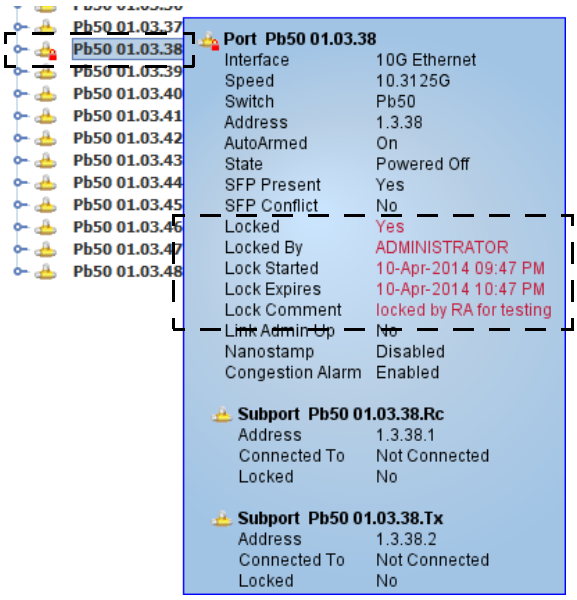
2 Select the Port Locking check-box to enable port locking.

3 Select the lock time:

- Unlimited (default) - locking time starts from the displayed current time
- 1 hour - locking time starts from the displayed current time to 1 hour later
- 1 day - locking time starts from the displayed current time to 1 day later
- Lock Until - selecting this option displays a calendar to select the expiration date/time of the lock for the selected port(s)



4 Optionally, enter information (e.g., reason for port locking) into the Comment text field (80 characters maximum). The text in the comment field is displayed when performing a hover-over on a locked port, and in the Locked Ports screen (refer to Locked Ports on page 4-45).



5 Click **OK** to save the port locking settings. A locked port icon (refer to Icon Legend Chart on page 2-45) is displayed on the port indicating the locked status.

If an already locked port is selected, the **Lock Started** field displays the date/time the lock started and the **Locked By** field displays the user who initiated the lock.

Configuring Multiple Ports on a Blade

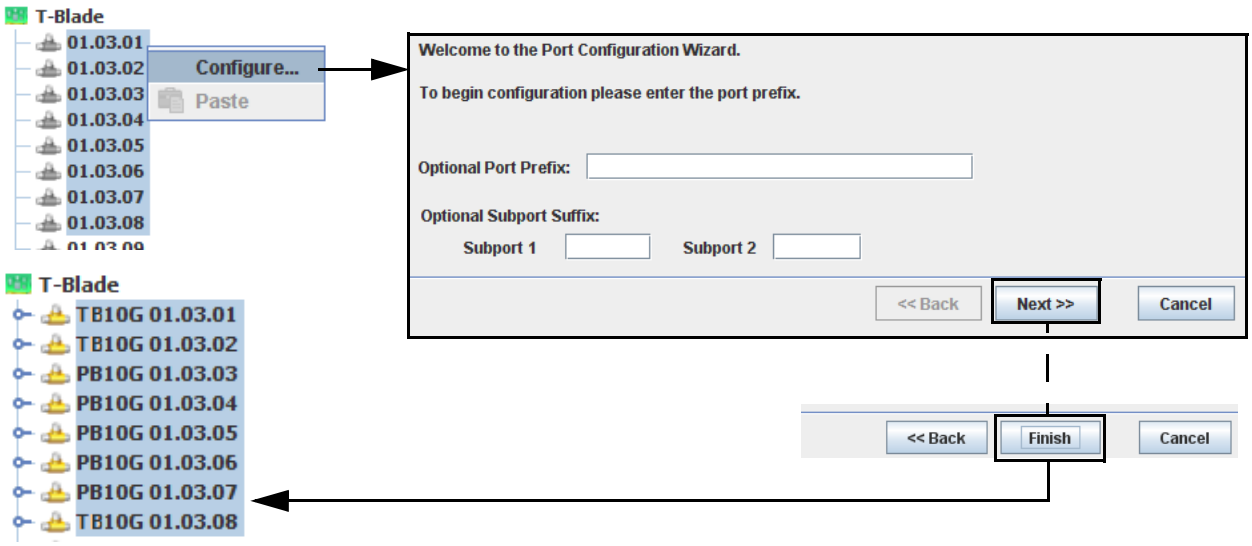
Multiple ports on a blade can be configured to the same settings in a single operation.

1. On the selected blade, from the port level, click on a port then hold down the Ctrl key and click on the remaining required ports to be configured.

Note: Selected ports must be of the same type (e.g., all normal, all test, all mirror); do not mix the port types.

2. On any of the ports selected, right-click and select **Configure**. The Port Configuration Wizard displays.
3. Optionally, enter a port prefix name in the **Optional Port Prefix:** field, and/or enter designations for Subport 1 (e.g., Tx) and Subport 2 (e.g., Rx).
   Click **Next**.
4. Refer to Configuring Blade Ports on page 3-57 for selecting the remainder of the configuration options for the multiple ports.

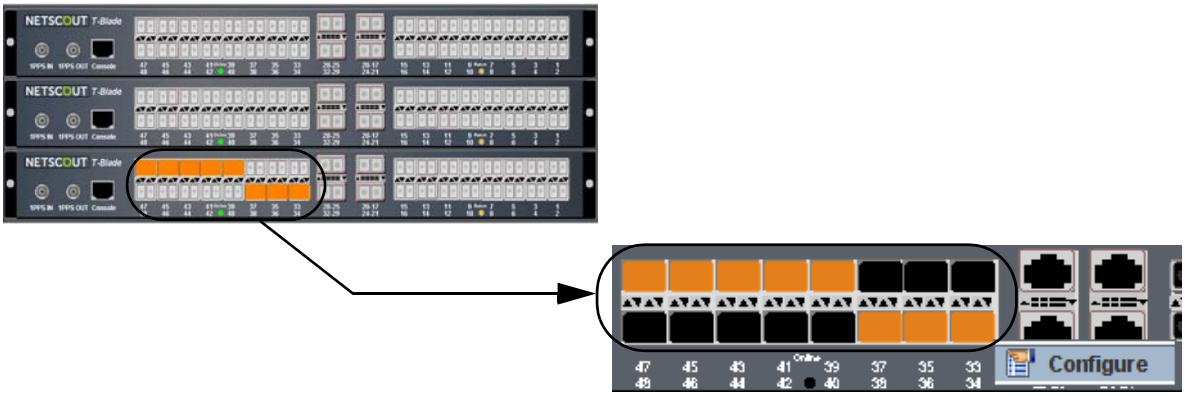
Note: Refer to Configuring Blade Ports from the Chassis View on page 3-101 for information regarding using the graphic view to configure ports.



Configuring Blade Ports from the Chassis View

Blade ports can also be configured from the Chassis View screen.

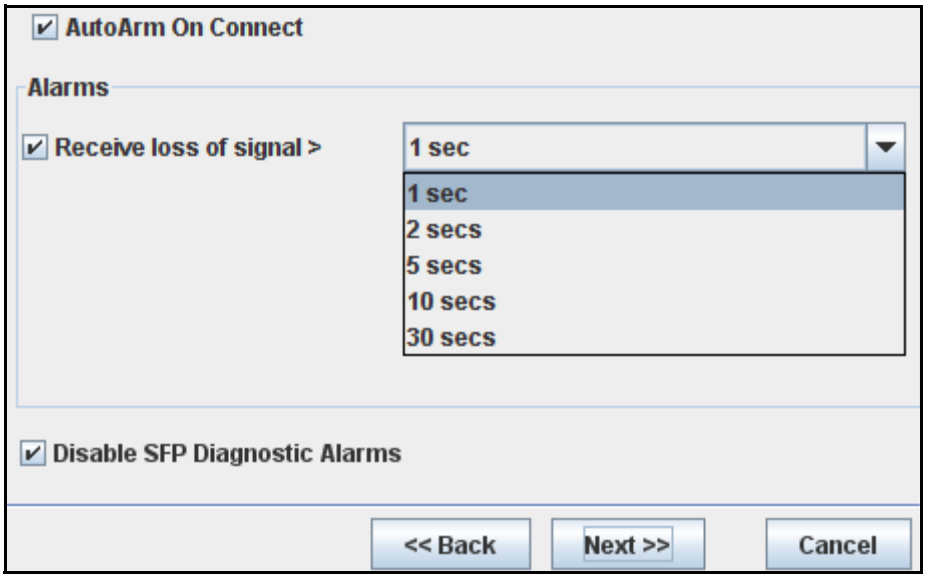
1. From the switch level, right-click on the required switch and select **View**, or from the toolbar, select the **Open Switch Graphic** icon.
2. From the switch graphic, click on the chassis where the blade is located.
3. **Single port:** Click on the required port, then right click and select **Configure**.
   Multiple ports: Hold down the Ctrl key and click on the required ports, then right click and select **Configure**.
   The Port Configuration Wizard displays.
4. **Single port:** Follow the single port configuration procedure described in Configuring Blade Ports on page 3-57.
   Multiple ports: Follow the multiple port configuration procedure described in Configuring Multiple Ports on a Blade on page 3-100.
5. Click **Finish**. The configured port(s) now display on the port level listing.



Receive Loss of Signal

The Loss of Signal (LOS) option is used to set a hold-time period (in seconds) prior to alarm generation or utilizing Automatic Circuit Protection (ACP) in a port connection. This optional time setting is selected during the port properties configuration setup procedure and prior to selecting/setting Automatic Circuit Protection.

From the port properties wizard, select the **AutoArm On Connect** checkbox. Select the **Receive Loss of Signal** checkbox then select from the drop-down listing the required LOS (1, 2, 5, 10, or 30 seconds) time.



Multi Switch Fabric

TestStream Lab Manager or TestStream Controller Server can manage multiple switches. The managed switches comprise a multi-switch fabric. In a multi-switch fabric, each switch has dedicated ports that are cabled to other switches in the fabric. These ports are called xSL (cross-switch link) ports. Users select which ports to use as xSL ports by setting the port type to 'xSL'. An xSL association is a link between two xSL ports located in different switches (physically these two ports are cabled together). When a connection is made between ports located in different switches, the TestStream server will calculate the path through the multi-switch fabric using xSL associations to connect the selected ports. A connection that has end ports located in different switches is called an xSL connection. xSL connections use xSL associations to create a circuit that spans more than one switch to create an end to end path through the multi-switch fabric.

Depending on the type of the end point switches, the TestStream Server supports one hop or multi-hop xSL connections. A one hop xSL connection uses one xSL association to create a circuit between two switches. A multi-hop xSL connection uses up to 7 xSL associations to create a circuit between two switches (i.e., the circuit may traverse through up to 6 other switches to connect the ports located in the end point switches).

TestStream Server uses 'L1 xSL Associations' for one hop xSL connections and 'xSL Trunk Associations' for multi-hop xSL connections.

xSL Configuration

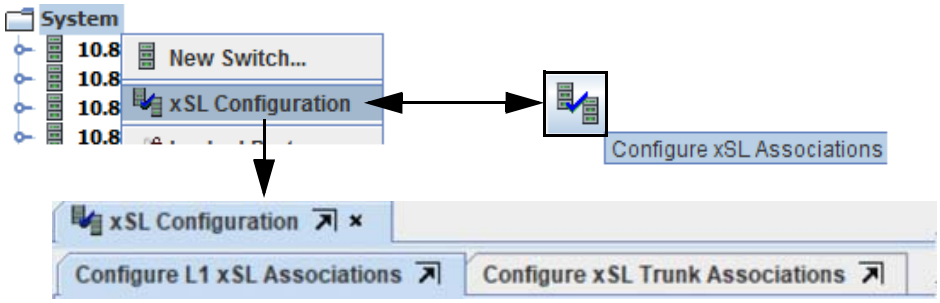
Note: L1 xSL Associations and xSL Trunk Associations require TestStream Lab Manager or TestStream Controller Server.

xSL Associated ports must be compatible (e.g., GigE > GigE, 10G > 10G).

Prior to configuring xSL associations,, verify that SFP / QSFP transceivers are installed in the blades.

A T-Blade trunk is a collection of one or more xSLs with the same origin blade and destination blade that function as a single, logical inter-switch path.

To configure xSL associations between switches, from the System tab, right-click on the System icon and select **xSL Configuration**, or from the toolbar, select the **Configure xSL Associations** icon.



L1 xSL Association Configuration

The L1 Cross-Switch Link (xSL) Associations table allows building a network of switches by specifying cross-switch links (xSL) associations among the switches. Once the xSL associations are configured, the user can select a port from each switch and TestStream Server will find an available xSL associations through the network to make the necessary end-to-end connections to connect a port to the other switch.

TestStream Lab Manager or TestStream Controller Server supports L1 xSL associations between switches for the following blades:

S-Blade /S-Blade Pro/S-Blade 64/MRV-Blade <-> S-Blade /S-Blade Pro/S-Blade 64/MRV-Blade

S-Blade /S-Blade Pro/S-Blade 64/MRV-Blade <-> OS-96/OS-192

S-Blade /S-Blade Pro/S-Blade 64/MRV-Blade <-> 3rd Party OOO

OS-96/OS-192 <-> OS-96/OS-192

OS-96/OS-192 <-> 3rd Party OOO

3rd Party OOO <-> 3rd Party OOO

Configure L1 xSL Associations

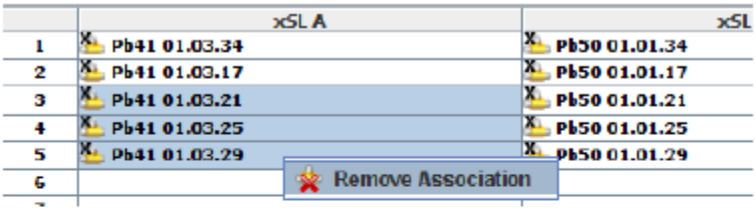
L1 xSL Associations are available for the following connections:

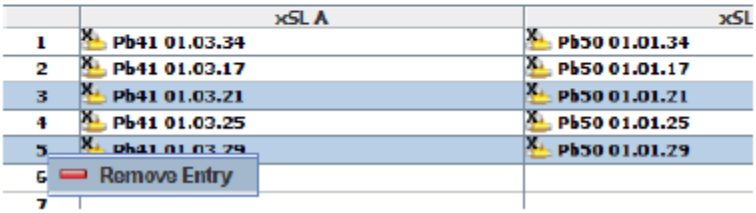
- Simplex (optical switches only)
- Duplex
- Mirror/test/multi-tap
- Multicast

Select an xSL port from one switch and place in the **xSL A** column. From another switch, select an xSL port to complete the association and place in the **xSL B** column. The total bandwidth of the xSL association is displayed in the **Max Speed** column.

L1 xSL Associations Menus

- Selecting one or more xSL cells in a column then right-clicking and selecting Remove Association allows removing multiple associations.
- Selecting one or more rows then right-clicking and selecting Remove Entry allows removal of the entire entry / association.





L1 xSL Associations Usage Examples

The following describes typical configuration examples for L1 xSL associations operation using TestStream Lab Manager or TestStream Controller Server GUI.

<u>Creating an L1 xSL connection</u>

Situation

User has two switches, named BldgA and BldgB, and wishes for data traffic received on port, TapHttp, on BldgA to be monitored by the security tool attached to port, SecMon, on BldgB.

Solution

Create an L1 xSL association between the two switches, BldgA and BldgB, and connect TapHttp to SecMon in the normal manner.

Physical Requirements

A cable connected between two ports, one each on the BldgA and BldgB switches - the cable can be added after the configuration is completed.

Configuring the xSL Ports

Using TestStream Lab Manager or TestStream Controller Server, locate the port with one end of the cable between BldgA and BldgB. Right click and select **Properties**. Name the port appropriately. For this example, Trunk1BldgA. Select xSL as the Port Type. Click **OK**. Repeat for the second port to which the cable is (or will be) connected. For this example, the second port is named, Trunk1BldgB.

CLI Usage

You can configure an xSL port through the CLI with the "ADD TO switchname [TESt|MIRror|XSl|CLone] PORt" command. While CLI can be used to configure an xSL port, there are no CLI commands to associate or disassociate xSL ports from one another to create or remove xSLs.

You can make a simplex connection through the CLI with the "CONnect [options] {PORt|PRTNum|GROup|GENerator|DEVICEPort} <source> [PORt|PRTNum|GROup|DEVICEPort] <destination>" command.

Associating the L1 xSL Ports

Open the **Configure L1 xSL Associations** tab. Drag port, Trunk1BldgA, into the "xSL A" column and drag port Trunk1BldgB into the "xSL B" column. Associating the xSL ports does not result in any physical action.

Making a Connection Across an L1 xSL Association

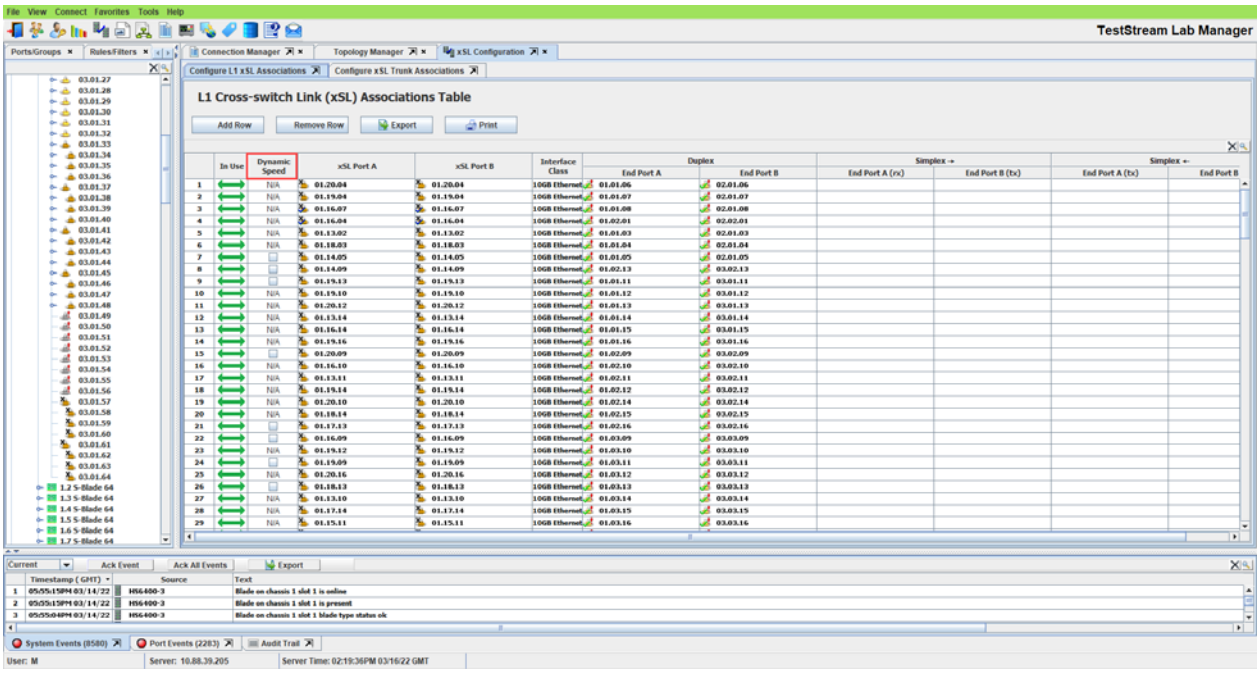
Configuring the Connection

You can now connect the TapHttp and SecMon ports using any of the usual methods. When the connection is made, the end ports will be displayed in L1 xSL Association table.

L1 xSL Dynamic Speed Configuration

The following describes how L1 xSL associations speed is dynamically configured by the TestStream Management Software based on the connection being made, thus minimizing the number of required xSL associations due to speed requirements.

To dynamically configure the L1 xSL association click the checkbox in the Dynamic Speed column of the Configure L1 xSL Associations tab.



xSL Trunk Configuration

TestStream Lab Manager supports xSL Trunk Associations between switches for the following blades:

OS-96/OS-192 <-> T-Blade

3rd Party OOO <-> T-Blade

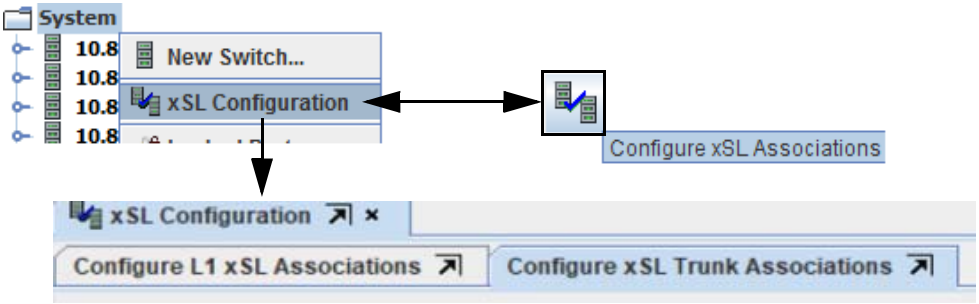
HS-3200/HS-6400 <-> T-Blade

HS-3200/HS-6400 <-> HS-3200/HS-6400

OS-96/OS-192 <-> HS-3200/HS-6400

3rd Party OOO <-> HS-3200/HS-6400

To setup xSLs trunk associations between switches, from the System tab, right-click on the System icon and select xSL Configuration, or from the toolbar, select the Configure xSL Associations icon.



Trunk xSL Associations are available for the following connections:

- Simplex
- Duplex
- Mirror/test/multi-tap (T-Blade only - any-to-many, 32x32)
- Multicast (1:32)

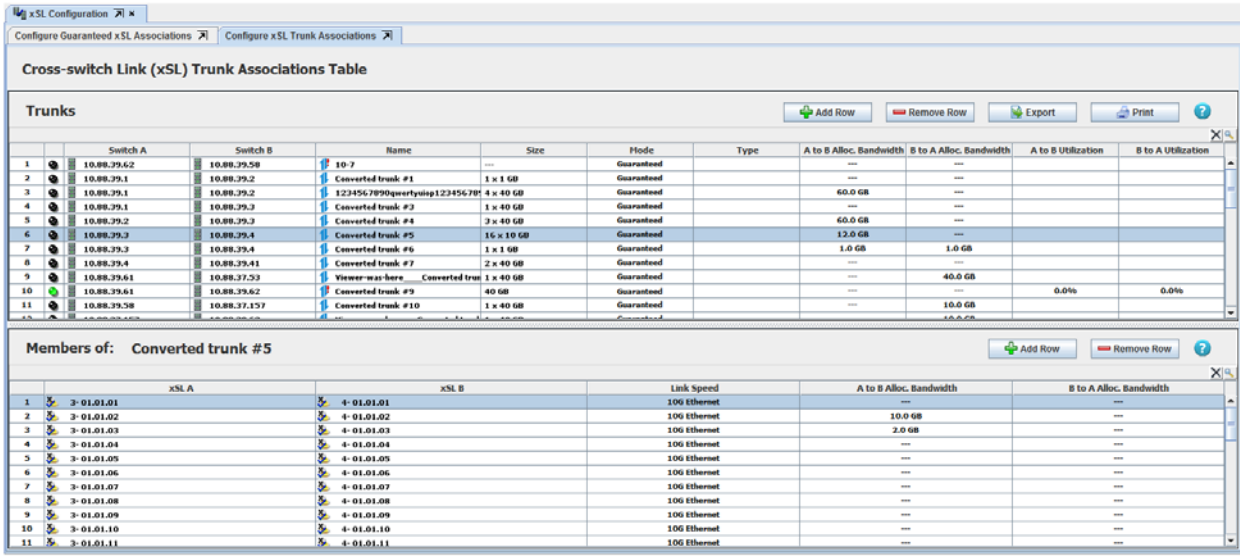
- Packet flow aggregation (T-Blade only - many-to-any, 32x32)
- Load balancing, session and equal (T-Blade only - any-to-many, 32x32)

Configure xSL Trunk Associations

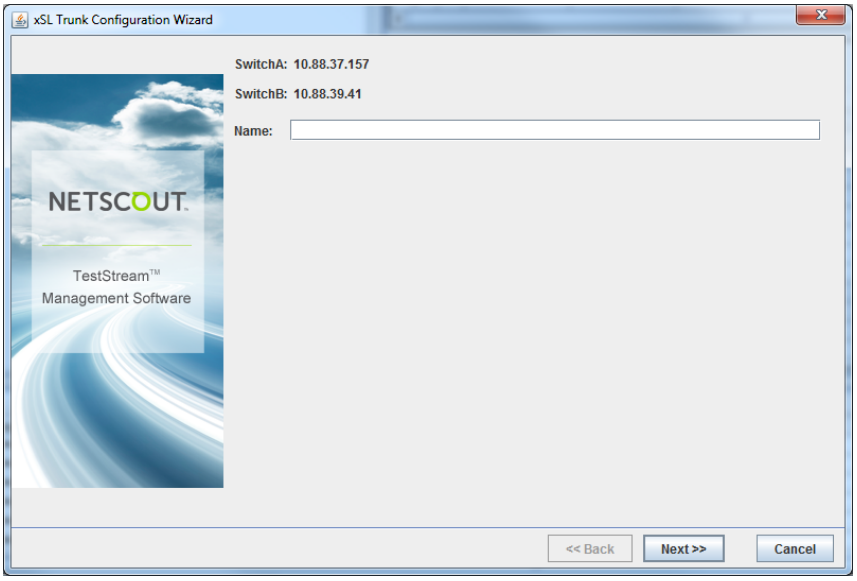
The Cross-Switch Link (xSL) Trunk Associations table displays:

- Switch-to-switch trunks
- Specific xSL Associations comprising each trunk

Each row in the Trunk Associations Table consists of an individual trunk containing one or more xSL associations.

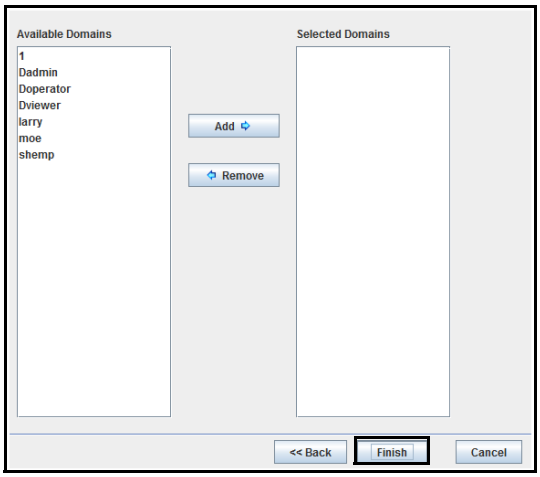


1 **Trunks Table:**
Select one switch from the System tree and place in the Switch A column. Select another switch and place in the Switch B column. The xSL Trunk Configuration Wizard screen displays.



2 Enter a name for the xSL trunk. Click **Next**

3 Select any domains to be associated to the xSL trunk (refer to Associating Domains with xSL Trunks on page 3-112). Click **Finish** to create the configured trunk.



Add xSLs to Trunks

Members Of: Table

The Cross-Switch Link (xSL) Members Table shows the xSL Associations for a selected Trunk. Administrators can add and remove xSL Associations per Trunk.

1 From the System tree, configure the appropriate Ports to be type 'xSL'.

Important: Physically cable/connect the xSL Ports that will form Associations in a Trunk.

2 Add xSL associations to the trunk:
In the Trunk Associations table, select the Trunk to populate.
Drag one or more xSL Ports from Switch A into the 'xSL A' column.
Drag one or more xSL Ports from Switch B into the 'xSL B' column.

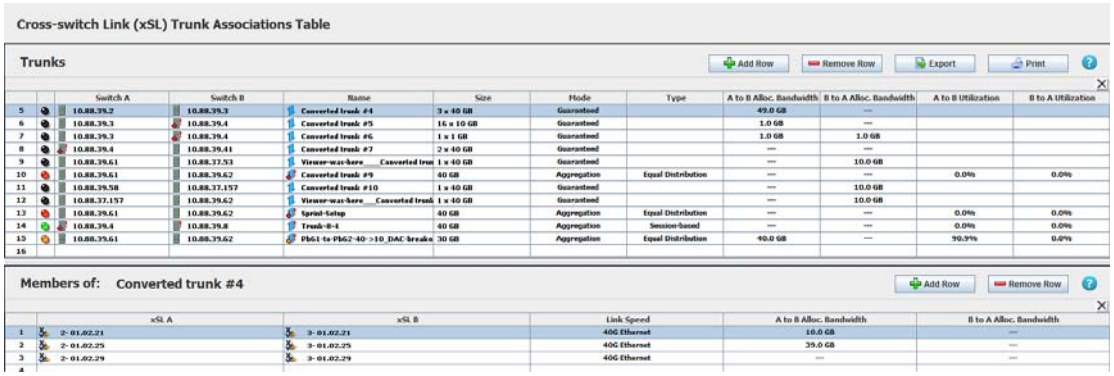
Note: All xSL ports in a trunk must:
Be the same speed.
Originate from the same blade on Switch A and terminate on the same blade on Switch B, otherwise TestStream Management will give an error for invalid combinations.

The Trunk is now ready to send traffic over the new xSL Associations.

Cross-Switch Link (xSL) Trunk Associations Table

The xSL Trunk Associations Table is comprised of two sections:

- Trunks: displays overall information on all configured trunks
- Members of: displays xSLs that are part of a selected trunk



The following columns are displayed:

Trunks

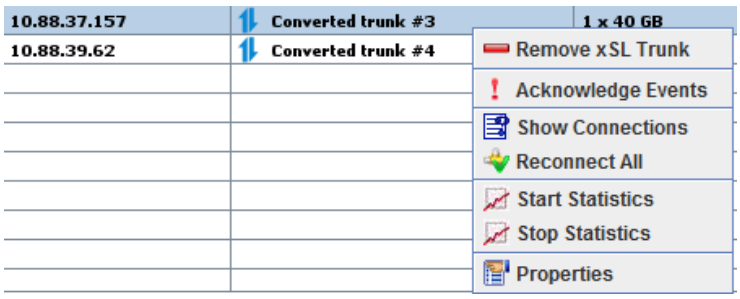
- Trunk Status - reflects the overall health of the trunk
  - Gray Indicator - Trunk contains no xSLs
  - Green Indicator - Trunk is operating properly
  - Black Indicator - Trunk is in guaranteed mode
  - Orange Indicator - Trunk has experienced:
    - Threshold alarms
    - Trunk degraded event
  - Red Indicator - Trunk has experienced:
    - Congestion alarm
    - Trunk failed event
- Switch A / Switch B - selected switches used to create a particular trunk
- Trunk Name - user defined name of the trunk
- Trunk Size:
  - Guaranteed Trunks - presented in the format (A x B) where A is the number of xSL links and B is the port size
  - Aggregation Trunks - the total size of the trunk
- Mode – current operating mode of the trunk
- Type – if the trunk is in aggregation mode, the load distribution type being used
- A to B Allocation Bandwidth:
  - Guaranteed Trunks – A sum of the input ports' full bandwidth of the connections using the trunk. The trunk is not aggregated despite how this value is presented. Guaranteed trunks are just a group of independent xSL links.
  - Aggregation Trunks – A sum the total bandwidth based on the input port connections for the whole trunk
- B to A Allocation Bandwidth – Same as A to B Allocation, only in the opposite direction
- A to B Utilization:
  - Guaranteed Trunks – not supported, value is empty
  - Aggregation Trunks - utilization from the past 5 seconds for traffic originating on switch A
- B to A Utilization – Same as A to B Utilization, only in the opposite direction

Members of:

- xSL A / xSL B - xSLs selected from each switch
- Link Speed - The total bandwidth of the xSL connections
- A to B Alloc. Bandwidth (applicable to Guaranteed trunks only) - amount of bandwidth associated with connections using the xSL association in the direction from xSL A to xSL B
- B to A Alloc. Bandwidth - Same as A to B Alloc. Bandwidth, only in the opposite direction

xSL Trunk Associations Table Menus

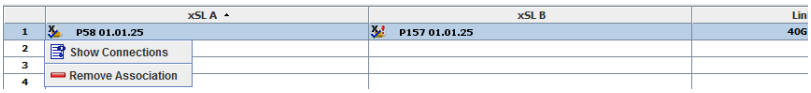
Right clicking on an xSL Trunk Associations Table row displays the following menu:

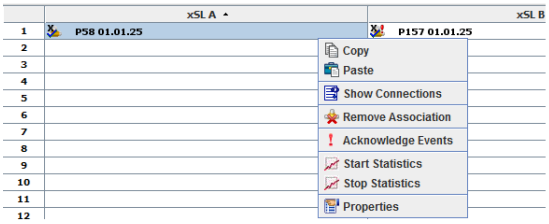


- Remove xSL Trunk - Remove selected trunk between switches.
- Acknowledge Events - Acknowledges the following events:
  - Congestion Alarms
  - Threshold Alarms
- Show Connections - Displays all of the connections routed through the trunk, grouped by direction.
- Reconnect / Disconnect All - Reconciles the connections of a selected trunk.
- Start / Stop Statistics - Begin / end statistics recording for the ports within the trunk.
- Properties - Refer to xSL Trunk Properties on page 3-110.

Members Of: Menus

Right clicking on a row or an individual cell in the Association table displays either of the following menus:





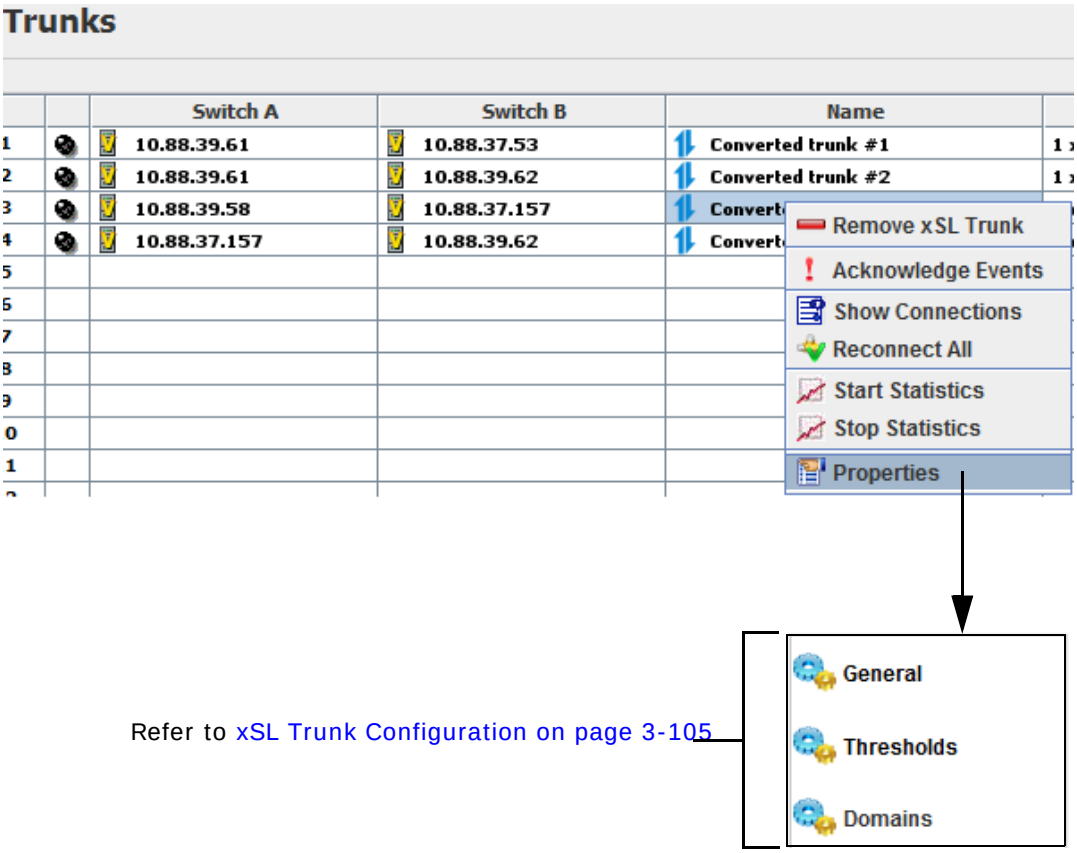
- Copy / Paste - Copies the configuration setting of a defined xSL port and assigns the configuration to another xSL port.
- Show Connections - Displays all of the connections routed through the trunk, grouped by direction.
- Remove Association - Remove xSL associations in a trunk.
- Acknowledge Events - Acknowledges all alarms pertaining to that port.
- Start / Stop Statistics - Begin / end statistics recording.
- Properties - Refer to Port Properties on page 3-170.

xSL Trunk Properties

To view xSL trunk configuration information:

1 From the xSL Trunk Associations Table, select and right click on a trunk from the Name column.

2 Select **Properties**. The xSL Trunk Properties window displays.



Refer to xSL Trunk Configuration on page 3-105

xSL Trunk Usage Examples

The following describes typical configuration examples for xSL Trunk operation using the TestStream Lab Manager or TestStream Controller Server GUI.

Creating an xSL Trunk

Situation

User has two switches, named BldgA and BldgB, and wishes for data traffic received on port, TapHttp, on BldgA to be monitored by the security tool attached to port, SecMon, on BldgB.

Solution

Create an xSL trunk between the two switches, BldgA and BldgB, and associate TapHttp with or without a filter (T-Blade only) to SecMon in the normal manner.

Physical Requirements

A cable connected between two ports, one each on the BldgA and BldgB switches - the cable can be added after the configuration is completed.

Configuring the xSL Ports

Using TestStream Lab Manager, locate the port with one end of the cable between BldgA and BldgB. Right click and select Properties. Name the port appropriately. For this example, Trunk1BldgA. Select xSL as the Port Type. Click OK. Repeat for the second port to which the cable is (or will be) connected. For this example, the second port is named, Trunk1BldgB. If the cable is not installed, you should expect the same two port events as the first xSL port.

CLI Usage

You can configure an xSL port through the CLI with the "ADD TO switchname [TESt|MIRror|XSl|CLone] PORt".

While CLI can be used to configure an xSL port, there are no CLI commands to associate or disassociate xSL ports from one another to create or remove xSLs.

Associating the xSL Ports

Open the Configure xSL Associations tab. Select "Configure xSL Trunk Association" tab. Drag switches BldgA and BldgB into "Switch A" and "Switch B" columns respectivly to create a trunk. Then drag port, Trunk1BldgA, into the "xSL A" column and drag port Trunk1BldgB into the "xSL B" column. Associating the xSL ports does not result in any physical action.

Making a Connection Across an xSL

Configuring the Connection

You can now associate the TapHttp and SecMon ports using any of the usual methods. When the association is activated, the "A to B Alloc. Bandwidth" and "B to A Alloc. Bandwidth" columns should reflect the bandwidth of the ingress port in the connection. If you made a simplex connection, only one column will have a value; a duplex connection will have values in both.

Associating Domains with xSL Trunks

A system administrator has the option to place trunks into one or more domains. This is typically done to partition part of a network to reserve xSL trunks for non-administrative users so that the trunks are available to the users as required.

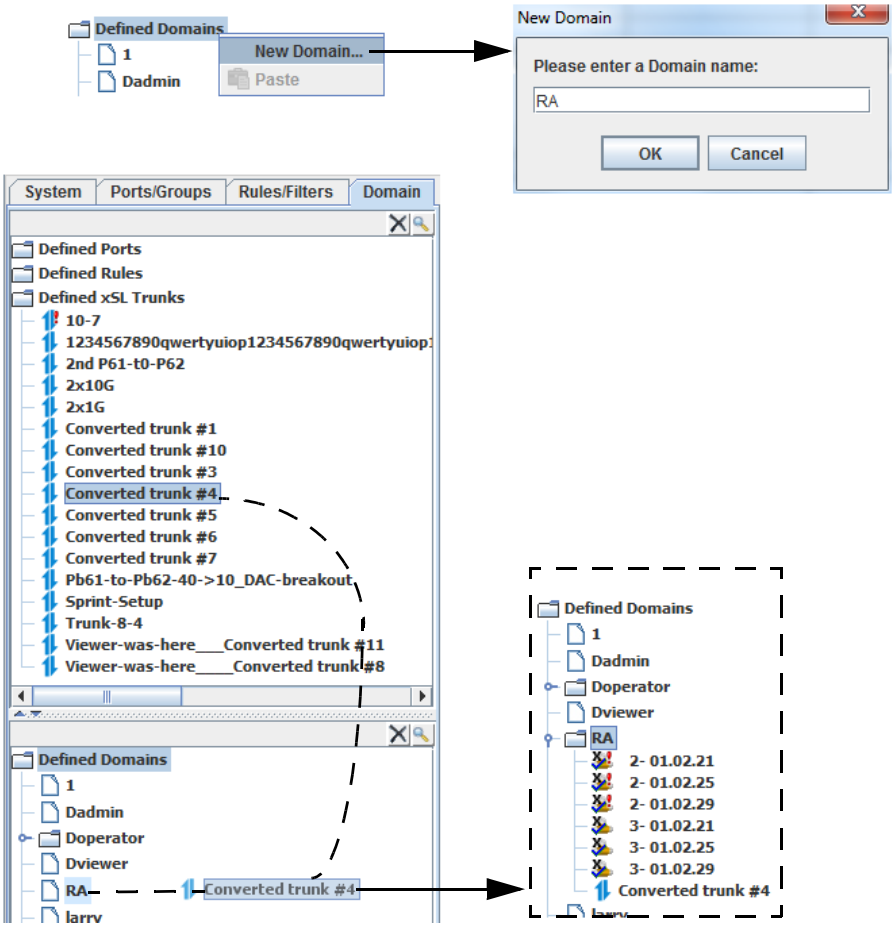
Adding a Trunk to a Domain

Note: Refer to Domain Restrictions on page 3-114 concerning changing domain membership on an xSL trunk.

---

1. If the type change is allowed with connections active, proceed to step 2.

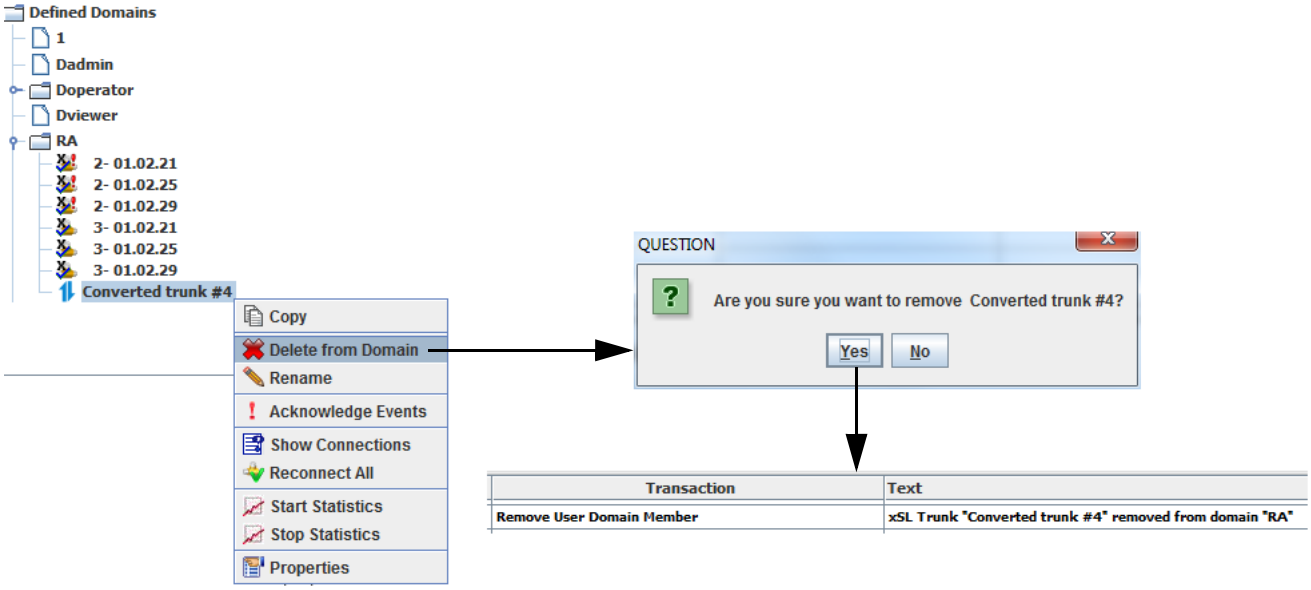
   If changing the type requires stopping traffic:
   - Determine the connections that are being made across the trunk.
   - Deactivate the required connections.
2. Click on the Domains tab.
3. If necessary, create a new domain folder for your requirements.
4. Double click on the **Defined xSL Trunks** folder, select and drag the desired trunk into the appropriate domain.
   - If change is permitted, the trunk is reconfigured and connections are re-established.
   - If the change is not permitted, an error is displayed.


Defined Domains
1
Dadmin
New Domain...
Paste
New Domain
Please enter a Domain name:
RA
OK
Cancel
System
Ports/Groups
Rules/Filters
Domain
Defined Ports
Defined Rules
Defined xSL Trunks
10-7
1234567890qwertyuiop1234567890qwertyuiop1
2nd P61-t0-P62
2x10G
2x1G
Converted trunk #1
Converted trunk #10
Converted trunk #3
Converted trunk #4
Converted trunk #5
Converted trunk #6
Converted trunk #7
Pb61-to-Pb62-40->10_DAC-breakout
Sprint-Setup
Trunk-8-4
Viewer-was-here___Converted trunk #11
Viewer-was-here____Converted trunk #8
Defined Domains
1
Dadmin
Doperator
Dviewer
RA
Converted trunk #4
Defined Domains
1
Dadmin
Doperator
Dviewer
RA
2- 01.02.21
2- 01.02.25
2- 01.02.29
3- 01.02.21
3- 01.02.25
3- 01.02.29
Converted trunk #4

Removing a Trunk from a Domain

Note: Traffic must be stopped on a trunk before it can be removed from a domain.

1. Determine the connections that are being made across the trunk.
2. Deactivate the required connections.
3. Click on the Domains tab.
4. Under Defined Domains, open the desired domain, select one or more trunks to remove and right click on the trunk (s) to delete.
5. Right click and select **Delete from Domain**. All associated xSLs/Trunks are removed from the domain.



Domain Restrictions

As an Administrator

- Creating/modifying an xSL trunk
  - When an xSL trunk domain membership is changed, all of the xSL ports in the trunk are set to match. This includes adding to and deleting from a domain.
  - Any xSL trunk property can be changed. Only administrators can change traffic affecting properties (session-based/equal-distribution).
  - When changing the type of a trunk (guaranteed/aggregation) or removing a trunk from a domain, the user must deactivate or move the connections through the trunk first.
- Adding ports to an xSL trunk
  - If an xSL port has no domain, it inherits the trunk's domain(s).
  - If an xSL port has a domain, it must match all trunk domains exactly or an error is given.
- Removing ports from an xSL trunk
  - Removing a port from a trunk does not automatically remove the port from any domains. That must be done as a separate step on the port.
- Adding an xSL trunk to a domain or additional domains is not restricted and does not affect live traffic.
  - All of the xSL ports in the trunk are automatically added to the additional domain(s).
  - Once an xSL port is in a trunk, its domain cannot be modified directly; it must be modified by modifying the trunk the port is in.

- Removing an xSL trunk from a domain.
  - To remove a trunk from a domain all connections through the trunk must first be deactivated or moved.
  - All of the xSL ports in the trunk are automatically updated to match the domain membership of the trunk.
  - The trunk may be removed from its last domain. The trunk and all its ports will then have no membership in a domain.

As a Non-administrator User

- Creating or deleting any xSL trunks is not allowed.
- Adding or removing xSL ports from a trunk is not allowed.
- Changing the domain of a trunk, the domain of its ports, or modifying any traffic-affecting properties of a trunk (aggregation/guaranteed, session-based/equal-distribution) is not allowed.
- Changing the trunk alarm settings if the trunk is in the users domain or if the user has no domain is allowed.

Connection Status of a Topology

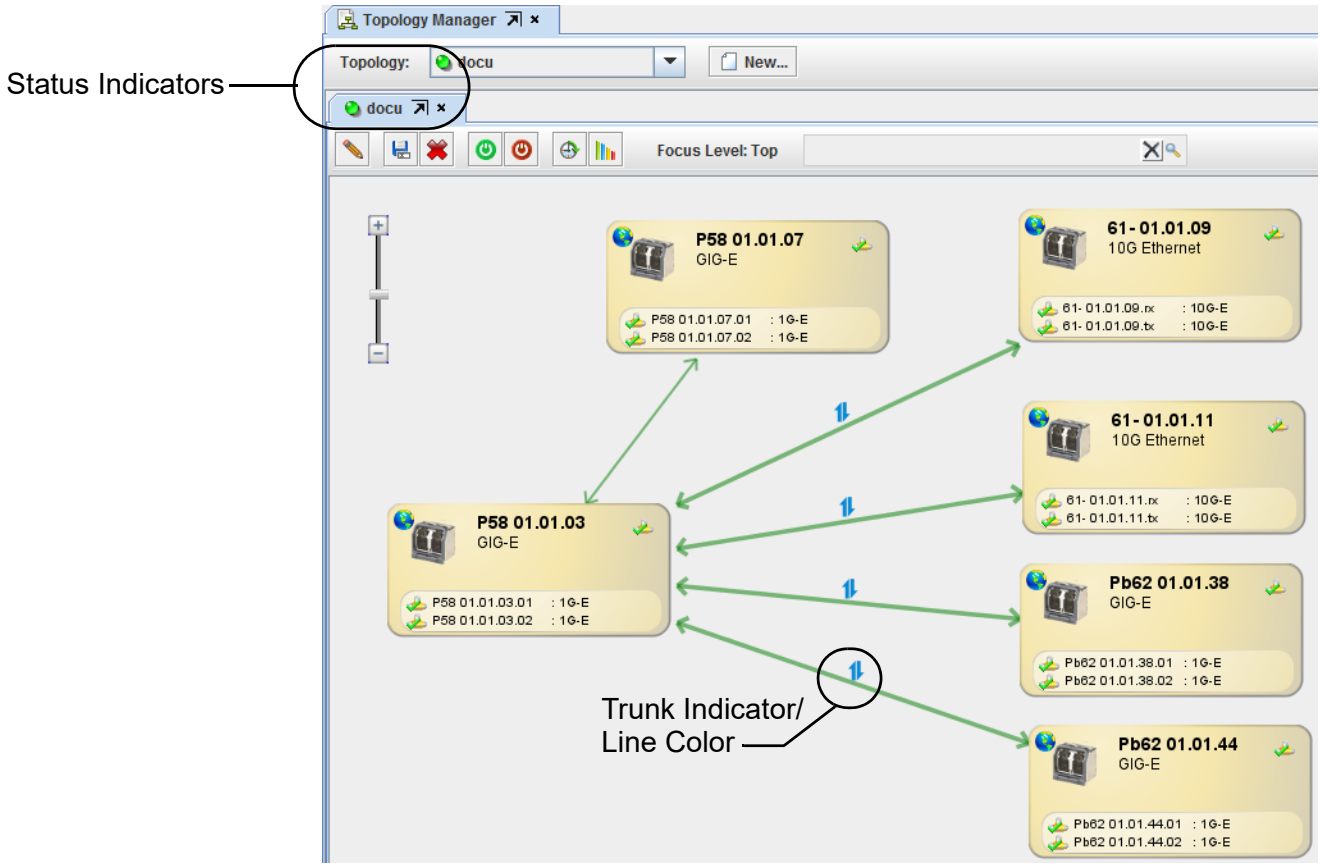
To determine the status of the connections in a topology:

Observe the status indicators next to the Topology name field in either the Topology Manager tab or the drop down menu.

The color of the live status indicator and connection line match with the color indicating that one or more connections in the topology are actively occurring:

Color	Conditions
Red: Packet Loss	xSL trunks in a failed state xSL trunk experiencing congestion drops A regular port connection is link down Note: In this condition, packets are being lost.
Orange: Warning	xSL trunks in a degraded state xSL trunk experiencing traffic above the high threshold value Note: In this condition, no packets are being lost.
Yellow: Partially Connected	Topology is partially connected All trunks are in a normal state
Green: Fully Connected	Topology is fully connected All trunks are in a normal state
Dark (Gray): Not Connected	Nothing on the topology is connected

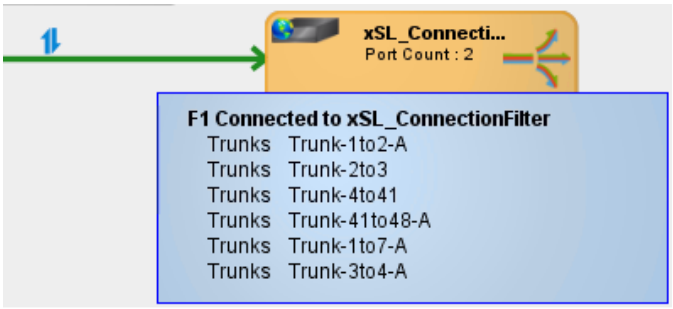
Connections that are affected by alarms show a red exclamation mark next to the trunk icon.



Note:
The topology status does not reflect the status of the backplane(s).

The association line can also be blue, indicating the connection is not activated. This status is independent of the xSL/trunk status.

Note: Tool-tip displays of a selected trunk may not show the correct path order of links in a trunk.



Multi-Hop Layer 1 xSL Connectivity

TestStream Management supports multi-hop Layer 1 xSL trunk connectivity between the following:

- HS-3200/HS-6400 and 39xx
- 39xx and39xx
- 39xx and HS-3200/HS-6400
- 39xx and O-Blade/OS-96/OS-192/Polatis
- HS-3200/HS-6400 and HS-3200/HS-6400
- O-Blade/OS-96/OS-192/Polatis and 39xx
- O-Blade/OS-96/OS-192/Polatis and HS-3200/HS-6400
- O-Blade/OS-96/OS-192/Polatis and O-Blade/OS-96/OS-192/Polatis

Members of the trunk must have one endpoint in an HS-3200 switch and one endpoint in a 3900 switch or OS-96/192 switch, both endpoints in HS-3200 switches, or both endpoints in OS-96/192 switches.

As a L1 xSL Trunk, each member supports one connection. The speed of the connected ports must match the xSL association ports speed. HS-3200 ports must be configured as L1 ports.

Supported Endpoints

Supported endpoints for xSL Trunk Associations include:

- HS-3200 to S-Blade

  When creating a Layer 1 xSL Trunk member with one end in an S-Blade and the other end in a HS-3200 switch, only 10G ETH is supported, requiring that the HS-3200 port use a breakout cable.
  Options for the breakout cable include:

  - MTP to 4 LC multimode
  - MTP to 4 LC singlemode
  - 40G QSFP+ to 4x10G SFP+ Passive Direct Attach Copper
  - 40G QSFP to 4x10G SFP+ Active Optical Cable

- HS-3200 to S-Blade Pro

  When creating a Layer 1 xSL Trunk member with one end in an S-Blade Pro and the other end in a HS-3200 switch, only 10G ETH and 40G ETH are supported.

- HS-3200 to OS-96/OS-192

  When creating a Layer 1 xSL Trunk member with one end in an OS-06/OS-192 and the other end in a HS-3200 switch, all speeds are supported. Since the OS-96/OS-192 only support single-mode, the following must be observed:

  - 100G: use 100GBase-LR4 or 100G CWDM4. HS-3200 ports 3-30 accept transceivers up to class 4 (3.5 watts maximum power consumption). If the transceiver power consumption is higher, it must use ports 1,2,31 or 32 of the HS-3200.
  - 40G: use 40G Ethernet LM4, 40GBase-LR4 or 40GBase-ER4. These transceivers may have the same power consumption limitation as the 100G ones.
  - 50G: same case as 100G.
  - 25G: use breakout cable MTP to 4 LC singlemode.
  - 10G: use breakout cable MTP to 4 LC singlemode

- OS-96/OS-192 to OS-96/OS-192

  When creating a Layer 1 xSL Trunk member with both ends in OS-06/OS-192, all speeds are supported.

xSL Configuration

From the toolbar, click on the Configure xSL Associations icon, (refer to xSL Trunk Configuration on page 3-105).

For a 1 hop Layer 1 to Layer 1 xSL involving S-Blade, S-Blade Pro, OS-96 or OS-192, select the **Configure Guaranteed xSL Associations** tab.

For a multi-hop L1 xSL association, select the **Configure xSL Trunk Association** tab.

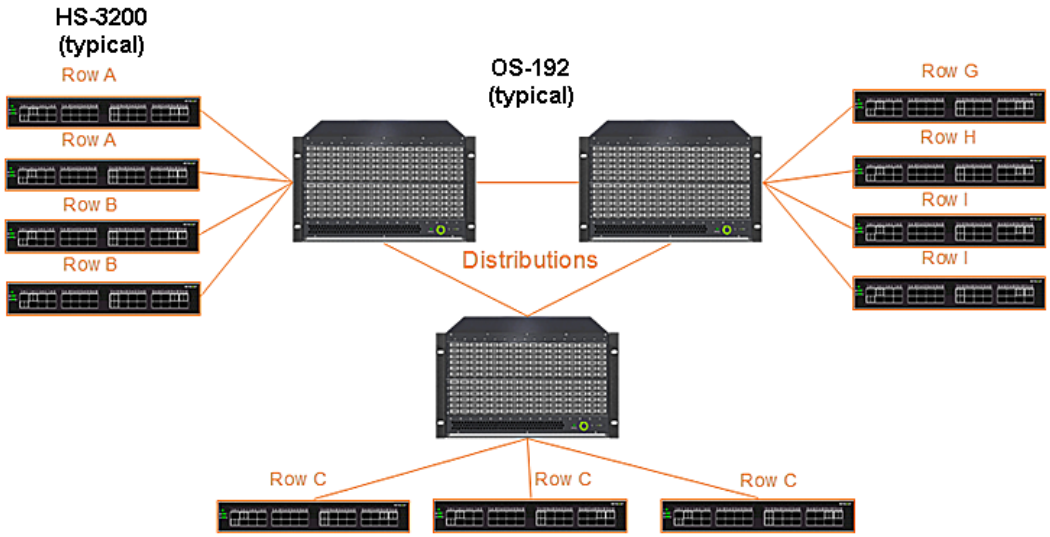
When assigning switches to the Switch A and Switch B columns, the following switch type combinations are supported:

Switch A	Switch B
HS-3200/HS-6400	39xx
39xx	39xx
39xx	HS-3200/HS-6400
39xx	O-Blade/OS-96/OS-192/Polatis
HS-3200/HS-6400	HS-3200/HS-6400
39xx	O-Blade/OS-96/OS-192/Polatis
HS-3200/HS-6400	O-Blade/OS-96/OS-192/Polatis
O-Blade/OS-96/OS-192/Polatis	HS-3200/HS-6400
O-Blade/OS-96/OS-192/Polatis	O-Blade/OS-96/OS-192/Polatis

When assigning ports to the xSL A and xSL B columns, they must belong to the corresponding Switch A and Switch B, and for the HS-3200/HS-6400, be configured as a Layer 1 port.

Multi-Hop Connectivity Topology Example

This example utilizes HS-3200 and OS-192 switches. Mulrti-hop allows the switches to make connections from any HS-3200 to any HS-3200 using multi-hop Layer 1 xSLs.



Scaling the Layer 1 (mix of HS-3200 and OS-192 Switches for Distribution)

- Maximum of 4 hops - electrical / mechanical mix
- 3 or more distributions (scales up/out)
- 22 posts usable per switch 40/100G (10 ports for interconnection)
- 6x40G and 4x100G links between each switch to distribution
- 15 switches per distribution (42 ports for distribution interlinks)
- Up to 45 Layer 1 HS-3200 switches (expandable with more distributions)
- 21 interlinks between distributions (14 40G, 7 100G)

Simplex Layer 1 xSL Connectivity

Layer 1 xSLs connectivity provides support for subport connections (simplex connections) for optical switches only.

Note: Optical ports only support the 'normal' and 'xSL' port types.

Connections

Connections of optical subports belonging to different optical switches can be made using the REST API, the CLI and the GUI Client. The connected ports can be members of a group or mapped to a device port.

REST API

The following command can be used to make a simplex connection:

```
POST /api/teststream/v1/topologies/<topology_name>/commands/connect
```

Refer to TestStream Restful API for details.

Note: The request body must have the 'connection type' set to "simplex".

CLI

The following commands can be used to make a simplex connection:

Usage: **CON**nect [options] {**POR**t|**PRTN**um|**GRO**up|**GEN**erator|**DEVICEP**ort} <source> [**POR**t|**PRTN**um|**GRO**up|**DEVICEP**ort] <destination>

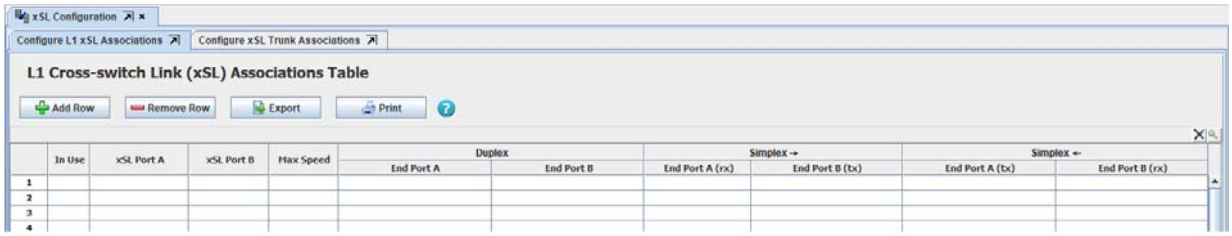
Refer to Command Line Interface Commands for details.

GUI

In the GUI client, both the 'Connection Manager' and the 'Topology Manager' can be used to make connections of optical subports belonging to different optical switches.

GUI

The 'Configure L1 xSL Associations' tab of the 'xSL Configuration' application displays simplex connections.



If the xSL association is used for a duplex connection, the 'Duplex' columns will be populated with the connection information.

Duplex	
End Port A	End Port B

If the xSL association is used for one or two simplex connections, the 'Simplex' columns will be populated. Note that there are two sets of 'Simplex' columns - one for each direction (A--> B and B--> A).

Simplex →		Simplex ←	
End Port A (rx)	End Port B (tx)	End Port A (tx)	End Port B (rx)

The 'In Use' column reflects the xSL Association directions being used by connections. For a duplex connection:

	In Use	xSL Port A	xSL Port B	Max Speed	Duplex	
					End Port A	End Port B
1	⟷	oA- 01.01.95	oB- 01.01.95	Optical	oA- 01.01.01	oB- 01.01.01

The 'In Use' column for a simplex connection (A -- > B):

	In Use	xSL Port A	xSL Port B	Max Speed
1		oA- 01.01.95	oB- 01.01.95	Optical
2	→	oA- 01.01.96	oB- 01.01.96	Optical

Simplex →		Simplex ←	
End Port A (rx)	End Port B (tx)	End Port A (tx)	End Port B (rx)
oA- 01.01.02.rx	oB- 01.01.02.tx		

The 'In Use' column for a simplex connection (B -- > A):

	In Use	xSL Port A	xSL Port B	Max Speed
1	←	oA- 01.01.95	oB- 01.01.95	Optical

Simplex →		Simplex ←	
End Port A (rx)	End Port B (tx)	End Port A (tx)	End Port B (rx)
		oA- 01.01.03.tx	oB- 01.01.03.rx

The 'In Use' column for 2 simplex connections (A -- > B, B -- > A):

	In Use	xSL Port A	xSL Port B	Max Speed
1	⇄	oA- 01.01.95	oB- 01.01.95	Optical

Simplex →		Simplex ←	
End Port A (rx)	End Port B (tx)	End Port A (tx)	End Port B (rx)
oA- 01.01.02.rx	oB- 01.01.02.tx	oA- 01.01.03.tx	oB- 01.01.03.rx

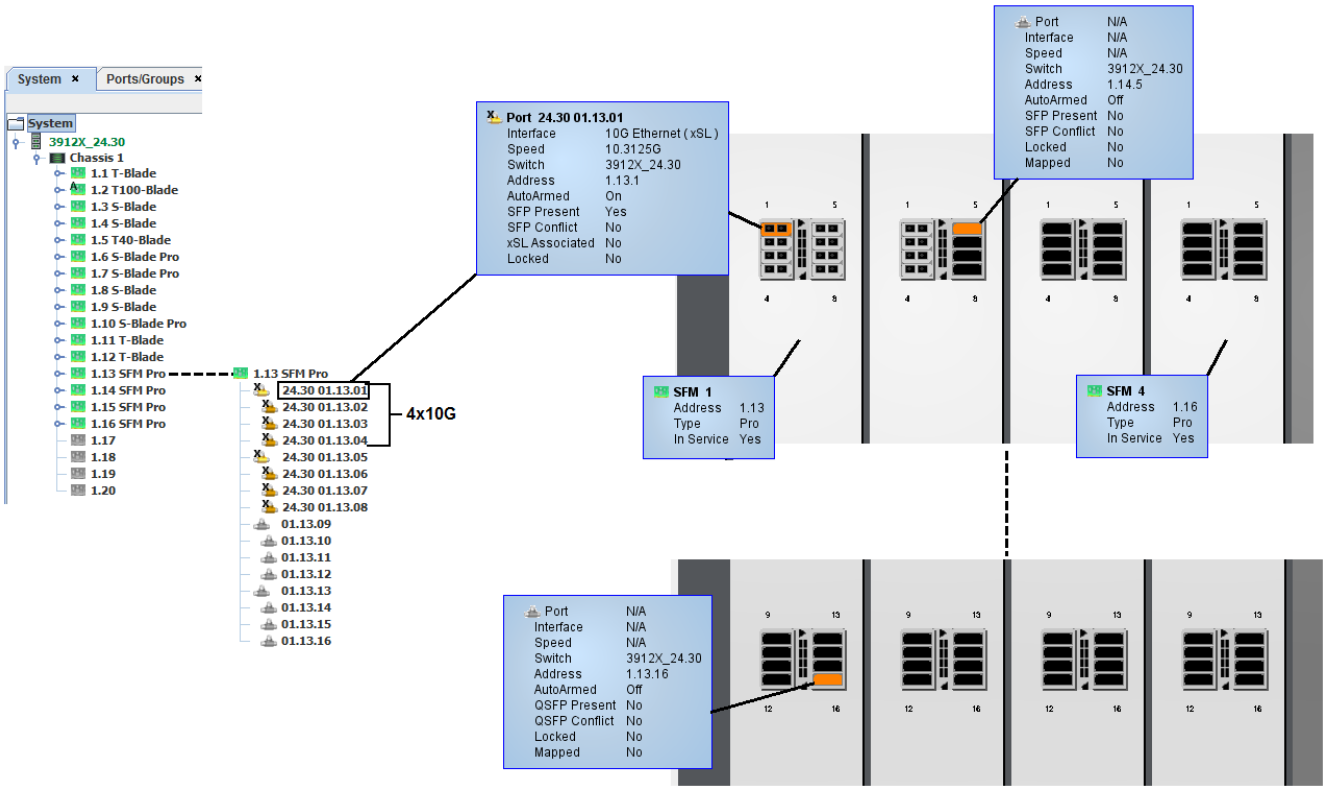
SFM Pro Trunking (xSL Configuration)

Four QSFP ports on the SFM Pro are available for use as xSL ports. These ports support running as 4x10Gb or 4x1Gb (each lane speed can be independently set as 10Gb or 1Gb) for a total of 16 ports with speed 10Gb or 1Gb. As xSL ports they can only be used in the 'Configure Guaranteed xSL Associations' table.

Defined SFM Pro ports are listed under the System and Ports/Groups tabs as xSL ports. The 3912 rear view switch graphic displays the SFM Pro ports as QSFP modules.

3912 SFM Pro slots are displayed in the System tree as ports 13 through 20. Each SFM Pro module, when expanded, displays 4 QSFP ports in a 4x10G configuration.

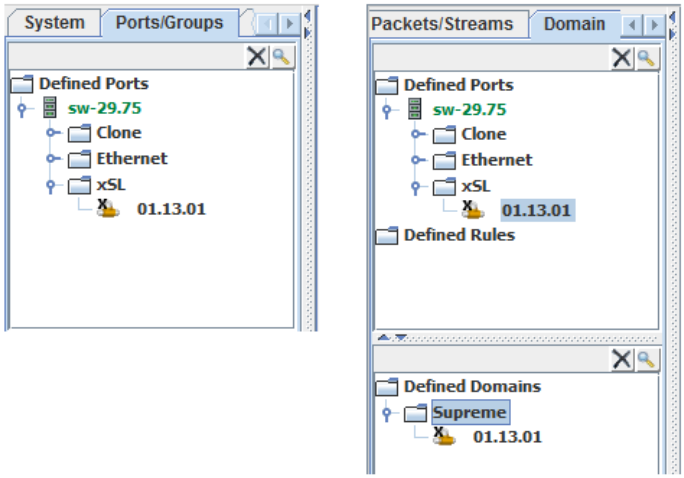
If auto discrepancy is enabled on the 3912 (refer to Adding a Switch on page 3-2), when a transceiver is installed into an SFM Pro module, the corresponding port is automatically configured based on the transceiver type.



Port/Groups and Domains

Defined SFM-Pro ports become part of the xSL Defined Ports under the Ports/Groups tab.

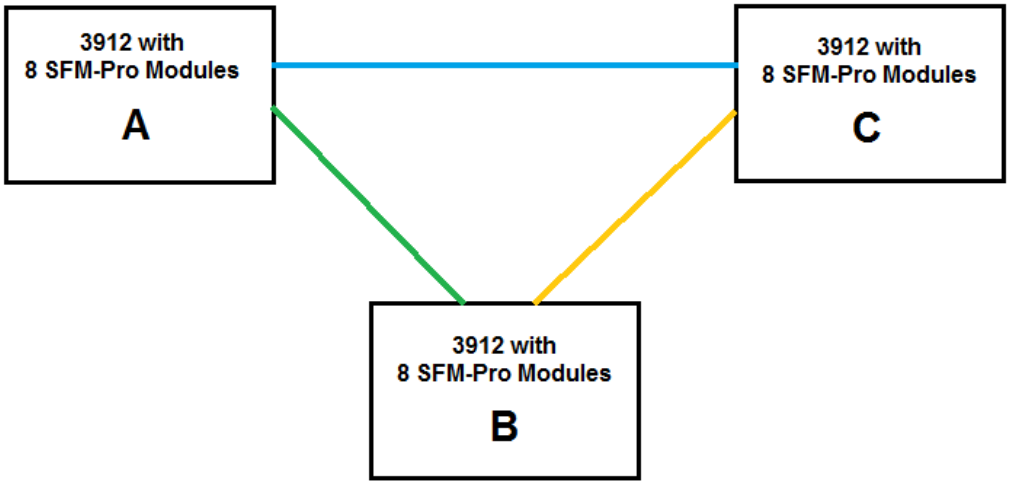
Defined SFM-Pro ports can be added to domains. In addition you can add xSL Trunks to domains.



Making xSL Connections

TestStream Management supports 1 hop xSL connections using the SFM Pro trunking feature in the same way as it is currently accomplished in any 3900 to 3900 connection. You can create Guaranteed Cross-switch Link (xSL) Associations, then utilize either the Connection Manager or Topology Manager to connect the required ports (3900 – 3900, 3900 - OS-96/OS-192).

The following example shows a possible topology that can be built using this feature.



In this topology, three (3) 3912 switches each containing 8 SFM-Pro modules are cabled together in a mesh network. From each SFM-Pro in the 3912s, 80G are connected to each of the other 3912 switches. This way a 640G bandwidth is available between any 2 switches.

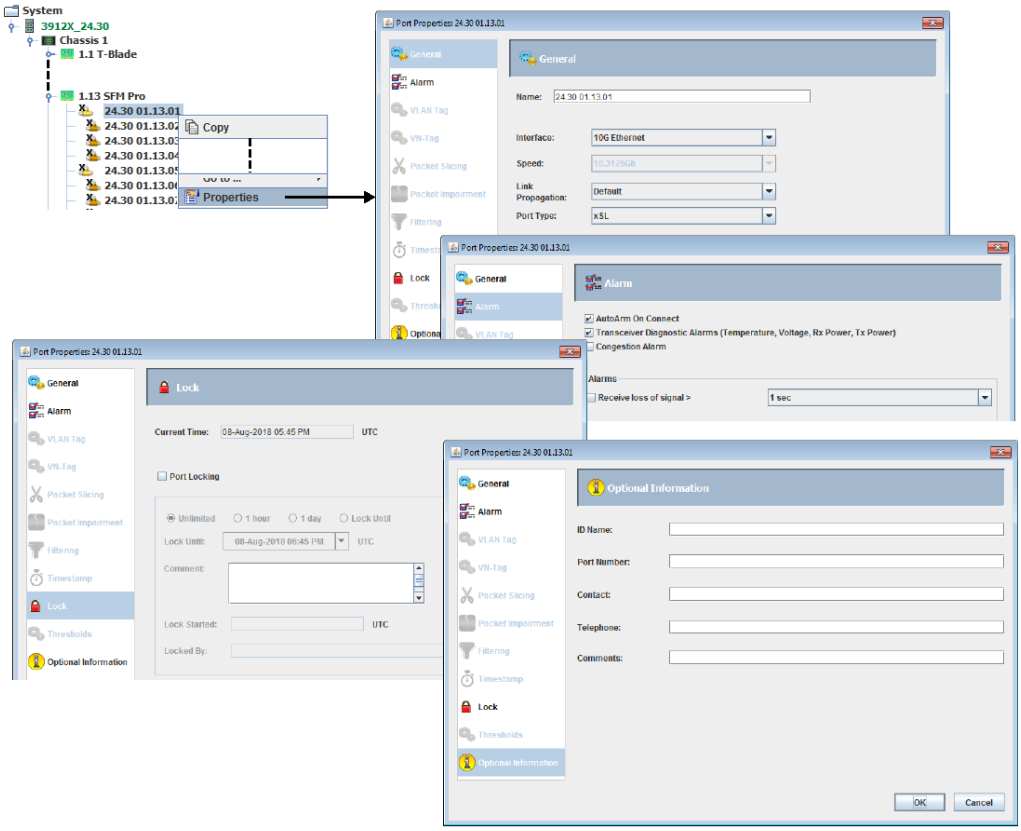
Configure SFM Pro Ports

When you install a QSFP into one of the SFM Pro ports, the installed QSFP is automatically recognized. If required, you can reconfigure the QSFP ports through Port Properties.

From the System or Ports/Groups view, right-click on a defined SFM Pro port and select **Properties**. The Port Properties window displays.

The SFM Pro QSFP has the following port configuration tabs (refer to Revising Configuration Settings on a Blade Port on page 3-132):

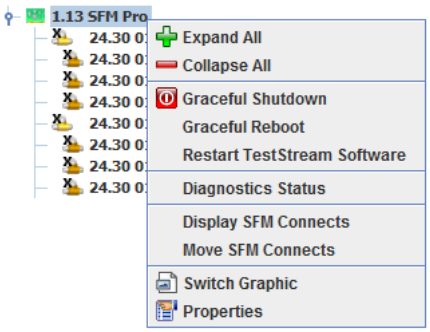
- General: Port Type can only be set to xSL
- Alarm
- Lock
- Optional Information



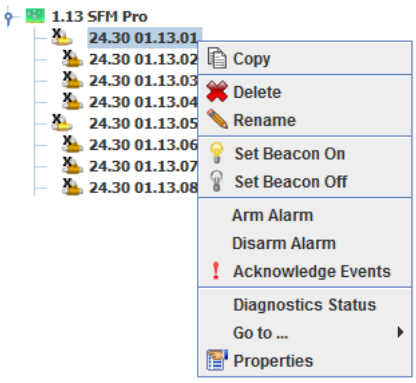
SFM Pro Blade / Port Menus

Right clicking on an SFM Pro blade or port displays the following menus:

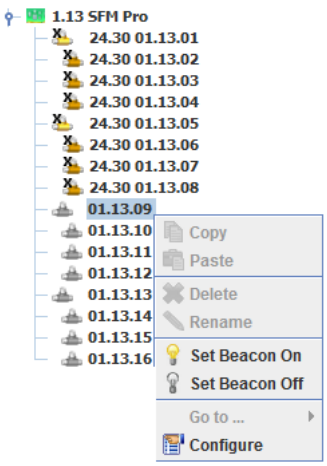
SFM Pro Blade



SFM Pro Defined Port



SFM Pro Undefined Port



SFM Pro Blade

- Expand All / Collapse All - Maximizes / minimizes the port and subport level views.
- Graceful Shutdown - Refer to Graceful Shutdown on page 3-160.
- Graceful Reboot - Allows a user (with Administrator security level) to reboot the selected blade; all services running on the blade are stopped avoiding any system corruption.
- Restart TestStream Software - Allows a user (with Administrator security level) to restart TestStream Management Software on the selected blade.
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.
- Display SFM Connects - Allows selecting an SFM and displaying all of the connections going through the SFM.
- Move SFM Connects - Allows selecting then moving backplane connections out of an SFM (e.g., for servicing purposes). The connections from the selected SFM are disconnected and reconnected to a different SFM.
- Delete - Remove a blade from the switch. This function is displayed when Auto Discrepancy Detection on the switch is off.
- Switch Graphic - Displays Switch Graphic screen (refer to Viewing Switch Details on page 3-13).
- Properties - Refer to Blade Properties on page 3-168.

SFM Pro Defined Port

- Copy / Paste - Copies the configuration setting of a defined port and assigns the configuration to another port.
- Delete - Remove (undefine) the configuration settings of a port.
- Rename - Change the assigned name of a port.

Important: Port names cannot be made up of four (4) dotted numbers (nn.nn.nn.nn - e.g., 10.88.99.11).

- Set Beacon On / Off - Activates green and yellow pair of LED indicators on the blade to visually locate a blade port in a chassis for maintenance or troubleshooting.
- Arm / Disarm Alarm - Activate / deactivate port alarms
- Acknowledge Alarms - Acknowledge all port alarms on the specified port
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.

- Go to ... - Links to the following:
  - Switch Graphic
  - Connection Manager
  - Topologies
- Properties - Refer to Port Properties on page 3-170 and Port Properties - VLAN Tagging on page 3-133.

SFM Pro Undefined Port

- Copy / Paste - Copies the configuration setting of a defined port and assigns the configuration to another port.
- Delete - Remove (undefine) the configuration settings of a port.
- Rename - Change the assigned name of a port.

Important: Port names cannot be made up of four (4) dotted numbers (nn.nn.nn.nn - e.g., 10.88.99.11).

- Set Beacon On / Off - Activates green and yellow pair of LED indicators on the blade to visually locate a blade port in a chassis for maintenance or troubleshooting.
- Go to ... - Links to the following:
  - Switch Graphic
  - Connection Manager
  - Topologies
- Configure - Define the properties of a currently undefined SFM Pro port.

HS Series Trunking with Aggregation

HS Series trunking with aggregation allows the xSL associations of an xSL trunks with HS series switches as their 'Switch A' and 'Switch B' end switches to aggregate connections. Since the xSL trunk is in 'guaranteed' mode (the only mode supported), the sum of the speed of each connection aggregated over an xSL association can not be higher than the xsl association link speed. For example, a 100G xSL association can carry 10x10G connections, or 2x40G and 2x10G connections, or 1x40G and 6x10G connections.

Note: Aggregation requires adding a header to be able to multiplex/demultiplex the connections. At full line rate, it will not be possible to aggregate 10x10G connections over a 100G xSL association because of the added header. The smaller the packets, the higher the overhead caused by the addition of the header. The smallest packet is:

64 bytes + 7 bytes preamble + 1 byte start frame delimiter + 12 bytes inter frame gap = 84 bytes

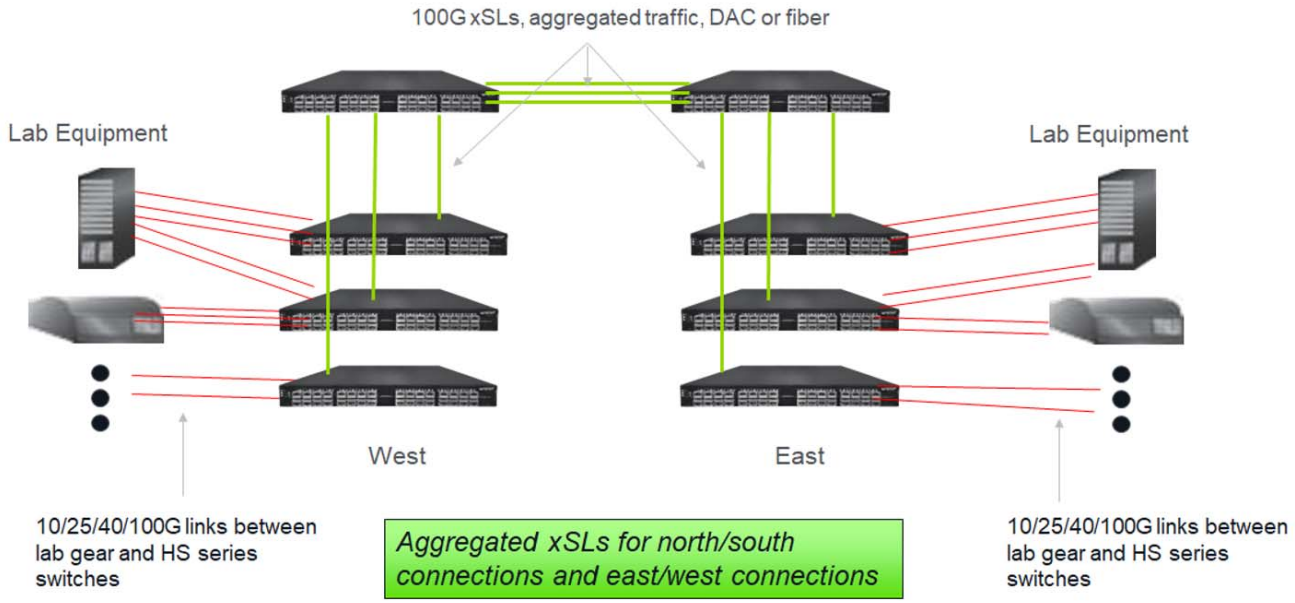
Adding a VLAN header increases the size to 88 bytes. The overhead is 4/84= 4.76%, so worst case scenario for a 100G xSL association:

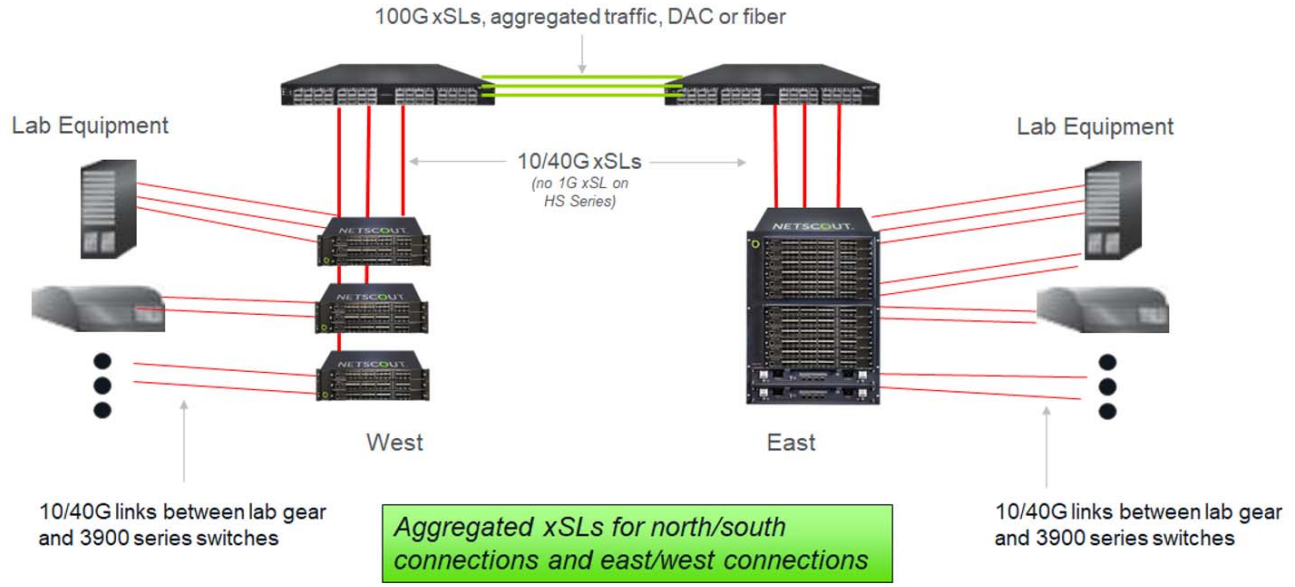
Aggregated bandwidth * 1.0476 = 100G
Aggregated bandwidth = 95.45G

Note: HS-3200 and HS-6400 do not provide the best 10G/25G port density. The HS-3200 has 32x100G but it supports only 64x10G or 64x25G ports (instead of 128). Similarly, The HS-6400 has 64x100G but it supports only 128x10G or 128x25G ports (instead of 256).

Note: In order to not to get confused with the aggregation mode of the trunk, the feature 'HS Series Trunking with Aggregation' may be renamed 'HS Series xSL Multiplexing'. A trunk in aggregation mode uses load balance groups and allows oversubscription. This feature uses the trunk in guaranteed mode but allows mux-demux of several connections over one xSL association.

The following graphics display applications that can use the HS Series Trunking with Aggregation feature.





Connections

Duplex and simplex connections are supported.

The end ports connected through the xSL association of an HS Series trunk must not have matching speeds.

Connecting end ports with different speeds through an xSL association of an HS Series trunk is allowed and each direction reserves a different speed - matching the ingress port speed.

Note: For the reserved bandwidth on the xSL association to match the lower speed among the speeds of the end ports connected there has to be a rate limiting feature on the HS where the higher speed port limits the amount of traffic forwarded to the the xSL association.

Congestion

Due to the addition of a header, packet sizes transmitted over the xSL association are bigger than the original packet size. It is possible that packets may be dropped on egress (going out of the HS switch on the xSL association).

Congestion Alarm

A Congestion alarm is available per HS port and can be configured using the CLI or the GUI.

CLI

The following CLI command can be used to enable or disable the congestion alarm on HS switch ports.

Usage: **REV**ise {**POR**t|**PRTN**um} port **CONG**estion **ALA**rm {**ENA**bled|**DIS**abled}

Revise a port's congestion alarm mode.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

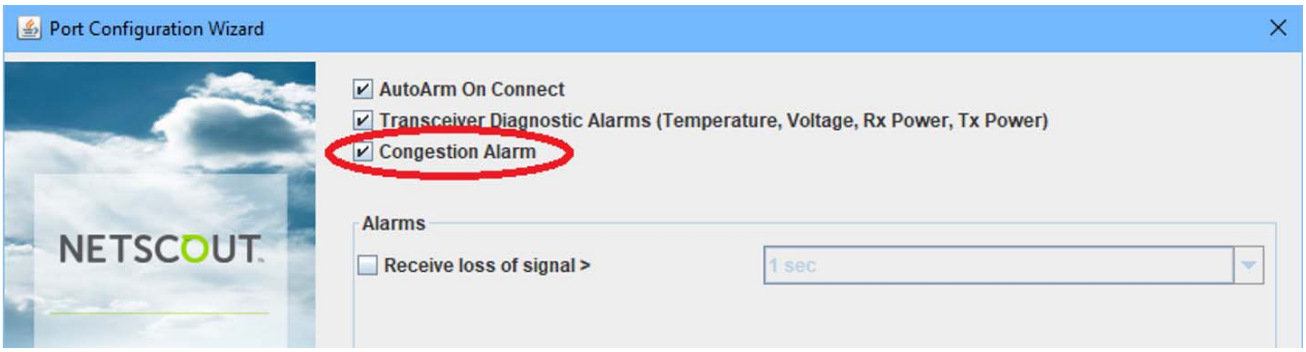
NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev prtn 1.2.4 cong ala ena

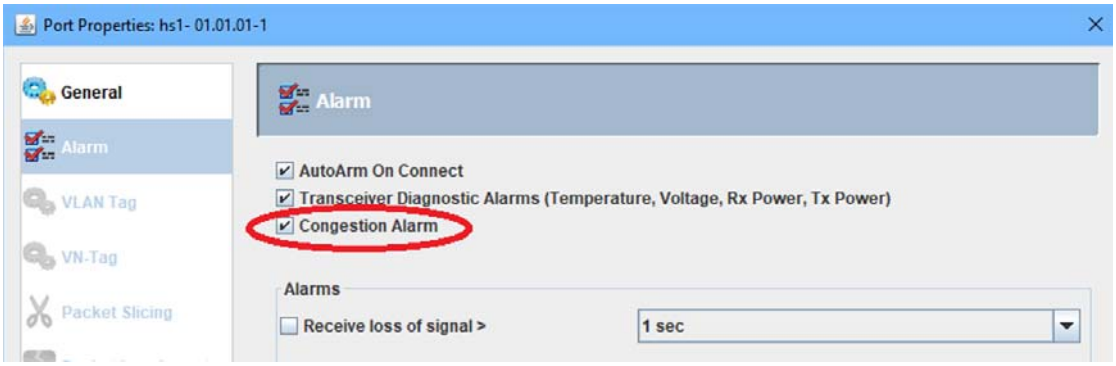
rev prtn 1.2.4 cong ala dis

GUI

HS port congestion alarm can be configured in the "Port Configuration Wizard"



and in the "Port Properties"



A congestion alarm will be generated when a packet is dropped due to congestion. Congestion alarms are locked - no new alarms will be generated till the last generated alarm is acknowledged.

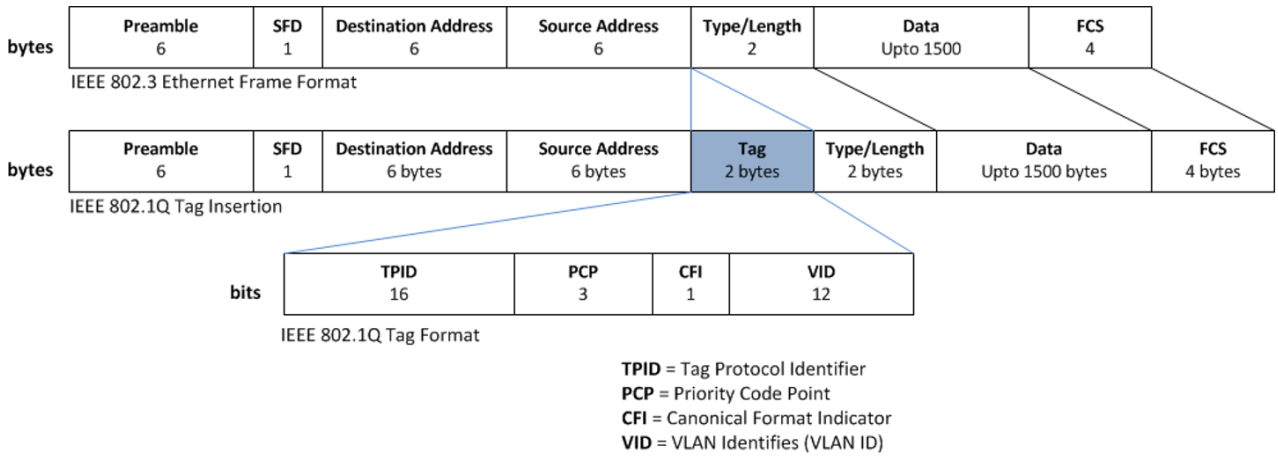
The congestion alarm will be generated for an xSL port - no indication will be provided as to which port the dropped packet arrived on.

VLAN versus VxLAN

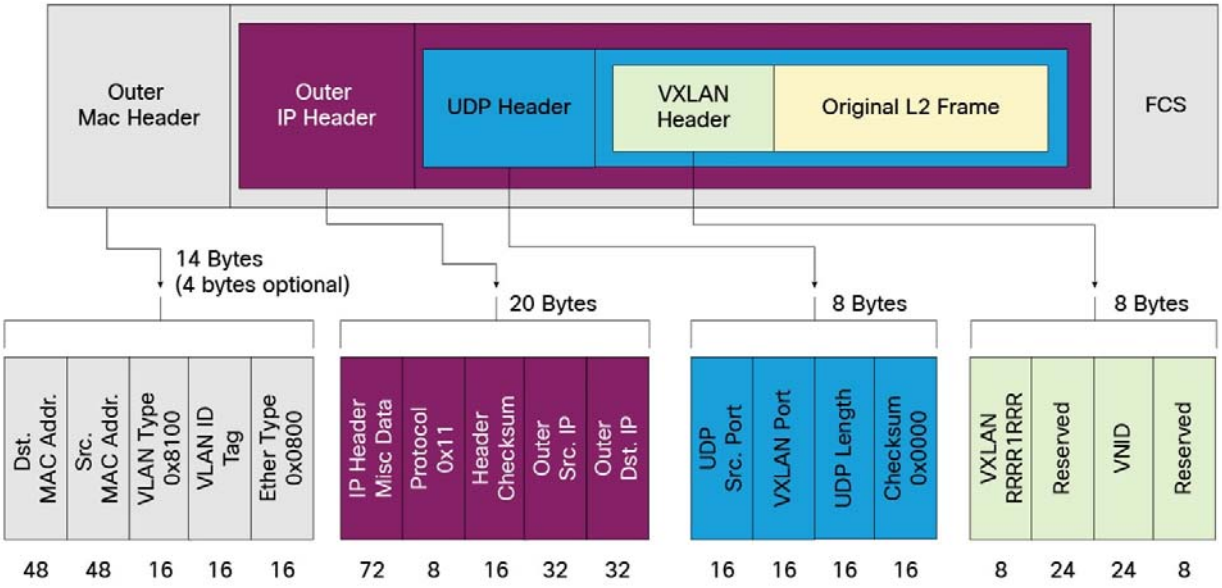
In order to multipex/demultiplex connections on a single xSL association, packets must carry information regarding which connection they belong (in different words, where to forward the packet once it arrives to a switch over the xSL association). There are two options:

- Add a VLAN tag
- Encapsulate the packet using VXLAN.

A VLAN tag adds 4 bytes to the original frame. From the 4 bytes, 12 bits are used for the VLAN ID (VID), providing 4094 different values (0 and 4095 are not used).



VXLAN is an encapsulation protocol that provides data center connectivity using tunneling to stretch Layer 2 connections over an underlying Layer 3 network. VXLAN encapsulation adds 46 to 50 bytes to the original frame. The VXLAN header carries a 24 bit VXLAN Network Identifier that provides more than 16 million values. The outer IP header allows the packet to traverse an IP network, providing the means to forward packets across a network to the destination switch.



Comparing VLAN with VXLAN:

	VLAN	VXLAN
Range of IDs	4093	> 16,000,000
Overhead (bytes)*	4	46
Reachability	Directly cabled switches	Switches across an IP network**

*The lower the overhead, the lower the added latency and processing.

**Requires configuration of MAC and IP header (source and destination addresses).

The VLAN range will allow creating a spine-leaf network with 4093 user (front) ports with minimum overhead. If reachability across a network is not necessary and the range is sufficient, then it is the optimal solution. For these reasons we have decided to use VLAN Tags.

HS Series Rate Conversion

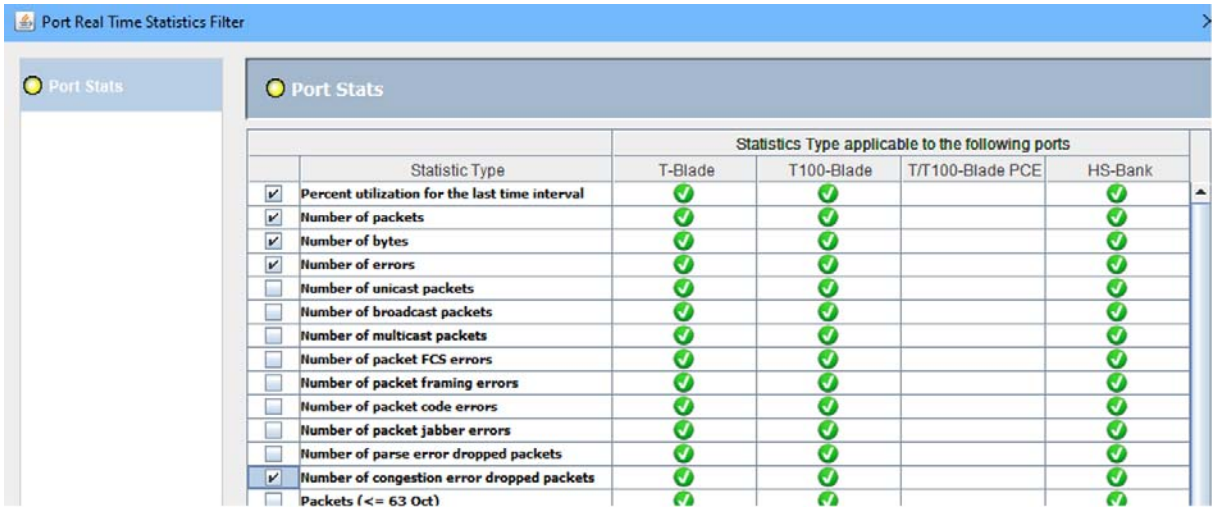
Connections between HS ports (ports located in HS-3200 or HS-6400 switches) when the ports do not have matching interface type are allowed. Note that these types of connections will be allowed for all the HS ports without having to change any configuration settings. Both ports must reside on the same HS Series switch.

Latency

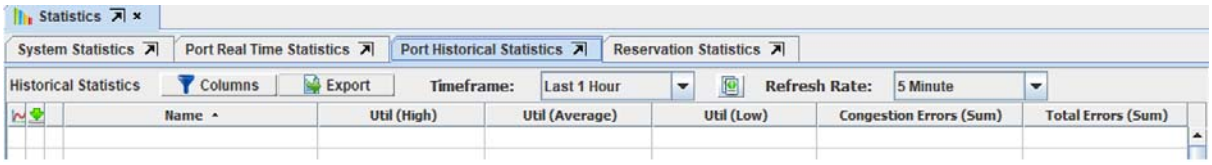
When connecting ports of different speed, cut-through mode is not supported in at least one direction: from the port with lower speed to the port with higher speed. Instead, to avoid underruns, store-and-forward mode will be used. Store-and-forward mode will increase the latency.

Congestion

When connecting ports of different speed, congestion errors may occur in the direction from the port with higher speed to the port with lower speed. A congestion error occurs when there is no memory available to hold an incoming packet. In that case the incoming packet is dropped, and the congestion error counter is incremented. A congestion alarm can be generated when packets are dropped due to congestion. See Congestion Alarm . Congestion errors are counted and displayed in the real time statistics window in the GUI Client. To display the real-time congestion error count, in the 'Port Real Time Statistics' tab in the 'Statistics' application click on the 'Columns' button and check the "Number of congestion error dropped packets' statistics type.



The 'Port Historical Statistics' tab in the 'Statistics' application displays the total number of congestion errors in the specified timeframe.



xSL Associations

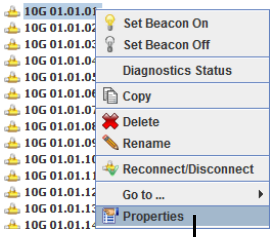
See section Connections in the section HS Series Trunking with Aggregation.

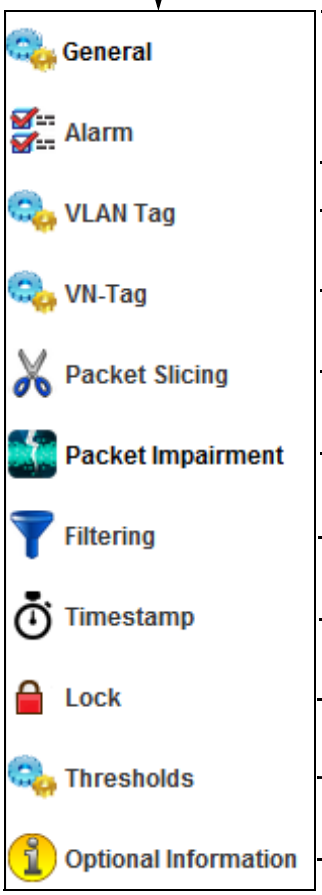
Revising Configuration Settings on a Blade Port

Note: Interface Type, Speed, and Alarm configuration settings cannot be modified if the selected port is connected.

To revise / update the configuration settings on a single blade port:

1. From the port level, select the port to update.
2. Right click, and select **Properties**. The Port Properties Screen displays. Make changes as required, then click **OK**.





Refer to Configuring Blade Ports on page 3-57

Refer to Port Properties - VLAN Tagging on page 3-133

Refer to Port Properties - VN-Tag Stripping on page 3-139

Refer to Port Properties - Packet Slicing on page 3-140

Refer to Port Properties - Packet Impairment on page 3-142

Refer to Destination Port Filters on page 3-200

Refer to Port Properties - Timestamping on page 3-144

Refer to Port Lock Settings on page 3-98

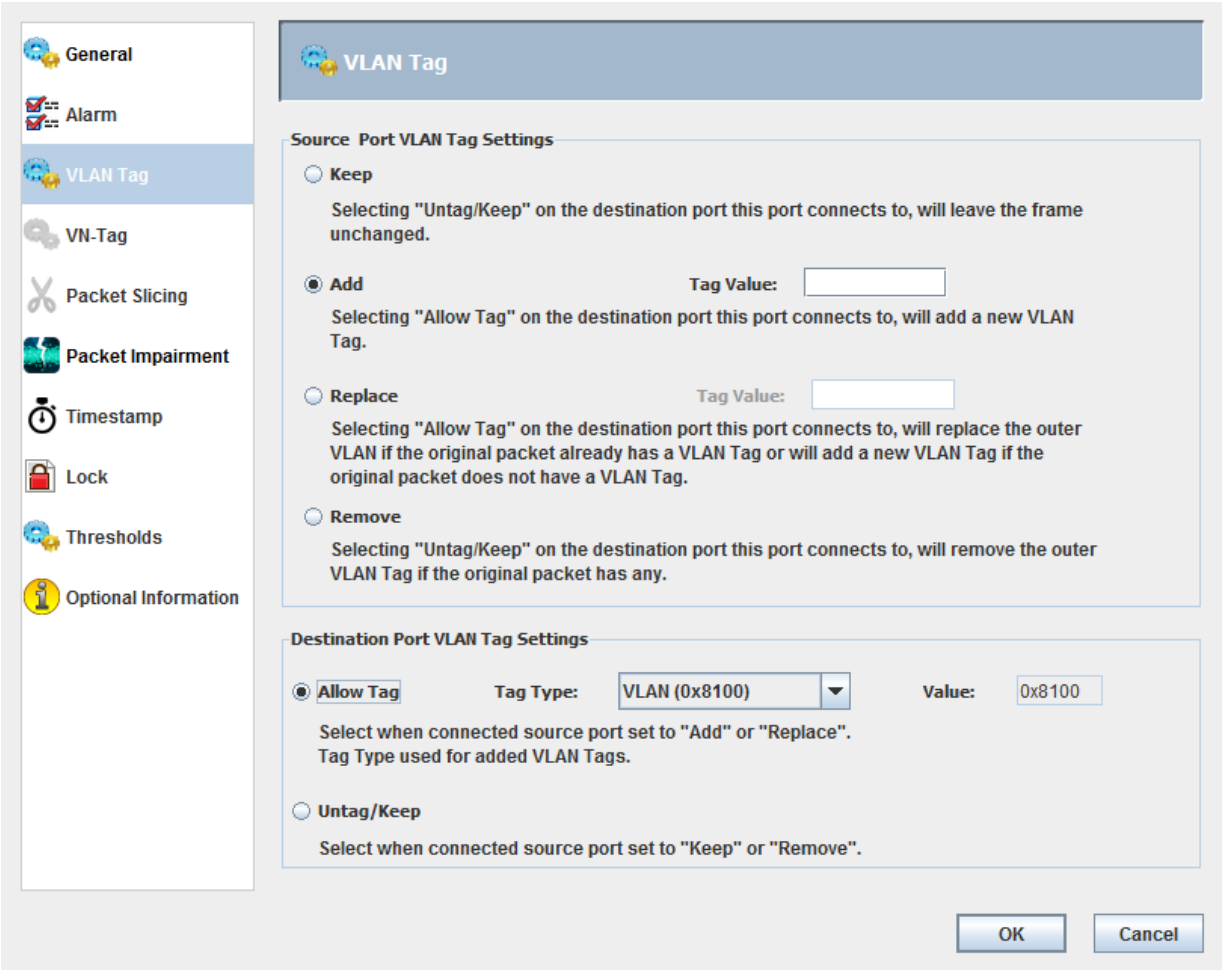
Refer to Port Properties - Threshold Settings on page 3-148

Refer to Configuring Blade Ports on page 3-57

Port Properties - VLAN Tagging

These settings allow adding, modifying, or removing a Virtual LAN (VLAN) Tag on a Source Port or just allow a packet frame to pass through unmodified.

Select a defined port, right click and select **Properties > VLAN Tag**. The VLAN Tag screen displays.



Under **Source Port VLAN Tag Settings**, the following configuration options are:

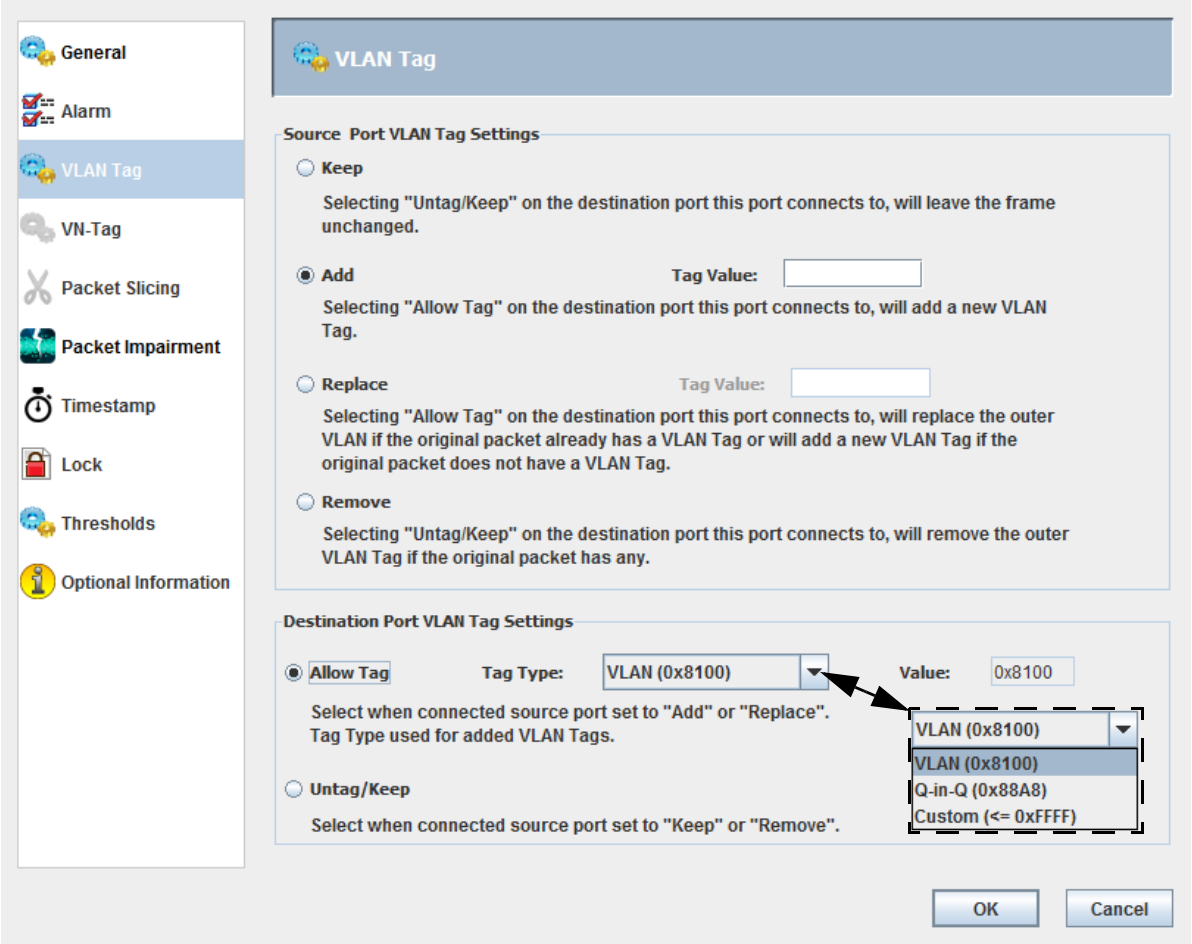
- **Keep** - Source frames are not modified. This source setting requires a destination port set to **Keep**. Setting the destination port to **Allow Tag** may result in unexpected behavior.
- **Add** - A new VLAN Tag will be added to the frame. The Tag Value field allows the user to choose the VLAN Tag value. This field is active only when Add is selected. This source setting requires a destination port set to **Tag**.
- **Replace** - If the source frame has a VLAN Tag, it is modified. If the source frame does not have a VLAN Tag, one is added. The Tag Value field allows the user to choose the VLAN Tag value. This field is active only when **Add** is selected. This source setting requires a destination port set to **Tag**.
- **Remove** - The outer VLAN Tag, if present, is removed. This source setting requires a destination port set to **Untag**.

When a VLAN Tag is added or replaced, the corresponding configured tag value is used. Valid tag values are integers 1 through 4094. When either of the Tag Value fields become active, it displays the last configured value used for the port.

Table 3-1 lists the recommended sequence of steps to follow when transitioning from one VLAN Tag setting to another. This assumes that live traffic is flowing through the ports where VLAN Tag setting changes are required.

Table 3-1 Recommended VLAN Tag Setting Sequences

Transition		First Port To Change	Setting Sequence	Transient Anomaly
From	To			
keep	add	ingress	1. ingress: keep -> add 2. egress: untag -> tag	none
keep	replace	ingress	1. ingress: keep -> replace 2. egress: untag -> tag	tagged frames are stripped of their outer tag until egress port is changed from "untag" to "tag"
keep	remove	ingress	1. ingress: keep -> remove 2. egress: no change	none
add	keep	egress	1. egress: tag -> untag 2. ingress: add -> keep	none
add	replace	ingress	1. ingress: add -> replace 2. egress: no change	none
add	remove	egress	1. egress: tag -> untag 2. ingress: add -> remove	"keep" behavior until the ingress port is changed from "add" to "remove"
replace	keep	ingress	1. ingress: replace -> keep 2. egress: tag -> untag	tagged frames will have the old replace tag added until the egress port is changed from "tag" to "untag"
replace	add	ingress	1. ingress: replace -> add 2. egress: no change	none
replace	remove	egress	1. egress: tag -> untag 2. ingress: replace -> remove	none
remove	keep	ingress	1. ingress: remove -> keep 2. egress: no change	none
remove	add	ingress	1. ingress: remove -> add 2. egress: untag -> tag	"keep" behavior until the egress port is changed from "untag" to "tag"
remove	replace	ingress	1. ingress: remove -> replace 2. egress: untag -> tag	none



After passing through the source port, a frame will have a new VLAN Tag, a replaced VLAN Tag, or was not modified. If forwarded, this frame then leaves the switch through one of the destination ports. These are the options at the destination port:

- **Allow Tag** - The VLAN Tag, if present, is kept. Valid values for the Tag Type are 0x8100 (VLAN), 0x88A8 (Q-in-Q), or a custom entered hex number smaller than 0xFFFF.
- **Untag/Keep** - The outer VLAN Tag, if present, is removed.

Note: VLAN ID Tagging Notice
For environments configured to support Cisco FabricPath or ISL traffic, if that traffic is routed through an nGenius 3900 Series Switch configured to insert the (source ID) port number to the VLAN ID field, the classification of that traffic may be incorrect. In such cases, VLAN ID tagging should not be used.

Note: VLAN Filtering Notice
For frames containing more than three VLAN tags, frames will be forwarded as long as VLAN1 and VLAN2 satisfies the filter: VLAN1 = outermost VLAN ID, VLAN2 = second VLAN ID.

VLAN Usage Examples

The following describes typical configuration examples for VLAN operation using either the TestStream Management GUI or CLI commands.

Adding VLAN Tag

Situation
User is aggregating five ports into one output, such as input ports 1,2,3,4,5 going out on port 6. On the end point device, user wants to be able to identify which packet is coming from what port.

Solution
Enable VLAN tagging on each input port so that packets coming from port 1 will have a VLAN tag of 101, port 2 will have 102, etc.

From the GUI
Select **Add** in the source port and give a unique VLAN ID, and select **Allow Tag** in the destination port.

From CLI
On the source port: REVISE PORT *port* VLANTAG ADD ID *vlan_id*
On the destination port: REVISE PORT *port* VLANTAG ALLOWTAG TPID *tpid_value*
Where *tpid_value* id is the VLAN tag's ethertype (default is 0x8100)

VLAN Tag Replacement

Situation
User is aggregating five ports into one output, and incoming packets already have VLAN tags on them, but user still wants to identify every port's traffic on the output. End point monitoring device cannot decode packets with two VLAN tags (Q-in-Q), so simply adding VLAN tags on the 3900 does not solve the issue.

Solution
Enable tag replacement and give each input port a different VLAN tag ID. This will replace the VLAN tags if the original packet had any, or will add the tags if the original packet is a non-VLAN packet.

From the GUI
Select **Replace** on the source port and give a unique VLAN ID per port, select **Allow Tag** on the destination port.

From CLI
On the source port: REVISE PORT *port* VLANTAG REPLACE ID *vlan_id*
On the destination port: REVISE PORT *port* VLANTAG ALLOWTAG TPID *tpid_value*

VLAN Tag Removal

Situation
User is aggregating five ports into one output, and incoming packets already have VLAN tags on them, but end point monitoring device cannot decode packets with VLAN tags.

Solution
Remove the VLAN tag from the packets before sending out to the monitoring device.

From the GUI
Select Remove on the source port, select **Untag/Keep** on the destination port.

From CLI
On the source port: REVISE PORT *port* VLANTAG REMOVE
On the destination port: REVISE PORT *port* VLANTAG UNTAGKEEP

No VLAN Operation Required

Situation
User wants to pass packets from input to output as they are, no manipulation.

Solution
Do not do anything.

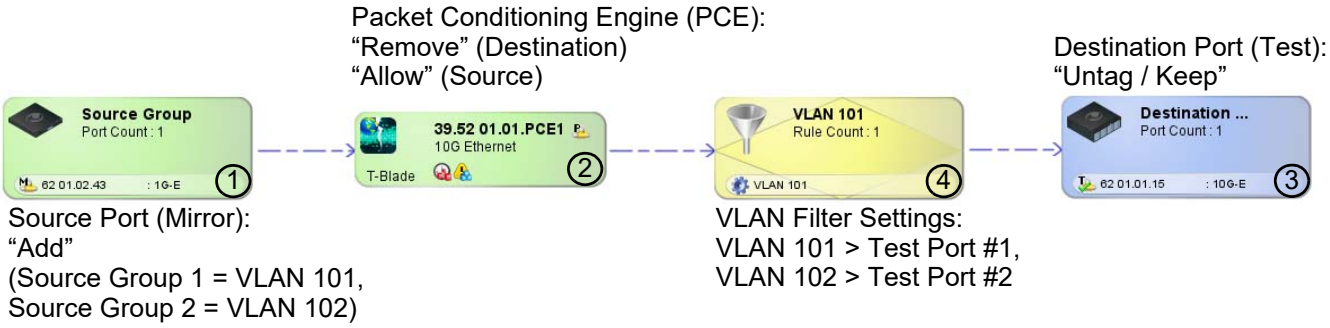
From the GUI
Select **Keep** on the source port, select **Untag/Keep** on the destination port.

From CLI
On the source port: REVISE PORT *port* VLANTAG KEEP
On the destination port: REVISE PORT *port* VLANTAG UNTAGKEEP

VLAN Tagging Across PCE Ports

The following example illustrates the use of VLAN tags in associating selected source (Mirror) ports to selected destination (Test) ports.

This diagram shows a Source Group on the left (#1) that is destined for a Destination Group (#3) on the right via a PCE (#2).



1. Set each of the ports in the Source Group to VLAN Tag = “Add” and assign a Tag Value (101).
2. Set the PCE to VLAN Tag = both “Allow Tag” and “Remove”. (Although counterintuitive, this “double setting” is an artifact of how the VLAN User Interface maps to the software).
3. Set each of the ports in the Destination Group to VLAN Tag = “Untag/Keep”.
4. Add a Filter for VLAN 101 and connect it to the Destination Group.

Using this method, moving from one Source and Destination Group to the next, the only change is:

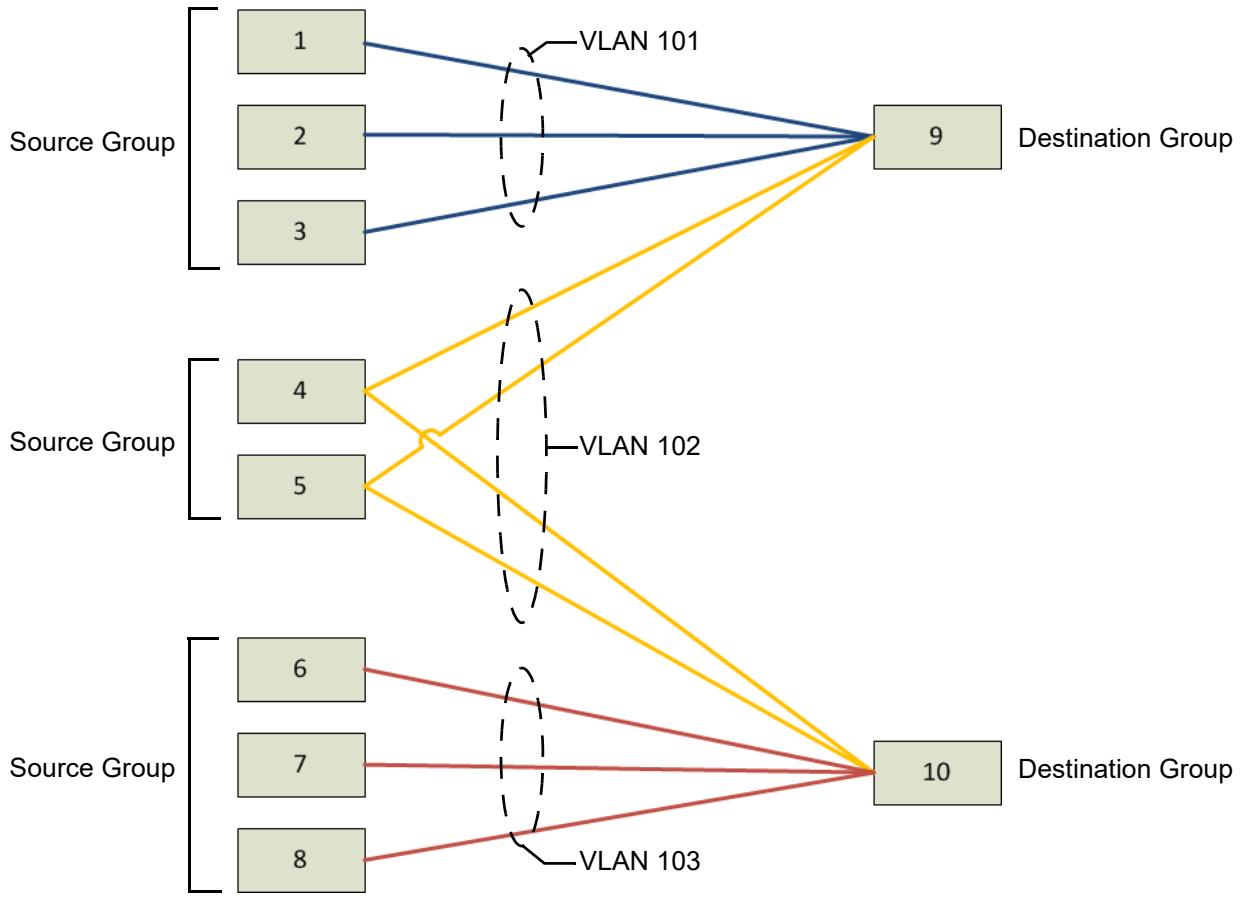
- The VLAN Tag added at the Source Ports.
- The VLAN Filter is connected to each Destination Group. The settings on the PCE or the Destination Ports are not changed.

Showing this in practice, here is an example:

1. Ports 1-4 (on the left) go to Destination Group 9 (on the right).
2. Ports 5-8 go to Destination Group 10.
3. Ports 4-5 go to both Destination Group 9 and 10.

In this case, configure three Source Groups (1-3, 4-5, and 6-8).

1. To the first Source Group, add VLAN 101.
2. To the second Source Group, add VLAN 102.
3. To the third Source Group, add VLAN 103.
4. Filter VLAN 101 to Destination Group 9.
5. Filter VLAN 102 to Destination Groups 9 & 10.
6. Filter VLAN 103 to Destination Group 10.

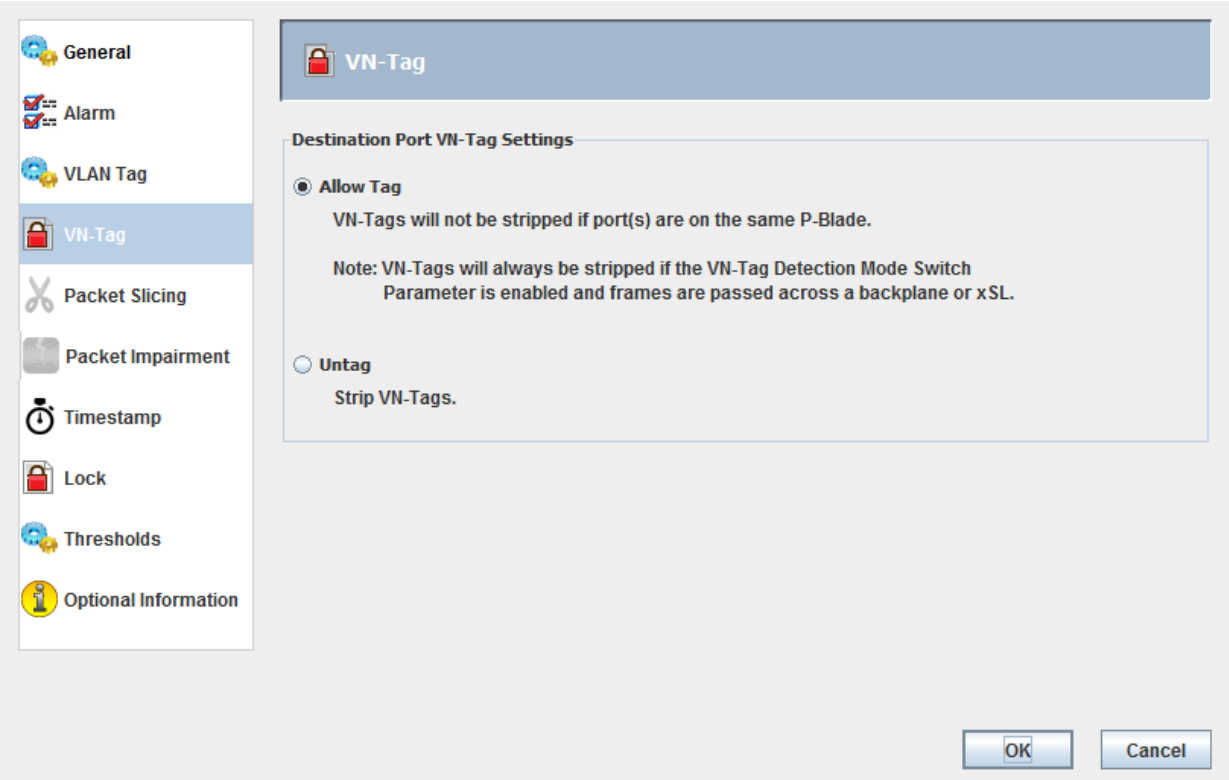

Source Group
1
2
3
VLAN 101
9
Destination Group
Source Group
4
5
VLAN 102
Source Group
6
7
8
VLAN 103
10
Destination Group

Port Properties - VN-Tag Stripping

These settings enable / disable VN-Tag Stripping on a Destination Port. These settings are not valid or selectable for Mirror and xSL ports.

> **Note:** The nGenius 3900 switch must have VN-Tag Detection Mode enabled (refer to Adding a Switch on page 3-2 > **Switch Parameters**) in order to set VN-Tag Detection.

Select a defined port, right click and select **Properties > VN Tag**. The VN-Tag screen displays.



Under **Destination Port VN-Tag Settings**, the following configuration options are:

- **Allow Tag** - VN-Tags will not be stripped if port(s) are on the same T-Blade. VN-Tags will always be stripped if the VN-Tag Detection Mode Switch parameter is enabled and frames are passed across a backplane or xSL.
- **Untag** - Strips VN-Tags.

VN-Tag CLI Commands

Stripping VN-Tags (when VN-Tag Detection is enabled)

REVise {**POR**t|**PRTN**um} *port* **VNT**ag {**ALL**owtag|**UNT**ag}

Examples:
rev prtn 1.2.4 vntag allow
REVISE PORT MyAnalyzer vntag untag

Enable / Disable VN-Tag Detection

REVise **SWI**tch switchname **VNT**ag **DET**ection {**ENA**bled|**DIS**abled}

Examples:
rev swi MySwitch vnt detect ena
rev swi MySwitch vnt det dis

Port Properties - Packet Slicing

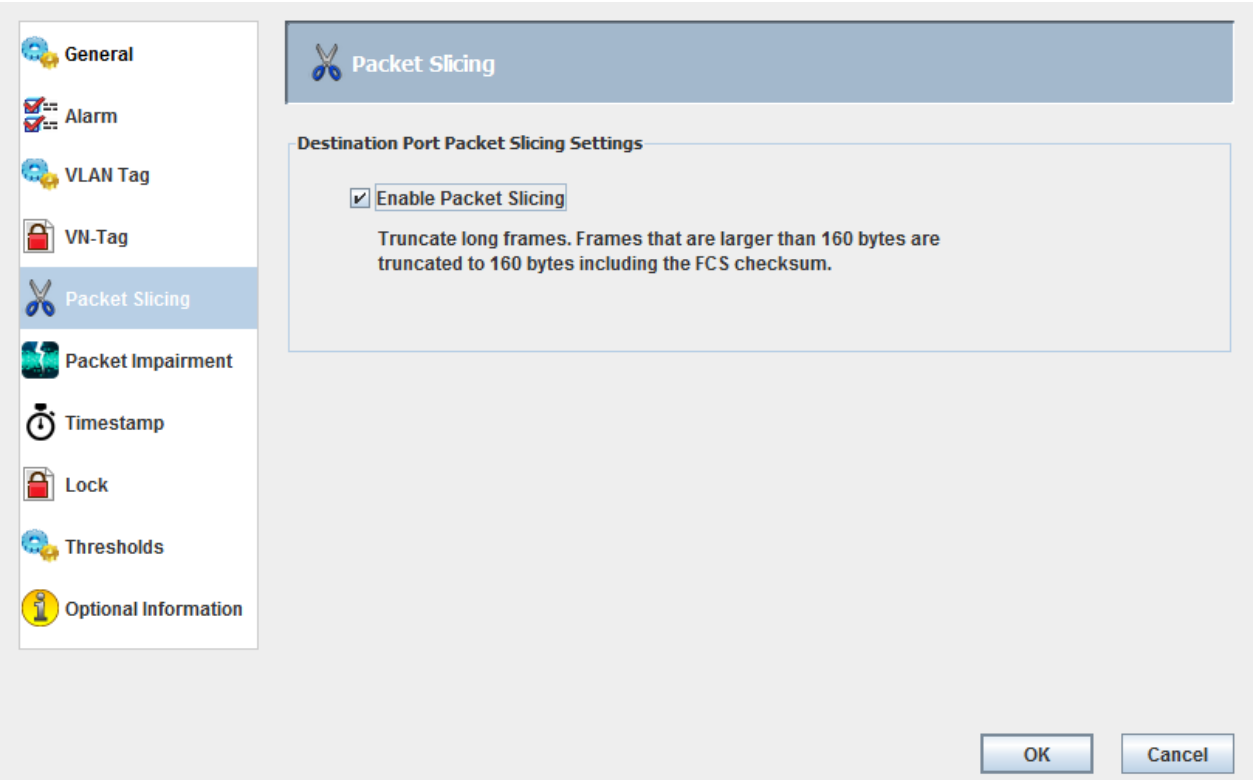
Packet slicing allows reducing the traffic load on a destination port to selected devices by truncating packets to 160 bytes, allowing devices to process and store more data, or process and store only data of interest. The 160 bytes includes the first 156 bytes of the packet plus a new 4-byte FCS checksum.

Note:
Nanostamping and packet slicing cannot be enabled on the same port.

Packet slicing is not applicable for Mirror or xSL ports.

The Transmit Byte Count Statistics for ports that have Packet Slicing enabled will be zero, so Tx utilization cannot be calculated and will be 0%.
Packets are counted with zero length, and so show up in the count of packets with less than 63 octets.
To see the actual byte counts and utilization percentage, send the traffic through a Clone port first and configure the Clone port to slice the traffic rather than the destination port.

Select a defined port, right click and select **Properties > Packet Slicing**. The Packet Slicing screen displays.



Click **Enable Packet Slicing** to activate packet slicing on the selected port.

Packet Slicing CLI Command

Enable / Disable Packet Slicing

REVise {**POR**t|**PRTN**um} port **SLIC**ing {**ENA**ble|**DIS**able}

Examples:

revise port "Analyzer Tool" slicing enable
rev prtn 1.2.4 slic dis

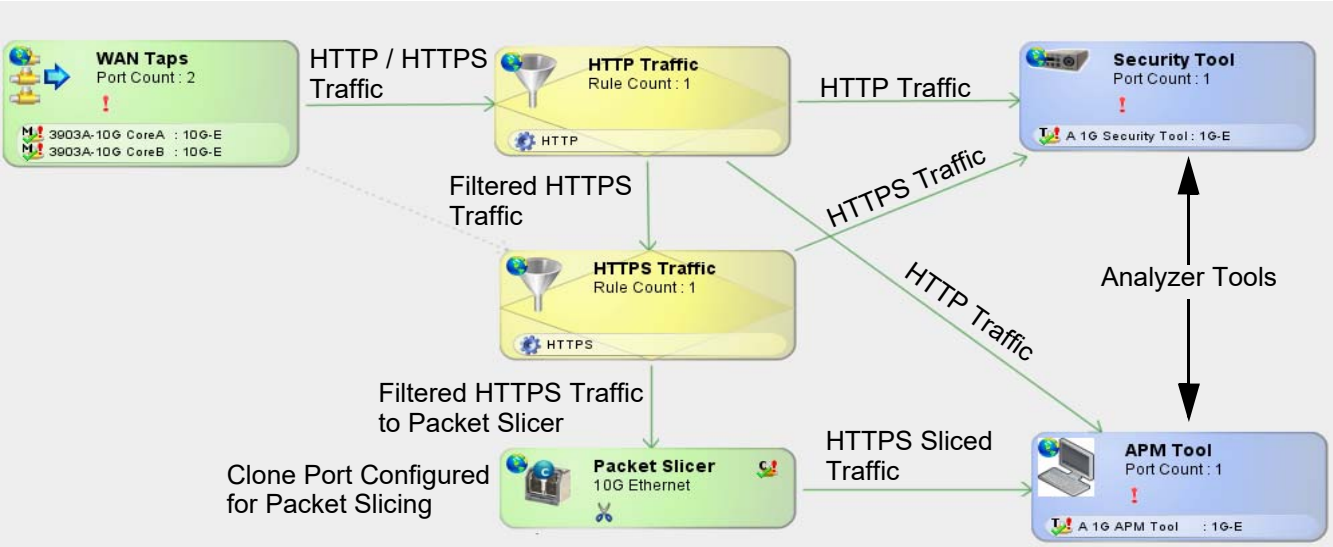
Conditional Packet Slicing

Conditional packet slicing enables users to set slice points at different offsets for each packet as well as specify the types of traffic to be sliced.

Conditional packet slicing is achieved using a Clone port. Filtered traffic to be sliced is redirected to a Clone Port that is configured for slicing. The traffic received on the Clone port is then directed to the actual destination port. Traffic that should not be sliced is sent directly to the destination port.

Use Case Example:

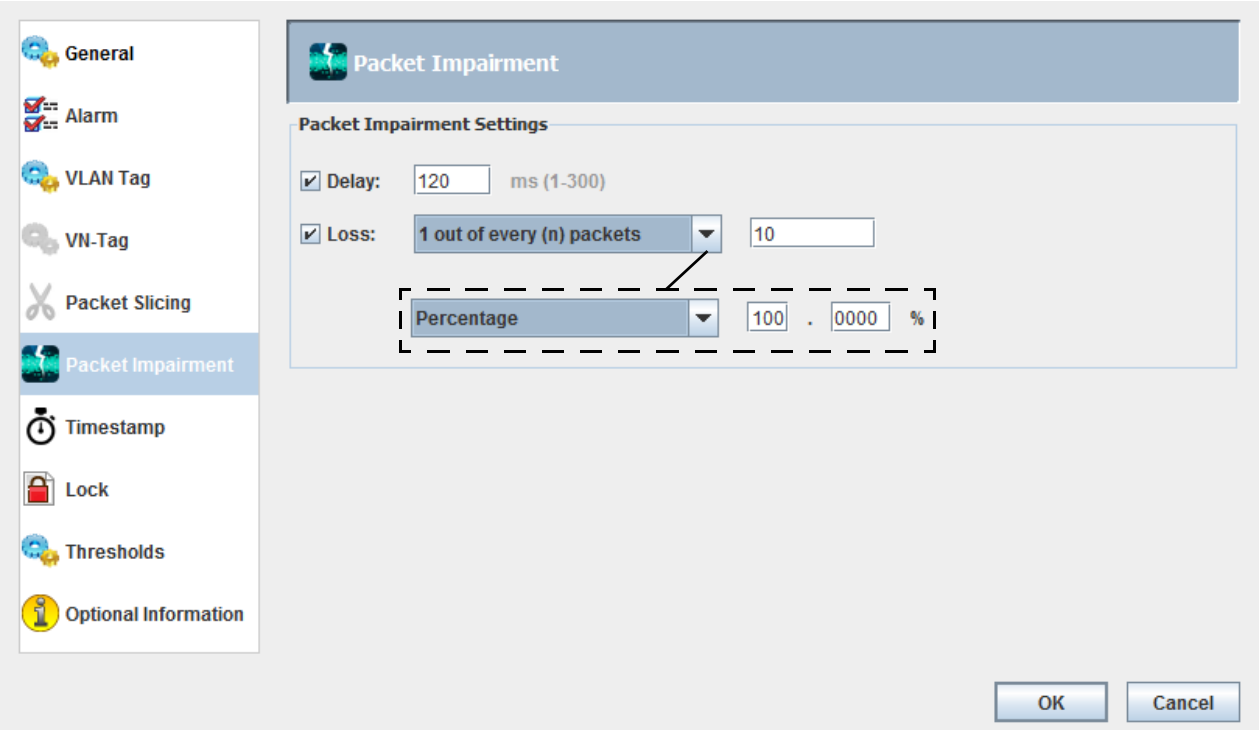
- Customer has taps with HTTP and HTTPS traffic
- Using two tools analyzing web traffic: Security Tool and APM Tool
- Security Tool wants all HTTP/HTTPS traffic without slicing
- APM Tool wants HTTPS traffic sliced
- User configured an unused front port as a Clone Port (Packet Slicer)
- Logged into Linux Shell - Enabled packet slicing on the Clone Port



Port Properties - Packet Impairment

Packet impairment allows defining Packet Conditioning Engine (PCE) port impairments.

Select the defined Packet Conditioning Engine (PCE) port (refer to Blade Properties on page 3-168), right click and select **Properties > Packet Impairment**. The Packet Impairment screen displays.

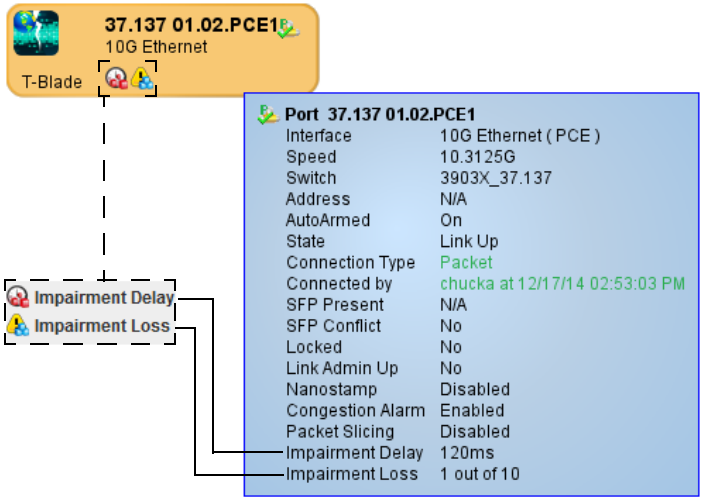


Either or both of the following configuration options can be selected:

- **Delay** - Set packet delay from 1 to 300 ms.
- **Loss** - Set packet loss. Two selections are available:
  - 1 out of every (n) packets
  - Percentage: Defines the percentage of packets dropped over time (range = 0.0001 - 100).

Note: The following types of frames will be dropped as errored by the PCE port/drivers:
Frames larger than 1600 bytes
Frames less than 64 bytes
Truncated frames
FCS errored frames
Frames that fail layer 3 header validations (e.g., IP header checksum, total IP packet length in header not matching actual packet length)

From the topology manager, the configured PCE port is displayed:



Packet Impairment CLI Command

REVise **PCE** {**POR**t|**PRTN**um} *portname* **IMP**airment {**DIS**able|**ENA**ble} {**DEL**ay|**LN**|**LP**} [value]
Revise PCE port properties to enable / disable Impairment on the PCE Port.
Set 'Enable' to turn on an impairment

DELay: Number of milliseconds to delay (range 1 - 300).

LN: Drop 1 out of every N packets.

LP: Drop percentage of packets (range .0001 - 100)
PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Examples:
rev pce port myport imp enable delay 50
rev pce prtnum 01.01.PCE1 imp enable LP .001

Note: CLI Usage:
Prior to changing Impairment settings, first disable Impairment, then re-enable Impairment with the revised settings.

Port Properties - Timestamping

Time stamping provides the capability to determine the time a packet is received on an ingress port. The time stamp is synchronized to a distributed wall clock for accurate comparison across nGenius 3900 series systems, providing nanosecond-level accuracy. This time stamp can then be used to report latency and other performance measurements.

There are two types of time stamping frames:

- Regular Ethernet frames received from the network for which a nanostamp is added
- Keyframes generated from within the nGenius 3900 series switch used to synchronize a nanostamp at the end of each frame into a date and time (wall clock time)

Each frame is marked with a four byte nanostamp at the end of each packet, and FCS is recalculated to reflect the additional bytes. Keyframes can be configured with frequency, which can be used by the customer (e.g., packet analyzer) to calibrate the UTC timestamp for all packets.

Nanostamp Field Format

The nanostamp setting enables / disables nanostamping on a destination port. When enabled, a nanosecond-level free running counter is added to the end of every packet sent on the destination port.

This nanostamp is a 31-bit value that increments once every 2.962963 nanoseconds and wraps every 6.36 seconds. The nanostamp provides a means for tools to perform nanosecond-level transaction timing analysis.

The nanostamp is placed in the location of the original frame check sequence (FCS) and a new FCS value is appended to the end of the frame. The format of the nanostamp is as follows (note the position of bit 7 of the nanostamp):

Preamble	Original Packet	Nanostamp					FCS
		Bits 30-23	Bits 22-15	Bits 14-7	0	Bits 6-0	

Note: The nanostamp is generated when the last byte of the packet is received on the T-Blade source port. The nanostamp represents the arrival time of the packet at the nGenius 3900 switch if the source and destination ports are on the same T-Blade. If the source and destination ports are on different T-Blades, the nanostamp is generated at the ingress to the destination T-Blade.

Each T-Blade generates nanostamps using a free running counter that is not synchronized with counters on other T-Blades. Therefore, to allow for the most accurate comparison of packet arrival times, it is highly recommended that all ports used in a specific nanostamp timing analysis be located on the same T-Blade.

Keyframe Configuration

The keyframe is used to translate a nanostamp at the end of a frame into a date and time (wall clock time). The keyframe provides a cross reference showing what the nanostamp value was for a particular blade at a given date and time.

The two fields required to determine time and date are ASIC time (a running nanostamp counter) and UTC time. The date and time that frames arrived at the blade can be calculated by looking at the frame's nanostamp and using the keyframe information to calculate the date and time.

Field	Size	Description
Destination MAC *	6	FF:FF:FF:FF:FF:FF
Source MAC *	6	00:80:8C:FF:FF:FF (Netscout OUI + all FFs)
Ethertype *	2	0x0806 (ARP)

Field	Size	Description
Type	2	Type of the payload. Set to 1.
Payload Length	2	Payload length of following bytes (46)
ASIC time	8	The full 64-bit counter used for frame timestamping. Each tick represents approx. 2.962963 ns. This is useful for determining the relationship between the count value in a nanostamp in another frame and the time of day. To compare to a nanostamp in another frame, use the least significant 31 bits.
UTC time	8	Unix (POSIX) time in nanoseconds (high 4 bytes == number of seconds, low 4 bytes = number of nanoseconds) Nanoseconds are calculated by the number of microseconds in NTP time X 1000
Last sync time	8	Always 0
Keyframe Timestamp	8	The same as UTC Time The generation time of the keyframe itself, in nanoseconds (Unix time).
Egress interface drops	8	Always 0
Device ID	2	Slot number, for example 1, 2, or 3 in a 3903. Not user configurable. Not unique across switches.
Egress interface	2	The egress switchport of the keyframe, the blade's front port number 1-48
FCS type	1	Always 1 The timestamping mode configured on the keyframe's egress port. 0 = timestamping disabled 1 = timestamp is appended to the payload and a new FCS is added to the frame 2 = timestamp overwrites the existing FCS
Reserved	1	Reserved for future use

Note: Four extra bytes of zero will come here, after the Keyframe payload.

Keyframe Configuration File

A configuration file for Timestamp Keyframes resides on each T-Blade in the following location: **`/HorizON/Server/TimeKeyframeCfg.xml`**

```
<?xml version="1.0" ?>
<KeyframeConfig enabled="no">
      <Rate msec="20" />
      <L2Header dst="FF:FF:FF:FF:FF:FF" src="00:80:8C:FF:FF:FF"  ethType="0x0806"/>
      <Ports>
            <Port portNum="1" />
            <!-- To add more ports copy the line above and change the number -->
      </Ports>
</KeyframeConfig>
```

Note: The **`TimeKeyframeCfg.xml`** configuration file is read only at startup, so after making any changes to the configuration file, UCSMgmt must be shutdown and restarted.

- **Enabling Keyframes**

  Timestamp Keyframe generation is disabled by default. To enable Timestamp Keyframes, modify the file on each blade where the keyframes should egress. To enable KeyFrame generation, change the line:

```
<KeyframeConfig enabled="no">
  to
<KeyframeConfig enabled="yes">
```

- **Changing the KeyFrame Rate**

  Change the number of milliseconds in the line below to a value between 20 and 5000 (5 seconds).

  ```
  <Rate msec="20" />
  ```

- **Changing the Ethernet Layer-2 Header**

  The values for destination MAC, source MAC and Ethertype may be changed in the following line:

  ```
  <L2Header dst="FF:FF:FF:FF:FF:FF" src="00:80:8C:FF:FF:FF"  ethType="0x0806"/>
  ```

- **Changing Keyframe Egress Ports**

  Change the port number or add multiple ports to generate KeyFrames by adding multiple lines in the <Ports> section:

  ```
  <Ports>
        <Port portNum="1" />
        <Port portNum="2" />
        <Port portNum="3" />
        <!-- To add more ports copy the line above and change the number -->
      </Ports>
  ```

Note: At startup the port will be powered on. However, several user actions may cause the port to be powered down again and the keyframes stopped. These include connecting and then disconnecting the port, starting and stopping real time statistics on the port. To prevent these situations, configure the port property by selecting **Link Admin Up/Always Collect Rx Stats** (refer to Configuring Blade Ports on page 3-57, Screen 2) to keep the port enabled.

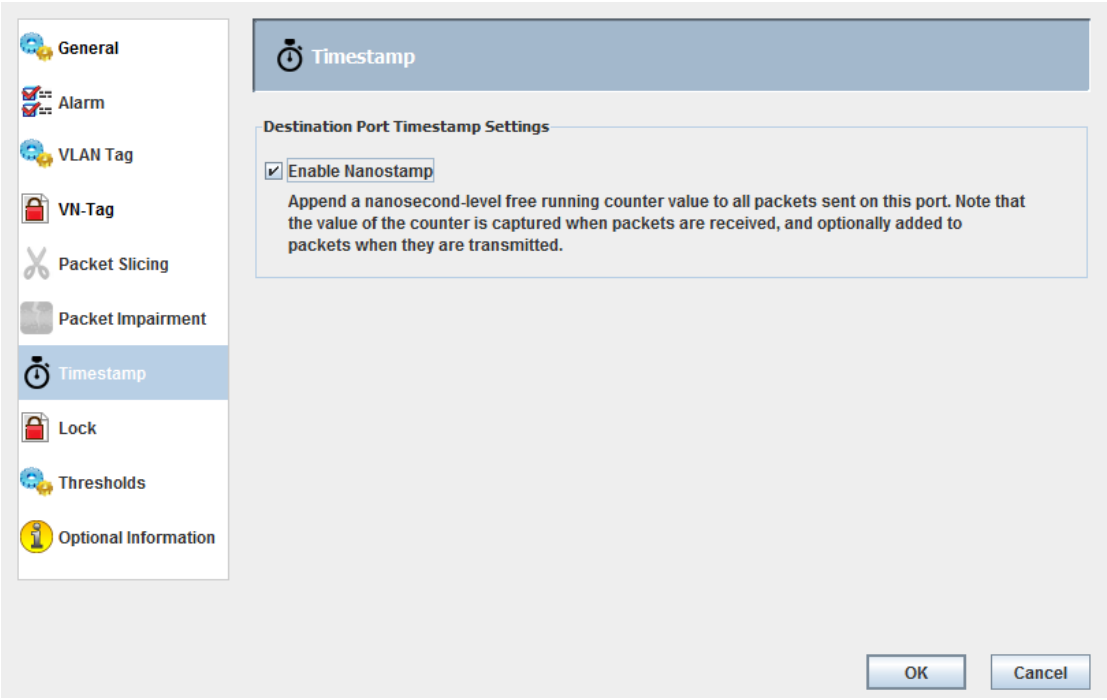
There are 4 extra bytes, all zeroes, at the end of the Keyframe payload.

If a Keyframe egresses a port that has Nanostamping enabled, the Keyframe will have an additional 4-byte Nanostamp appended but the value will be zero.

A 4-byte FCS checksum is the final field transmitted in the frame.

Enable Nanostamping

Select a defined port, right click and select **Properties > Timestamp**. The Timestamp screen displays.



Under **Destination Port Timestamp Settings**, the following configuration options are:

- **Enable Nanostamp** - Selecting **Enable** adds the nanosecond counter to the selected port. Unselecting **Enable** disables nanostamping.

Nanostamp CLI Commands

Enable / Disable Nanostamp

REVise {**POR**t|**PRTN**um} *port* **NANO**stamp {**ENA**ble|**DIS**able}

Examples:
rev prtn 1.2.4 nano enable
rev prtn 1.2.4 nano disable

Port Properties - Threshold Settings

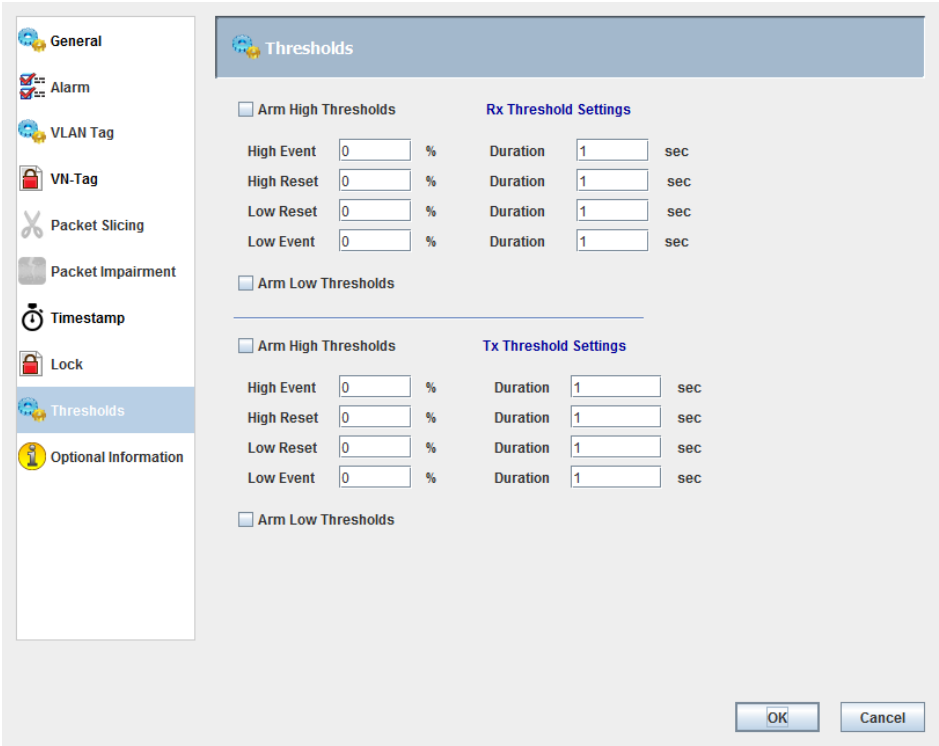
Up to four alarms can be configured for each T-Blade port; a high and low alarm each for Tx and Rx. Each alarm contains an upper and lower boundary with an associated time period. The threshold settings determine when the alarms are raised and cleared.

Note: If a configured port receives a threshold alarm, the port remains in the alarmed state until the alarm is acknowledged (refer to Acknowledging Events on page 2-23).

Upper Threshold Alarm - The upper (high) threshold alarms trigger when utilization is above the High Event boundary for at least the specified duration. The alarm clears when utilization is below the High Reset boundary for at least the specified duration. No action occurs if the utilization crosses a boundary for less than the specified duration.

Lower Threshold Alarm - The lower (low) threshold alarms trigger when utilization is below the Low Event boundary for at least the specified duration. The alarm clears when utilization is above the Low Reset boundary for at least the specified duration. No action occurs if the utilization crosses a boundary for less than the specified duration.

Select a defined port, right click and select **Properties > Thresholds**. Click either (or both) **Arm High Thresholds / Arm Low Thresholds** to activate the required threshold alarming. Enter (in percentages) the High Event/Reset, Low Event/Reset settings and their respective time settings (Duration, in seconds).



Subport Properties - Threshold Settings

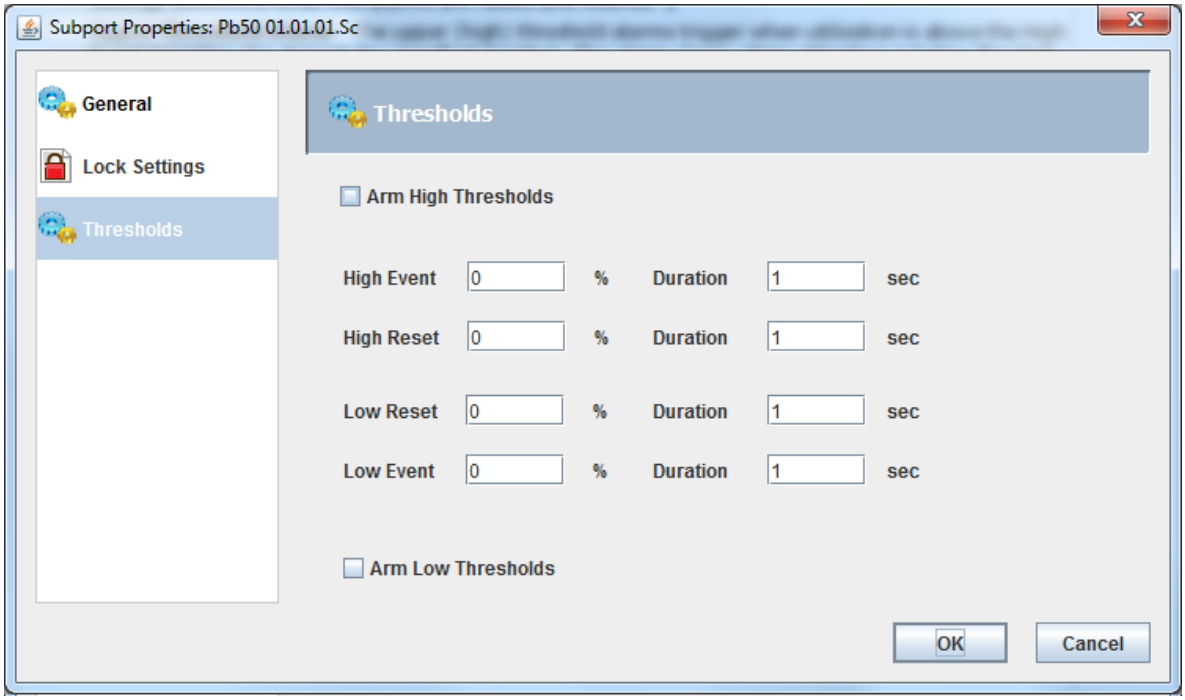
Up to four alarms can be configured for each T-Blade subport; a high and low alarm each for Tx and Rx. Each alarm contains an upper and lower boundary with an associated time period. The threshold settings determine when the alarms are raised and cleared.

> **Note:** If a configured subport receives a threshold alarm, the subport remains in the alarmed state until the alarm is acknowledged (refer to Acknowledging Events on page 2-23).

Upper Threshold Alarm - The upper (high) threshold alarms trigger when utilization is above the High Event boundary for at least the specified duration. The alarm clears when utilization is below the High Reset boundary for at least the specified duration. No action occurs if the utilization crosses a boundary for less than the specified duration.

Lower Threshold Alarm - The lower (low) threshold alarms trigger when utilization is below the Low Event boundary for at least the specified duration. The alarm clears when utilization is above the Low Reset boundary for at least the specified duration. No action occurs if the utilization crosses a boundary for less than the specified duration.

Select a subport from a defined port, right click and select **Properties > Thresholds**. Click either (or both) **Arm High Thresholds / Arm Low Thresholds** to activate the required threshold alarming. Enter (in percentages) the High Event/Reset, Low Event/Reset settings and their respective time settings (Duration, in seconds).



Revising Configuration Settings on Multiple Blade Ports

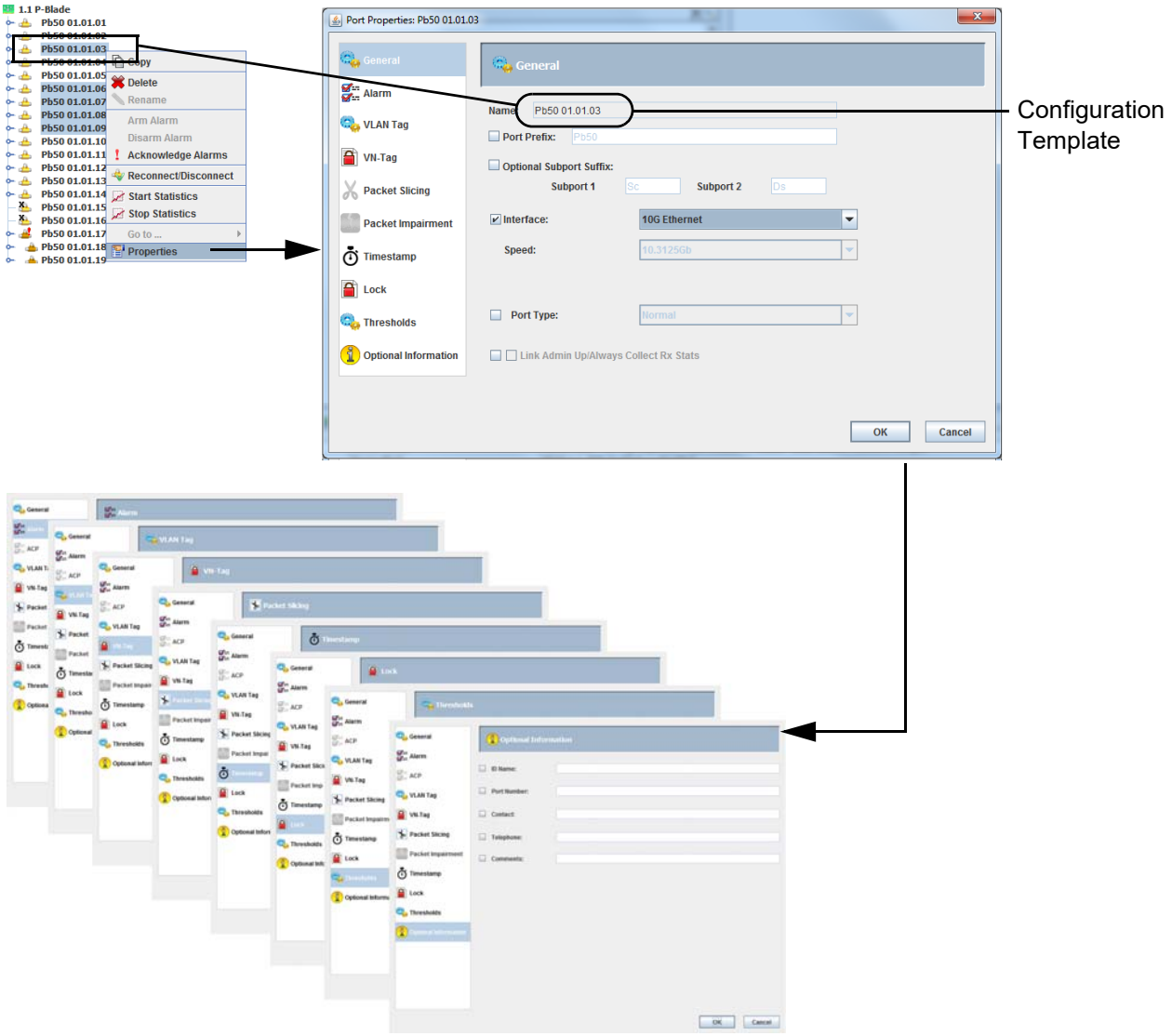
Note: Interface Type, Speed, and Alarm configuration settings cannot be modified if the selected ports are connected.

The following allows revising multiple blade ports (on the same blade) to the same configuration settings of another port at one time.

For example, Port 3 of a T-Blade is configured as a 10G Ethernet port. To change a series of ports (in this case, ports 6, 7, 8, and 9) to the same configuration as port 3, select ports 6, 7, 8, 9 then 3. Right click on the last selected port (port 3), select **Properties**.

Note: TestStream Management assigns the last port selected as the configuration template for the other selected ports.

To change the interface / speed, from the Port Properties screen, select **General**, click on the checkbox next to Interface, and select the interface type from the drop down list (in this example 10G Ethernet). If additional configuration setting changes are required (e.g., alarm, port type, optional information), access the required port properties screen and select the checkbox of the required feature. Click **OK** to make the changes. Reviewing the properties of the three additional ports shows that the ports now have the same configuration settings as the original port 3 (10G Ethernet).

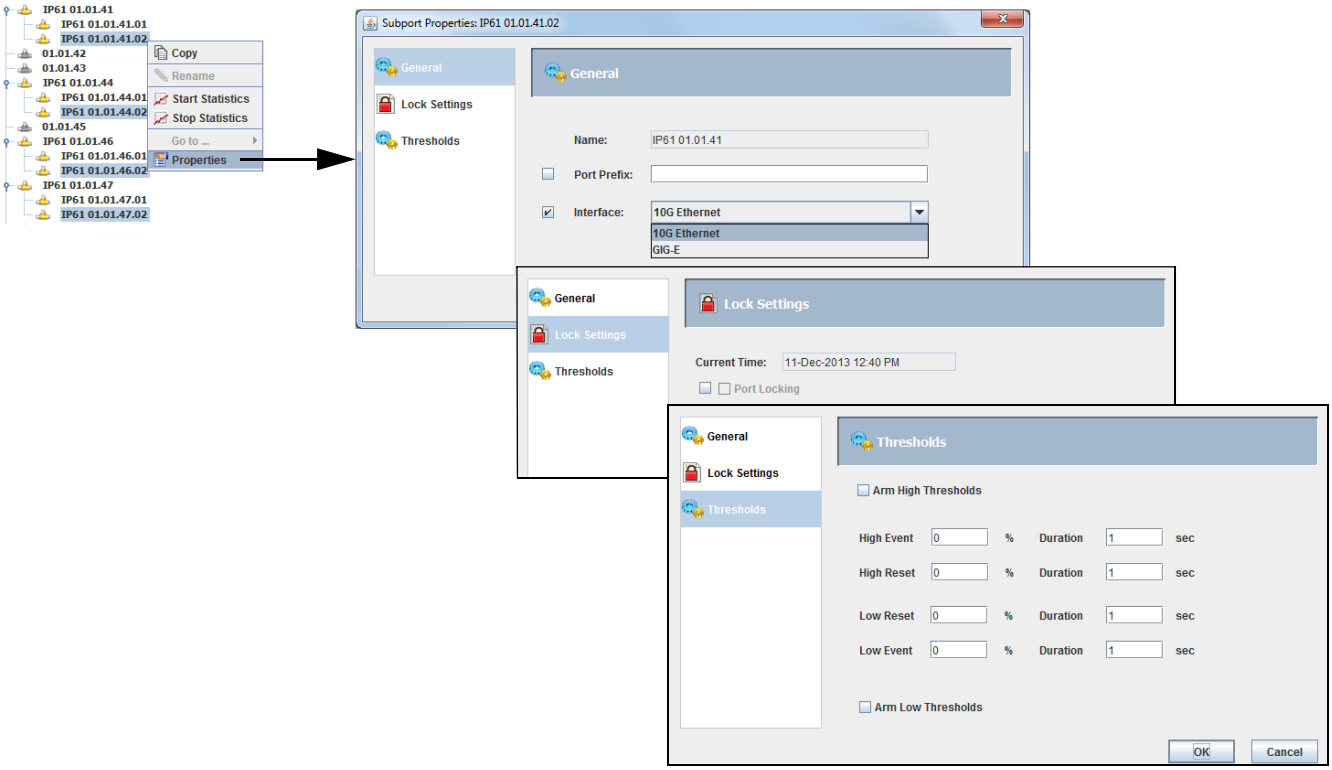


Revising Configuration Settings on Multiple Blade Sub-Ports

Similar to changing the configuration settings on multiple ports (refer to Revising Configuration Settings on Multiple Blade Ports on page 3-150), groups of sub-ports (on the same blade) can be modified.

To change a series of sub-ports to the same configuration another sub-port, select the sub-ports then the configuration-selected sub-port. Right click on the configuration-selected sub-port, then select **Properties**.

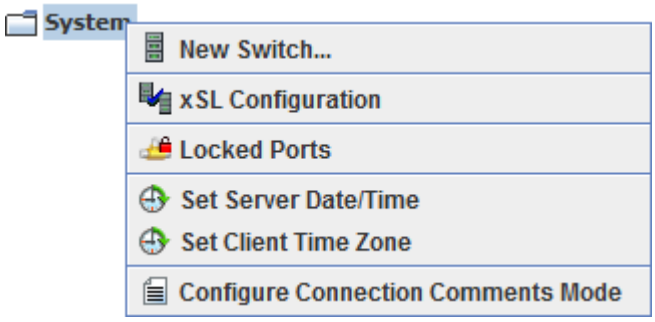
Select from either the General, Port Locking, or Thresholds sections the properties to copy to the sub-ports. Click OK to make the configuration changes.



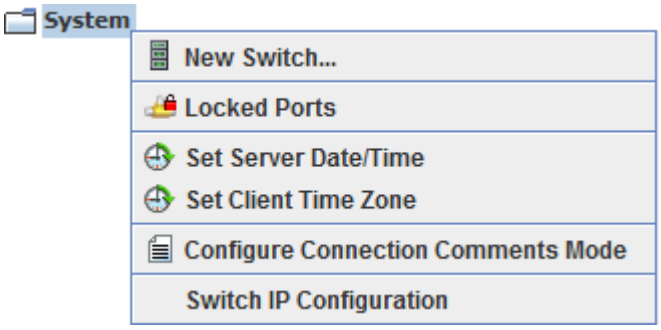
System Menu

A sub-menu, displayed when right clicking on the System icon displays the following functions:

External Server / Networked Switches



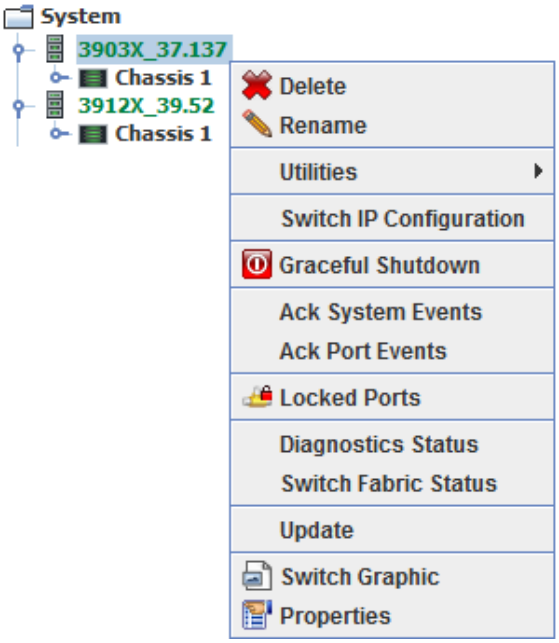
Embedded Switch



- New Switch - Refer to Adding a Switch on page 3-2.
- xSL Configuration - Refer to xSL Trunk Configuration on page 3-105.
- Locked Ports - Refer to Locked Ports on page 4-45.
- Set Server Date/Time - Refer to Set Server Date/Time on page 3-158.
- Set Client Time Zone - Refer to Client Time Zone on page 4-24.
- Configure Connection Comments Mode - Refer to Connection Comments Mode on page 4-42.
- Switch IP Configuration - Refer to Configuring Server IP Addresses on page 3-183.

Switch Menu

The nGenius 3900 series switches contain a sub-menu for additional functions. Right clicking on a defined switch displays the following menu:



- Delete - Refer to Deleting a Switch on page 3-159.
- Rename - Refer to Renaming a Switch on page 3-165.
- Utilities - Refer to Switch Utilities on page 3-156.
- Switch IP Configuration - Refer to Switch IP Configuration for nGenius 3900 Series Switches Embedded Servers on page 3-183.
- Graceful Shutdown - Refer to Graceful Shutdown on page 3-160.

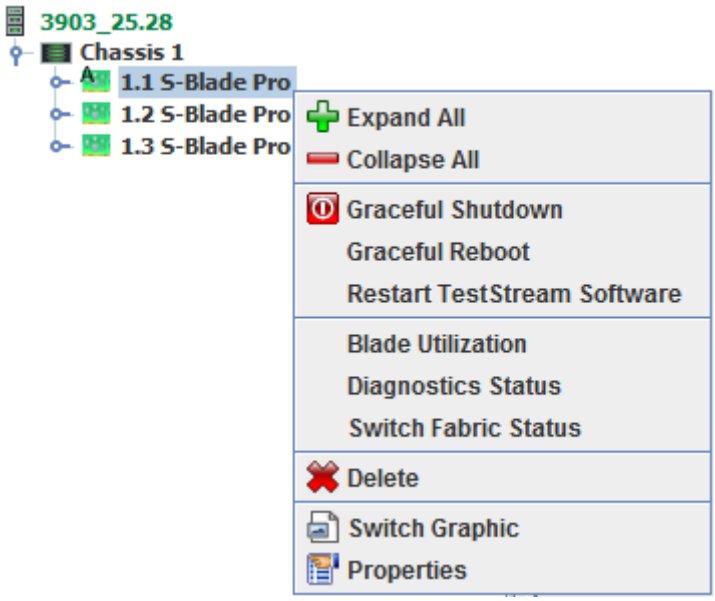
- Ack System / Port Events - Refer to Acknowledge System/Port Events from the Switch Level on page 3-165.
- Locked Ports - Refer to Locked Ports on page 4-45.
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.
- Switch Fabric Status - Refer to Switch Fabric Status on page 3-162.
- Update - Refer to Updating nGenius 3900 Series Switches on page 2-53
- Switch Graphic - Refer to Viewing Switch Details on page 3-13.
- Properties - Refer to Switch Properties on page 3-166.

Blade-Level Menus

A series of sub-menus are available for additional functions from the blade, port, and subport levels.

Blade Menus

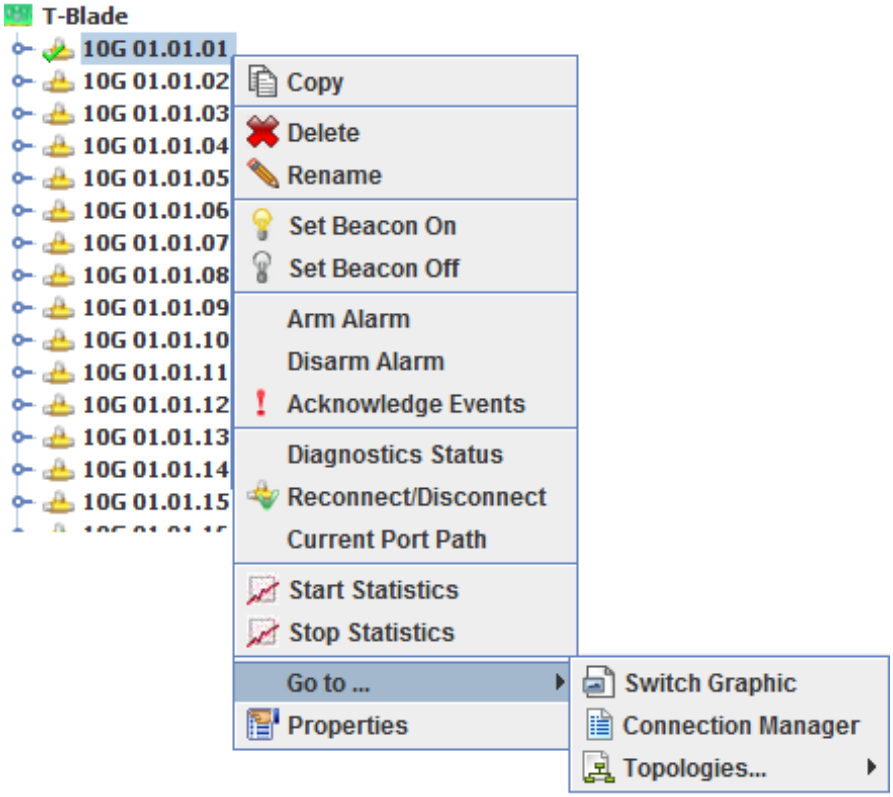
Right clicking on a defined blade displays the following menu:



- Expand All / Collapse All - Maximizes / minimizes the port and subport level views.
- Graceful Shutdown - Refer to Graceful Shutdown on page 3-160.
- Graceful Reboot - Allows a user (with Administrator security level) to reboot the selected blade; all services running on the blade are stopped avoiding any system corruption.
- Restart TestStream Software - Allows a user (with Administrator security level) to restart TestStream Management Software on the selected blade.
- Blade Utilization (S-Blade Pro) - Refer to Blade Utilization on page 3-161.
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.
- Eye Pattern (S-Blades) - Refer to Eye Pattern (Eye Diagram Analyzer) on page 7-19
- Switch Fabric Status - Refer to Switch Fabric Status on page 3-162.
- Delete - Remove a blade from the switch. This function is displayed when Auto Discrepancy Detection on the switch is off.
- Switch Graphic - Displays Switch Graphic screen (refer to Viewing Switch Details on page 3-13).
- Properties - Refer to Blade Properties on page 3-168.

Blade Port Menus

Right clicking on a defined or connected blade port displays the following menu:



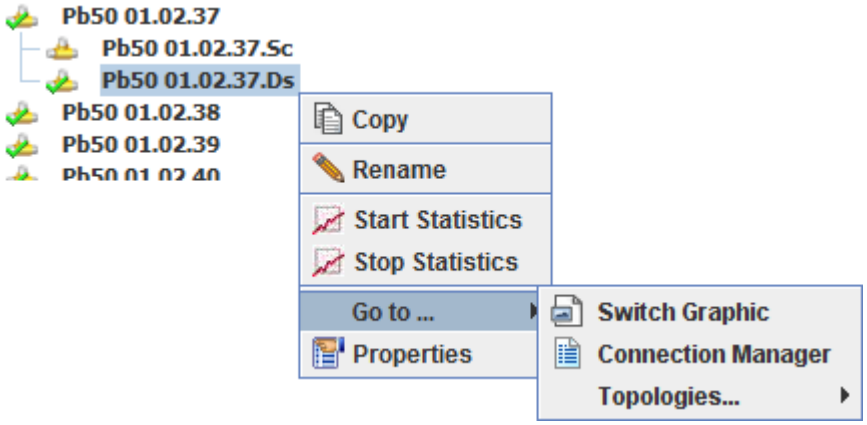
- Copy / Paste - Copies the configuration setting of a defined port and assigns the configuration to another port.
- Delete - Remove (undefine) the configuration settings of a port.
- Rename - Change the assigned name of a port.

Important: Port names cannot be made up of four (4) dotted numbers (nn.nn.nn.nn - e.g., 10.88.99.11).

- Set Beacon On / Off - Activates green and yellow pair of LED indicators on the blade to visually locate a blade port in a chassis for maintenance or troubleshooting.
- Arm / Disarm Alarm - Activate / deactivate port alarms
- Acknowledge Alarms - Acknowledge all port alarms on the specified port
- Eye Pattern (S-Blade) - Refer to Eye Pattern (Eye Diagram Analyzer) on page 7-19
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.
- Reconnect/Disconnect - Reconciles the connections of a selected port.
- Statistics Report (S-Blade Pro) - Refer to Statistics Report on page 4-15
- Current Port Path - Refer to Current Port Path on page 7-14.
- Start Statistics - Begin statistics recording
- Stop Statistics - End statistics recording
- Go to ... - Links to the following:
  - Switch Graphic
  - Connection Manager
  - Topologies
- Properties - Refer to Port Properties on page 3-170 and Port Properties - VLAN Tagging on page 3-133.

Blade Subport Menus

Right clicking on a defined or connected blade subport displays the following menu:



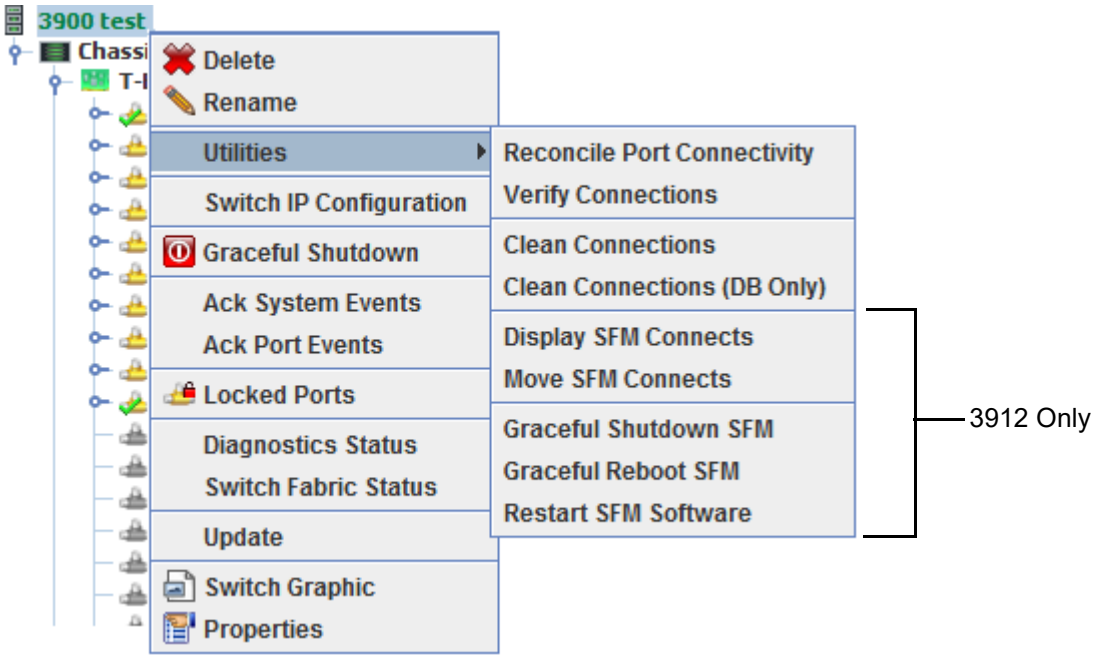
- Copy / Paste - Copy the configuration setting of a defined subport to another subport.
- Rename - Change the assigned name of a subport.

Important: Subport names cannot be made up of four (4) dotted numbers (nn.nn.nn.nn - e.g., 10.88.99.11).

- Start Statistics - Begin statistics recording
- Stop Statistics - End statistics recording
- Go to ... - Links to the following:
  - Switch Graphic
  - Connection Manager
  - Topologies
- Properties - Refer to Subport Properties on page 3-171 and Subport Properties - Threshold Settings on page 3-149.

Switch Utilities

Right-clicking on a switch and selecting **Utilities** displays the following sub-menu.



Reconcile Port Connectivity

Reconcile Port Connectivity updates the configuration in the selected switch to match the configuration stored in the TestStream Management server database (i.e., to make the switch connectivity consistent with the TestStream Management connectivity database).

Verify Connections

Verify Connections compares the TestStream Management server and controller connectivity databases on a selected switch, displaying any discrepancies between the two databases.

Clean Connections / Clean Connections (DB Only)

Clean Connections allows clearing all connections from only the TestStream Management database or from the TestStream Management database and the switch controller's databases.

- Selecting Clean Connections results in the connections in the server and the switch controller to be disconnected.
- Selecting Clean Connections (DB Only) results in the connections in the server database to be disconnected, however, all connections at the switch controller remain intact.

Note: The Clean Connection command will not clear out the Real Time Statistics status of ports enabled by a different user.

nGenius 3912 Sub-Menu Selections

Note: The sub-menu selections **Display SFM Connects** and **Move SFM Connects** are also accessible from the 3912 rear graphic view by right clicking on an active SFM and selecting either of the menu selections.

Display SFM Connects

Display SFM Connects allows selecting an SFM and displaying all of the connections going through the SFM.

Move SFM Connects

Move SFM Connects allows moving backplane connections out of an SFM (e.g., for servicing purposes). The connections from the selected SFM are disconnected and reconnected to a different SFM.

Graceful Shutdown SFM

Graceful Shutdown SFM allows selecting an SFM and gracefully shutting it down.

Graceful Reboot SFM

Graceful Reboot SFM allows selecting an SFM and rebooting the SFM.

Restart SFM Software

Restart SFM Software allows selecting an SFM and restart its TestStream Management Software.

Set Server Date/Time

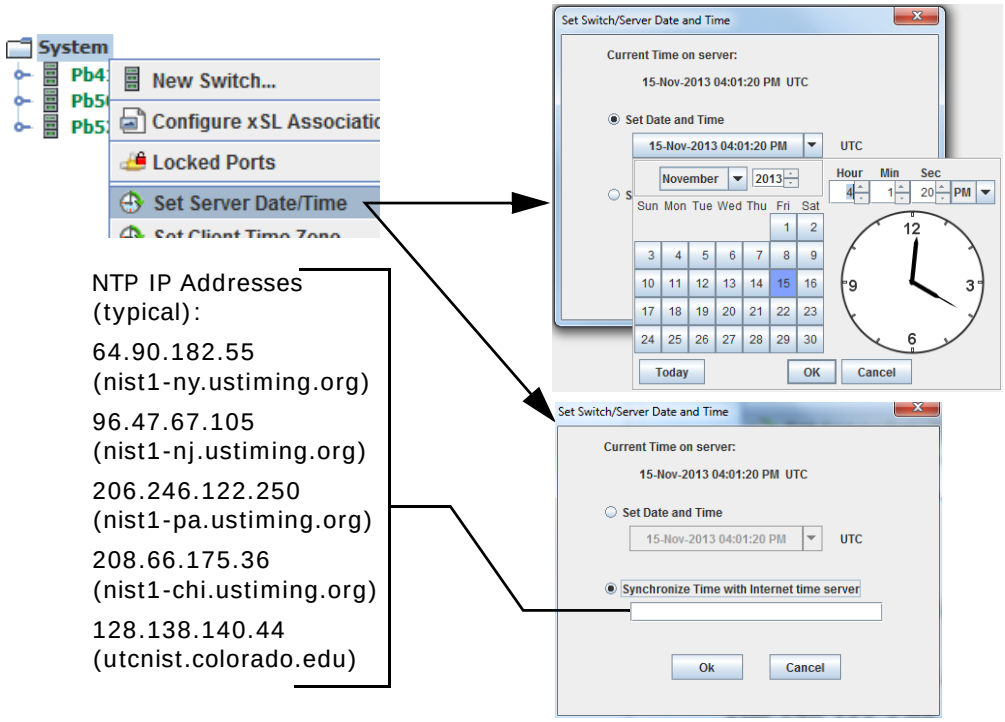
The internal real time clock of the embedded / external TestStream Management server maintains the system's date and time settings. The Set Server Date/Time menu selection allows adjusting the embedded / external TestStream Management server internal clock either manually or by using dedicated Internet Time Servers (e.g., NIST).

Note: Daylight Savings Time is not supported in TestStream Management. The time must be set manually to adjust to the time change.

---

1. From the System level, right click and select **Set Server Date/Time**. The Set Switch/Server Date and Time control screen displays.
2. Click **Set Data and Time** and select the date/time drop down menu to manually adjust the date/time settings.
   - or -
   Click **Synchronize Time with Internet Time Server** to set the date/time settings with a user defined NIST time standard. Enter a known web site (e.g., **http://nist.time.gov/**) or up to three unique NTP IP address (separated by a single space) of verified time standard sites [**example:** 64.90.182.55 206.246.122.250 128.138.140.44].

   Typical NTP Server Responses in TestStream Management Audit Trail:
   Time Synchronization switched to manual mode
   Time Synchronization started - no server selected
   Time Synchronization synchronized to xxx.xxx.xxx.xxx
3. Click **OK** on the date/time drop down menu then **OK** on the Set Switch/Server Date and Time control screen.



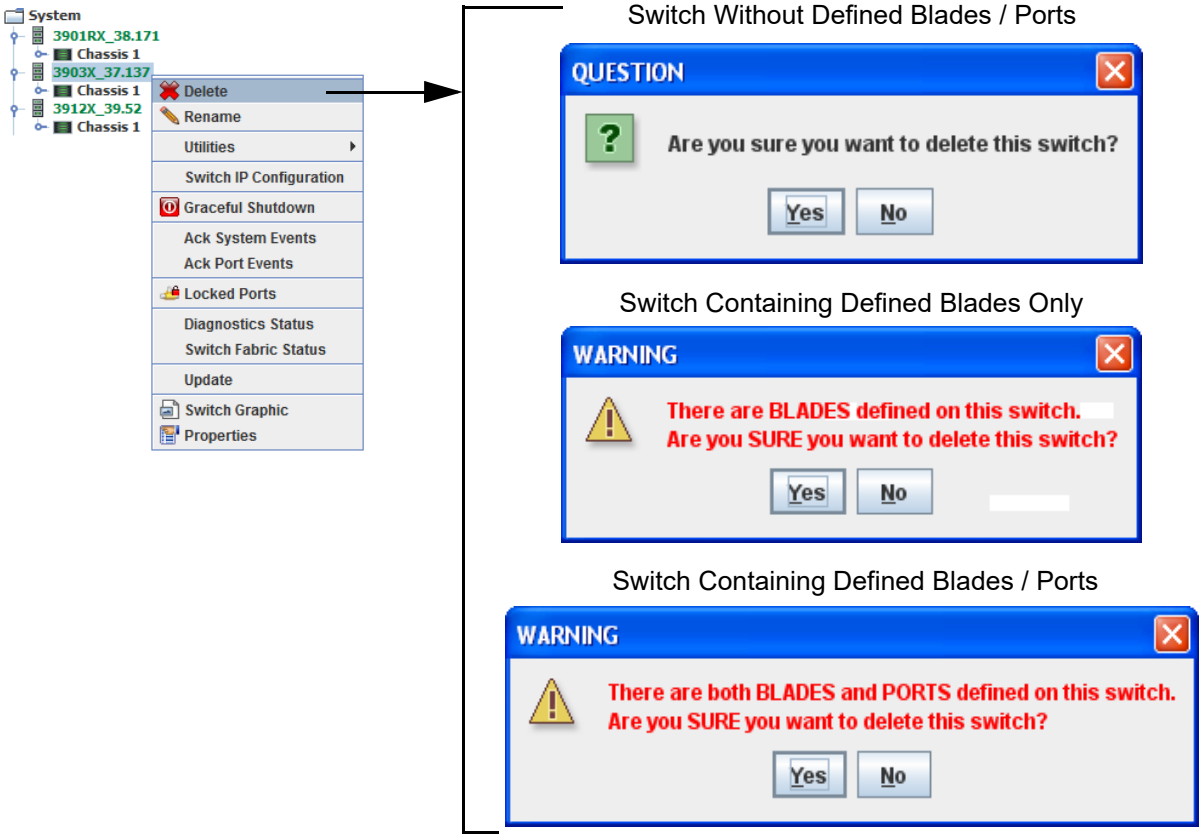
Deleting a Switch

1. From the switch level, right click on the switch name.
2. Select **Delete**.

   For switches not containing defined blades/ports (i.e., empty chassis), a question verification prompt displays.

   For switches containing defined blades/undefined ports, a warning verification prompt displays.

   For switches containing defined blades/ports, a warning verification prompt displays.
3. Click **Yes**. The selected switch is removed from the switch level listings.



Graceful Shutdown

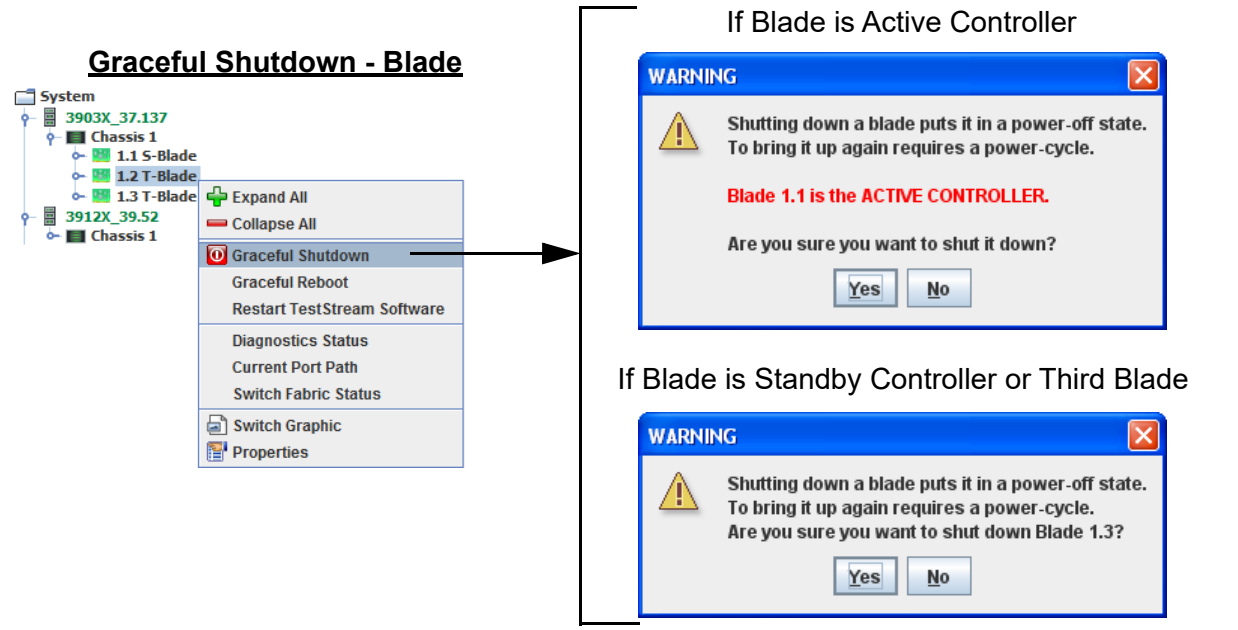
Graceful Shutdown allows shutting down the processes in a switch or an individual blade in the switch from the network. This does not physically power down the switch.

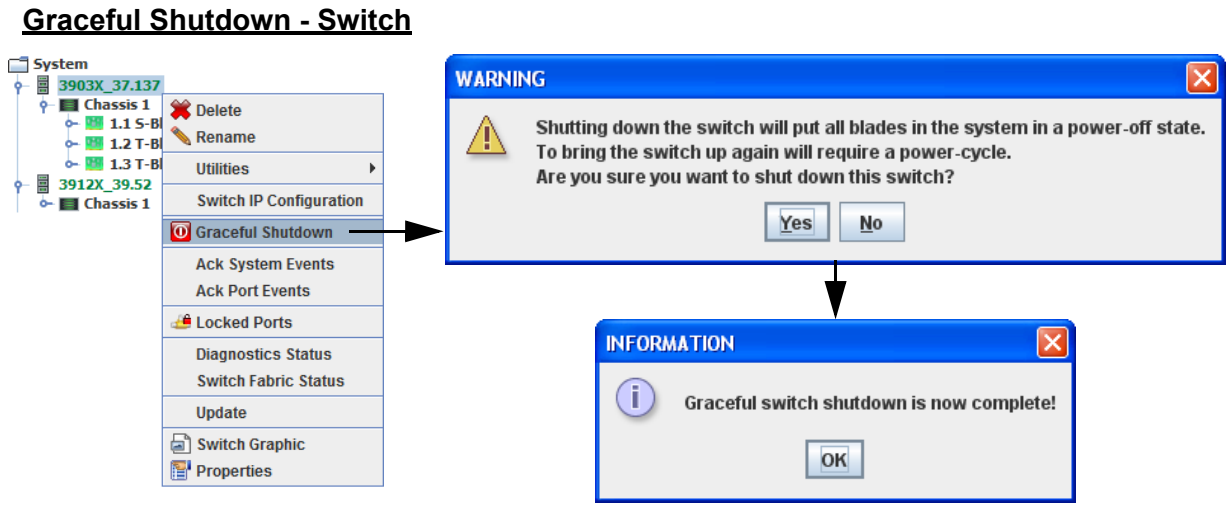
Blade Shutdown

From the blade level, select the blade to shutdown; right click and select **Graceful Shutdown**. A warning prompt displays for verification to continue with the shutdown. Click **Yes**. An information screen displays informing that the blade shutdown has finished, placing the blade in a power-off state. If the active/primary blade is shutdown, the standby/secondary blade assumes control.

Switch Shutdown

From the switch level, select the switch to shutdown; right click and select **Graceful Shutdown**. A warning prompt displays for verification to continue with the shutdown. Click **Yes**. An information screen displays informing that the switch shutdown has finished, placing the switch in a power-off state.

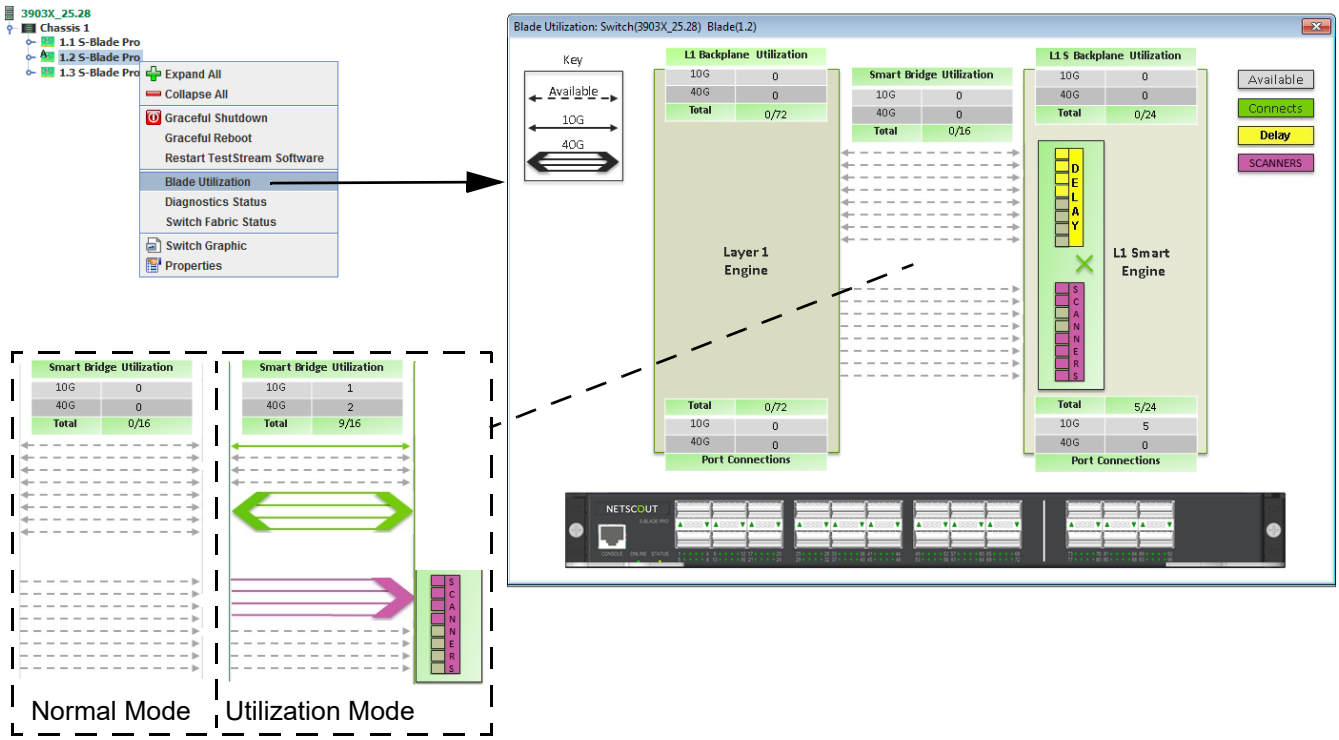




Blade Utilization

Blade Utilization describes the available / connected ports (Traditional Layer 1, Smart Layer 1, and Smart Bridge), and scanners available on a selected S-Blade Pro. The use of impairments and defined reserved lane allocations for a selected S-Blade Pro is also displayed.

From the system level, select and right-click on an S-Blade Pro blade then select Blade Utilization from the drop down menu. The Blade Utilization screen displays.



Switch Fabric Status

Switch Fabric Status displays the number of currently available 1G / 10G / 40G backplane connections between blades on a selected switch.

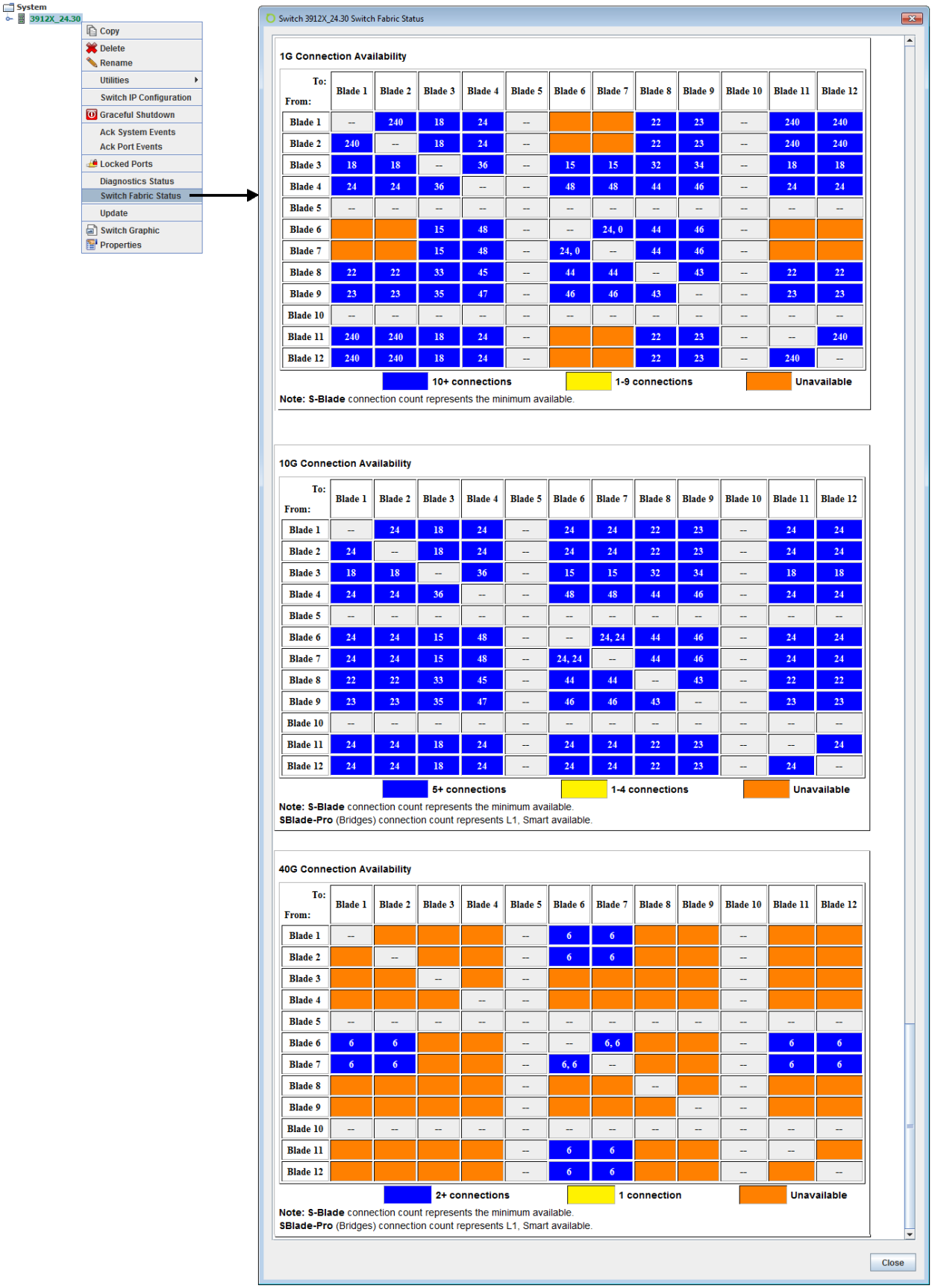
Note: Switch Fabric Status is reported only on nGenius 3903 and 3912 series switches.

Switch Level

From the switch level, right click on a switch and select **Switch Fabric Status**. A window showing the available backplane connections in relation from the active blade to each of the other installed blades, broken out by blade type and 1G / 10G / 40G connectivity, is displayed. The switch type (3903 / 3912) determines the number of blades displayed (i.e., 3903 - 3 blades, 3912 - 12 blades).

3903 System

3912 System



1G Connection Availability

From: \ To:	Blade 1	Blade 2	Blade 3	Blade 4	Blade 5	Blade 6	Blade 7	Blade 8	Blade 9	Blade 10	Blade 11	Blade 12
Blade 1	--	240	18	24	--			22	23	--	240	240
Blade 2	240	--	18	24	--			22	23	--	240	240
Blade 3	18	18	--	36	--	15	15	32	34	--	18	18
Blade 4	24	24	36	--	--	48	48	44	46	--	24	24
Blade 5	--	--	--	--	--	--	--	--	--	--	--	--
Blade 6			15	48	--	--	24, 0	44	46	--		
Blade 7			15	48	--	24, 0	--	44	46	--		
Blade 8	22	22	33	45	--	44	44	--	43	--	22	22
Blade 9	23	23	35	47	--	46	46	43	--	--	23	23
Blade 10	--	--	--	--	--	--	--	--	--	--	--	--
Blade 11	240	240	18	24	--			22	23	--	--	240
Blade 12	240	240	18	24	--			22	23	--	240	--

10G Connection Availability

From: \ To:	Blade 1	Blade 2	Blade 3	Blade 4	Blade 5	Blade 6	Blade 7	Blade 8	Blade 9	Blade 10	Blade 11	Blade 12
Blade 1	--	24	18	24	--	24	24	22	23	--	24	24
Blade 2	24	--	18	24	--	24	24	22	23	--	24	24
Blade 3	18	18	--	36	--	15	15	32	34	--	18	18
Blade 4	24	24	36	--	--	48	48	44	46	--	24	24
Blade 5	--	--	--	--	--	--	--	--	--	--	--	--
Blade 6	24	24	15	48	--	--	24, 24	44	46	--	24	24
Blade 7	24	24	15	48	--	24, 24	--	44	46	--	24	24
Blade 8	22	22	33	45	--	44	44	--	43	--	22	22
Blade 9	23	23	35	47	--	46	46	43	--	--	23	23
Blade 10	--	--	--	--	--	--	--	--	--	--	--	--
Blade 11	24	24	18	24	--	24	24	22	23	--	--	24
Blade 12	24	24	18	24	--	24	24	22	23	--	24	--

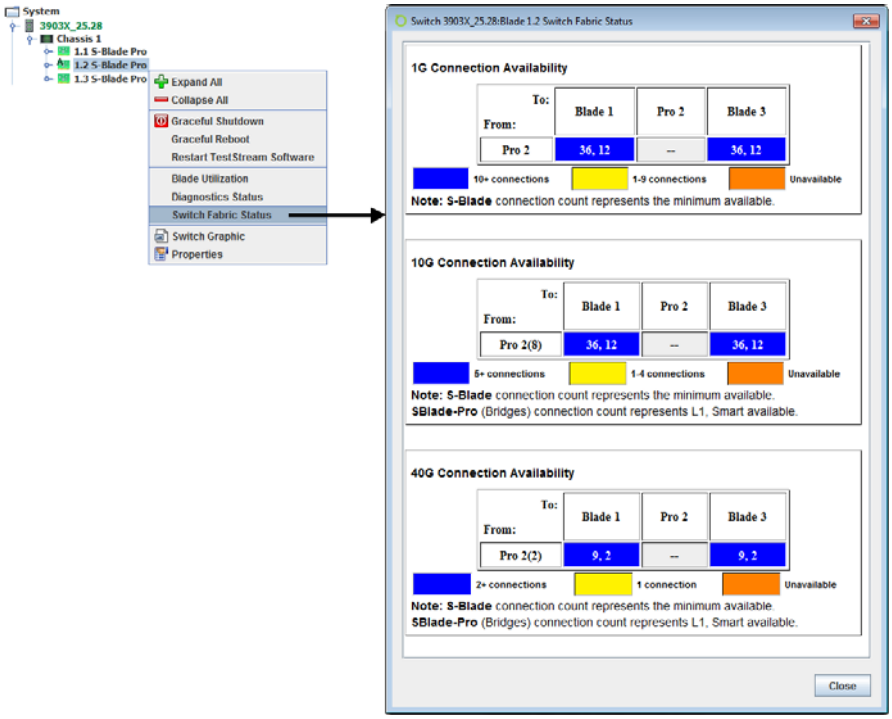
40G Connection Availability

From: \ To:	Blade 1	Blade 2	Blade 3	Blade 4	Blade 5	Blade 6	Blade 7	Blade 8	Blade 9	Blade 10	Blade 11	Blade 12
Blade 1	--				--	6	6			--		
Blade 2		--			--	6	6			--		
Blade 3			--		--					--		
Blade 4				--	--					--		
Blade 5	--	--	--	--	--	--	--	--	--	--	--	--
Blade 6	6	6			--	--	6, 6			--	6	6
Blade 7	6	6			--	6, 6	--			--	6	6
Blade 8					--			--		--		
Blade 9					--				--	--		
Blade 10	--	--	--	--	--	--	--	--	--	--	--	--
Blade 11					--	6	6			--	--	
Blade 12					--	6	6			--		--

Blade Level

From the blade level, right click on a blade and select **Switch Fabric Status**. A window showing the available backplane connections in relation to the selected blade and the other blades in the chassis, broken out for 1G / 10G / 40G connections, is displayed. The switch type (3903 / 3912) determines the number of blades displayed (i.e., 3903 - 3 blades, 3912 - 12 blades).

3903 System

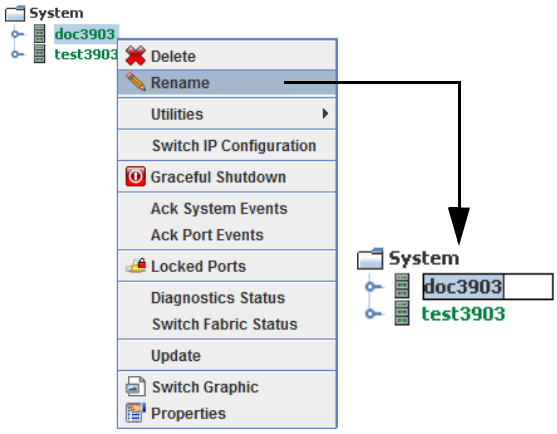


3912 System

Renaming a Switch

1 From the switch level, right click on the switch name.

2 Select **Rename**. Type the new name in the highlighted text field. Click outside of the text field to retain the changes.

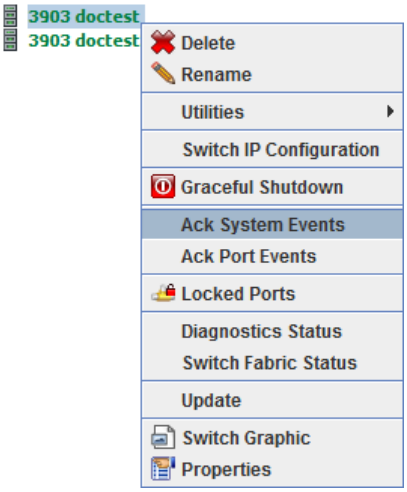


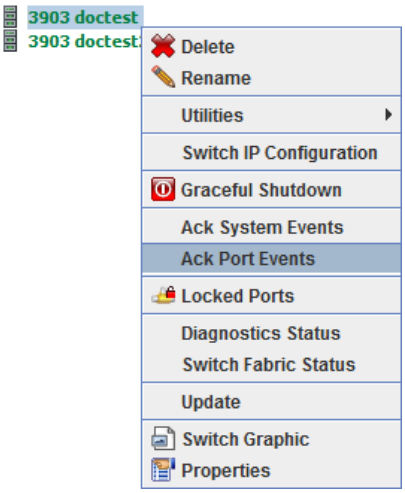
Acknowledge System/Port Events from the Switch Level

To acknowledge system or port events on a single switch from the switch level:

1 From the switch level, right click on the switch name.

2 For system events, select **Ack System Events**. All system events on the selected switch are now acknowledged.
For port events, select **Ack Port Events**. All port events on the selected switch are now acknowledged.





Switch Views

Refer to Viewing Switch Details on page 3-13.

Diagnostics Status

Refer to Diagnostics Status on page 7-1.

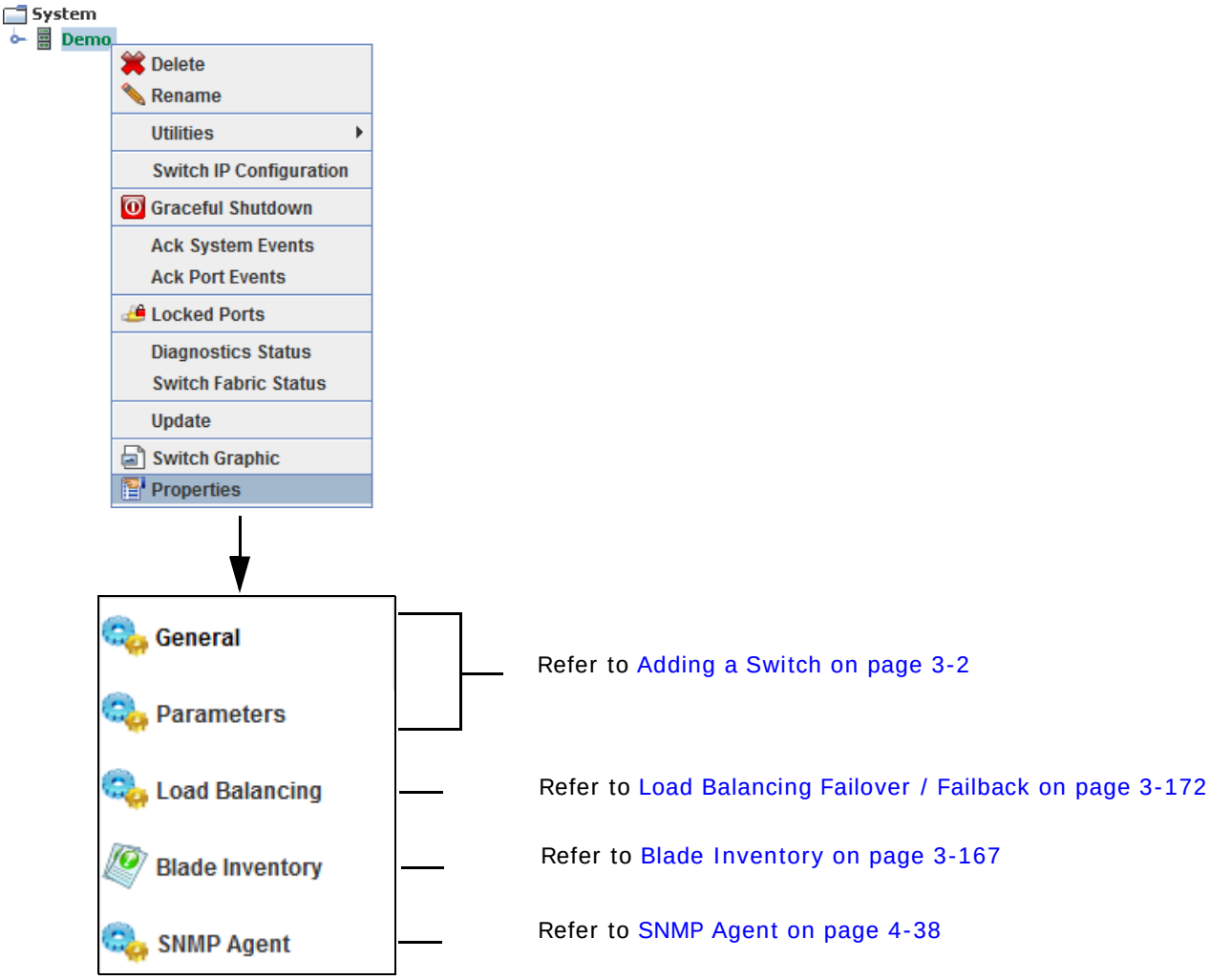
Properties

Selecting **Properties** under their respective areas (i.e., Switch, Blade, Port, Subport) provides a summary of the current configuration settings.

Switch Properties

To view switch configuration information:

1. From the switch level, right click on the switch name.
2. Select **Properties**. The Switch Properties window displays.



Blade Inventory

Blade Inventory displays a list of installed devices (3901 / 3903 / 3912 / HS-3200 / HS-6400), SFM / SFM Pros (3912), and the version of TestStream Management Software installed in each device / SFM / SFM Pro in a switch.

Blade Slot Blade Information TestStream Version / Build

Blade Inventory

```
BLADE 1     T-BLADE  UBoot 9 0234 ED:: 0317132010008   04.02.200.045
```

3901 / 3901R

Blade Inventory

```
BLADE 1     S-Blade Pro  UBoot 106   3.10. E2::PSB160488047   04.02.200.045
BLADE 2     S-Blade Pro  UBoot 106   3.10. E2::PSB160688002   04.02.200.045
BLADE 3     S-Blade Pro  UBoot 106   3.10. E2::TSP161288004   04.02.200.045
```

3903

Blade Inventory

```
BLADE 1     T-BLADE  UBoot 9 0234 ED:: 031803010010   04.02.200.045
BLADE 2
BLADE 3     S-BLADE  UBoot 4 0234 E1:: 031408010013   04.02.200.045
BLADE 4     S-BLADE  UBoot 4 0234 E1:: 031703020022   04.02.200.045
BLADE 5
BLADE 6
BLADE 7
BLADE 8
BLADE 9
BLADE 10
BLADE 11
BLADE 12
BLADE 13    SFM    U4  24d 0234 AAAA:: 031843080031   04.02.200.045
BLADE 14
BLADE 15
BLADE 16
BLADE 17
BLADE 18
BLADE 19
BLADE 20
```

3912 (SFMs)

Blade Inventory

```
BLADE 1     T-Blade     UBoot 9     0234 F0::TSB140688043   04.02.200.045
BLADE 2     T100-Blade  UBoot 106   0234 EE::T1234567890    04.02.200.045
BLADE 3     S-Blade     UBoot 4     0234 E1::020101100015   04.02.200.045
BLADE 4     S-Blade     UBoot 4     0234 E1:: 031703020022  04.02.200.045
BLADE 5
BLADE 6     S-Blade Pro  UBoot 106   3.10. E2::PSB160688005   04.02.200.045
BLADE 7     S-Blade Pro  UBoot 106   3.10. E2::PSB160688001   04.02.200.045
BLADE 8     S-Blade     UBoot 4     0234 E1:: 031408010015  04.02.200.045
BLADE 9     S-Blade     UBoot 4     0234 E1:: 031703010028  04.02.200.045
BLADE 10
BLADE 11    T-Blade     UBoot 9     0234 F0:: T318767010001  04.02.200.045
BLADE 12    T-Blade     UBoot 9     0234 F0::T318767010002  04.02.200.045
BLADE 13    SFM Pro     UBoot 106   3.10. E1::TFP170188007   04.02.200.045
BLADE 14    SFM Pro     UBoot 106   3.10. E1::TFP170188015   04.02.200.045
BLADE 15    SFM Pro     UBoot 106   3.10. E1:: TFP170188016  04.02.200.045
BLADE 16    SFM Pro     UBoot 106   3.10. E1::TFP160988004   04.02.200.045
BLADE 17
BLADE 18
BLADE 19
BLADE 20
```

3912 (SFM Pros)

Blade Inventory

```
BLADE 1     HS-Bank 32x100G, 64x50G, 32x40G, 64x25G, 64x10G   04.04.200.049
```

HS-3200

Blade Inventory

```
BLADE 1     HS-Bank 64x100G, 128x50G, 64x40G, 128x25G, 128x10G   05.01.000.019
```

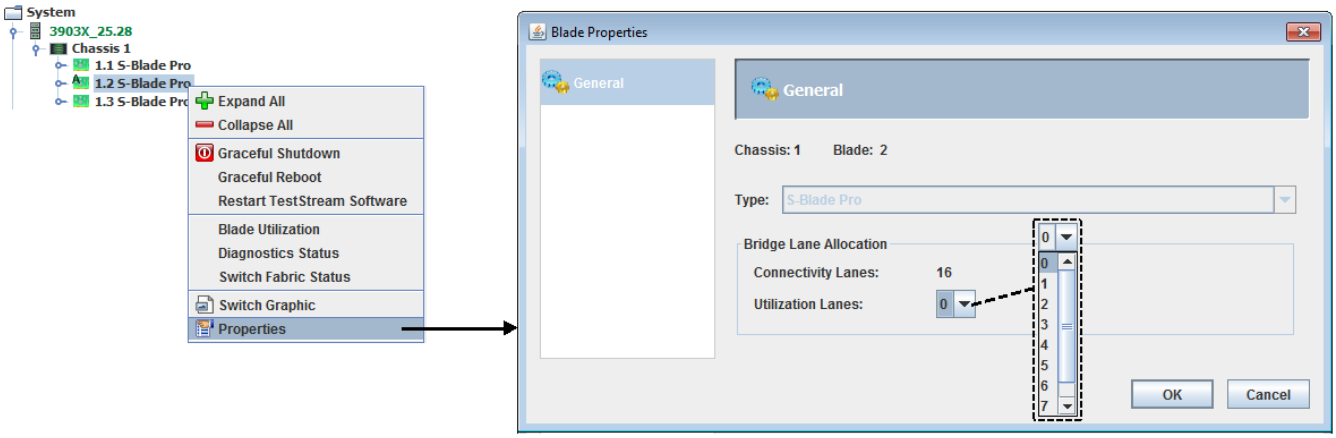
HS-6400

Blade Properties

To view blade type information:

1. From the blade level, right click on the blade name in the switch.
2. Select **Properties**. The Blade Properties window displays.

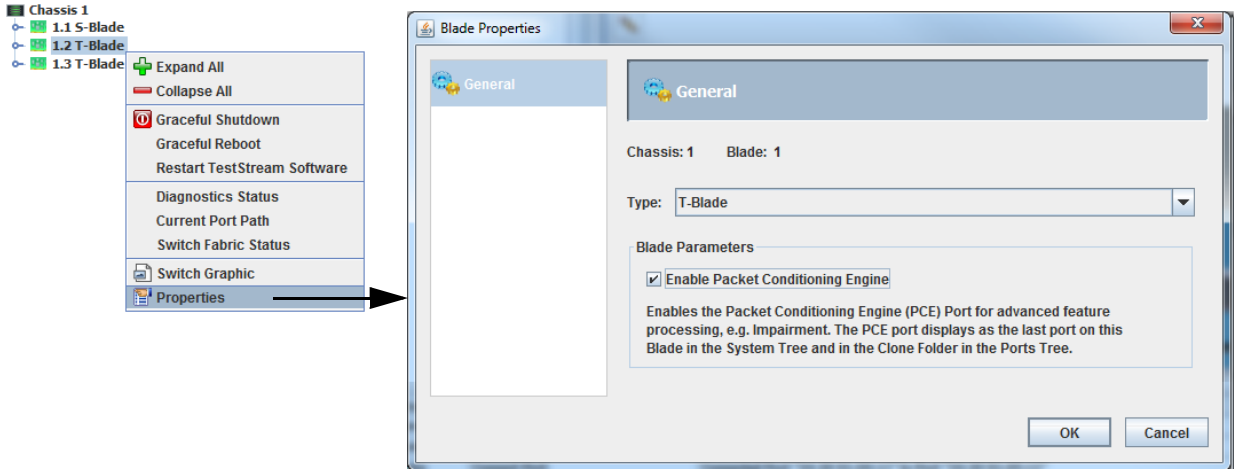
S-Blade Pro



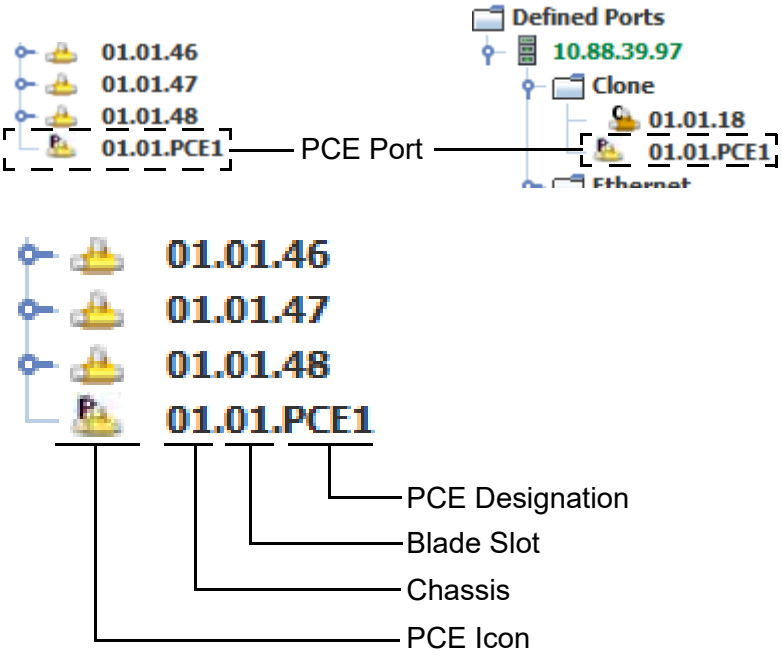
Bridge Lane Allocation - In the S-Blade Pro, 16 bridge lanes are available for sharing across features. You can assign the number of bridge lanes (from 0 to 8) for Utilization Mode (refer to **S-Blade Pro Mode** on page 3-7). All remaining lanes are available for connectivity.

By default, a new switch will have all 16 bridge lanes allocated for connectivity. An upgraded switch will have all 16 lanes allocated for connectivity if the switch was in Normal Mode (refer to **S-Blade Pro Mode** on page 3-7), otherwise the lanes are allocated for 8 connectivity / 8 utilization.

T-Blades

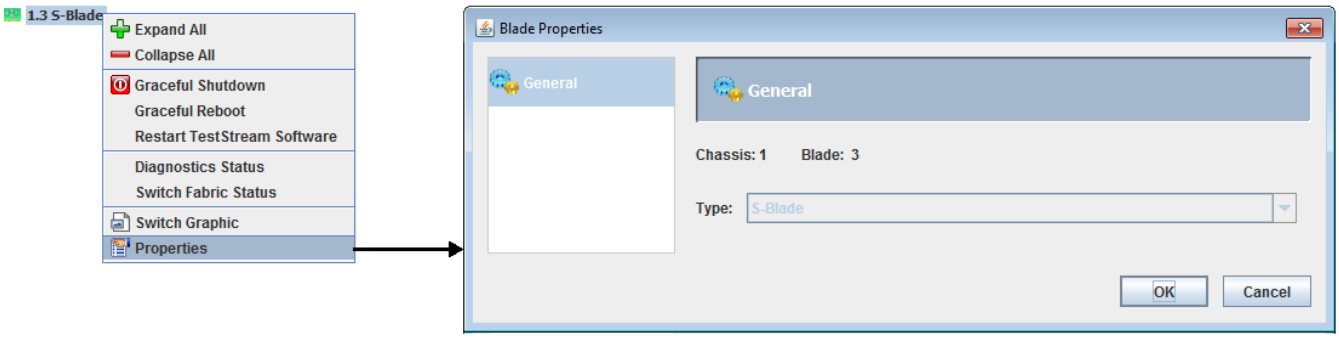


Optionally, to enable the Packet Conditioning Engine (PCE) port on the blade for advanced feature processing (e.g., Impairment; refer to Port Properties - Packet Impairment on page 3-142), click on **Enable Packet Conditioning Engine** then **OK**. A new PCE port is displayed under the System tab at the port level of the blade and under the Ports/Groups tab under Defined Ports in the Clone ports folder.



The PCE port contains the functionally of a Clone port, including configuration, use within topologies, alarming, and statistics.

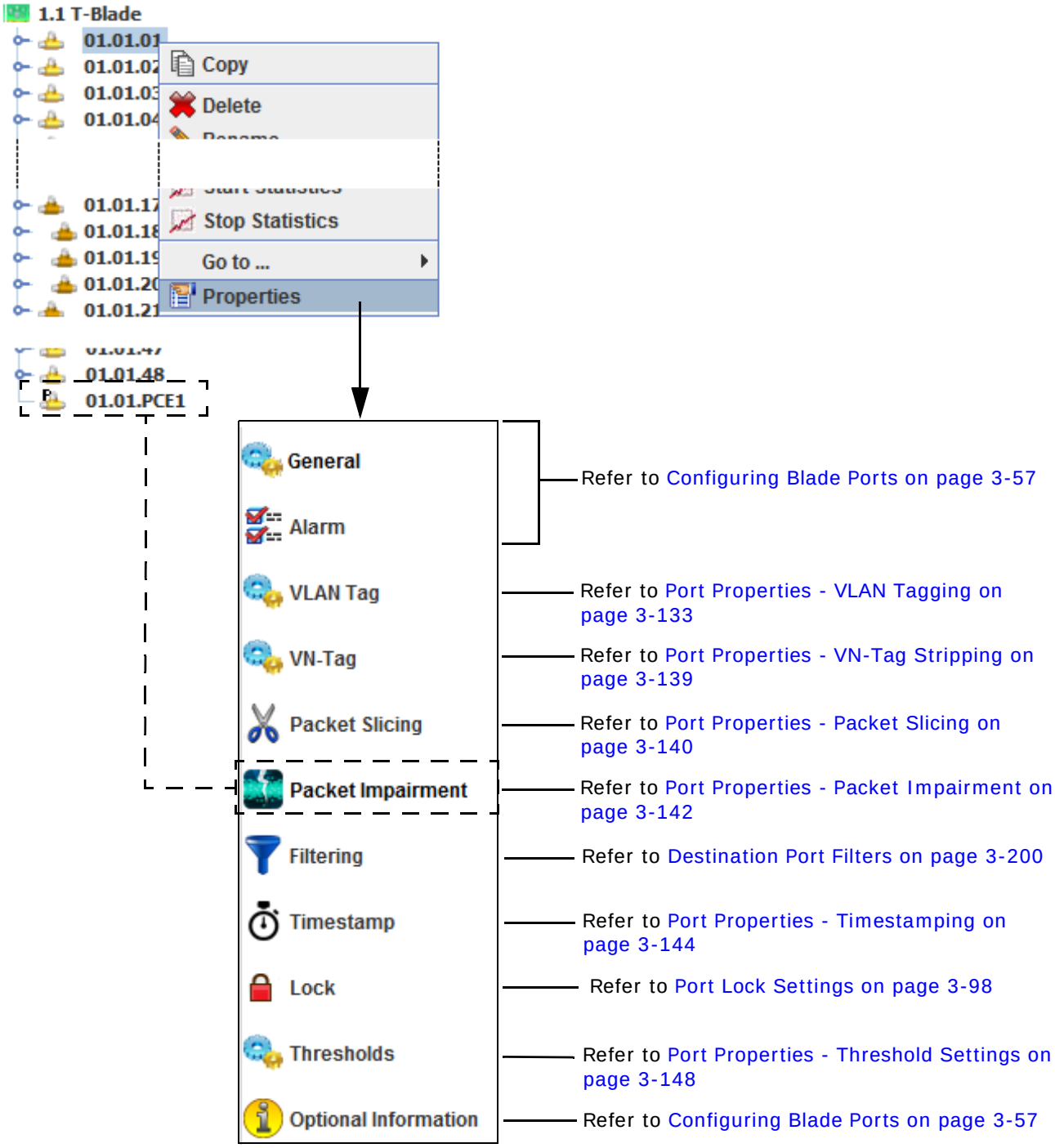
S-Blades



Port Properties

To view port configuration information:

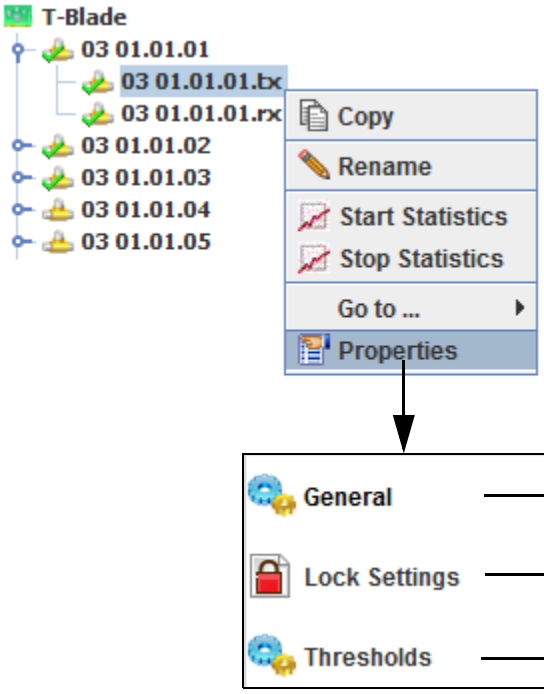
1. From the port level, right click on the port name in the blade.
2. Select **Properties**. The Port Properties window displays.



Subport Properties

To view subport configuration information:

1. From the subport level, right click on either subport name under a port.
2. Select **Properties**. The Subport Properties window displays.



Refer to Configuring Blade Ports on page 3-57

Refer to Port Lock Settings on page 3-98

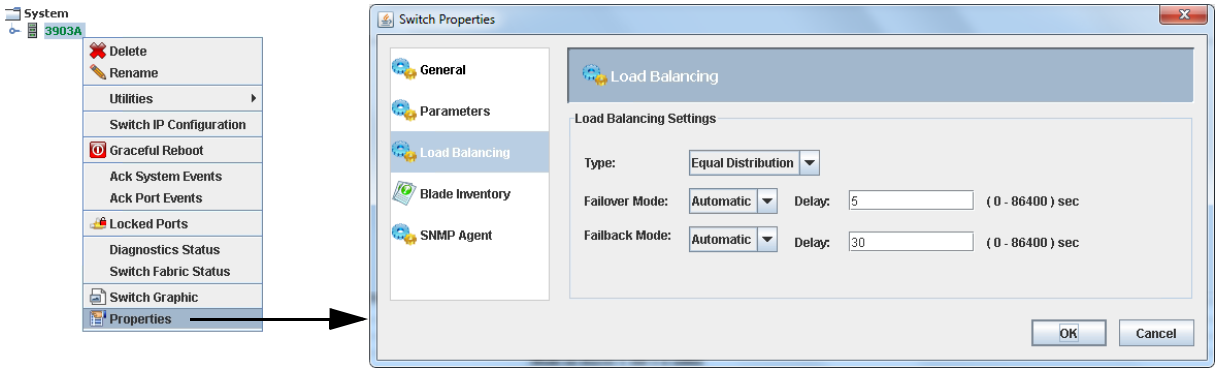
Refer to Subport Properties - Threshold Settings on page 3-149

Load Balancing Failover / Failback

Load Balancing Failover provides the ability of identifying link failures in a load balancing group (LBG), automatically re-balancing the traffic on the remaining good links of the LBG, and provides Failback capability when a failed link in an LBG recovers; minimizing monitor traffic loss in the event of a link failure to monitoring tools. This feature automatically recovers the full traffic stream into the tool when a link failure occurs, allowing the end-user to investigate and resolve the issue as their schedule permits.

Load Balancing Failover is configured on a per switch basis from the Switch Properties screen.

1. From the switch level, right click on a switch name.
2. Select **Properties > Load Balancing**. The Load Balancing window displays.



Set the Load Balancing Type to either Equal Distribution (default) or Session-Based. This setting defines the method used to distribute output traffic to multiple destinations:

- Equal Distribution – distributes packets evenly across all ports within the Load Balancing Group. The equal balancing helps reduce the risk of over-subscription on any given port.

  When generating traffic where all of the frames are the exact same size, you can use a formula to figure out how many ports will have more traffic than the other ports. The T-Blade distributes traffic into 96 bins, with each bin assigned to an egress port. More than one bin can be assigned to the same egress port. Whether every egress port in the load balancing group gets assigned the same number of bins depends on how many ports there are in the load balancing group.

  Example 1:
  A load balancing group contains 32 ports (96 bins /32 ports = 3). In this case each port is assigned three bins, all of the same type; therefore, you should see about the same amount of traffic on each port.

  Example 2:
  A load balancing group contains only 31 ports (96 bins / 31 ports = 3, with a remainder of 3). In this case, all of the ports will have at least 3 bins assigned to them, with three ports having one extra bin assigned to them for a total of 96 bins. The three ports with the extra bins will get more traffic than the other ports.

- Session-Based – distributes packets to ports based on their session. A session is determined by the following fields in the packet header:
  - Non-IP frames:
    - Source and Destination MAC Addresses
    - EtherType
  - IPv4 and IPv6 Frames:
    - Source and Destination IP Addresses
    - Layer 4 Protocol

Session-based load balancing sends all frames of a session, either direction, to the same port of the Load Balancing Group.

Unicast MPLS-Tagged IP frames are load balanced as IPv4 or IPv6 frames based on the fields in the encapsulated IP packet. MPLS-MULTICAST frames are treated as non-IP frames, therefore the session is based on the source and destination MAC address. All MPLS-MULTICAST frames that have the same source and destination MAC addresses should be sent to the same destination port of a load balancing destination group. MPLS-UNICAST frames that carry IP packets base the session on the source and destination IP addresses and L4 Protocol in the encapsulated IP packet.

For VN-Tagged frames, the Switch Parameter for VN-Tag Detection must be enabled in order for session-based load balancing to be based on the fields in the encapsulated frame. When VN-Tag Detection is not enabled, VN-Tagged frames are treated as non-IP frames.

Note:
A Destination Group configured for load balancing supports up to 32 egress ports.

When using Session-based Load Balancing, all of the destination ports in a load balancing group must be on the same switch, but may reside on any T-Blade within that switch.

When using Equal-distribution Load Balancing, all of the destination ports in a load balancing group must reside on the same T-Blade.

Source ports being load balanced do not have any restrictions with respect to their location relative to the destination ports in the load balancing group; they may reside on any T-Blade within the 3900 switch containing the destination ports, or on other 3900 switches when using Cross-switch Links (xSLs) to reach the destination ports.

Set Failover Mode: Select either Automatic (default) or Manual mode. Enter the delay timer value (in seconds, range = 0 to 86400 (24 hours), default is 5 seconds).

Set Failback Mode: Select either Automatic or Manual (default) mode. Enter the delay timer value (in seconds, range = 0 to 86400 (24 hours), default is 30 seconds).

Load Balancing Failover / Failback Configurations

Load Balancing Failover / Failback configurations are applicable from the switch level and applies to all of the Load Balancing groups existing on the nGenius 3900 series switch.

The following combinations are supported:

- Manual Failover and Manual Failback
- Manual Failover and Automatic Delayed (in seconds) Failback
- Automatic Delayed (in seconds) Failover and Manual Failback
- Automatic Delayed (in seconds) Failover and Automatic Delayed (in seconds) Failback

Note: If a delay of zero seconds is specified, then the Failover / Failback event happens immediately.

Manual Failover / Failback

When operating in the Automatic failover / failback mode for some time, and then the link recovers and failback occurs, many sessions being monitored will be moved, which is not desirable. In order to address this issue the Manual failover/failback mode will be provided. When the Manual failback is set as well as the Automatic failover with 5 second delay, if the failed link recovers, the failback won't kick in until a user sets the failback mode to Automatic. All the pending failback operation will be applied with the delay.

Automatic Failover / Failback with Delay

Frequent link state up/down events, which sometimes can be caused by the connected tool, shall cause unnecessary packet drops under the link state up and down and its subsequent failover operation. In order to address this issue, CLI commands will be provided so that a user can set the delay (one for the failover and the other for the failback) per an nGenius 3900 switch. The delay timer values for failover and failback will range from 0 to 86400 seconds (24 hours). The default delay for failover is 5 seconds, and that for failback is 30 seconds.

Failover / Failback Status Conditions

Failover/Failback actions happen on a per port basis so depending on whether a port is linkup/down and belonging to a set of the ports that are being load balanced, it will have different states. The allowed states for the ports that are a part of an LBG are as follows:

- Load Balancing Normal – Port is up and actively load-balancing traffic.
- Load Balancing Failover Pending – ort is down and dropping traffic as its traffic has not yet rebalanced.
- Load Balancing Failover Active – Port is down and its traffic has been actively rebalanced to other ports in the LBG.
- Load Balancing Failback Pending – Port has come back up but the traffic has not yet rebalanced.

As there are multiple ports in a load balancing group, they can all be in various states and based on their states the load balancing group can have the following conditions:

- LBG Normal – All ports in the LBG are actively load-balancing the traffic.
- Failover Pending – Port(s) have failed but have not been failed over either due to the Failover being set to Manual or the delay timer not having expired.
- Failover Active – Failed port(s) are failed over and their traffic rebalanced.
- Failback Pending – Previously failed port(s) whose traffic was rebalanced to other ports has come back up but not carrying traffic yet either due to the Failback being set to Manual or the delay timer not having expired.
- Failover Pending and Failover Active – At least one port is in the failover pending state and another port is in the failover active state.
- Failback Pending and Failover Active – At least one port is in the failback pending state and another port is in the failover active state.
- Failover Pending and Failback Pending – At least one port is in the failover pending state and another port is in the failback pending state.
- Failover Pending, Failback Pending and Failover Active – There are three ports in three different states of being in failover pending, failback pending and failover active.
- Deactivated – Topology which has the group disabled.

T-Blade Failure / Restart

When a T-Blade fails or restarts in the Automatic failover mode with delay, the failover is applied immediately no matter what kind of delay settings a user has defined. When a T-Blade fails in the Manual Failover mode, the failover is deferred until a user responds to the failure.

Table 3-2 describes the behavior of the Load Balancing Group (LBG) during a T-Blade restart.

Table 3-2 Load Balancing Group Restart Combinations

	Manual Failover	Manual Failover	Automatic Failover	Automatic Failover
	Manual Failback	Automatic Failback	Manual Failback	Automatic Failback
Chassis Startup	No LGB Rebalance occurs for failed ports	No LGB Rebalance occurs for failed ports	Down LGB ports are failed over	Down LGB ports are failed over

Table 3-2 Load Balancing Group Restart Combinations

T-Blade Goes Down (Note 1)	No LGB Rebalance occurs; traffic is dropped	No LGB Rebalance occurs; traffic is dropped	LGB is rebalanced for the ports on the failed T-Blade	LGB is rebalanced for the ports on the failed T-Blade
T-Blade Comes Up (Note 2)	No LGB Rebalance occurs; traffic resumes	LGB is rebalanced for the ports that come up	No LGB Rebalanced occurs; traffic is not dropped	LGB is rebalanced for the ports that come up
Note 1: If the T-Blade that goes down is an Active controller and Standby exists (with Ethernet connectivity), switchover occurs and the new Active Controller re-balances the LBGs based on the Failover and Failback settings. **Note 2:** If the T-Blade that goes down is an Active controller and Standby does not exist (or exists but doesn't have Ethernet connectivity), Active controller comes back up, learns the current LBG port availabilities from the cards that are already ONLINE, and re-balances the LBGs based on that information.				

Re-balancing a Load Balancing Group

Changing the mode from Manual to Automatic results in a re-balancing of all the LBGs. When Failover is changed from Manual to Automatic, only the ports that are DOWN are rebalanced and when the Failback is changed from Manual to Automatic, only the ports that are UP and were previously DOWN has the traffic rebalanced to them. Re-balancing happens after the newly configured delay timer expires. Specifying a delay of zero seconds ensures an immediate re-balance.

Note: An alternative method can be done through Port Properties. Select (right-click) the port that is down and set Configure Power Always Off. This should cause an immediate re-balance. When the port is available again, the power option can be returned to “as needed” or “always on”.

Viewing Load Balancing Settings

The current state of the Load Balancing Group and associated ports are displayed using various icon overlays as well as tool-tips. Whenever a port in a LBG is in any state other than *LB Normal* it displays a red triangle on the top right corner of the port icon to indicate some condition. In addition, the Load Balancing Group icon displays the same red triangle on it indicating the same.

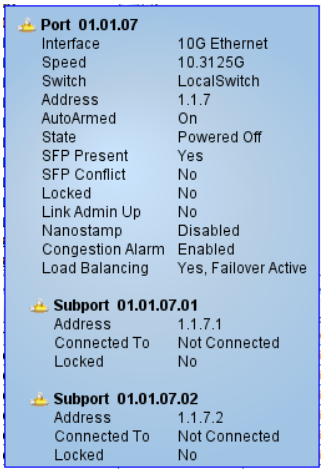
The default state for a LBG where all ports are up and actively load balancing the traffic is the *LBG Normal* state.

Load Balancing Group Is Normal (all ports in LBG up)

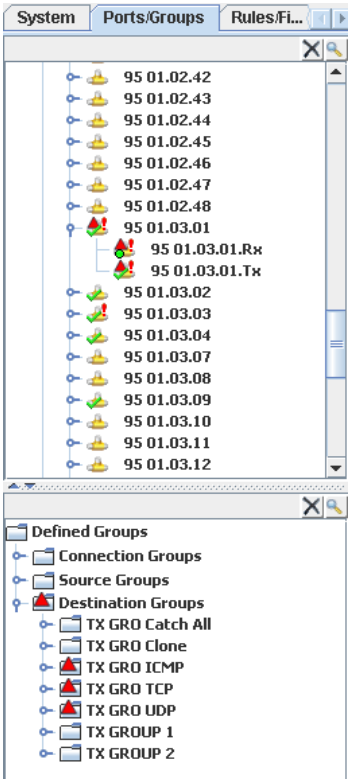
When a port is in a state other than “LB Normal” it displays a red triangle indicating that there is some problem with it. In addition, the group icon displays the same red triangle.

The tool-tip for the LBG displays the red triangle to indicate the state the port is in that warrants the warning indicator.

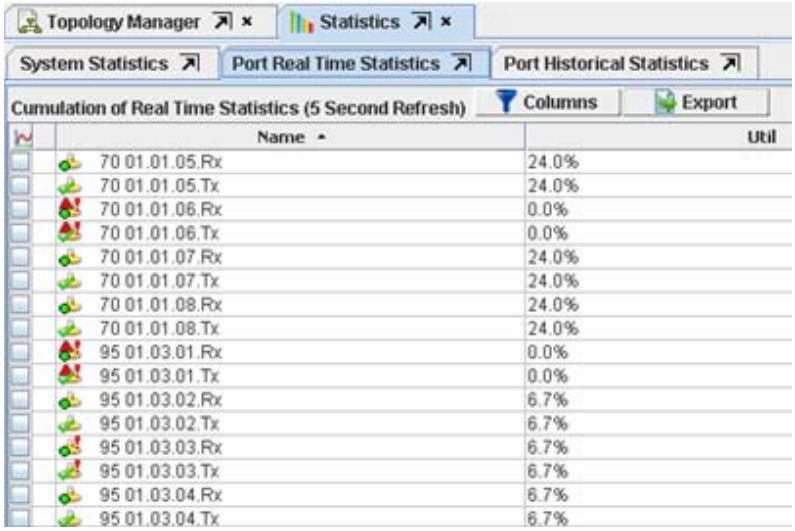
The port tool-tip also indicates whether the port is a part of a LBG as well as its current LB state.



When the load balancing group is in any state other than "LBG Normal" it shows a red triangle warning indicator to denote that there is some issue with that LBG. This warning indicator is also displayed in the Topology Manager and in the Ports/Groups tab.

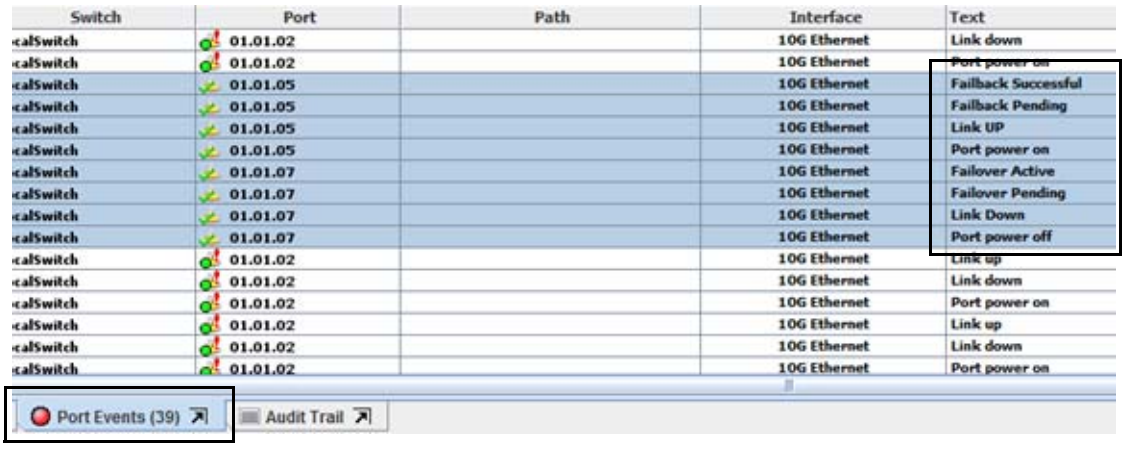


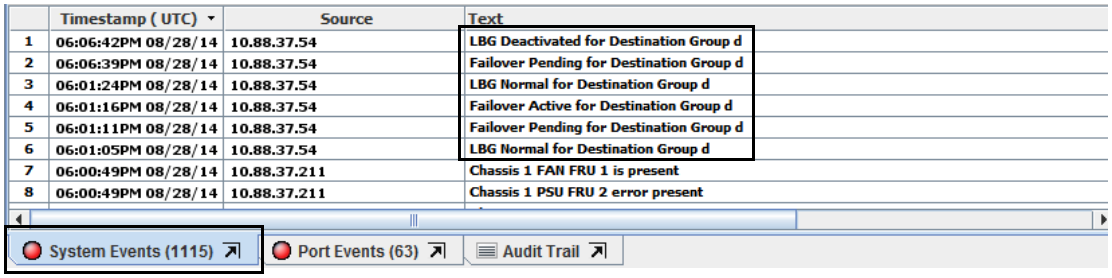
The Port Real-Time Statistics and the Port Historical Statistics indicates the failover icon for the port in an LBG being monitored for statistics.



Event Logs

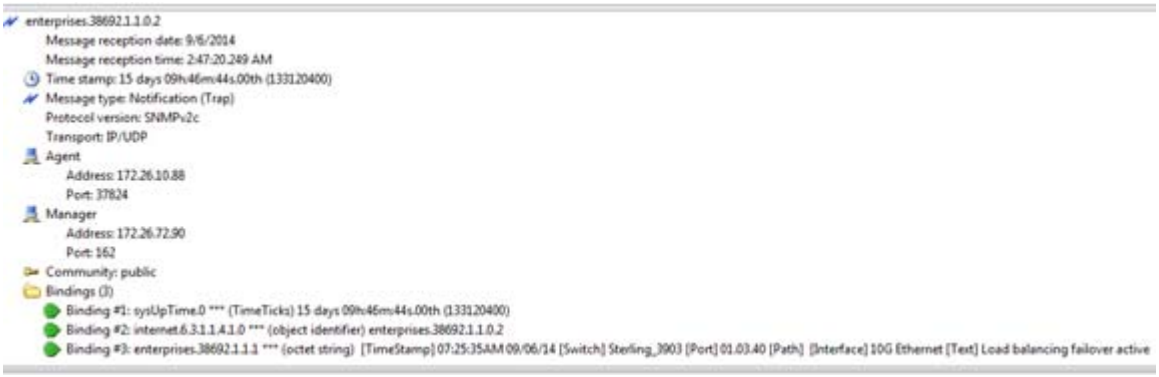
All state changes are logged under the Port Events and System Events tables. All of the port state transitions for ports in an LBG are logged into the Port Events tab and the Load Balancing Group state transitions are logged into the System Events.





Events to Remote Destinations

In addition to logging LBF events at the GUI and CLI, if remote logging destinations have been configured these events will also be logged at those destinations. If syslog forwarding is configured then these events will be sent to the remote syslog server. If an SNMP Trap destination has been configured then these events are sent as SNMP Traps to the remote destination.



Load Balancing Failover Operational Considerations

The following examples provide important considerations when utilizing Load Balancing Failover and the behavior of Load Balancing groups during certain conditions.

1 New Load Balancing Failover design maintains the link's availability for all ports that are "powered up", even if they are not part of any load balancing group. This is done to allow monitoring of ports that are "always on", so that when the first connection to an LBG containing one of these ports is activated, the newly activated LBG may have ports that are already failed-over. Consider the following example where Failover is Automatic, but Failback is Manual:

- Ports 33, 34 and 35 are set to "always on", therefore powered up and monitored.
- Port 33 reports LINK_DOWN, and after the configured Failover delay, it is marked as "unavailable for use" in an LBG.
- Port 33 reports LINK_UP, but Failback is Manual, so it remains "unavailable".
- A connection is activated to send data from port 1 to an LBG with ports 33, 34 and 35.

Therefore, when the new connection is made, port 1's data sent only to port 34 and 35, even though port 33 is currently reporting LINK_UP.

2 Depending on the sequence in which the user enables and disables the "Manual" and "Automatic" Failover/Failback the ports in a LBG will behave differently during a card restart. Consider the following two scenarios as examples:

– Card restart for a port that is UP but "pinned" as unavailable:

a Failover is set to Automatic and Failback is set to Manual.

b Port in the LBG fails resulting in a re-balance of traffic since the Failover is Automatic and the port is deemed as unavailable.

c The port comes back up but a re-balance is not done since the Failback is Manual.

d Failover is set to Manual.

e The card that has this port restarts but no re-balance occurs because Failover is Manual. This results in traffic to that card being dropped.

f Once the card comes back up, no re-balance occurs and the traffic that was originally going to the card resumes.

g Even though the port (described in point b) comes back up it is considered "unavailable" and not traffic goes to it.

– Card restart for a port that is DOWN but "pinned" as unavailable:

a Failover is set to Automatic and Failback is also set to Manual

b Port in the LBG fails, it is deemed "unavailable" and is rebalanced

c Failover is changed to Manual

d The card that has this port restarts but no re-balance occurs since Failover is now Manual. This results in traffic to that card being dropped.

e Once the card comes back up, no re-balance occurs and the traffic that was originally going to the card resumes.

f The port (described in point b) is down and would normally be considered as "available" to send LBG traffic to because of Manual Failover state but the prior "unavailable" state is maintained and no re-balance occurs to route traffic to that port.

Failback Operational Considerations

The Failback setting – Auto or Manual – only applies once the port has achieved failover active state. When a port first goes down, the port normally changes to the Failover Pending state, however, it has not yet achieved Failover Active state.

Note: The port always goes to Failover Pending before Failover Active except when the port is configured for Failover Auto with zero seconds delay; in that case, it will change to Failover Active instantly.

If the port should subsequently return to Link Up while in Failover Pending state, the port will resume carrying traffic immediately. Even if there is a Failback Auto Timer, it does not apply because the port never achieved Failover Active state. The Failback process does not start until:

- The port first achieves Failover Active
  - and -
- The port returns to Link Up.

- Example #1:
  – Failover = Automatic @ 30 seconds
  – Failback = Automatic @ 60 seconds

1 Port changes to Link Down.

2 Failover timer starts.

3 15 seconds later, port returns to Link Up.

4 Traffic flow immediately over the port
(i.e., it does not wait 60 seconds because it was never in Failover Active).

- Example #2:
  – Failover = Manual
  – Failback = Automatic @ 60 seconds

1 Port changes to Link Down.

2 User does NOT do any Manual Failover; all traffic to that port continues to drop.

3 15 seconds later, Port returns to Link Up.

4 Traffic flows immediately over the port
(i.e., it does not wait 60 seconds because it was never in Failover Active).

Load Balancing Failover CLI Commands

REVise **SWI**tch

REVise **SWI**tch *switchname* **LOA**dbalance {**FAILO**ver|**FAILB**ack} {**MAN**ual|**AUTO**matic **DEL**ayed seconds}
Revise a switch's loadbalancing group failover or failback mode and delay timer in seconds. In Automatic mode, valid numbers are between 0 and 86400 seconds (24 hours). These timers determine how long the system will wait after a link down event to move traffic from the down port(s) to other up port(s) in the load balancing group; or how long the system will wait after a link up event to move traffic from failed-over port(s) back to the original port(s) in the load balancing group. In Manual mode traffic is not moved.

Examples:
REVISE SWITCH MySwitch LOAD FAILO AUTO DEL 5
rev swi MySwitch loadbalance failover automatic delay 60
REVISE SWITCH MySwitch LOAD FAILO MANUAL
REVISE SWITCH MySwitch LOAD FAILB AUTO DEL 30
rev swi MySwitch loadbalance failback automatic delay 600
Revise Switch MySwitch Loadbalance FAILBACK Manual

Manual Mode Failover / Failback CLI Examples

REVise **SWI**tch <*switchname*> **LOA**dbalance **FAILO**ver **MAN**ual

Example:
REV SWI 3901R-LBF LOA FAILO MAN
Successful.
3901R-LBF revised.

REVise **SWI**tch <*switchname*> **LOA**dbalance **FAILB**ack **MAN**ual

Example:
REV SWI 3901R-LBF LOA FAILB MAN
Successful.
3901R-LBF revised.

Automatic Failover / Failback with Delay CLI Examples

REVise **SWI**tch <*switchname*> **LOA**dbalance **FAILO**ver **AUTO**matic **DEL**ayed <*0 to 86400 seconds*>

Example:
REV SWI 3901R-LBF LOA FAILO AUTO DEL 0
Successful.
3901R-LBF revised.

REVise **SWI**tch <*switchname*> **LOA**dbalance **FAILB**ack **AUTO**matic **DEL**ayed <*0 to 86400 seconds*>

Example:
REV SWI 3901R-LBF LOA FAILB AUTO DEL 0
Successful.
3901R-LBF revised.

SHOw **SWI**tch

The CLI command, **SHO**w **SWI**tch <*switchname*>, provides the current user settings for the Load Balancing Feature, whether it is Equal or Session-based distribution and if Failover/Failback are in Automatic with delay or Manual mode.

Examples:

SHO SWI 3901R-LBF
Switch: 3901R-LBF
Switch MAC: D8E72B000001
Switch Model: 3901R, Ipv4: 10.88.39.171, Discovery: Auto Eth, Link Prop: Disable, Status: Active
Backplane: N/A

VN-Tag Inspection: Enabled
Local Console: Disabled
Load Balancing Type: Equal Distribution
Failover Mode: Manual
Failback Mode: Manual

SHO SWI 3901R-LBF
Switch: 3901R-LBF
Switch MAC: D8E72B000001
Switch Model: 3901R, Ipv4: 10.88.39.171, Discovery: Auto Eth, Link Prop: Disable, Status: Active
Backplane: N/A
VN-Tag Inspection: Enabled
Local Console: Disabled
Load Balancing Type: Equal Distribution
Failover Mode: Automatic with 0 seconds delay
Failback Mode: Automatic with 0 seconds delay

show switch "LBF_3903"
Switch: LBF_3903
Switch MAC: D8E72B0006E8
Switch Model: 3903, Ipv4: 172.26.10.66, Discovery: Auto Eth, Link Prop: Disable, Status: Active
Backplane: Guaranteed
VN-Tag Inspection: Enabled Local Console: Disabled
Load Balancing Type: Session-based
Failover Mode: Automatic with 5 seconds delay
Failback Mode: Automatic with 30 seconds delay

Load Balancing Group Status

=> show topologies all

Defined Topologies:
LBG_SingleSwitch : 4
CrossSwitch_LBF : 3
Across_Blades : 3
LBF_Test_23 :1
PCE_Test_1 : 0

=> show topology members LBG_SingleSwitch

Topology : LBG_SingleSwitch
Total Members : 4
Ports : 0
Subports : 0
Connection Groups : 0
Source Groups : 2
S1
S2
Destination Groups : 2
LBG_1 : **Failover Active**
LBG_2 : **Failover Pending and Failback Pending**
Filters : 0

Load Balancing Port Status

=> show group members d

Ports in Destination Group d:
1 54 01.01.06 : **LB Normal**
2 54 01.01.07 : **LB Normal**
3 54 01.01.08 : **LB Normal**
4 54 01.01.15 : **LB Failover Active**

Note: If the group is a Multicast Group (i.e. not a LBG), the " : LB Normal" or " : LB Failover Active" would not be present.

Show group members <LB GROUP NAME> where the destination group's name is "LBG_2":

=> show group members LBG_2

Ports in Destination Group LBG_2:
1 01.02.36 : **LB Normal**
2 01.02.37 : **LB Failover Pending**
3 01.02.38 : **LB Failback Pending**

Show port <PORT NUMBER> :

=> show port 01.02.37

Name: 01.02.37
Port: 01.02.37
Type: Normal
Switch: DC04_3903
Speed: 10G ETH
Connected: Yes
Lock: No
Link Propagation: Default
AutoArm: Yes
Armed: No
Alarmed: No
VLAN ID: 1
VLAN Tag SRC: Keep
VLAN Tag DST: Untag/Keep
VN-Tag DST: Allow Tag
Nanostamp: Disabled
Packet Slicing: Disabled
Congestion Alarm: Enabled
Load Balancing: **Yes, Failover Pending**
SFP Diagnostic Alarm: Enabled
SFP Present: Yes
SFP Information:

SFP Port: 37
Vendor: Amphenol
Part #: 571540001 Rev: M
Id: 3 [SFP transceiver]
Connector: 21 [Copper pigtail]
Serial Num: APF10470010013, Date: 11/28/2010

SFP does not support SFF-8472 (diagnostic monitoring)

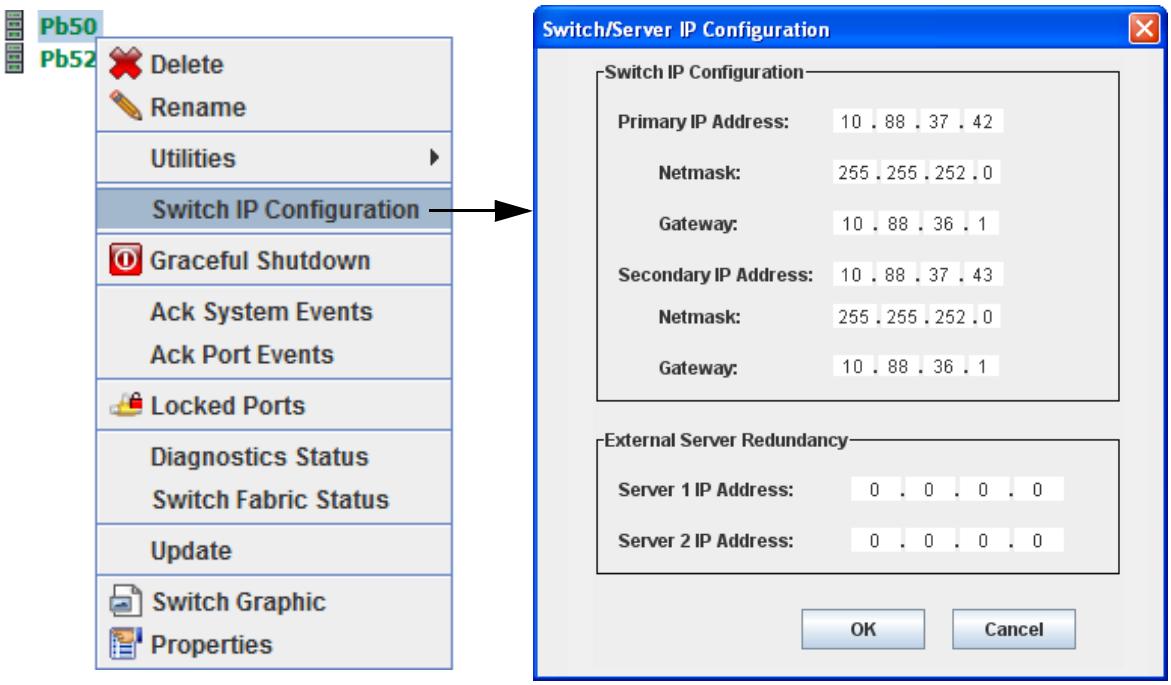
Configuring Server IP Addresses

The IP addresses of the nGenius 3900 series switches (embedded / TestStream Management servers) can be changed by the user to accommodate network requirements.

Note: IP Address Ranges
The following range of IP addresses are NETSCOUT reserved for the nGenius 3900 series switches and must not be assigned to your TestStream Management network:
172.16.0.0/24 or **192.168.0.0/24**.

Switch IP Configuration for nGenius 3900 Series Switches Embedded Servers

1 From the switch level, right click on the switch name and select **Switch IP Configuration**. The Switch/Server IP Configuration window displays, showing the currently assigned network configurations.



2 In the Switch IP Configuration section, make the required changes for your network:

- Primary IP Address
- NetMask
- Gateway
  and if required,
- Secondary IP Address
- NetMask
- Gateway

Important: Do not assign an IP address for an External TestStream Management server unless a server is physically connected and operational in the TestStream Management network; otherwise TestStream Management will default to the TestStream Management Server IP and not to the Primary IP address of the nGenius 3900 series embedded server.

---

3 Click **OK** to save the new IP settings. The server performs a shutdown then a restart of the server to apply the new IP configuration settings. Re-logon to TestStream Management using the new IP address.

Changing the Switch IP Configuration from the CLI Command Interface

Note: Refer to CLI Access using an nGenius 3900 Series Blade Console Port on page 2-13 and depending on your system configuration, either CLI Access - Telnet on page A-3 or CLI Access - SSH on page A-4.

1. Establish a connection with the nGenius 3900 series switch and enter the following CLI commands as shown in the following example:

   => logon administrator netscout1 (example login)

   => show switch * (list all switches in the network)

   => select switch *switchname* (enter name of the switch to change)

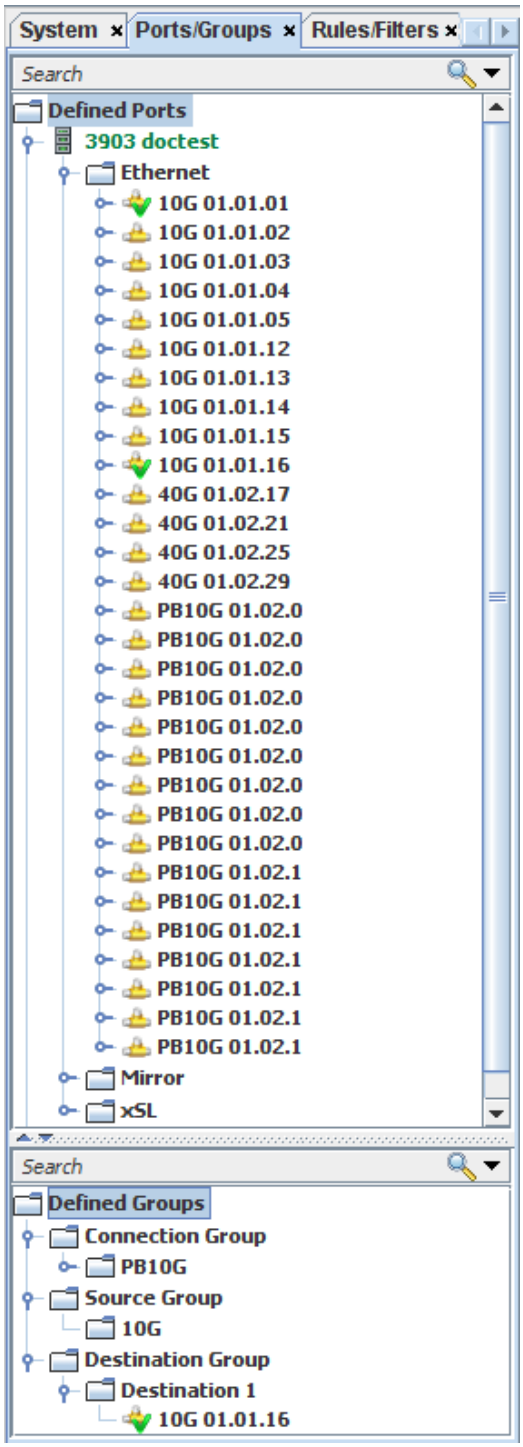
   => revise switch IP -I 10.88.37.204 -N 255.255.255.0 9 -G 10.88.37.1 (example IP, NetMask, and Gateway settings only)

   => This will reboot the switch, do you want to continue? (Y/N): (selecting **Y** will reboot the nGenius 3900 series switch)

2. The switch can now be accessed using the new IP address.

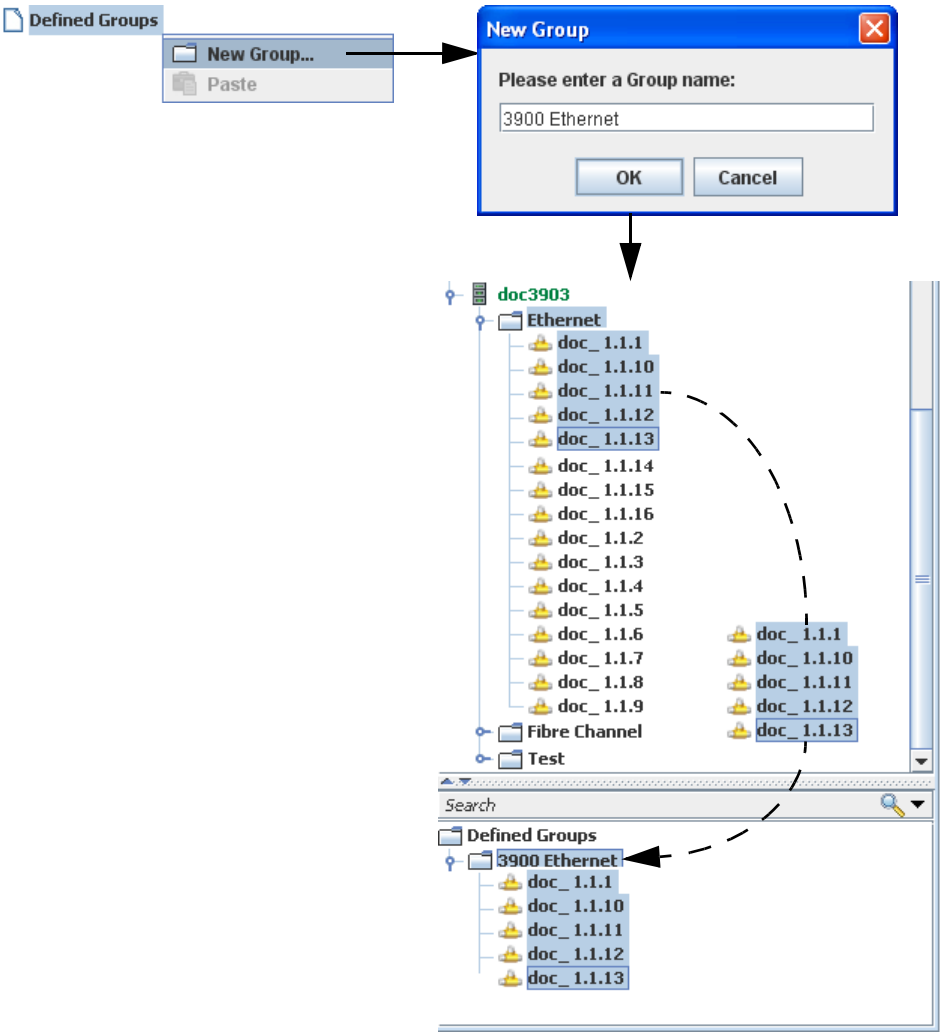
Ports/Groups

Selecting the Ports/Group tab allows viewing of defined ports and groups in a switch by protocol, and creation and modification of groups. Defined ports are displayed by switch and interface type (i.e., Ethernet (Normal), Mirror, xSL, Test, and Clone). The Defined Groups section is used to create custom groups and add ports to these groups for ports requiring more than one connection at a time.



Creating a New Group

1 Right click on the Defined Groups icon in the Defined Groups list window and select **New Group**. A New Group screen displays.



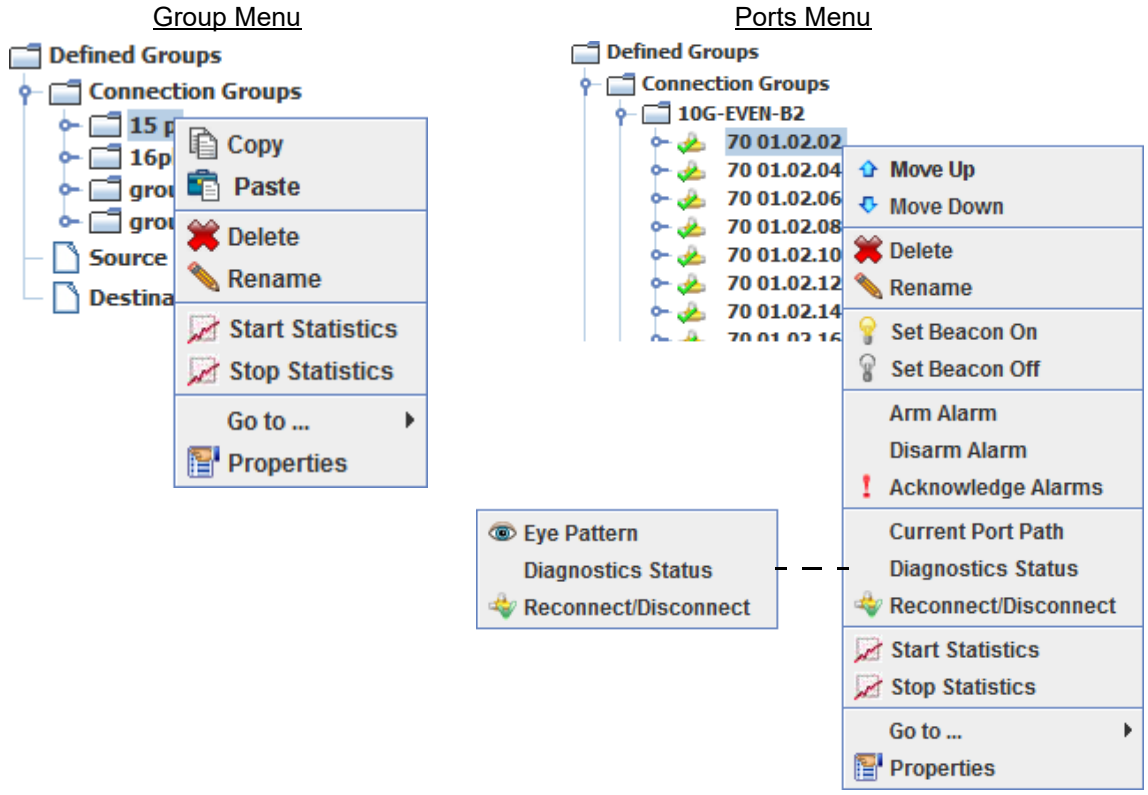
2 Type in the name of the new group. Click **OK**. The new group is listed under the Defined Groups icon.

3 Select the required ports from the Defined Ports window listing all of the defined blade ports, and either drag the selected ports to the new group or right-click and copy/paste the selected ports to the new group. The selected ports are now assigned to the group.

Note: The order of ports in a group matters. When connected to another group, the ports in one group will be connected to the port in the same position in the second group.

Group Sub-Menus

A series of sub-menu functions, similar to the functions under the Systems tab, are available for the Defined Groups.



- Copy - Duplicates (with a new defined name) a selected group or port.
- Paste - Inserts a copied group or ports into the Defined Group.
- Delete - Remove a selected group.
- Rename - Change the name of a group/port.

> **Important:** Group/port names cannot be made up of four (4) dotted numbers (nn.nn.nn.nn - e.g., 10.88.99.11).

- Move Up/Down - Reposition a port in a group.
- Set Beacon On/Off - Turns On/Off the beacon LED on a selected port.
- Arm / Disarm Alarm - Activate / deactivate port alarms
- Acknowledge Alarms - Acknowledge all port alarms on the specified port
- Eye Pattern (S-Blades) - Refer to Eye Pattern (Eye Diagram Analyzer) on page 7-19
- Current Port Path - Refer to Current Port Path on page 7-14.
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.
- Reconnect/Disconnect - Reconciles the connections of a selected port.
- Start Statistics - Begin statistics recording
- Stop Statistics - End statistics recording
- System View - Displays connection path of selected group.
- Go to ... - Links to the following:
  - Switch Graphic
  - Connection
  - Topologies
- Properties - Shows the characteristics and settings of a selected group or port.

Rules/Filters

Packet filtering is used to define selective criteria to be applied to Ethernet frames passing through TestStream. Frames that match the criteria will have an action applied to them, either permit or deny. Permitted frames will continue on to their destination port(s) while denied frames will be blocked by the filter. If a frame that passes through a filtered connection does not match any of the filter rules then it is implicitly denied.

Filters can be made up of one or more rules. The order of the rules within a filter may be important. Rules are processed as an if-then-else statement:
If the frame matches the criteria in the first rule then execute the action (permit or deny) of the first rule, else go to the next rule. Once a frame matches one rule it does not go on to be evaluated by the next rule. At least one criteria must be selected for Permit/Deny by Criteria, but any of them may be left blank.

Important: An error message, along with a letter "V" indicator over the switch, will be displayed if a user tries to use a filter rule specifying a range, on a switch using an unsupported version of TestStream Management software.

Maximum Number of Active Rules and Filters

TestStream Management currently supports the following number of active rules and filters:

- Rules: Up to 128 rules per filter
- Filters: Up to 240 active filters per T-Blade, 48 active filters per port, 5,000 active rules per blade

Ingress Filter Resources

The nGenius 3900 series switch supports up to 5,000 active rules per blade when all fields are of a single type (e.g., 5,000 IP Source Address rules). For configurations that include multiple rule fields on a single blade (e.g., IP Source Address, IP Destination Address, Source Port and Destination Port), whether they are part of the same rule or not, the number will be lower.

Note: A safe "rule of thumb" is to divide (a) the total number of field types (e.g., IP Source Address and UDP Destination Port would count as two field types) that are used across all of the rules that apply to the blade into (b) 5,000 to get (c) a rough approximation of the number of rules that the blade can support. For example, IP Source Address + IP Destination Address + Source Port = 3 rule types = approximately 1,666 rules.

The total number of active rules is the sum of all the rules on all of the ingress ports to which they apply (e.g., a rule that applies to 3 ingress ports counts as three rules; likewise, a rule that appears in four filters counts as four rules). For more complex rule configurations and for those that include IPv6, please contact NETSCOUT Support.

If attempting to activate a filter that exceeds the maximum number of rules the system supports, the activation (a) will fail, (b) will interrupt traffic passing through the associated filter, and in some cases, (c) may interrupt traffic on other connections that share the same source port(s). Should this happen, (a) remove the new filters that were just added and (b) remove at least one other filter associated with the same port, then (c) add the last filter back again to restore the filter condition to its previous state.

Supported Filtering Formats

MPLS (Multiprotocol Label Switching)

TestStream Management supports the following MPLS packet formats:

- Ethernet Types: MPLS-MULTICAST (0x8848) and MPLS-UNICAST (0x8847).
- MPLS-UNICAST frames that carry an IP packet have the additional capability of filtering on Layer-3, Layer-4, and DPI on the encapsulated IP packet.
- Layer 3 Criteria: Ethernet (type Unicast 0x8847) - MPLS Label(s) - IPv4

- Layer 3 Criteria: Ethernet (type Unicast 0x8847) - MPLS Label(s) - IPv6
- MPLS VPN: TestStream Management supports parsing MPLS headers up to 4-MPLS labels if immediately followed by an IPv4 or IPv6 header, using L3/L4/DPI filters. If any other header follows the MPLS header (e.g. VLAN) only filtering on Src MAC, Dst MAC, EtherType of the frame is allowed.

FabricPath

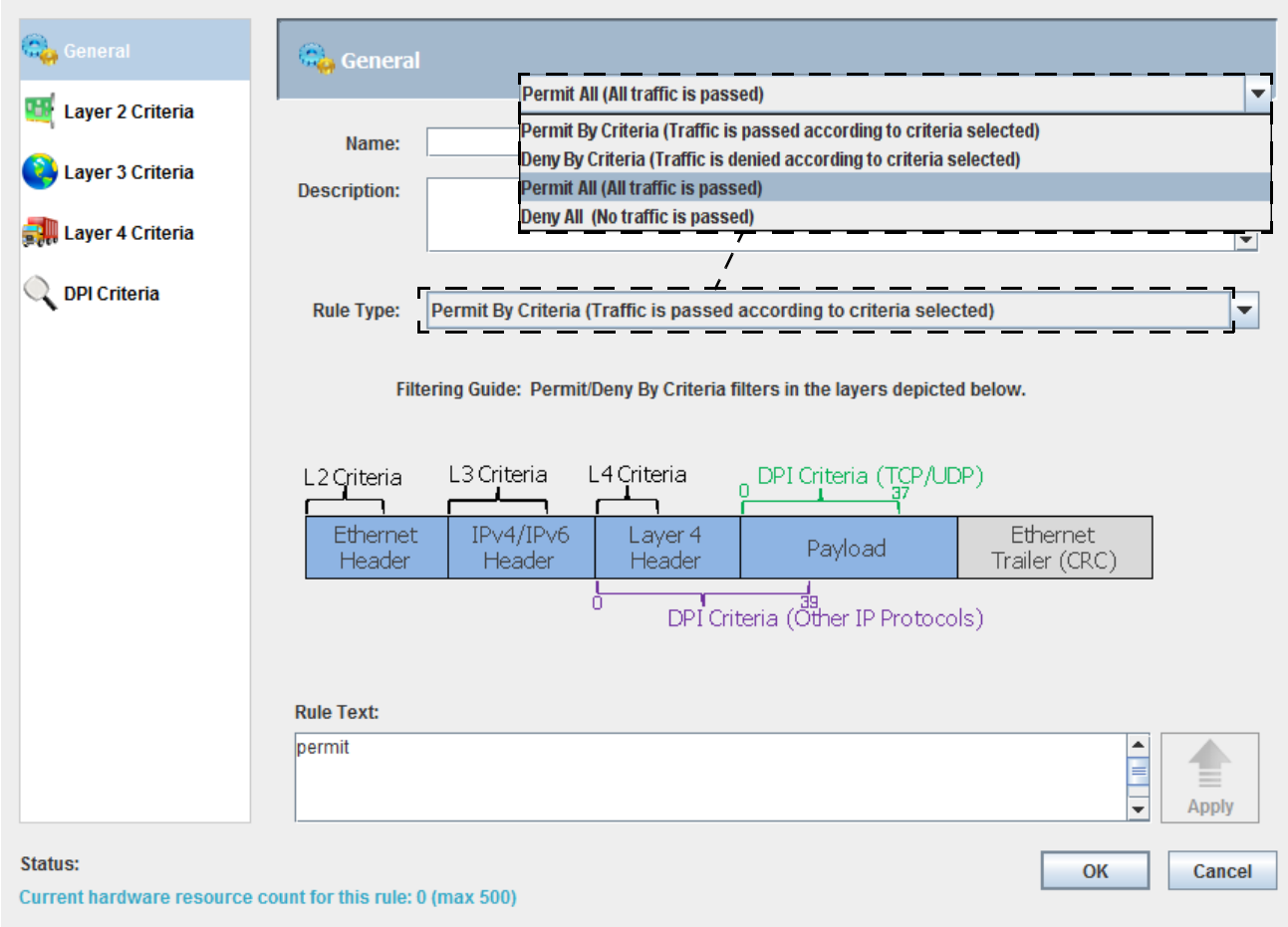
TestStream Management supports filtering on Src MAC, Dst MAC, EtherType if FabricPath frame; detecting the FabricPath and sending it to a specific tool, and manual load balancing based on MAC ranges.

GRE Tunnels

TestStream Management supports filtering on L2/L3 headers, detecting IP Protocol Type = GRE, and utilizing DPI filtering to filter into the GRE header and payload (up to 40 bytes into the GRE header/payload).

Defining Rules

1 Click on the Rules/Filters tab. Under Defined Rules, right click on the Rules folder and select **New Rule**. The Rule - General screen displays.



2 Enter a name for the rule in the Name text field. Optionally, enter a description of the new rule.

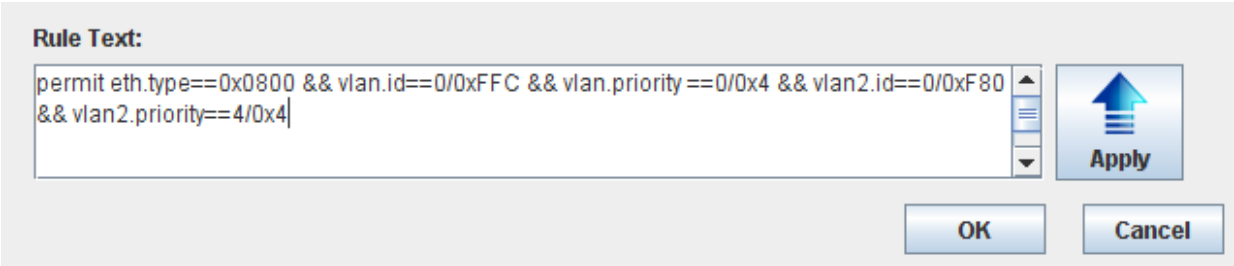
3 From the Rule Type drop down menu, select the required type of rule:

- Permit All - Allow all data packets to pass through the filter
- Deny All - Block all data packets from passing through the filter
- Permit by Criteria - Allow only data packets meeting a specified filter criteria to pass through the filter
- Deny by Criteria - Block data packets meeting a specified filter criteria from passing through the filter

the selected filter rule displays in the rule text field.

4 If either Permit All or Deny All is selected, click **OK**. If **Permit by Criteria** or **Deny by Criteria** is selected, click on the applicable layer criteria (2, 3, 4, and/or DPI Criteria) from the icon bar to continue.

As an alternate method of defining a rule if **Permit by Criteria** or **Deny by Criteria** is selected, a pre-defined rule (e.g., subset of Wireshark format) can be copied and pasted into the Rule Text field. Click on the **Apply** icon to input the rule text configuration into the appropriate layer criteria (2, 3, 4, and/or DPI Criteria). Click **OK** to save the new rule. The new rule is displayed in the Defined Rules listing.



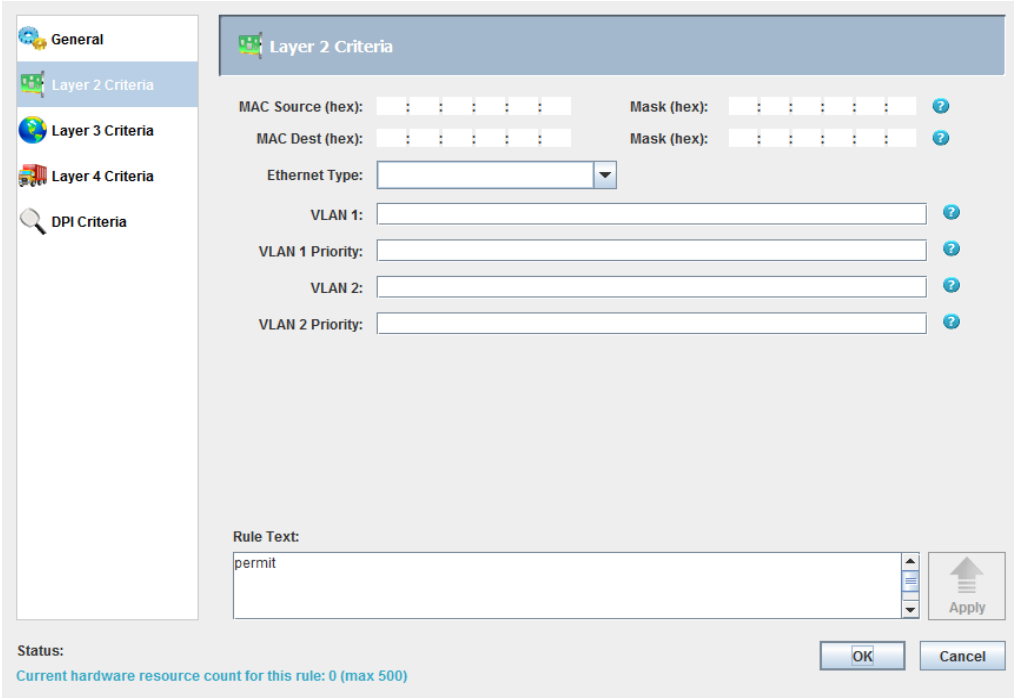
Note: Refer to Defining Filter Rules Using Ranges on page A-17 for a list of defined syntax rules.

Layer 2 - Data Link - Ethernet

Note: This screen is accessible only if Permit by Criteria or Deny by Criteria is selected.

1. Click on the **Layer 2 Criteria** icon.
2. Enter the MAC source and/or destination addresses and an optional mask in hexadecimal if desired. Zero means "don't care"; FF means must match the value in the corresponding position in the MAC address.
3. Select an Ethernet type from the drop down menu or type in a value.
4. Enter the Virtual LAN 1 (VLAN 1), VLAN 1 Priority ranges (refer to Defining Filter Rules Using Ranges on page A-17). Repeat for the VLAN 2 settings. Click OK to save the new rule or go on to another layer. The new rule is displayed in the Defined Rules listing.

Note: VLAN 2 ID and VLAN 2 Priority do not apply to Destination filters.



Field Definitions

MAC Source / Mask - Enter the desired source MAC address to match. If more than one value is desired, enter a mask in the mask field. Values are matched based on the bitwise AND between the two fields. Values are entered in hexadecimal notation. Maximum range for each field = 00 - FF.

MAC Destination / Mask - Enter the desired destination MAC address to match. If more than one value is desired, enter a mask in the mask field. Values are matched based on the bitwise AND between the two fields. Values are entered in hexadecimal notation. Maximum range for each field = 00 - FF.

VLAN Tag 1 - when a single tag is entered, this is the 802.1Q tag; for a double tagged frame, the field is the Outer tag (the tag closest to the beginning of the Ethernet frame).

Supported Formats
Ranges: x-y (where x and y are two positive numbers with y > x).
Lists: x, y, z (where x, y, z are any arbitrary lists of numbers of varying length).
Masks: x/y (where x is a value and y is a mask. The result of the bitwise AND operation are the values that are filtered).
Combos: Ranges can be used in lists; masks can not be used.
Maximum range = 0 - 4095

VLAN Tag 1 Priority - when a single tag is entered, this is the 802.1Q tag's Quality of Service Priority; for a double tagged frame, the field is the Outer tag's priority (the tag closest to the beginning of the frame).

Supported Formats
Ranges: x-y (where x and y are two positive numbers with y > x).
Lists: x, y, z (where x, y, z are any arbitrary lists of numbers of varying length).
Masks: x/y (where x is a value and y is a mask. The result of the bitwise AND operation are the values that are filtered).
Combos: Ranges can be used in lists; masks can not be used.
Maximum range = 0 - 7

VLAN Tag 2 - when the frame is double tagged, this field is the Inner tag (the second tag from the beginning of the Ethernet frame).

Supported Formats
Ranges: x-y (where x and y are two positive numbers with y > x).
Lists: x, y, z (where x, y, z are any arbitrary lists of numbers of varying length).
Masks: x/y (where x is a value and y is a mask. The result of the bitwise AND operation are the values that are filtered).
Combos: Ranges can be used in lists; masks can not be used.
Maximum range = 0 - 4095

VLAN Tag 2 Priority - when the frame is double tagged, this field is the Inner tag's priority (the second tag from the beginning of the Ethernet frame).

Supported Formats
Ranges: x-y (where x and y are two positive numbers with y > x).
Lists: x, y, z (where x, y, z are any arbitrary lists of numbers of varying length).
Masks: x/y (where x is a value and y is a mask. The result of the bitwise AND operation are the values that are filtered).
Combos: Ranges can be used in lists; masks can not be used.
Maximum range = 0 - 7

Note: For VN-Tagged frames the Ether Type refers to the outer Ether Type when the Switch Parameter for VN-Tag Detection is not enabled. When VNTag Detection is enabled then the EtherType refers to the inner Ether Type of the encapsulated IP packet.

Interaction of VLAN Port Property Configuration and Filtering on VLAN Fields

Source Port Setting	Required Destination Port Setting	Rules with vlan.id are based upon	Rules with vlan.priority are based upon	Notes
Keep	Untag/Keep	original VLAN ID	original VLAN priority	
Add	Allow Tag	original VLAN ID	original VLAN priority	The VLAN priority in the added VLAN tag is set to the original VLAN priority, or 0 for untagged frames
Replace*	Allow Tag	replaced VLAN ID	0	VLAN Priority: Replace/Allow sets the VLAN 1 priority field to 0. VN-Tagged frames: If the frame is VN-Tagged, then rules do not match VLAN ID. The original VLAN 1 priority is not replaced with 0 and VLAN priority Rules are based upon the original VLAN priority.
Remove*	Untag/Keep	original VLAN ID	original VLAN priority	Priority-tagged frames: Rules do not match the VLAN ID or VLAN priority for frames with VLAN ID = 0 (i.e., for priority-tagged frames).
* VN-Tag Detection must be enabled in order to Replace or Remove the VLAN tag in VN-Tagged frames				

Layer 3 - Network - Internet (IP)

Note: This screen is accessible only if Permit by Criteria or Deny by Criteria is selected.

Note: For VN-Tagged frames, the Switch Parameter for VN-Tag Detection must be enabled in order to match fields in the encapsulated IP packet.

1. Click on the **Layer 3 Criteria** icon.
2. **IP Selection:** Select either **None**, **IPv4** or **IPv6** for the type of packet to match.
3. **IP Addresses:** Select either **Match Address(es) For Either Direction** or **Specify Each Direction Separately**, then enter the desired source and/or destination addresses.
4. **IPv4 Layer 4 Protocol:** If desired, select an L4 Protocol from the drop down menu and optional mask value.
   IPv6 Layer 4 Protocol: If desired, select an L4 Protocol from the Next Header drop down menu and optional mask value.
5. **IPv4:** If desired, type in a value for the Time To Live setting.
6. Optionally, select DSCP/ECN and enter specified bits (refer to the information (**i**) pop-up screen for value definitions).
7. Click **OK** to save the new rule or go on to another layer. The new rule is displayed in the Defined Rules listing.

Field Definitions

IP Addresses - IP Addresses can be either set separately for each direction or as an either/or operation. For example, selecting Specify Each Direction Separately and setting Source to 192.168.0.1 and Destination to 172.16.0.1 will cause frames that have both of these conditions met to match the filter. Selecting Match address(es) for Either Direction and setting Address(es) to 192.168.0.0, 172.16.0.0 will cause frames that match either of those values in either direction to be matched.

Source IPv4 Address(es) - Enter the desired source IP address to filter on.

Destination IPv4 Address(es) - Enter the desired destination IP address to match.

Supported Formats (Source and Destination IPv4 Addresses)
Ranges: x.x.x.x - y.y.y.y (where x and y are IP addresses in dotted decimal notation).
Lists: x.x.x.x, y.y.y.y, z.z.z.z (where x, y, z are any arbitrary list of IP addresses in dotted decimal notation).
Netmask Format: x.x.x.x / y.y.y.y (where x.x.x.x is an IP address and y.y.y.y is a mask.
CIDR Mask Format: x.x.x.x / y (where x.x.x.x is an IP address and y is the number of left-most 1 bits in the mask).
Combos: Ranges can be used in lists; masks can not be used.

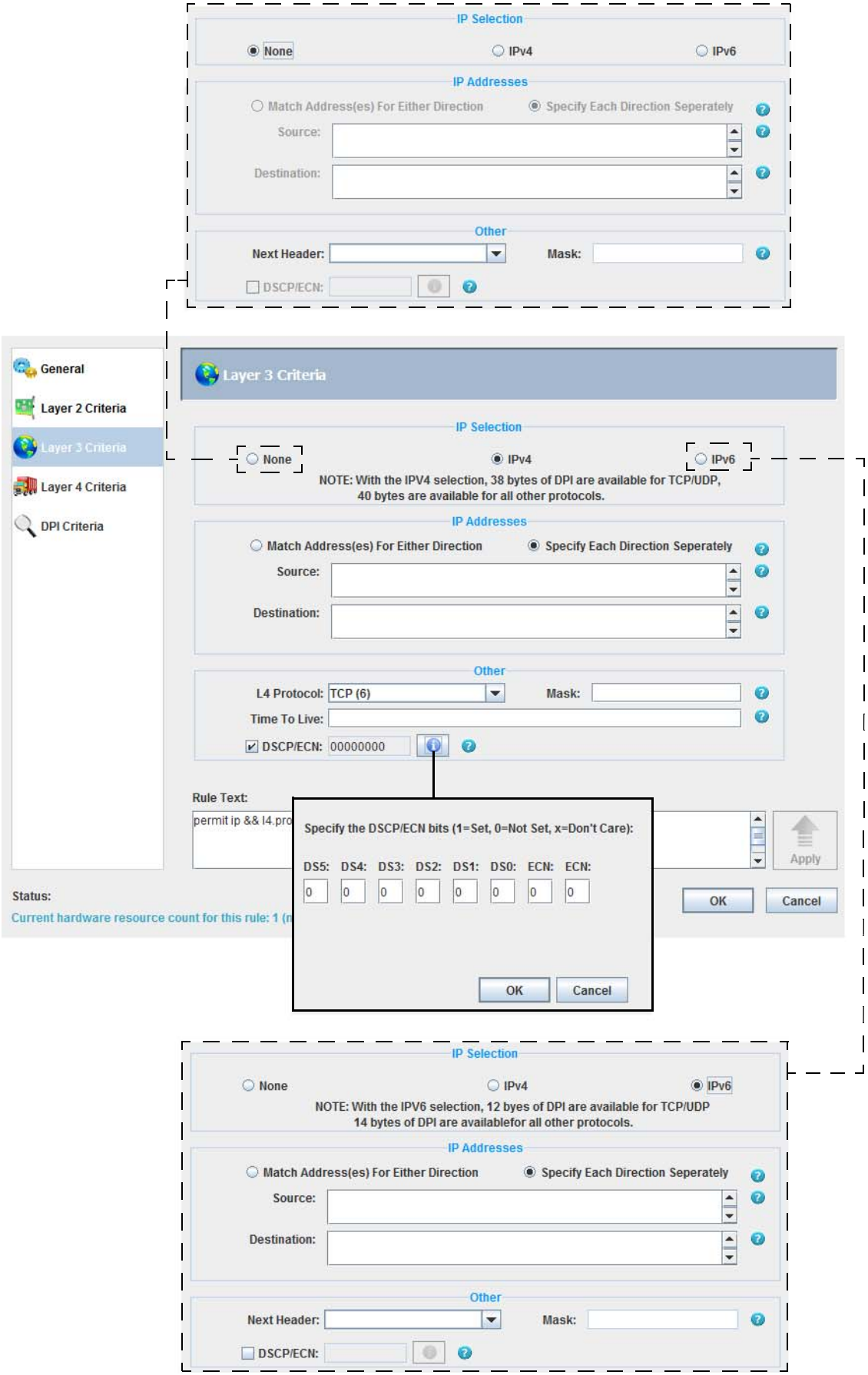
L4 Protocol - Select the desired L4 protocol to filter on. Multiple values can be filtered on by setting the mask field, which will filter on the bitwise and the two fields. Avoid using a mask if also filtering for DPI, as it will produce unexpected results as different protocols change the location of the start of the DPI section.

Maximum Range of the Mask Field - 0 - 255 (values can be entered as a hex number with 0x prefix.

Time to Live - Value of the time to live field.

Supported Formats
Ranges: x-y (where x and y are two positive numbers with y > x).
Lists: x, y, z (where x, y, z are any arbitrary lists of numbers of varying length).
Masks: x/y (where x is a value and y is a mask. The result of the bitwise AND operation are the values that are filtered).
Combos: Ranges can be used in lists; masks can not be used.
Maximum Range = 0 - 255

DSCP / ECN
Differentiated Services Code Point: Defined by RFC 2474. Denotes use of real time streaming data.
Explicit Congestion Notification: Defined by RFC 3168. Denotes use of end-to-end notification of network congestion.
Values are entered by enabling the field, then clicking on the (i) button to open the bit field control.


IP Selection
None
IPv4
IPv6
IP Addresses
Match Address(es) For Either Direction
Specify Each Direction Seperately
Source:
Destination:
Other
Next Header:
Mask:
DSCP/ECN:
General
Layer 2 Criteria
Layer 3 Criteria
Layer 4 Criteria
DPI Criteria
Layer 3 Criteria
NOTE: With the IPV4 selection, 38 bytes of DPI are available for TCP/UDP,
40 bytes are available for all other protocols.
L4 Protocol:
TCP (6)
Time To Live:
00000000
Rule Text:
permit ip && l4.pro
Apply
Status:
Current hardware resource count for this rule: 1 (n
OK
Cancel
Specify the DSCP/ECN bits (1=Set, 0=Not Set, x=Don't Care):
DS5: DS4: DS3: DS2: DS1: DS0: ECN: ECN:
0 0 0 0 0 0 0 0
NOTE: With the IPV6 selection, 12 byes of DPI are available for TCP/UDP
14 bytes of DPI are availablefor all other protocols.

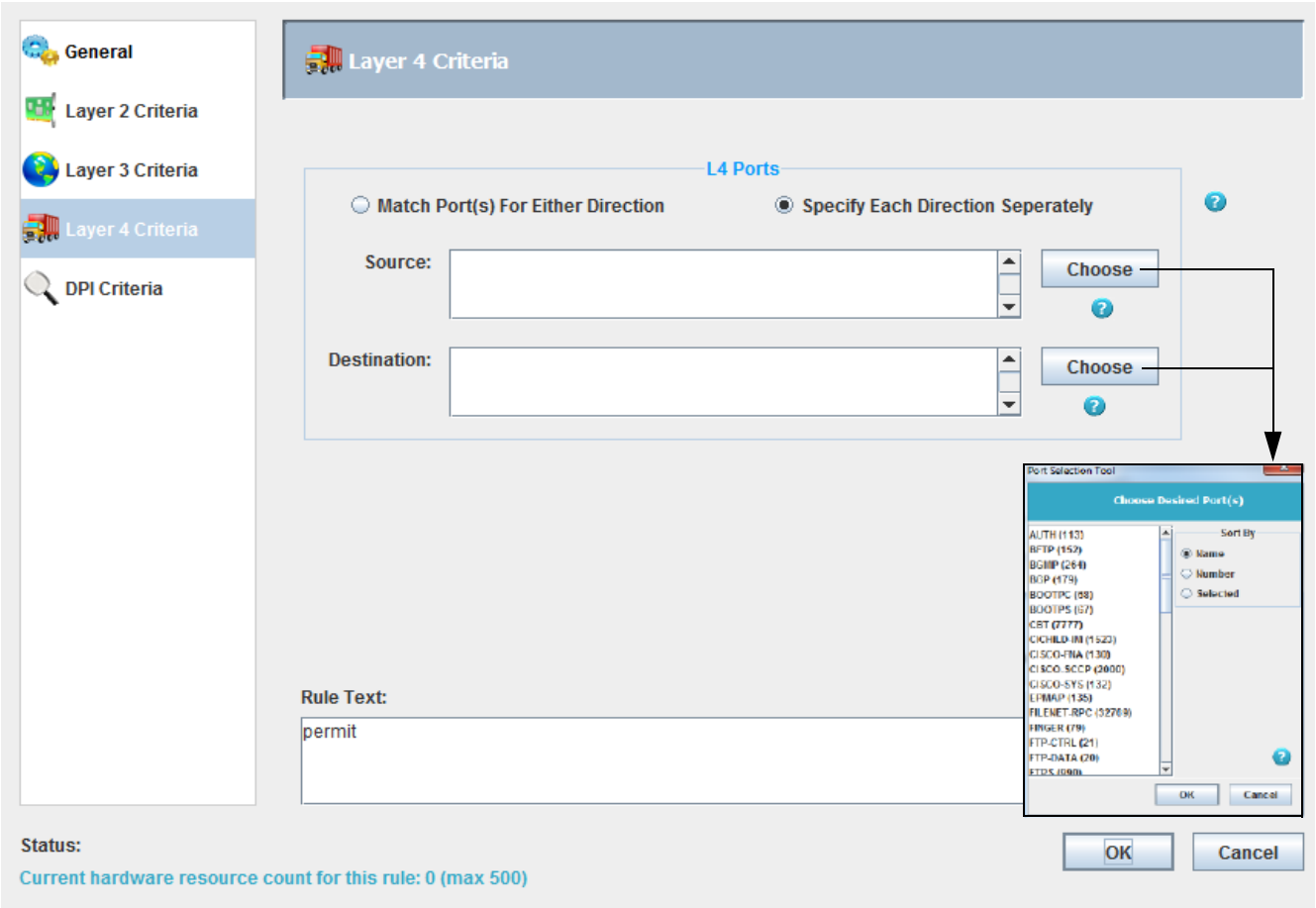
Layer 4 - Transport - TCP/UDP

Note: This screen is accessible only if Permit by Criteria or Deny by Criteria is selected.

1 Click on the **Layer 4 Criteria** icon.

2 Select either **Match Port(s) For Either Direction** or **Specify Each Direction Separately**.

3 **Specify Each Direction Separately**: Click **Choose** and select the source and destination ports from the drop-down menus.
Match Port(s) For Either Direction: Click **Choose** and select the desired ports from the drop-down menu



4 Click **OK** to save the new rule. The new rule is displayed in the Defined Rules listing.

Field Definitions

L4 Ports - Layer 4 ports can be either set separately for each direction or as an either/or operation. For example, selecting **Specify Each Direction Separately** and setting Source to 23 and Destination to 50 will cause frames that have both of those conditions met to match the filter. Selecting **Match Port(s) in Either Direction** and setting Port(s) to 23, 50 will cause frames that match either of those values in either direction to be matched.

Source / Destination Port(s) - Enter the desired ports to match using the text field or the port selection tool pop-up menu. The port selection can be used to add or remove known ports only; the text field can be used to add or remove any port.

Supported Formats
Ranges: x-y (where x and y are two positive numbers with y > x).
Lists: x, y, z (where x, y, z are any arbitrary lists of numbers of varying length).
Masks: x/y (where x is a value and y is a mask. The result of the bitwise AND operation are the

values that are filtered).
Combos: Ranges can be used in lists; masks can not be used.
Maximum Port Value= 0 - 65535 (values can be entered as a hex number with 0x prefix.

Port Selection Tool - This window can be used to build lists of known ports. Clicking OK will feed the selected values back to the desired port field on the L4 filter criteria form.

Selecting Multiple Values: Hold the control key and click on the desired value(s) to select. Click again to de-select.
Sorting: The list of values can be sorted by name, port number, or values that are selected. When sorting by **Selected**, all of the presently selected values will be listed at the top of the control.

Note: Values entered on the main screen which do not match any known values are ignored by this control. Add / Modify / Delete those values directly in the desired port field of the L4 filtering criteria.

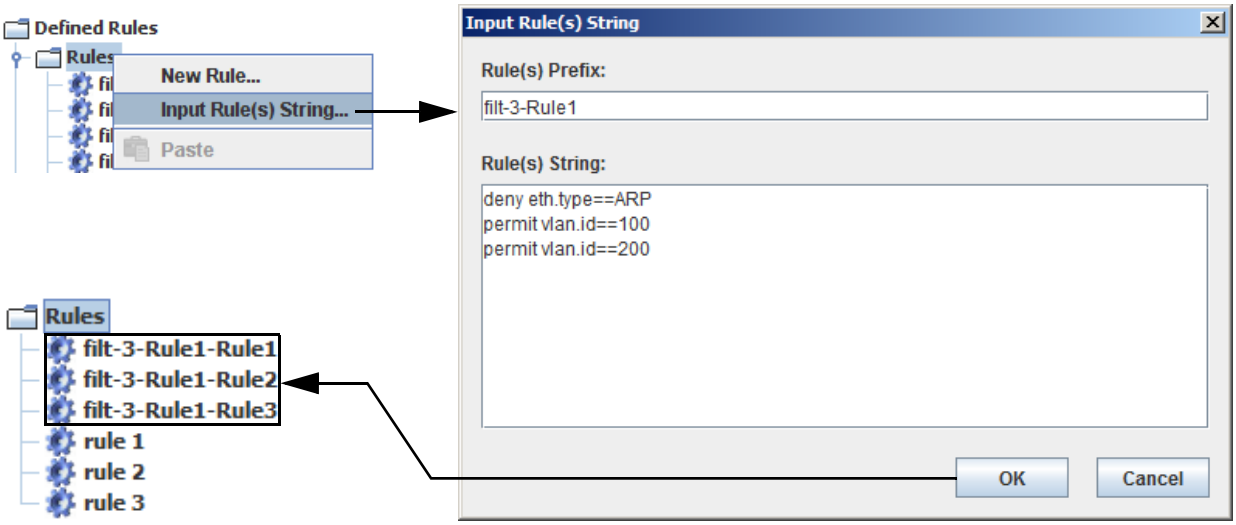
DPI Criteria

Refer to DPI Criteria in Rules on page 3-208.

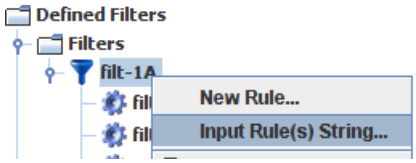
Rule Strings

Note: Refer to the **ADD RULE** command on page A-16 for a list of defined syntax rules.

To add multiple rules at one time, right-click on the Rules folder and select **Input Rule(s) String**. An Input Rule(s) String screen displays. Enter a prefix for the rule and the rule(s) into the Rule(s) String field. Click **OK**. The new rule displays in the Rules listing.

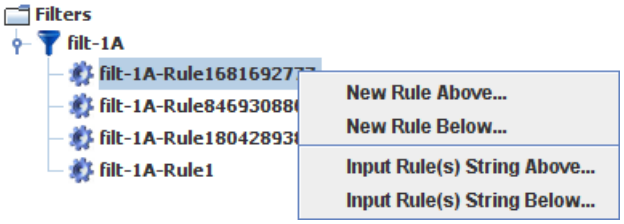


To add multiple rules to a defined filter, right-click on a defined filter and select **Input Rule(s) String**. An Input Rule(s) String screen displays. Enter a name for the rule and the rule(s) into the Rule(s) String field. Click **OK**. The new rules displays in the Filters listing.



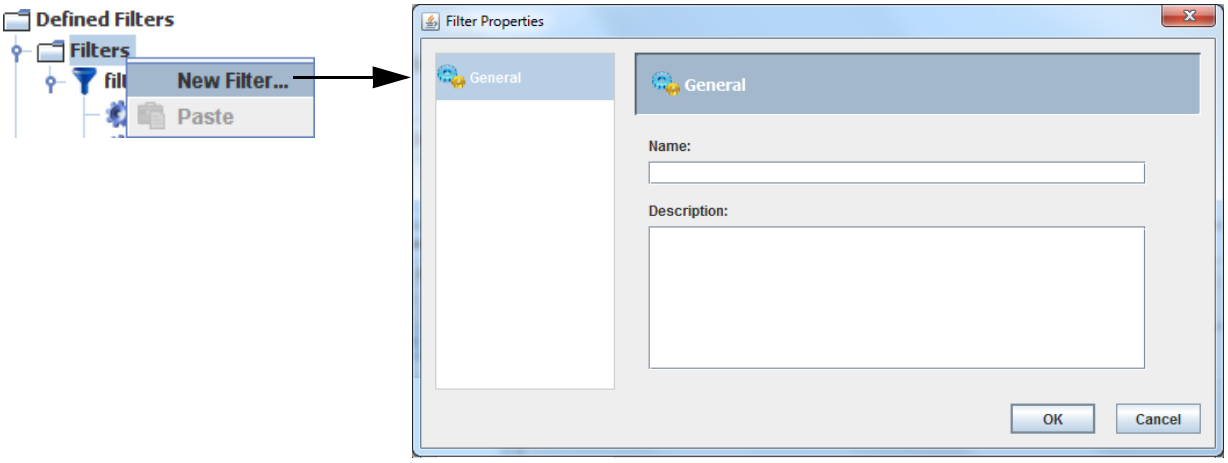
Additional rules can also be added from inside a defined filter. Right-click on a defined filter rule or rule string and select on of the following:

- New Rule Above / Below - positions the new rule in relation to the selected rule
- Input Rule(s) String Above / Below - positions the new rule string in relation to the selected rule string



Creating Filters

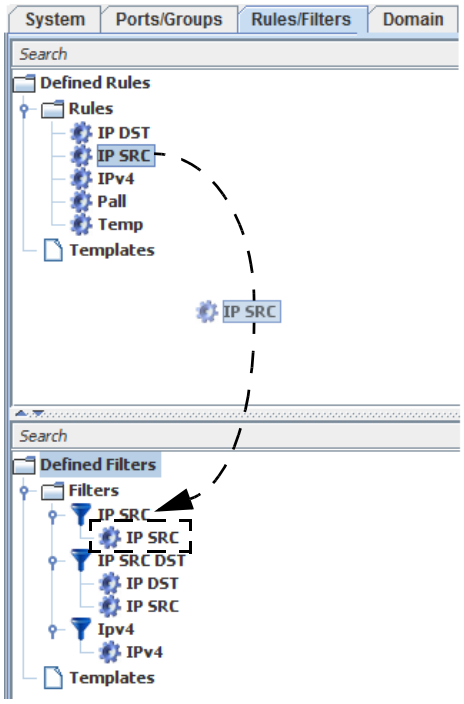
1 Click on the Rules/Filters tab. Under Defined Filters, right click on the Filters folder and select **New Filter**. The Filter Properties screen displays.



2 Enter a name for the filter in the Name text field. Optionally, enter a description of the new filter. Click **OK**. The new filter displays in the Defined Filters listing.

Associating Defined Rules within a Filter

Select a rule from the list of defined rules and drag down (or copy/paste) to a filter from the list of defined filters. The selected rule is then displayed as a subset of the filter. Additional rules can be added to a filter as required.



Destination Port Filters

Destination Port Filters provide the capability of defining filters on destination ports so that many users can share the same stream of traffic without affecting each other. This is not possible with Connection filters, since a rule match causes a frame to be redirected to a destination and effectively takes it out of the stream. With Destination filters, all destination ports can get all the traffic, and each can drop the unwanted frames.

Destination Port Filters uses existing Rules and Filters. These allow users to define rules with a condition and an action that either permits or denies frames passing through the port. Rules are organized into filters with each filter containing one or more Rules. Only Global Filters, the ones that appear in the Filter Tree, can be used as Destination Filters.

There is a difference between filters that are used in connections and Destination Port Filters. In the first case it is assumed that traffic is denied unless specifically permitted. In the latter case it's the opposite, traffic is assumed to be permitted unless specifically denied. So, Destination Port Filters would typically contain a series of "deny" rules, or a series of "permit" rules followed by a "deny all". Without the "deny all" rule at the end all traffic would be permitted.

One Destination Filter per port can be selected for any of the user-configurable front ports. The Destination Filter becomes active when the port is connected. Destination Port Filter hardware rules are allocated in groups of 32. Multiple 32-rule groups many be used by any given Destination Port Filter, the allocation is flexible.

The maximum number of active Destination Port Filters per blade would be 24 with up to 32 hardware rules each. The maximum number of hardware rules that can be contained in any Destination Port Filter is 256, with a limit of three 256-rule Destination Port Filters per blade. Note that a single rule with a range or list may consume multiple hardware rules.

Each Rule that uses VLAN ID and/or VLAN Priority will consume 3 times the number of hardware rule resources in a Destination Filter as compared to a Connection Filter.

Any of the active Destination Filters can be used by multiple ports on the same blade, in effect allowing all user-configurable ports to be destination-filtered at the same time, as long as they are applying the same set of filters. Active Destination Filters may be modified while traffic is running and are applied immediately without a separate activation step.

Destination Filters can be used with regular connection Filters at the same time. The regular Filters do their filtering on the source port(s) and reside on the source port blade. Destination Filters do their filtering on the destination port(s) and reside on the destination port blade.

Destination Filters do not reduce the number of available rules for regular connection filters.

To summarize:

- A port can select only one Destination Filter
- Multiple ports on the same blade can select the same filter without using more hardware resources
- Rules are allocated in groups of 32 rules (using one rule allocates all 32)
- 24 groups of rules (768 rules) per blade available for users
- Rule groups are flexibly allocated (24 filters with 1-32 rules per blade, up to 3 filters with 256 rules per blade)
- Traffic is assumed to be permitted unless specifically denied.
- Destination Filters and regular connection filters can coexist and be used on the same stream of traffic.
- Destination Filters do not reduce the number available rules for regular connection filters.
- Destination and Connection Filters will not work with 802.3 frame types; only filtering of Source and Destination MAC addresses is supported. Ethernet II frames can be filtered beyond the MAC addresses.

Destination Port Filter Usage

- Connection Filter VLAN Rules may include VLAN 1 ID and Priority and VLAN 2 ID and Priority. Destination Filter VLAN Rules may include VLAN 1 ID and VLAN 1 Priority only (i.e., they may not include VLAN 2 ID nor VLAN 2 Priority).
- Each Rule that uses VLAN ID and/or VLAN Priority will consume 3 times the number of hardware rule resources in a Destination Filter as compared to a Connection Filter.

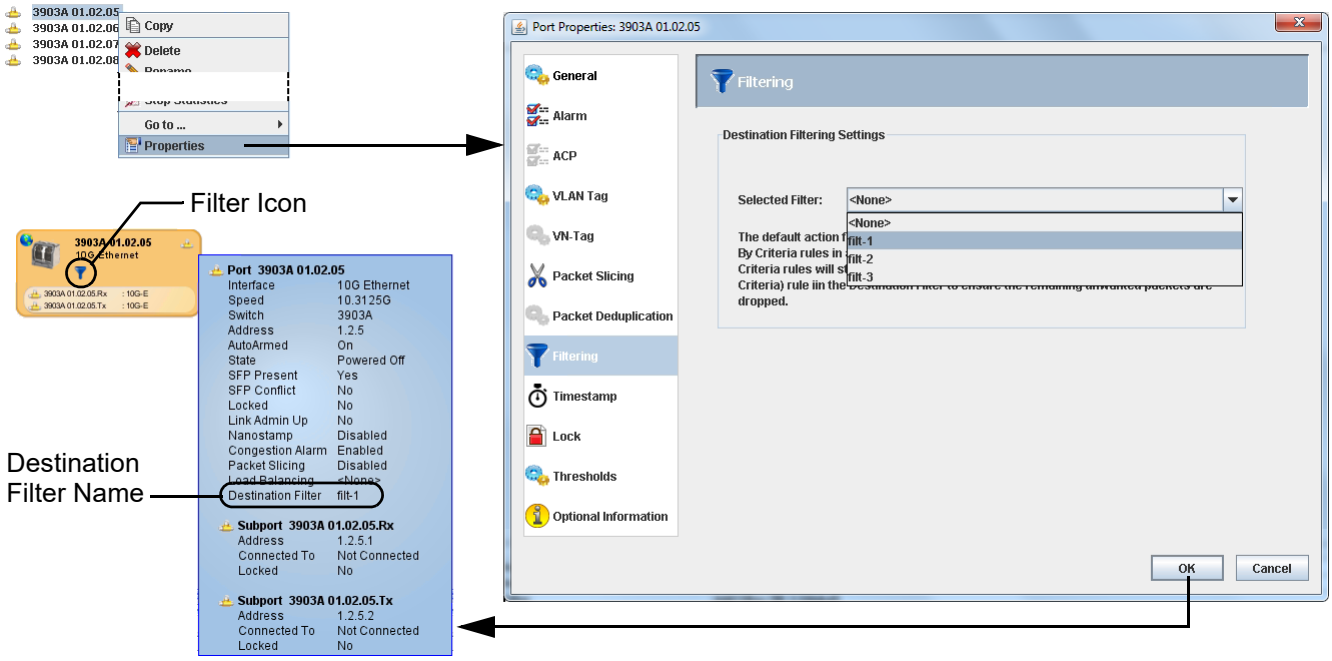
Defining a Destination Filter to a Port

1 Select a defined port, right-click and select **Properties**, then **Filtering**.

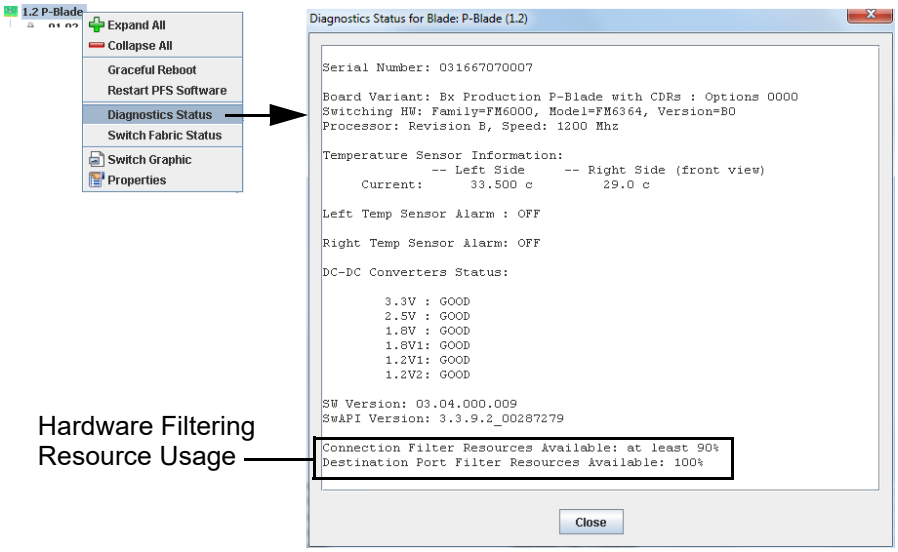
> **Note:** The Filtering Tab is grayed out under the following conditions:
> Mirror ports, since they are never used as a destination.
> xSL ports, since they carry traffic for possible many different connections.
> Ports on switches running an older version of the TestStream Management software that does not support Destination Filters.

2 Select a defined Global filter (located in the Filter tree) for the port from the Selected Filter drop down menu then click **OK**.

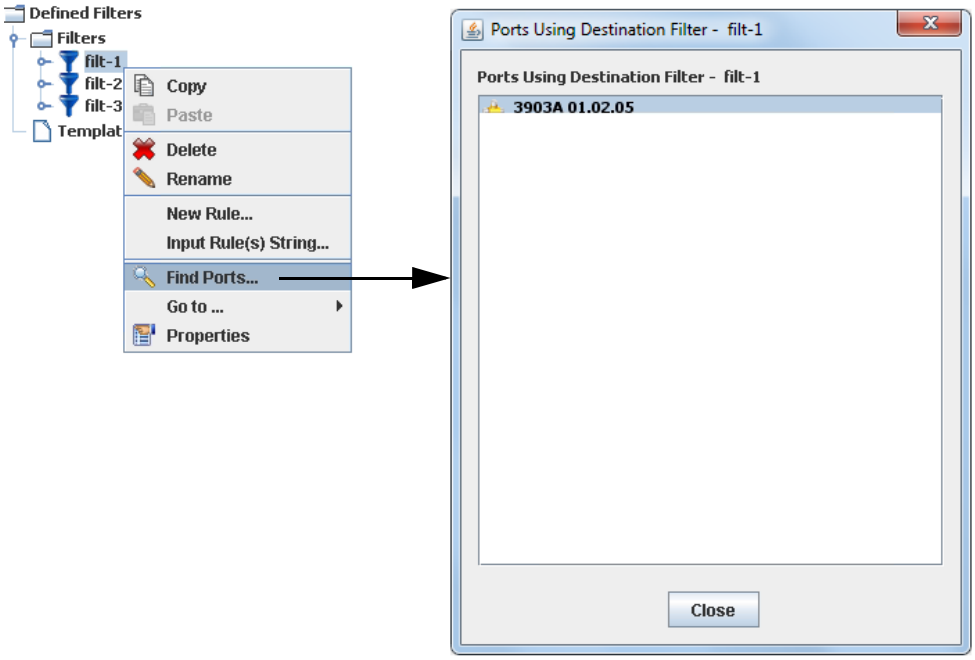
The status of the port / filter combination can be observed by floating the mouse over the defined port in the port System tree or from the port object if placed in a Topology Manager screen. The Destination Filter name is displayed in the information screen. In addition, if the port is placed in the Topology Manager the port object displays a Filter icon, indicating that Destination Filtering is enabled.



Hardware filtering resource usage can be observed from the blade Diagnostic Status screen.



Filters may not be deleted if they are being used, either on a Topology or as a Destination Filter in a Port Property. This is true even if the Port is not in a connection or the Destination Filter is disabled. To locate all places where a filter is used, so that it can then be deleted, right click on a defined filter and select **Find Ports** from the drop down menu. A window listing all ports connected to a filter displays.



Destination Port Filter CLI Commands

Revise Port

REVise {**POR**t|**PRTN**um} *port* **DES**tination **FIL**ter {*filtername*|**NONE**}
Revise the Destination Filter of the specified port. Destination filters can permit and deny Ethernet frames that would be transmitted from this port. There is an implicit 'permit all' if no filter is selected and for frames that do not match any rules of a selected filter. Selecting 'NONe' stops Destination Filtering on the port. port must be a port name if PORt is used, otherwise port is cc.ss.pp
PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Examples:
rev por 'Tool 1' Destination Filter 'No HTTPS'
revise prtnum 1.2.4 DES FIL 'Feed 1'
Revise Port Network1 Destination Filter NONE

Note: You cannot name a filter **NON**e, **ENA**ble, or **DIS**able if using the CLI.

Find Used Filters

SHOw **FIL**ters [**SEA**rch *text*]
Display a list of all defined filters and the number of rules in each.

Example:
show filter FilterA

SHOw **POR**ts **WIT**h [*options*]
Display a list of defined ports with a matching configuration.
Port names can use the wildcard symbols asterisk (*) and question mark (?).
***** will match any number of characters.
? will match any single character.

For example:
--name Tool* (will match any name starting with 'Tool')
--name Network? (will match any name starting with 'Network' and followed by a single character, such as Network1, Network2, NetworkA, etc.)
Surround names containing spaces with double quotes ("name").

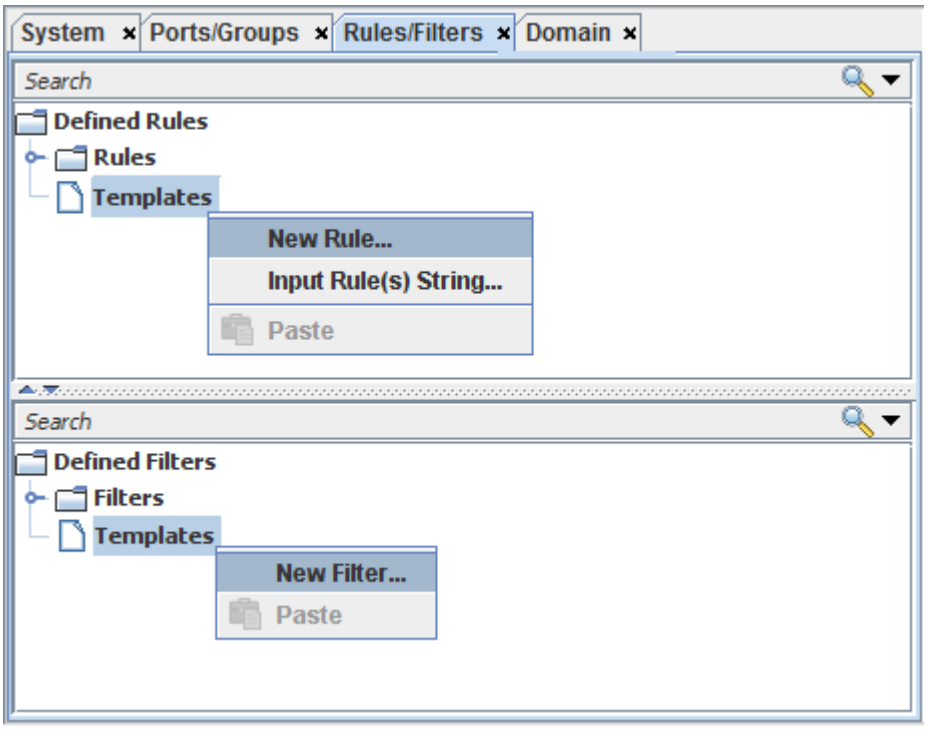
options (case sensitive):
-h [**--help**] Show options help
--dstfilter arg Destination Filter name
--name arg Port name
--verbose Verbose output

Examples:
SHOW Ports with --dstfilter "Drop HTTPS Filter"
SHO POR WIT --dstfilter "Only VOIP Filter"
SHOW PORTS WITH --name Tool*
sho por wit --name Network?
SHOw PORts WITH --name Tool* --dstfilter "Drop HTTPS" --verbose

Using Rules/Filters Templates

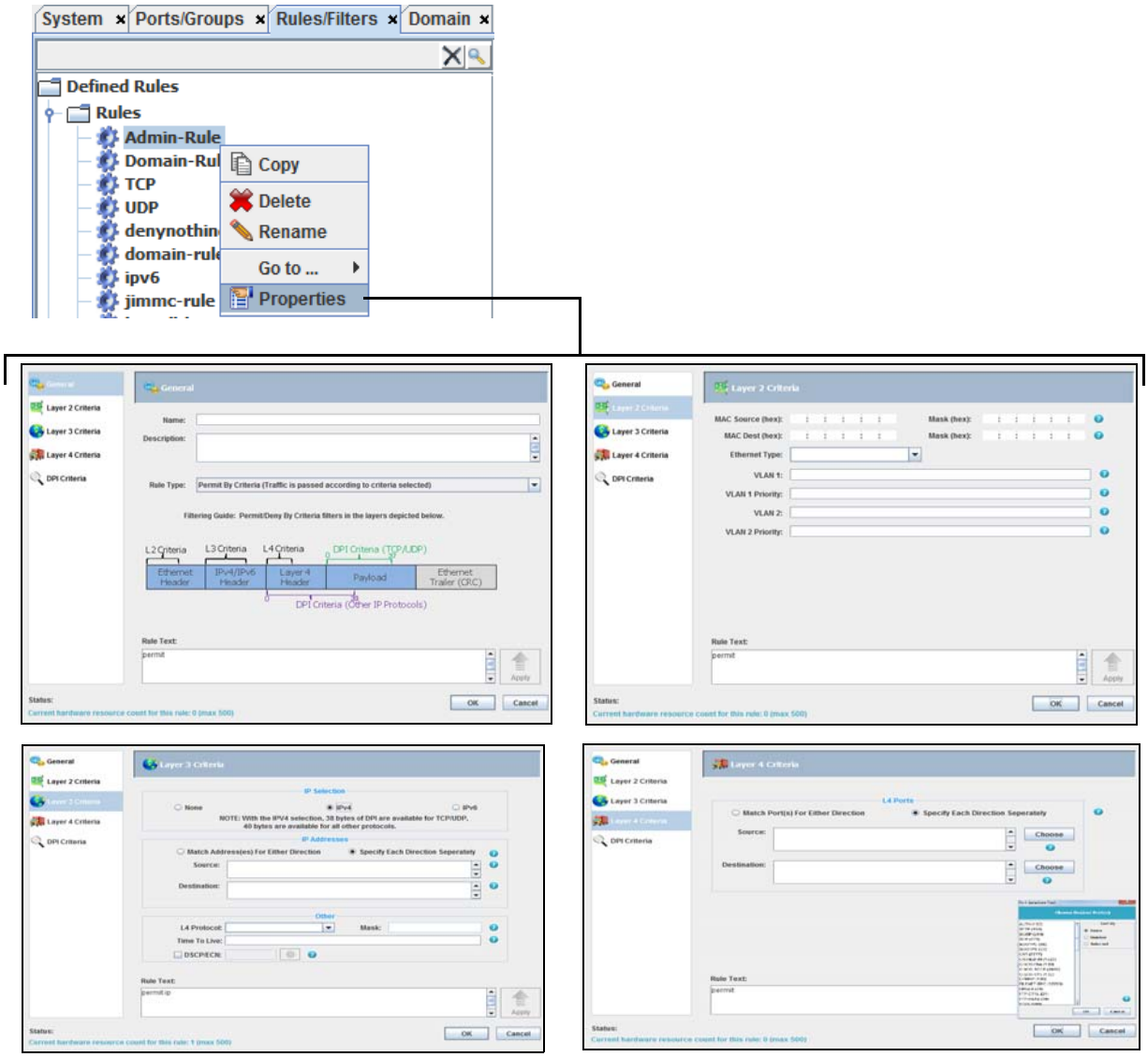
Rules and Filters templates are used to test out a new defined rule/filter prior to actually implementing in TestStream Management. The rules/filters templates are generated by right-clicking on the Templates folder and selecting New Rule (or New Filter) and using the same procedures described in Defining Rules on page 3-190 and Creating Filters on page 3-199.

A template is meant to be used as a foundation / testing area for creating a defined rule/filter. Using either copy/paste or drag/drop to the tree area or topology will create a new rule/filter using the template as a base; by assigning a new Rule name prior to the actual placement within the filter, the original baseline template is not altered.



Reviewing Defined Rule Properties

To review / edit configuration settings of a defined rule, right-click on a rule name from the list of defined rules and select **Properties**.



DPI Filtering

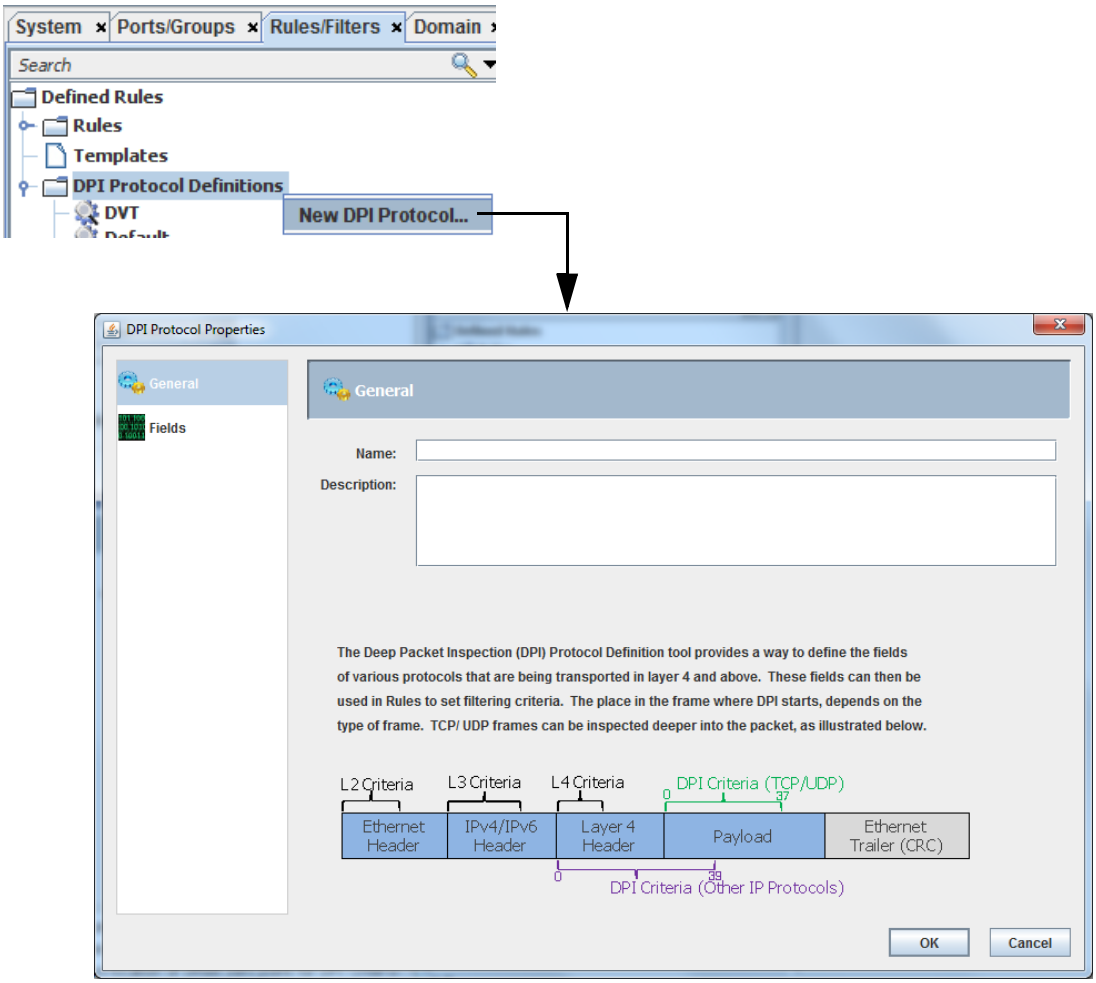
Deep Packet Inspection (DPI) filtering is used to examine parts of the packet in layer 4 and beyond. Like other filtering criteria, it can be used to route Ethernet frames to different destinations or to drop the frame.

40 bytes of DPI are available for IPv4 frames, and 14 bytes of DPI are available for IPv6 frames.

DPI Protocol Definitions

DPI Protocol Definitions are provided to make DPI filtering easier to use. Without a DPI Protocol Definition, the values in the DPI Criteria fields of a filter rule may only be entered one byte at a time. DPI Protocol Definitions allow the naming of fields and defining their various sizes and types.

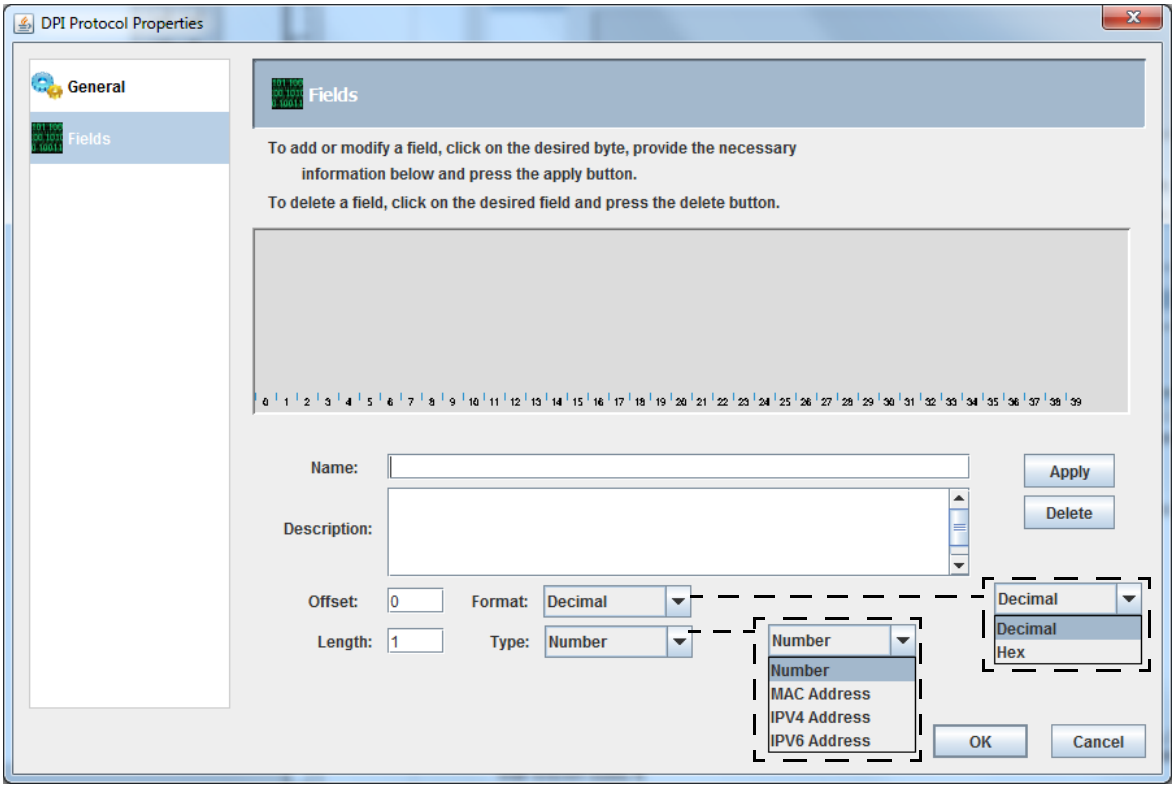
DPI protocols are maintained under **Defined Rules > Dpi Protocol Definitions**. To create a new protocol, right click on DPI Protocol Definitions and select **New DPI Protocol**. The DPI Protocol Properties screen displays.



- Name - Defined protocol name
- Description - Describes feature / function of protocol
- Graphic - Displays location of offset zero point for DPI Criteria (TCP/UDP and other IP protocols)

DPI Protocol Definition Fields

Clicking on **Fields** displays the following screen. This screen allows defining formats for protocols residing in the deep inspection area of Ethernet frames.



One or more fields can be defined. The fields defined do not have to be contiguous; there can be gaps. Click on a field and enter the following information:

- Field Name - Name of the field within the protocol
- Field Description - Information such as a description of a protocol, instructions to users (e.g., set IP L4 protocol to UDP, L4 dst port to 254), or any additional text
- Field Offset – Zero-relative offset from the start of the deep inspection area
- Field Format - Select either Decimal or Hex display
- Field type - Select from the following:
  - Number - Number spanning one or more bytes
  - MAC Address
  - IPv4 address
  - IPv6 address
- Field length (number of bytes) - if not implied as part of field format/type (for example, IPv4 type implies a length of 4 bytes). Numbers may have various sizes but IP and MAC addresses have well known sizes.

Click **Apply** to save the entered byte field information. Continue selecting fields / entering field information as required. Click **OK** to save the new defined protocol.

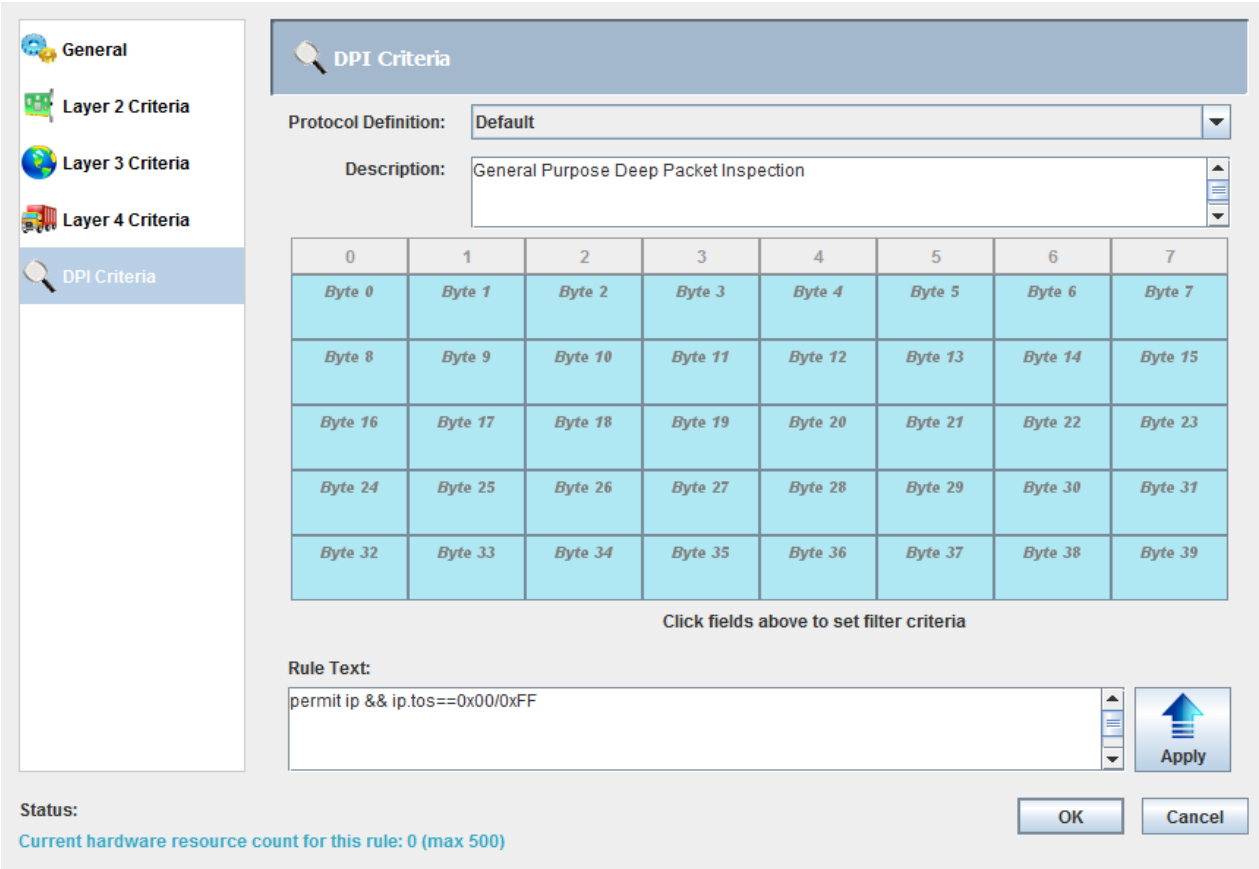
DPI Criteria in Rules

To filter on values in the DPI area of Ethernet packets, go the DPI Criteria window and fill in the desired values.

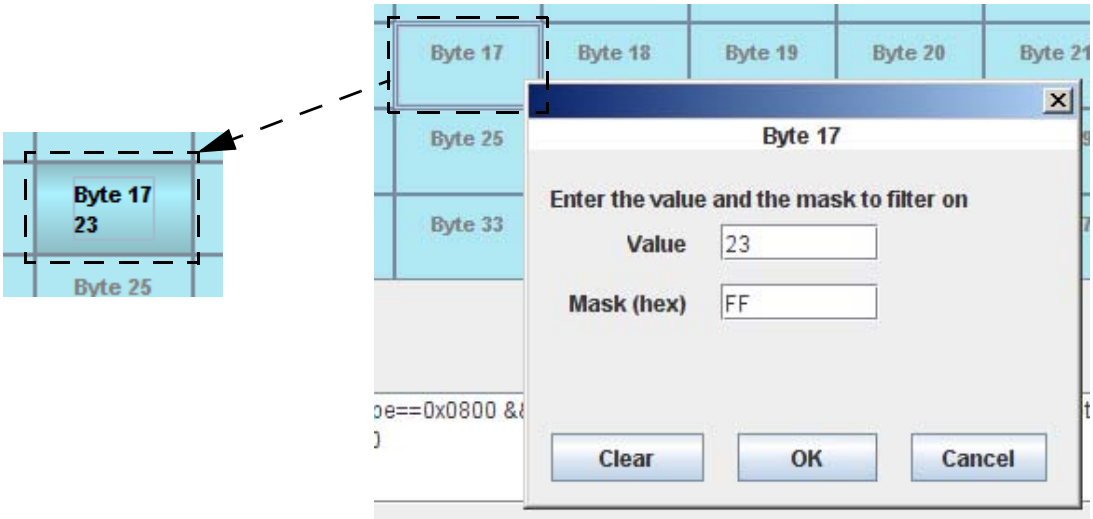
Note: DPI filtering also requires that a Layer 4 protocol be selected from Layer-3 criteria. The first 112 bytes of an Ethernet frame can be inspected by a rule. For frames with many optional headers (e.g., MPLS and IPV6), some DPI bytes might be beyond this limit and not be compared.

Note: Some DPI bytes might be beyond this limit and not be compared.

From **Defined Rules** right click on a rule, select **Properties > DPI Criteria**. The DPI Criteria screen displays.

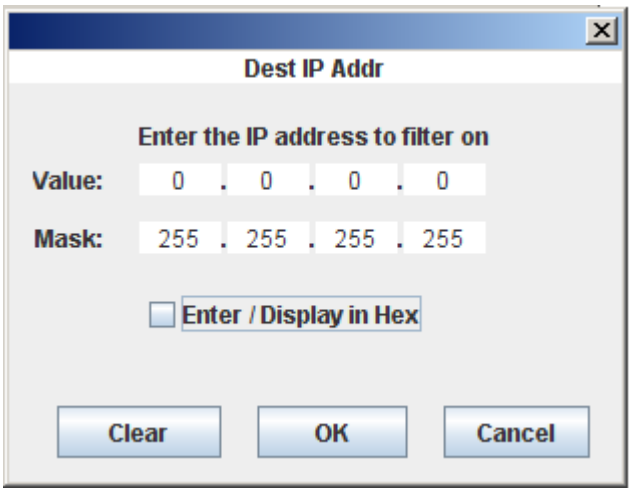


Select a protocol profile from the Protocol Definition drop down list if desired (default = single byte fields). To modify a data value field, click on the field - a popup screen displays. Enter the byte value and mask and click **OK**. The selected byte field now displays the entered value. Continue editing byte fields as required. Click **OK** from the DPI Criteria main screen to save the rule to the Defined Rules listing.

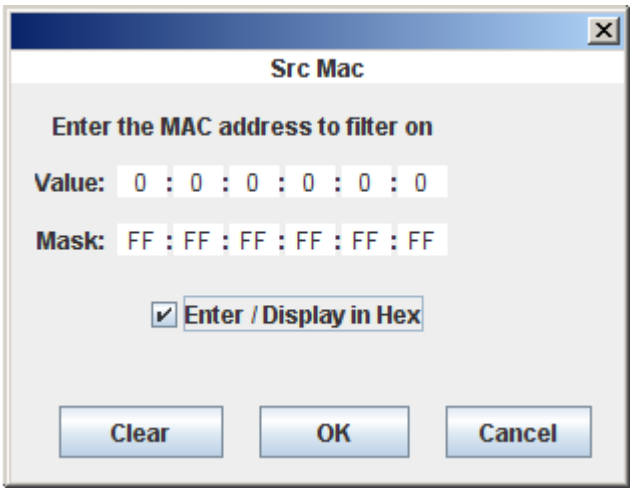


Field Data Examples

IPV4 Addresses



MAC Addresses



DPI Criteria Example - GTP-U

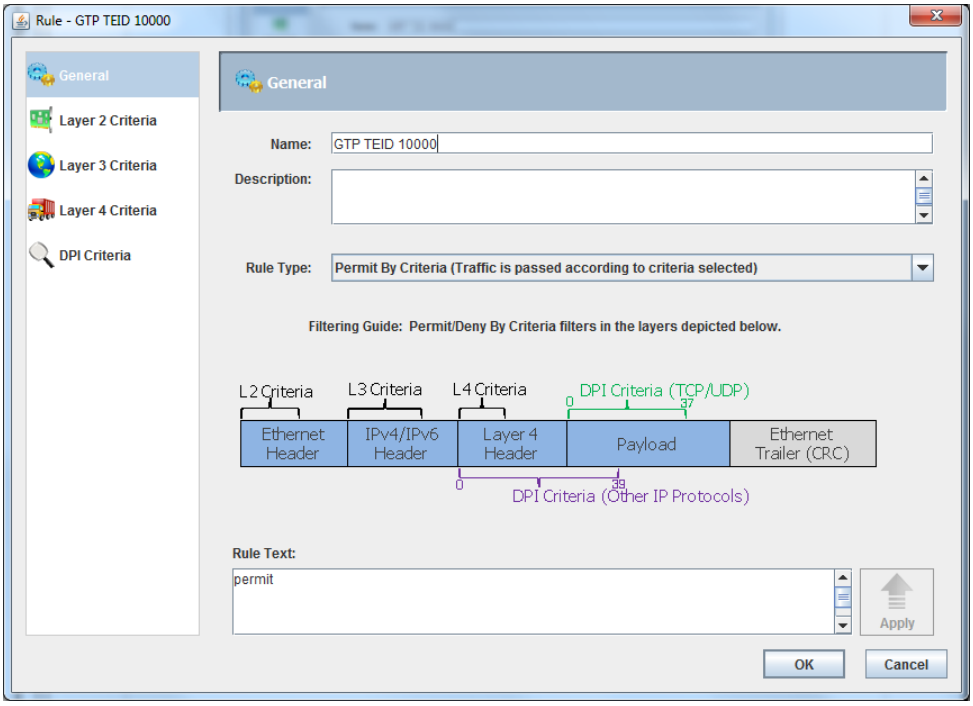
In the following example, a rule is created to match a value in the TEID field of a GTP (GPRS Tunneling Protocol) User Packet. We assume that GTP is carrying an IP version 4 packet in its payload.

DPI Rule Criteria using the GUI

GTP-U is a protocol that comes predefined in your database. There are several variations of the GTP header that are possible. This is because there are optional fields in the header, plus there is version 1 and version 2. You will have to know which type of GTP headers your traffic uses in order to configure a working filter. We recommend creating a Rule Template that can be reused for creating all your GTP Rules. By using the Rule Template you will only have to make the selections for L4 Protocol and Source/Destination Port once.

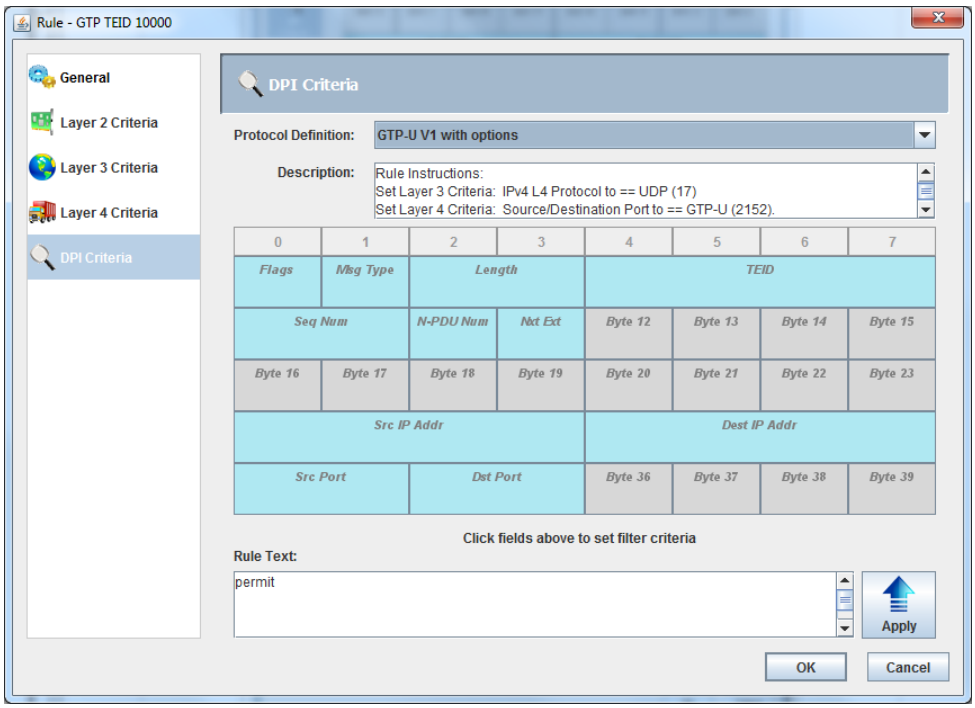
You could also create your own DPI Protocol Definition for any IP protocol and use it in a similar manner.

In this example we create a Rule (as opposed to a Rule Template). First create the new Rule and give it a name. Here we name it “GTP TEID 10000”. We leave the Rule Type as Permit by Criteria. You could also select Deny by Criteria.

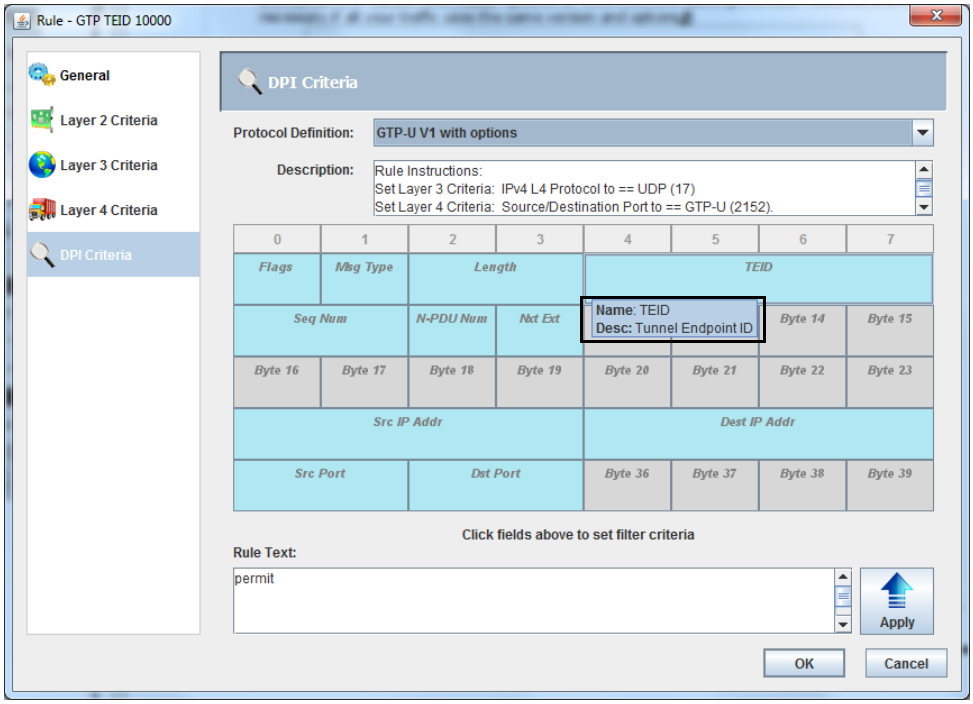


Next go to the DPI Criteria tab and choose one of the GTP-U DPI Protocol Definitions in the Protocol Definition pull down menu. Here we choose “GTP-U V1 with options”. This is GTP version 1 with the optional Sequence Number but no additional extension headers. The interesting fields are named and highlighted in blue according to that DPI Protocol Definition. Other bytes are gray. The gray bytes may still be set with values to match on if necessary. We will not need them in this example.

You will see some instructions in the Description box. These instructions were placed there when the GTP-U Protocol definition was created. They are there as a reminder about the other fields in the rule that must be set. It is always required to set a layer-4 protocol when using DPI. It is also a good idea to set the source or destination port to specify that only frames using the GTP-U port should match this rule’s criteria. Notice that the TEID field is defined starting at byte 4.

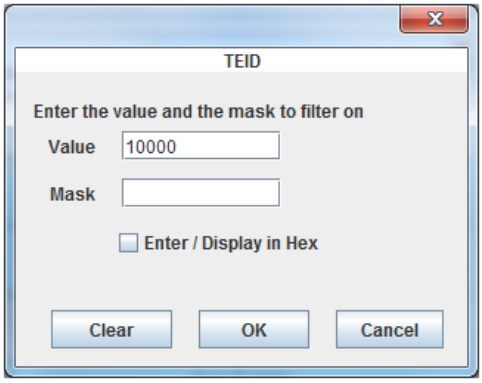


Hovering over a defined field will show a tool tip. The Flags field tool tip describes the flag bit settings. You may want to match certain bits in the Flags field for GTP in this Rule to ensure that frames match the correct GTP version and header options for which you are defining the Rule. However, this is not necessary if all your traffic uses the same version and options.

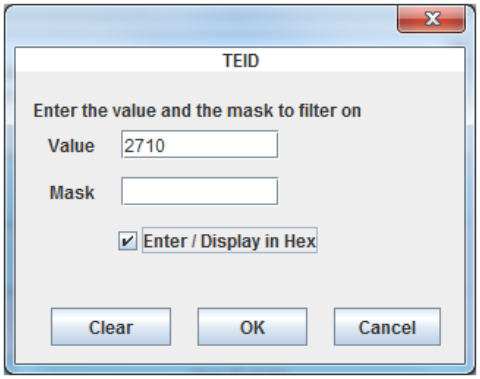


Click on the TEID field and fill in a value. It can be displayed in decimal or hexadecimal format. Do not enter a mask if you want to match a single TEID value. Refer to a discussion of masks elsewhere in this document to match a range of values.

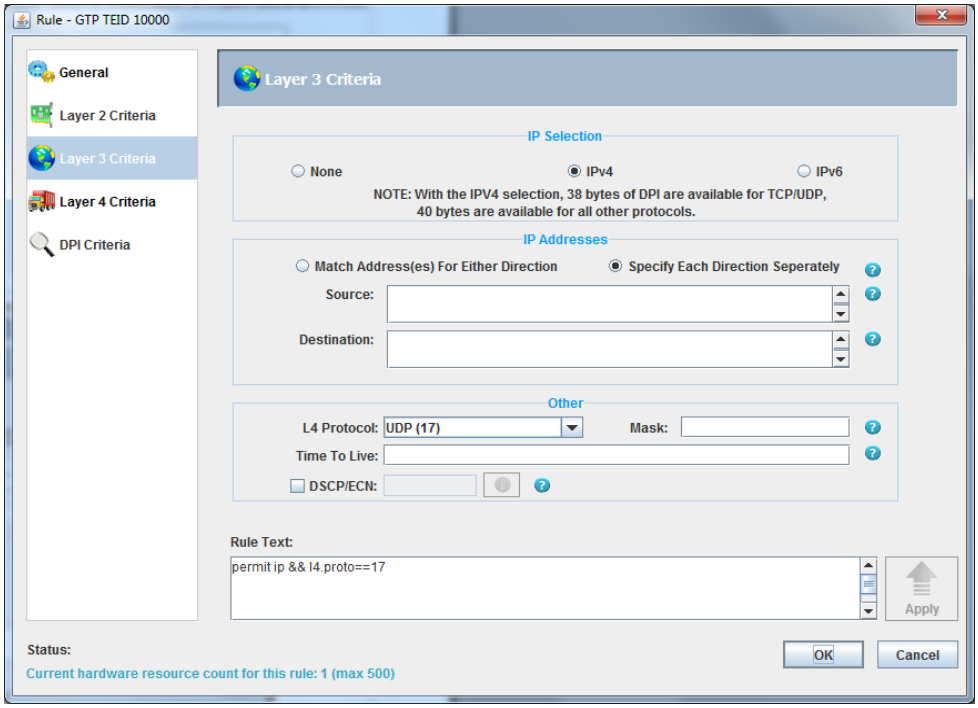
Decimal Value Display



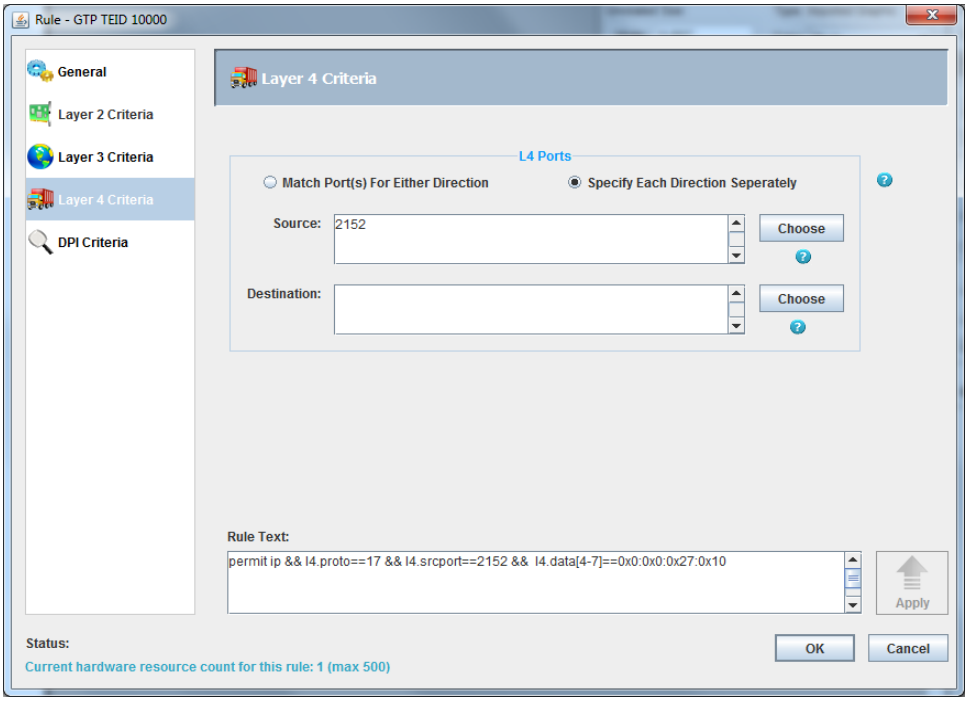
Hexadecimal Value Display



Next select a layer-4 protocol. In this case we know that GTP-U is a protocol that is carried in UDP.



Finally, following the instructions, select a source and/or destination port. Click **OK**, the rule is finished.



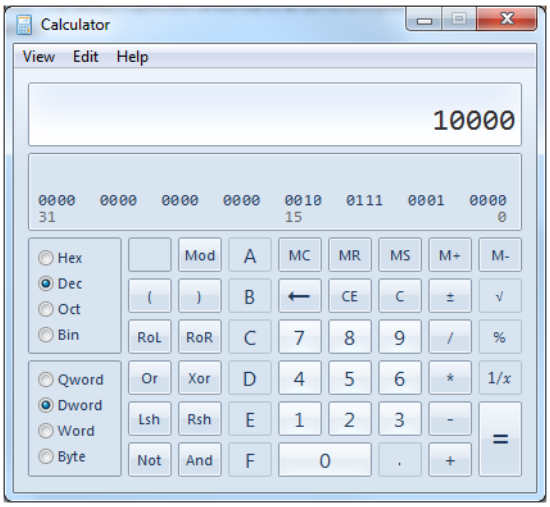
DPI Rule Criteria using CLI Commands

This same rule as above may be created using the Command Line Interface with rule text:

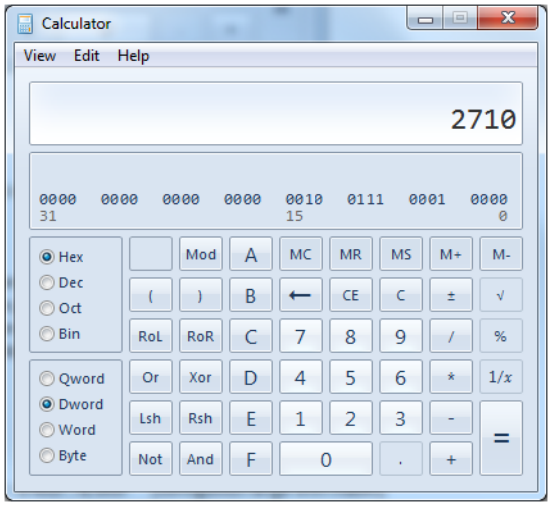
ADD RULE "TEID 10000" "permit ip.proto==UDP && udp.srcport==GTP-U && l4.data[4-7]== 0x0:0x0:0x27:0x10"

Note that the CLI does not use the DPI Protocol Definitions such as GTP-U, etc.; instead every byte must be entered separately. In the rule above the text "l4.data[4-7]==0x0:0x0:0x27:0x10" means that the DPI bytes from byte 4 to byte 7 should have the values 0, 0, 0x27, and 0x10. The byte values are separated by colons. These hexadecimal bytes are the converted decimal number 10,000. Note that you must enter all 4 bytes including the two leading zeros, because TEID is a 4-byte field.

Decimal



Hexadecimal



The general DPI syntax for CLI is:
l4.data[n] == x

where:
n is a number (0-37 for TCP or UDP IPv4 packets, 0-39 for other protocols over IPv4, 0-12 for TCP or UDP IPv6 packets, 0-14 for other protocols over IPv6) and indicates the offset into the deep inspection area. Ranges can be given, as well as a series of offsets separated by commas.

x is a number between 0 and 255 (it can also have a mask)

multiple numbers/masks are separated by colons

Examples:
l4.data[5]==1 (basic)
l4.data[5]==1/0x0f (with mask)
l4.data[0-3]==1:2:3:4 (contiguous range)
l4.data[0-3]==1/0x0f : 2/0x0f : 3/0x0f : 4/0x0f (contiguous range with masks)
l4.data[1,3,5,7]==1:2:3:4 (separate bytes)
l4.data[1-3,7,10]==1:2:3:17:100 (mixture of ranges and separate bytes)

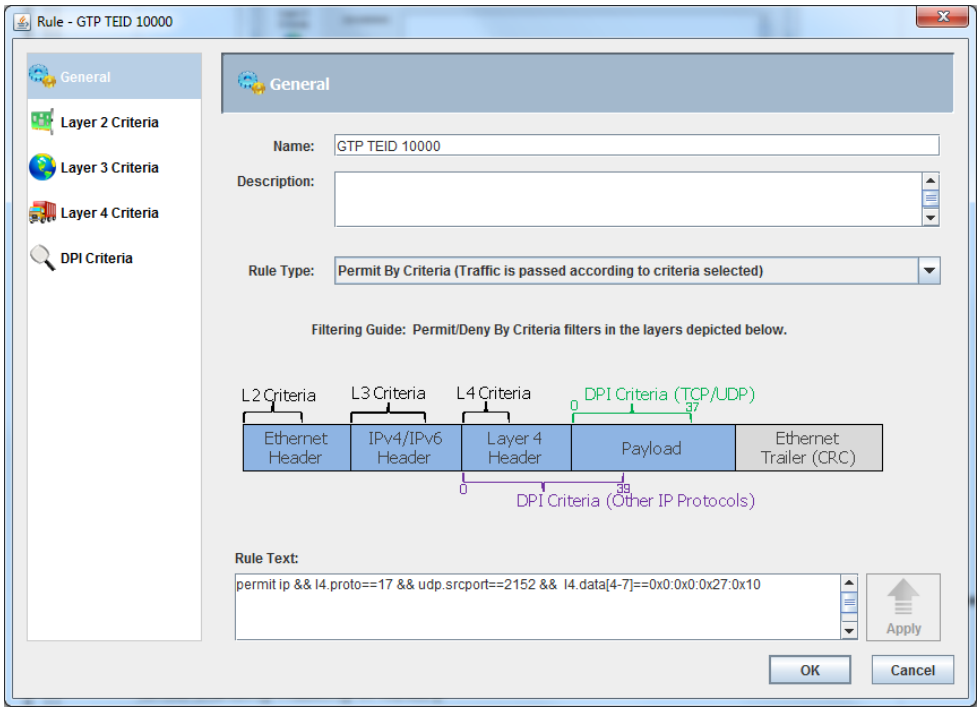
The number within the brackets, as in l4.data[5], specifies the offset of the byte in question, where 0 refers to the first byte in the deep inspection area.

Numbers may be given in hexadecimal or decimal. Hexadecimal numbers start with “0x”.

You can add spaces around the colons if that makes it easier to read:
“l4.data[4-7]==0x0 : 0x0 : 0x27 : 0x10”

You can also define bytes or groups of bytes separately:
“l4.data[4]==0x0 && l4.data[5]==0x0 && l4.data[6,7]== 0x27 : 0x10”

Offset 0 starts at the first byte following the layer-4 header for TCP/UDP packets and at the start of the layer-4 header for other protocols. Refer to the packet diagram in the General tab of the Rule window.



Note that the Layer-4 Criteria and the DPI Criteria for protocols other than TCP and UDP (shown in purple below the frame) overlap. The L4 Source Port overlaps with the first 2 bytes of DPI, and the L4 Destination Port overlaps with the next 2 bytes of DPI. An error message will be displayed if you attempt to use both for these protocols. DPI bytes do not overlap for TCP and UDP packets (shown in green above the frame).

Filter Usage Examples - Using Filters to Load Balance Traffic

Filtering can be used as an alternative to Load Balancing Groups to divide a traffic stream among multiple destinations. The destinations can be ports, multicast destination groups, or even load balancing destination groups. The filter-load balancing method would be useful, for example, in the following cases:

- You wish to load balance based on a field not included in standard Session-based load balancing
- Your switch load balancing parameter is set to Equal Distribution but for this stream you want to guarantee that packets with the same values will be sent to the same destination.

Any Rule criteria field (refer to Defining Rules on page 3-190) that has a mask available in any layer (2, 3, 4, or DPI) can be used.

First choose a relevant field, for example TCP Source Port, to use to divide your traffic. The simplest example is to divide the traffic to two streams. Usually a more well-balanced distribution is achieved by sending frames with odd numbers to one destination and even numbers to the other, rather than dividing by high numbers vs. low numbers. The table below shows the value/mask combinations you will need.

Divide into 2 Streams	Value	Mask
Stream 0 - Even	0	0x01
Stream 1 - Odd	1	0x01

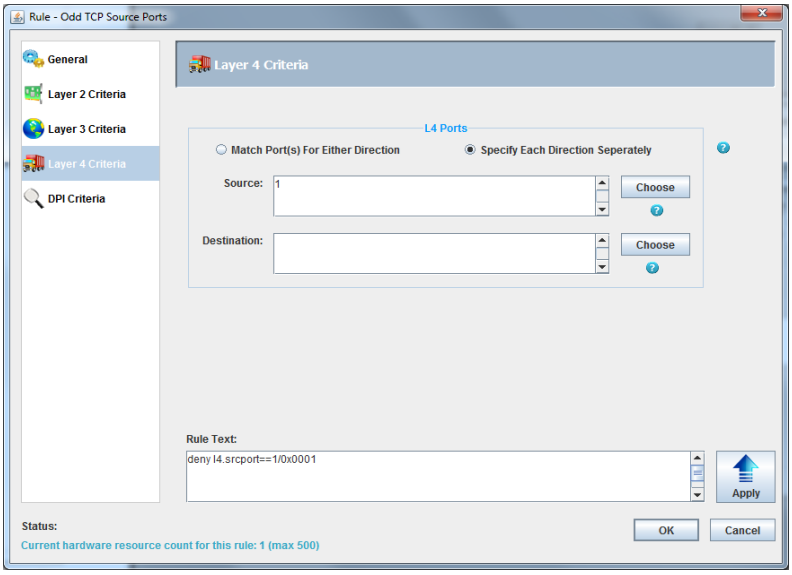
In the example above the first filter would have the rule:
“permit tcp.srcport==0/0x01”

The first filter would be connected to the first destination.

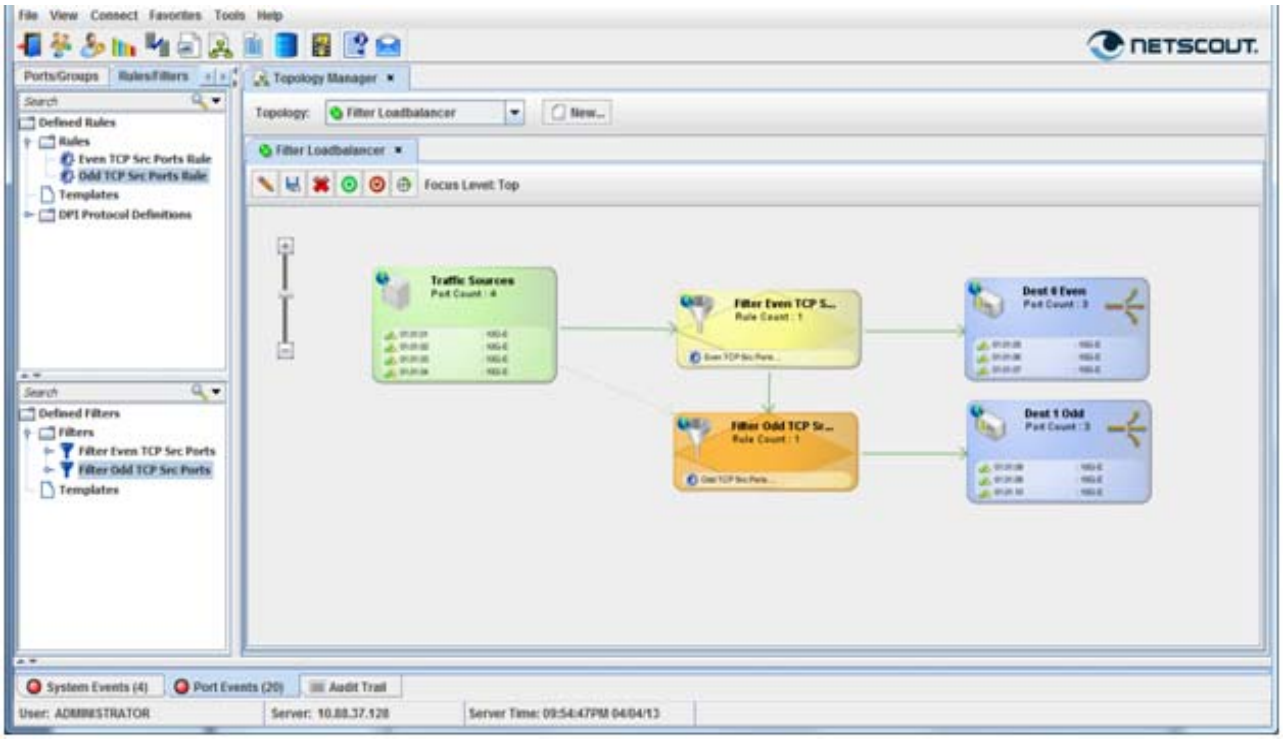
The second filter would have the rule:
“permit tcp.srcport==1/0x01”

The second filter would be connected to the second destination.

The Odd TCP Source Port Rule configuration is below. For the Even TCP Source Port Rule change the Source Port value to 0 and leave the Mask as 0x0001.



Create two separate filters, each with one of the rules. Then connect your sources and the two destinations, as shown below.



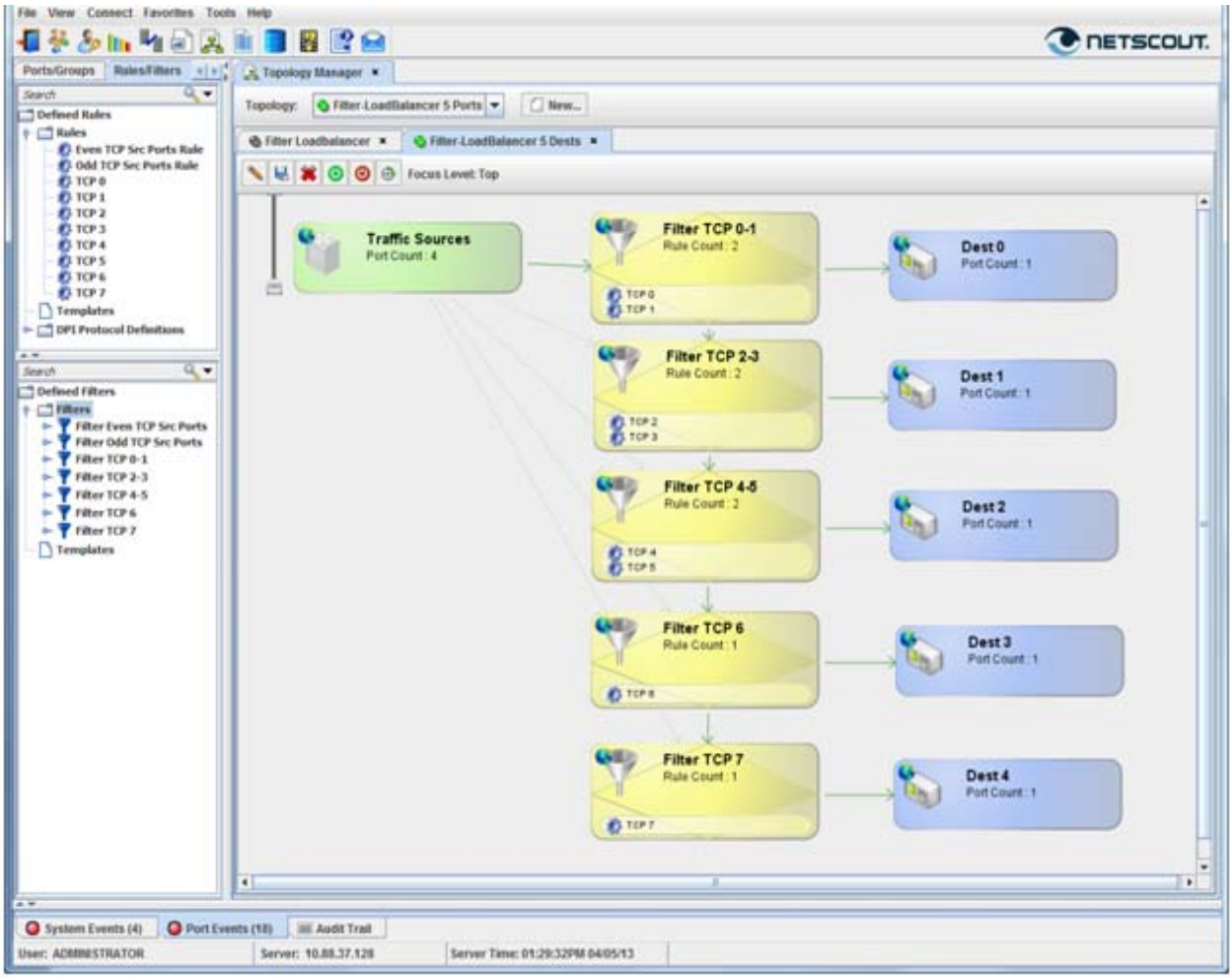
Values and masks for dividing traffic into four, eight, and sixteen streams are shown in the following tables. The number of value/mask combinations must always be a power of two, in other words 2, 4, 8, 16, 32, 64, etc.

Divide into 4 Streams	Value	Mask
Stream 0	0	0x03
Stream 1	1	0x03
Stream 2	2	0x03
Stream 3	3	0x03

Divide into 8 Streams	Value	Mask
Stream 0	0	0x07
Stream 1	1	0x07
Stream 2	2	0x07
Stream 3	3	0x07
Stream 4	4	0x07
Stream 5	5	0x07
Stream 6	6	0x07
Stream 7	7	0x07

Divide into 16 Streams	Value in Decimal	Value in Hexadecimal	Mask
Stream 0	0	0x00	0x0F
Stream 1	1	0x01	0x0F
Stream 2	2	0x02	0x0F
Stream 3	3	0x03	0x0F
Stream 4	4	0x04	0x0F
Stream 5	5	0x05	0x0F
Stream 6	6	0x06	0x0F
Stream 7	7	0x07	0x0F
Stream 8	8	0x08	0x0F
Stream 9	9	0x09	0x0F
Stream 10	10	0x0A	0x0F
Stream 11	11	0x0B	0x0F
Stream 12	12	0x0C	0x0F
Stream 13	13	0x0D	0x0F
Stream 14	14	0x0E	0x0F
Stream 15	15	0x0F	0x0F

If you have a number of destinations that is not a power of two, for example 5 destinations, then you would still have to create all the rules for a higher number that is a power of two. In this case the smallest number of streams possible would be 8. Refer to the table above for 8 Streams. You would add the 8 rules to 5 filters, each filter going to one destination. Some filters would get 2 rules and some filters would have a single rule.



Creating Number Ranges in Rules Using Masks

Sometimes it is desirable to filter traffic based on a range of values, rather than just a single value. Masks can be used for this purpose. In Rules the Layer 1, 2, 3, and DPI Criteria allow the entry of a mask for most fields. You may be familiar with subnet masks of IP addresses (address 192.168.0.0, subnet mask 255.255.0.0). The mask shows which part of the address should be ignored. In a similar manner number ranges can be created by ignoring certain bits of a value in a Rule. A zero in a bit of a mask means ignore that bit in the value.

The tables below show how to create number ranges in Rules. The mask will change based on the size of the field you are masking, so that it will include the high bits of the value. Some example field sizes are:

- 1-byte (8-bit) fields:
  - Layer 4 Protocol (ip.proto, ipv6.nxt, l4.proto)
- 1 ½ -byte (12-bit) fields:
  - VLAN ID (vlan.id, vlan2.id)
- 2-byte (16-bit) fields:
  - Ethernet Type (eth.type)
  - TCP/UDP Source/Destination Port (tcp.srcport, tcp.dstport, udp.srcport, udp.dstport, l4.srcport, l4.dstport)

- 4-byte (32-bit) fields:
  - TEID in the DPI GTP-U Protocol

The following table shows the masks to use for number ranges starting at zero. The field value to use for any range would always be zero, only the mask changes. Note that VLANs have a special column because they are a 1½ byte field, 12 bits. If the mask column for a number range is blank, then this number range is not available for that size field.

Start of Range	End of Range	Value to Use	Mask to use for 1-byte fields	Mask to use for VLAN 12-bit fields	Mask to use for 2-byte fields	Mask to use for 4-byte fields
0	1	0	0xFE	0xFFE	0xFFFE	0xFFFFFFFE
0	3	0	0xFC	0xFFC	0xFFFC	0xFFFFFFFC
0	7	0	0xF8	0xFF8	0xFFF8	0xFFFFFFF8
0	15	0	0xF0	0xFF0	0xFFF0	0xFFFFFFF0
0	31	0	0xE0	0xFE0	0xFFE0	0xFFFFFFE0
0	63	0	0xC0	0xFC0	0xFFC0	0xFFFFFFC0
0	127	0	0x80	0xF80	0xFF80	0xFFFFFF80
0	255	0		0xF00	0xFF00	0xFFFFFF00
0	511	0		0xE00	0xFE00	0xFFFFFE00
0	1023	0		0xC00	0xFC00	0xFFFFFC00
0	2047	0		0x800	0xF800	0xFFFFF800
0	4095	0			0xF000	0xFFFFF000
0	8191	0			0xE000	0xFFFFE000
0	16383	0			0xC000	0xFFFFC000
0	32767	0			0x8000	0xFFFF8000
0	65535	0				0xFFFF0000
0	131071	0				0xFFFE0000
0	262143	0				0xFFFC0000
0	524287	0				0xFFF80000
0	1048575	0				0xFFF00000
0	2097151	0				0xFFE00000
0	4194303	0				0xFFC00000
0	8388607	0				0xFF800000
0	16777215	0				0xFF000000
0	33554431	0				0xFE000000
0	67108863	0				0xFC000000
0	134217727	0				0xF8000000
0	268435455	0				0xF0000000
0	536870911	0				0xE0000000
0	1073741823	0				0xC0000000
0	2147483647	0				0x80000000

The following table shows how to create number ranges starting at a number other than zero. There is a limitation in that the starting number of the range must be evenly divisible by a number in the first column. Also, only certain ranges are possible with masking. The second column shows how to calculate the ending number of the range. The value to use in the Rule field is called ‘n’, which is the starting number you have chosen for the range. A starting number may be evenly divisible by many numbers in

the first column. In fact, when you find a row with a number by which it is evenly divisible, then all the previous rows are evenly divisible too. Multiple rows mean you have several ranges to choose from. Again the masks are shown for various size fields.

Start of range, a number (n) evenly divisible by:	End of the range (the starting number plus this value)	Value to use (n= the starting number)	Mask to use for 1-byte fields	Mask to use for VLAN 12-bit fields	Mask to use for 2-byte fields	Mask to use for 4-byte fields
2	n + 1	n	0xFE	0xFFE	0xFFFE	0xFFFFFFFE
4	n + 3	n	0xFC	0xFFC	0xFFFC	0xFFFFFFFC
8	n + 7	n	0xF8	0xFF8	0xFFF8	0xFFFFFFF8
16	n + 15	n	0xF0	0xFF0	0xFFF0	0xFFFFFFF0
32	n + 31	n	0xE0	0xFE0	0xFFE0	0xFFFFFFE0
64	n + 63	n	0xC0	0xFC0	0xFFC0	0xFFFFFFC0
128	n + 127	n	0x80	0xF80	0xFF80	0xFFFFFF80
256	n + 255	n		0xF00	0xFF00	0xFFFFFF00
512	n + 511	n		0xE00	0xFE00	0xFFFFFE00
1024	n + 1023	n		0xC00	0xFC00	0xFFFFFC00
2048	n + 2047	n		0x800	0xF800	0xFFFFF800
4096	n + 4095	n			0xF000	0xFFFFF000
8192	n + 8193	n			0xE000	0xFFFFE000
16384	n + 16383	n			0xC000	0xFFFFC000
32768	n + 32767	n			0x8000	0xFFFF8000
65536	n + 65535	n				0xFFFF0000
131072	n + 131071	n				0xFFFE0000
262144	n + 262143	n				0xFFFC0000
524288	n + 524287	n				0xFFF80000
1048576	n + 1048575	n				0xFFF00000
2097152	n + 2097151	n				0xFFE00000
4194304	n + 4194303	n				0xFFC00000
8388608	n + 8388607	n				0xFF800000
16777216	n + 16777215	n				0xFF000000
33554432	n + 33554431	n				0xFE000000
67108864	n + 67108863	n				0xFC000000
134217728	n + 134217727	n				0xF8000000
268435456	n + 268435455	n				0xF0000000
536870912	n + 536870911	n				0xE0000000
1073741824	n + 1073741823	n				0xC0000000
2147483648	n + 2147483647	n				0x80000000

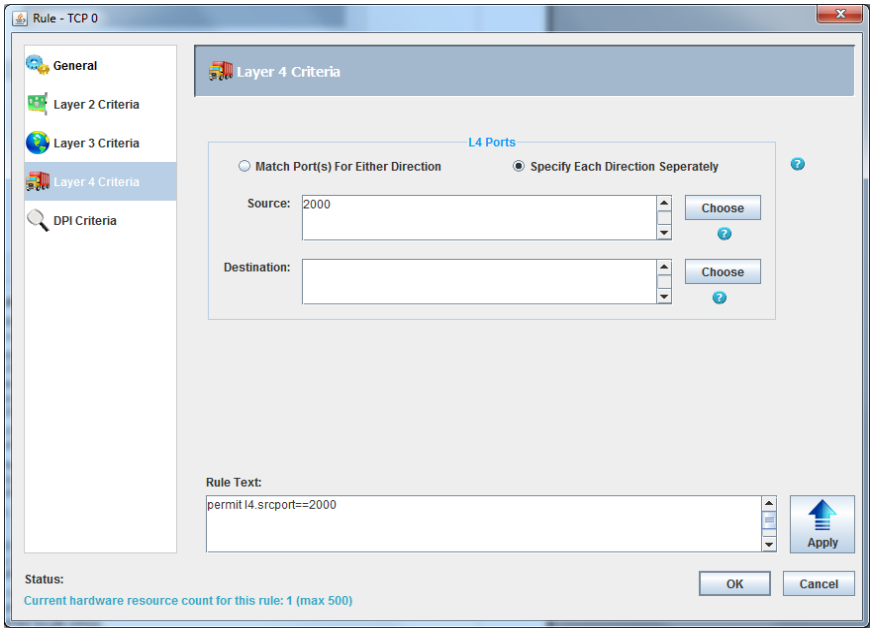
Masking Example - TCP Port 2000-2007

The starting number we choose for the range is 2000. This is evenly divisible by 2, 4, 8, and 16. So, the end of the range could be 2001, 2003, 2007, or 2015. We choose the range 2000-2007 for this example. We know that a TCP Port is a 2-byte field, so we go to the 2-byte column. The mask is 0xFFF8.

The rule will look like this:
"permit tcp.srcport==2000/0xFFF8"

Now any frame with a TCP Port from 2000 to 2007 will match the filter.

From the GUI, the Rule would look like this:



Masking Example - VLAN ID 120-200

In this example, the numbers do not map directly to one of the ranges in the table. In this case you must create multiple rules to cover all the numbers.

Looking through the numbers in the first column we find the first number greater than or equal to our starting number 120; we find it is 128. We calculate the ending value from that row, 128+127=255. This number is too big because it goes past the end of our desired range. We want to go only up to 200, not 255. So we go to the previous row where the end of the range is n+63. We can make one Rule using this row with a range from 128 to 191 (128+63).

To cover the range 128-191 we create the Rule:
"permit vlan.id==128/0xF80"

Next we need to cover the numbers 192 to 200. There is a range for n+7. That row shows we need a number evenly divisible by 8: 192 is evenly divisible by 8 so we make a second rule:
"permit vlan.id==192/0xFF8"

This gives up 192 to 199. So we need another rule for 200:
"permit vlan.id==200"

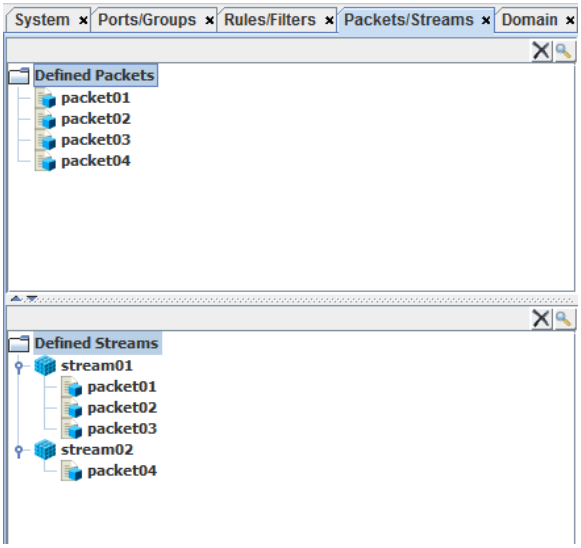
Now for the numbers 120 to 127:
120 is evenly divisible by 8, so we can make a rule to cover 120 to 127:
"permit vlan.id==120/0xFF8"

Here are all the rules for VLAN 120-200 from above in numerical order:
"permit vlan.id==120/0xFF8"(120-127)
"permit vlan.id==128/0xF80"(128-191)
"permit vlan.id==192/0xFF8"(192-199)
"permit vlan.id==200"(200)

With these 4 rules in one filter any frame with a VLAN ID of 120-200 will match the filter.

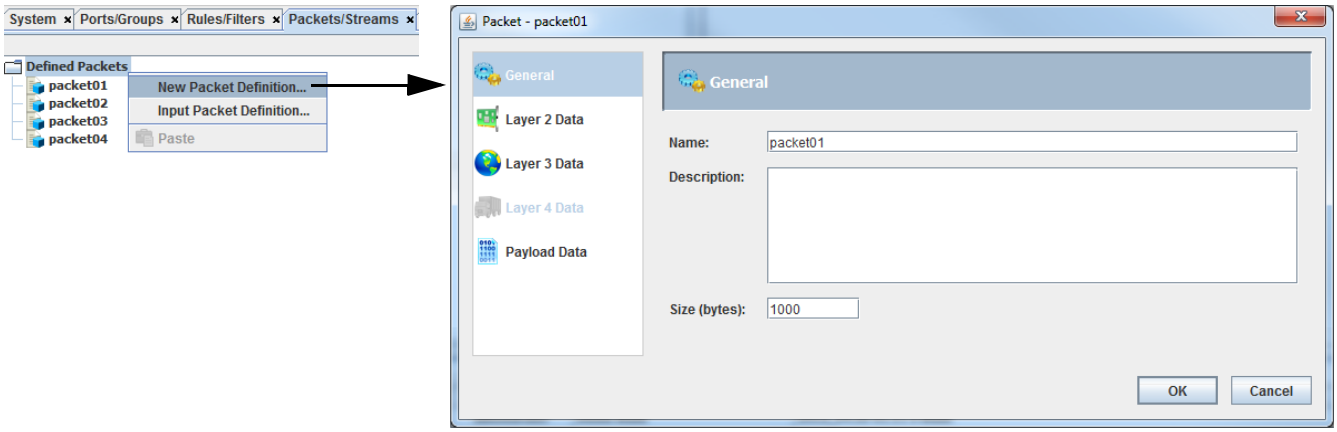
Packets/Streams

Selecting the Packets/Streams tab allows constructing individual packets and defining one or more packet streams for testing purposes. Similar to defining rules then assigning the rules to specified filters, you first define the packets then assign the packets to defined streams. The defined streams can then be used as Stream Generators, sending out data packets to one or more ports.



Defining Packets - New Packet Definition

1 Click on the Packets/Streams tab. Right click on the Defined Packets folder and select **New Packet Definition**. The Packet - General screen displays.



2 Enter a name for the packet in the **Name:** text field. Optionally, enter a description of the new packet.

3 Enter a value for the packet size (in bytes) in the **Size (bytes):** field (default = 64).

4 Click **OK** to save the new packet or go on to another layer. The new packet is displayed in the Defined Packets listing.

Layer 2 Data

1 Click on the **Layer 2 Data** icon.

2 Enter the desired MAC Source and/or Destination addresses in hexadecimal format (range = 00 - FF).

3 Select an Ethernet type from the drop down menu or type in a value.

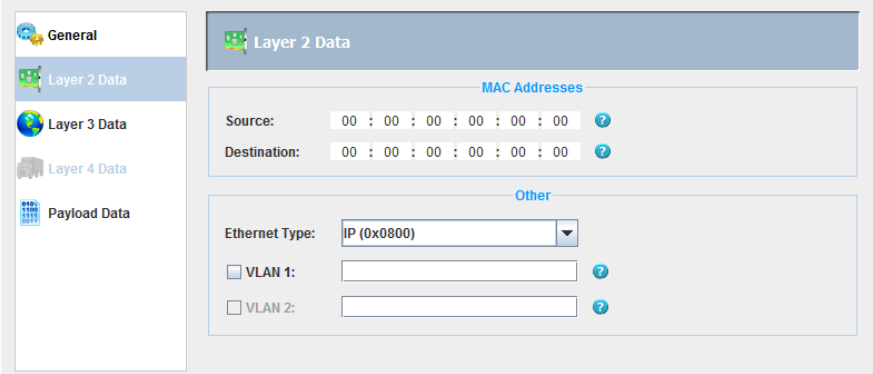
4 Select then enter the Virtual LAN tag (VLAN 1); allowed range = 0 - 4095.

> **Note:**
> When a single tag is inserted, this is the 802.1Q Tag.
>
> When the frame is doubled tagged (VLAN 2 also selected), this field becomes the Outer Tag (i.e., the tag closest to the beginning of the Ethernet frame).

5 Select then enter the second Virtual LAN tag (VLAN 2); allowed range = 0 - 4095.

> **Note:**
> When the frame is doubled tagged, this field becomes the Inner Tag (i.e., the second tag from the beginning of the Ethernet frame).

6 Click **OK** to save the new packet or go on to another layer. The new packet is displayed in the Defined Packets listing.



Layer 3 Data

> **Note:** This screen is accessible only if Ethernet type *IP* or *IPV6* is selected from the Layer 2 Data screen.

1 Click on the **Layer 3 Data** icon.

2 Enter the desired IPV4 Source and/or Destination addresses.

3 **Version:** Keep at the default value of 4.

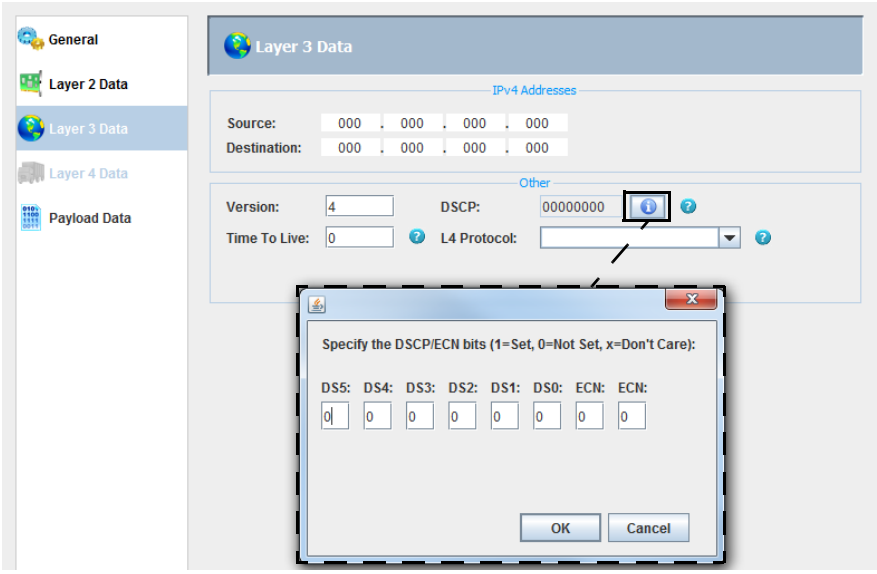
4 **Time to Live:** Optionally, enter in a value for the Time To Live setting (range = 0 -255):

5 **DSCP:** Enter specified bits (refer to the information (**i**) pop-up screen for value definitions):

Differentiated Services Code Point: Defined by RFC 2474. Denotes use of real time streaming data.
Explicit Congestion Notification: Defined by RFC 3168. Denotes use of end-to-end notification of network congestion.
Values are entered by enabling the field, then clicking on the (i) button to open the bit field control

6 **L4 Protocol:** Select the desired L4 protocol from the drop down list.

7 Click **OK** to save the new packet or go on to another layer. The new packet is displayed in the Defined Packets listing.



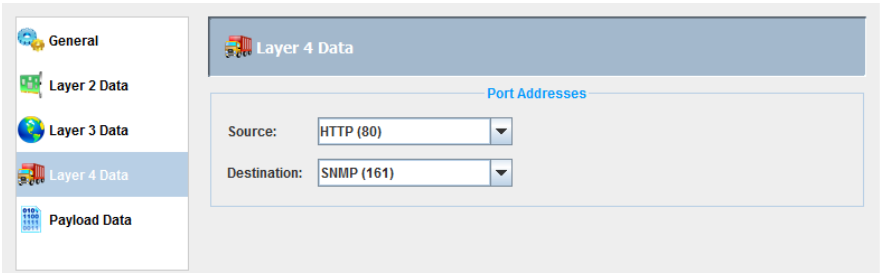
Layer 4 Data

Note: This screen is accessible only if L4 Protocol *TCP (6)* is selected from the Layer 3 Data screen.

1 Click on the **Layer 4 Data** icon.

2 Select the desired Port Source and/or Destination addresses from the drop down menus or type in a value.

3 Click **OK** to save the new packet or go on to another layer. The new packet is displayed in the Defined Packets listing.



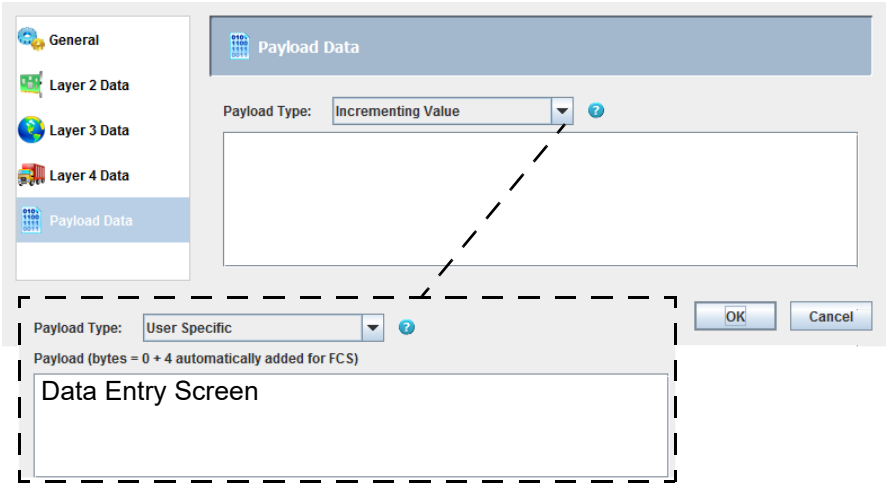
Payload Data

1 Click on the **Payload Data** icon.

2 Select the required Payroll Type from the drop down menu:

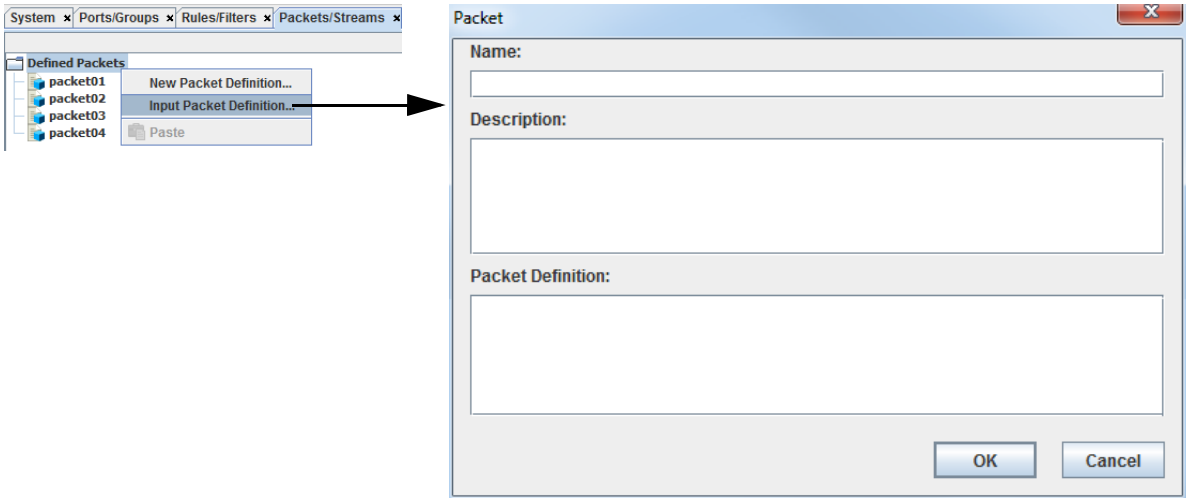
- Incrementing Value - 1st byte = 00, 2nd byte = 01, etc.,; repeating after FF
- Repeating Pattern - A byte pattern (up to N bytes) that will be repeated
- Random - Random payload
- User Specified - Pattern is user specified (bytes = 0 + 4 automatically added for FCS) - enter required pattern in data entry screen

3 Click **OK** to save the new packet. The new packet is displayed in the Defined Packets listing.



Defining Packets - Input Packet Definition

1 Click on the Packets/Streams tab. Right click on the Defined Packets folder and select **Input Packet Definition**. The Packet screen displays.



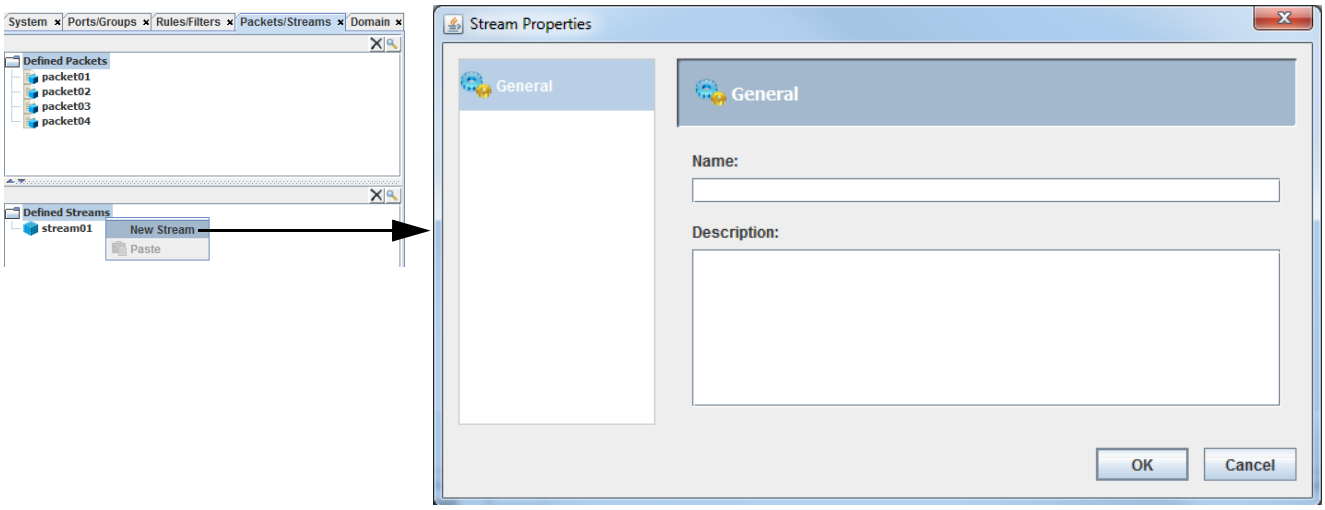
2 Enter a name for the packet in the **Name:** text field. Optionally, enter a description of the new packet.

3 Enter the packet requirements in the **Packet Description:** text field.

4 Click **OK** to save the new packet. The new packet is displayed in the Defined Packets listing.

Defining Streams

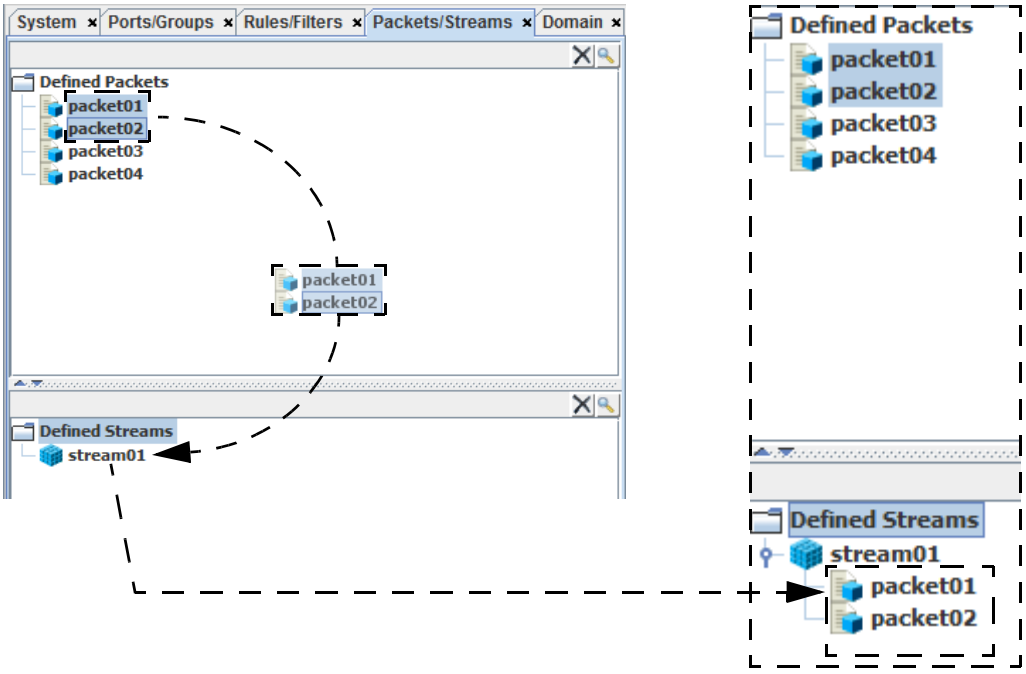
1. Click on the Packets/Streams tab. Right click on the Defined Streams folder and select **New Stream**. The Stream Properties - General screen displays.
2. Enter a name for the stream in the **Name:** text field. Optionally, enter a description of the new stream.
3. Click **OK** to save the new stream. The new stream is displayed under the Defined Stream folder.



Assigning Packets to Streams

To assign defined packets to a defined stream:

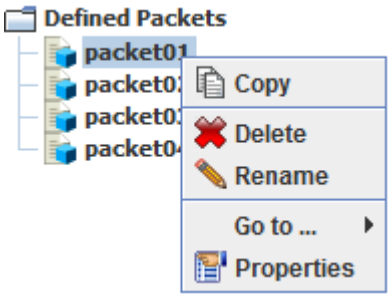
Select one or more packets from the Defined Packets folder and drag them to the selected stream in the Defined Streams folder. The selected packets are now displayed as part of the stream.



Packets/Streams Menus

Packet Menu

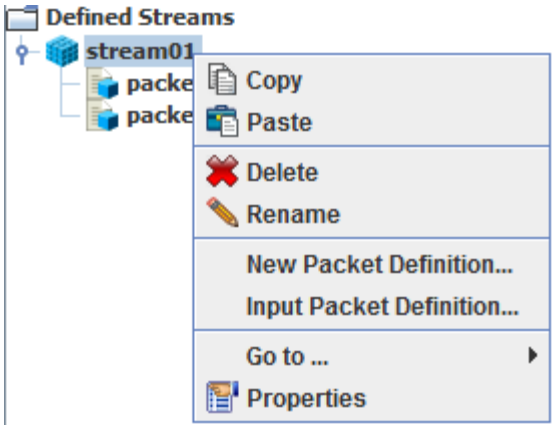
The following menu options are available for defined packets.

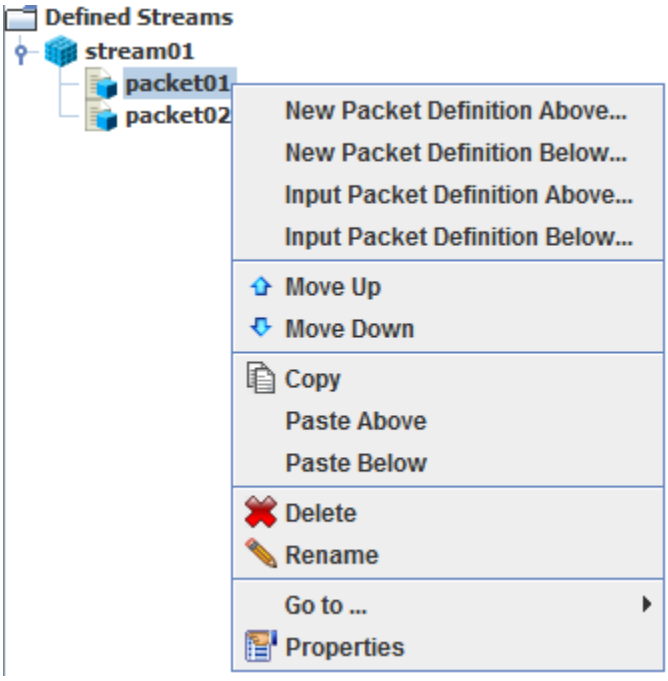


- Copy / Paste - Duplicates and places (with a new entered name) a selected packet into Defined Packets.
- Delete - Remove a selected packet.
- Rename - Change the name of a selected packet.
- Go to ... - Links to the following:
  - Topologies
- Properties - Shows the characteristics and settings of a selected packet.

Streams Menus

The following menu options are available for defined streams / packets associated with streams.





Defined Streams

- Copy / Paste - Duplicates and places (with a new entered name) a selected stream into Defined Streams.
- Delete - Remove a selected stream.

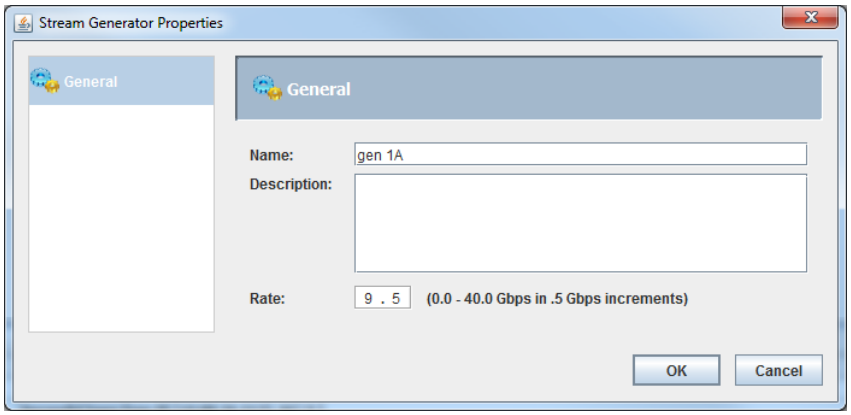
- Rename - Change the name of a selected stream.
- New Packet Definition - Allows creating a new packet within the stream (refer to Defining Packets - New Packet Definition on page 3-222).
- Input Packet Definition - Allows defining a new packet within the stream (refer to Defining Packets - Input Packet Definition on page 3-225).
- Go to ... - Links to the following:
  - Topologies
- Properties - Shows the characteristics and settings of a selected stream.

Associated Packets

- New Packet Definition Above / Below - Allows creating a new packet within the stream (refer to Defining Packets - New Packet Definition on page 3-222) at a selected location within the stream.
- Input Packet Definition Above / Below - Allows defining a new packet within the stream (refer to Defining Packets - Input Packet Definition on page 3-225) at a selected location within the stream.
- Move Up / Down - Reposition the order a packet is displayed in the stream list.
- Copy - Duplicates (with a new entered name) a selected packet.
- Paste Above / Below - Places (with a new entered name) a duplicated packet in a selected location in Defined Streams.
- Delete - Remove a selected stream.
- Rename - Change the name of a selected stream.
- Go to ... - Links to the following:
  - Topologies
- Properties - Shows the characteristics and settings of a selected stream.

Define / Associate Stream Generators to Ports

To define and associate a stream generator to blade ports, select a defined stream from the defined streams listing and drag into the topology manager screen. A Stream Generator Properties screen displays.



1 Assign a name for the generator in the **Name:** field.

Under **Rate:**, enter a packet data rate, definable in 0.5 Gbps increments (from 0.0 - 40.0 Gbps; default = 0.0).

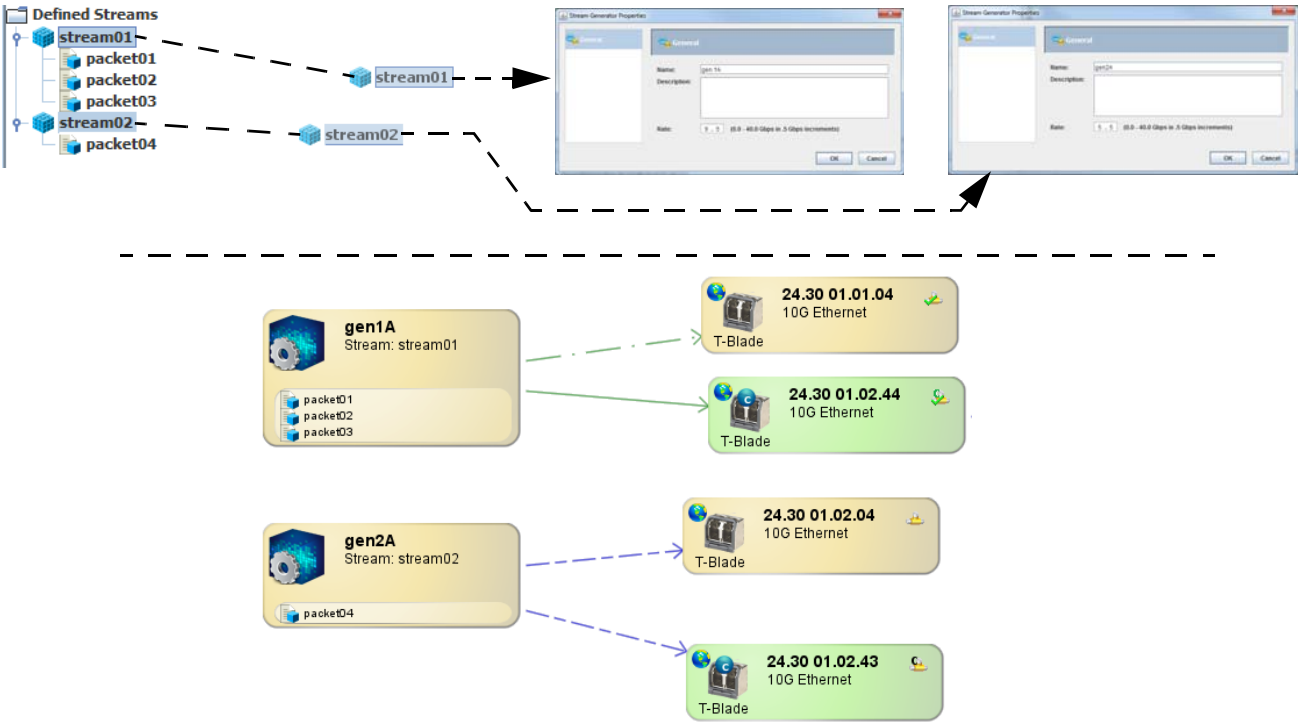
Optionally, enter any additional user information in the **Description:** field.

2 Click **OK** to save the generator settings.

A stream generator object containing the properties of the defined stream is added to the topology manager screen. Create any additional stream generators as required.

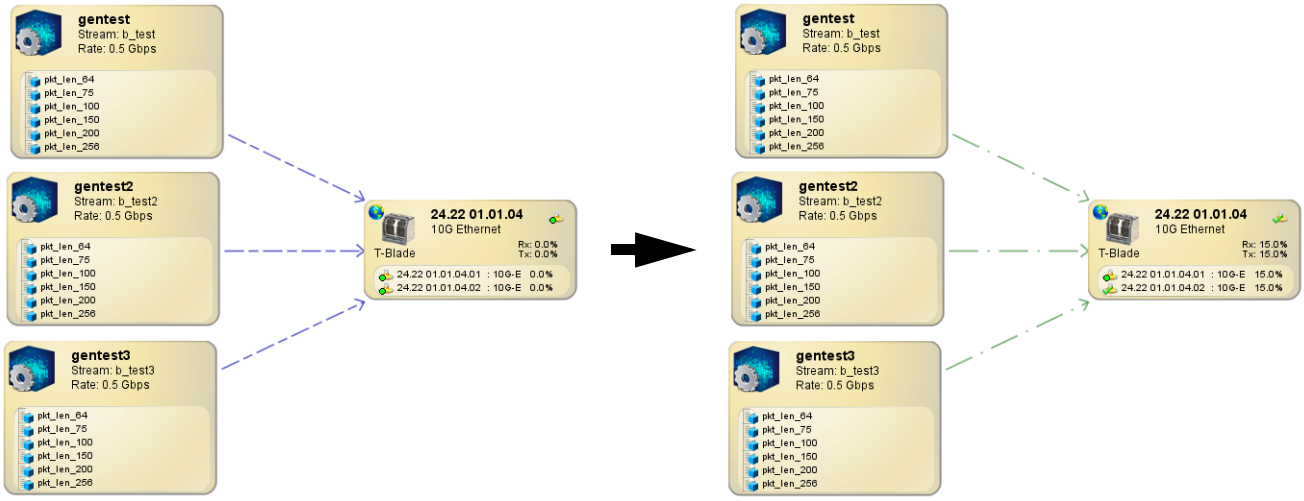
3 Drag required ports/groups into the topology manager then connect the stream generator(s) to the ports/groups as required.

Note: A stream generator can only be connected as a Source on a topology.



Multiple Stream Generator Usage

When connecting multiple stream generators to a single output port, the output stream may not produce a consistent and even distribution of packets. To minimize this unevenness and to control the distribution of frames, assign the required packet frames to the same stream generator.



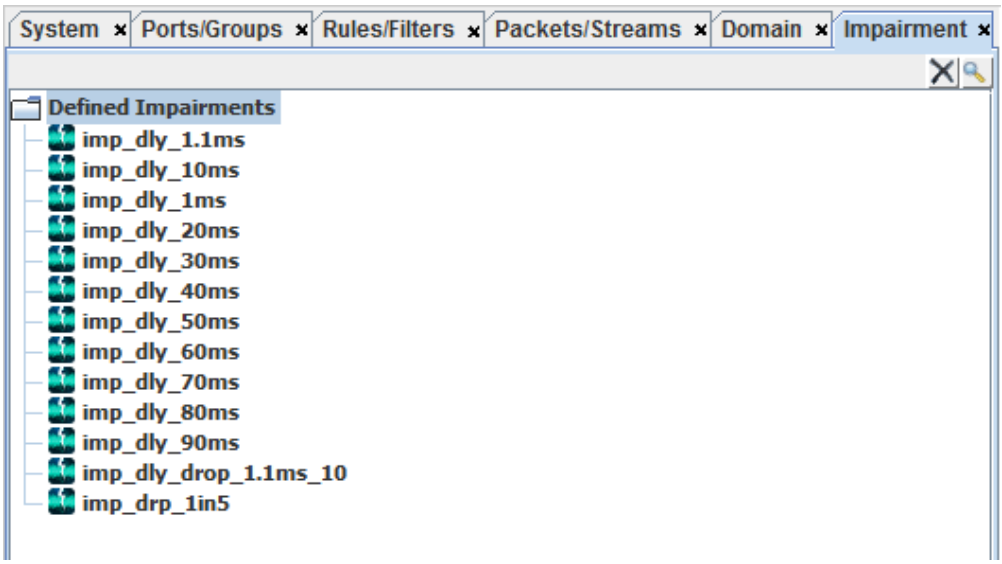
Note: Pre-defined packet streams for use with 100Gb load generation applications are available and recommended. Please contact your NETSCOUT systems engineer or Customer Support for additional information.

Impairment

Selecting the Impairment tab allows defining individual simplex impairments used to create disruptive packet-based test streams for testing purposes. Impairments can be applied to S-Blade Pro standard L1 ports and Smart L1 ports. The maximum capacity for impairment is 8x10G links, 2x40G links, or a combination of 4x10G and 1x40G links.

The following types of supported impairments include:

- Fixed Delay - Delays all packets by a fixed amount of time in order to simulate long transmission links (e.g., replacing the use of fiber spools in test labs). Delays can be applied in the range of 0.0001 ms up to 1600 ms on a 10Gbps connection.
- Deterministic Loss - Drop '1 out of every n' packets. Range is 2 - 4,294,967,296.
- Fixed Random Loss - Drop n% of all packets. Packet drops are random, but will approach the specified percentage as the sample size increases. Percentage is between 0.0001 - 99.9999%.

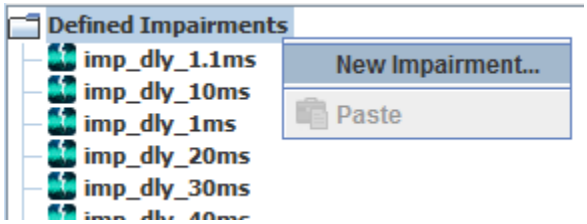


Creating Impairments

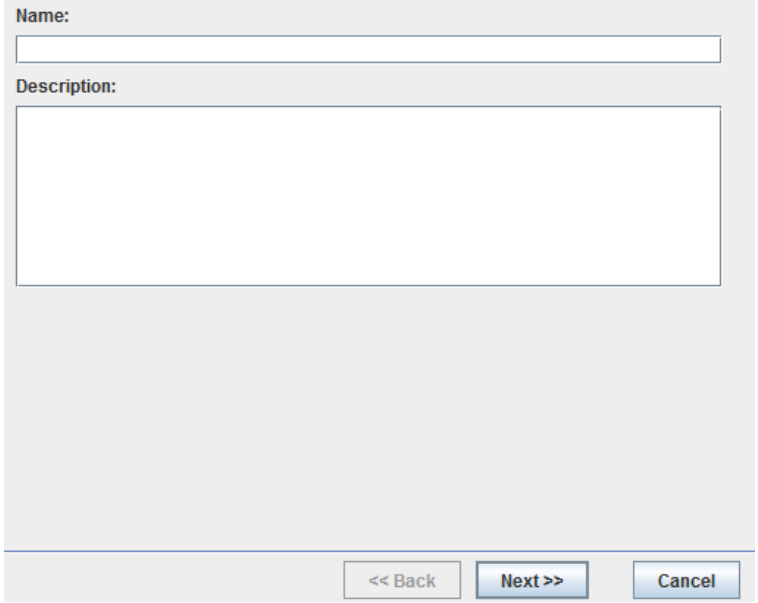
Impairments can be created either from Defined Impairments or the topology Manager.

Define from Impairments Tab

1 Select the Impairment tab, then right-click on **Defined Impairments**. Select **New Impairment** from the drop down menu. The Impairment Configuration wizard window displays.



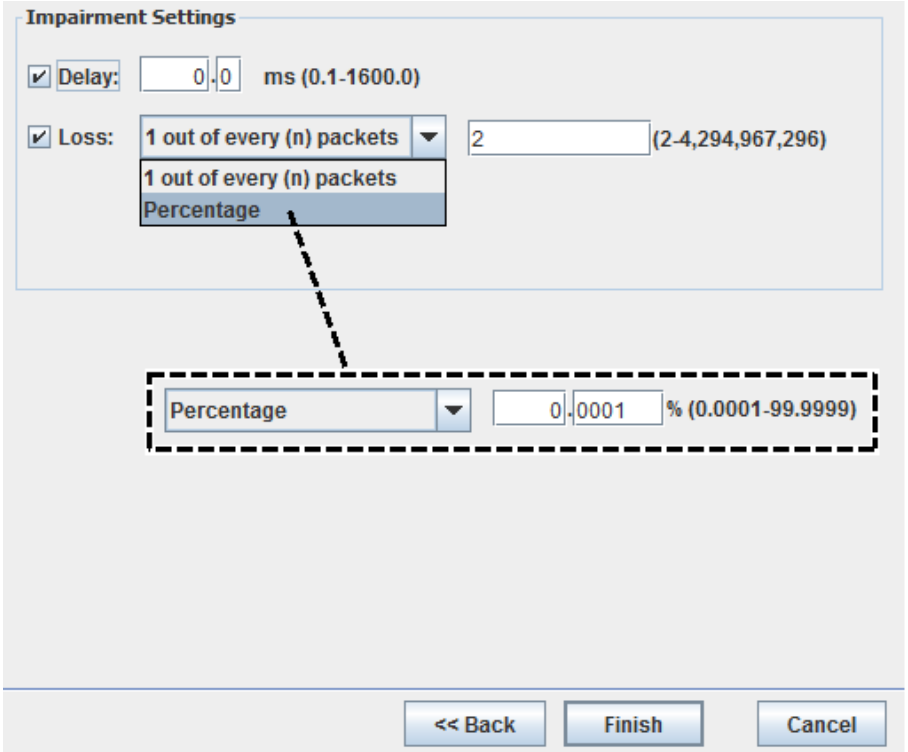
2 Enter a name for the impairment file in the Name field. Optionally, you can enter additional information in the Description field.



3 Click **Next**.

4 On the Impairment Settings window, define (either one or both) the Delay and Loss settings:

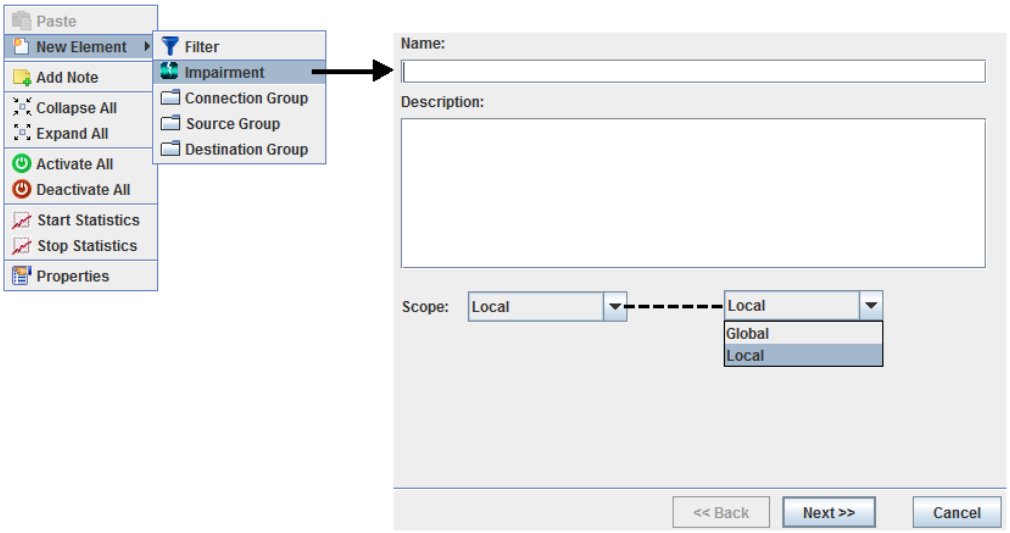
- **Delay** - Enter a value from 0.1 to 1600.0 ms (0.0001 to 1.6 seconds)
- **Loss** - Select either:
  1 out of every (n) packets - Enter a value between 2 to 4,294,967,296
  - or -
  Percentage - Enter a value between 0.0001 to 99.9999



5 Click **Finish**. The new impairment file is created and added to the impairment tree.

Define from Topology Manager

1 From the topology manager screen, right-click and select **New Element > Impairment** from the drop down menu. The Impairment Configuration wizard window displays.



2 Enter a name for the impairment file in the Name field. Optionally, you can enter additional information in the Description field.

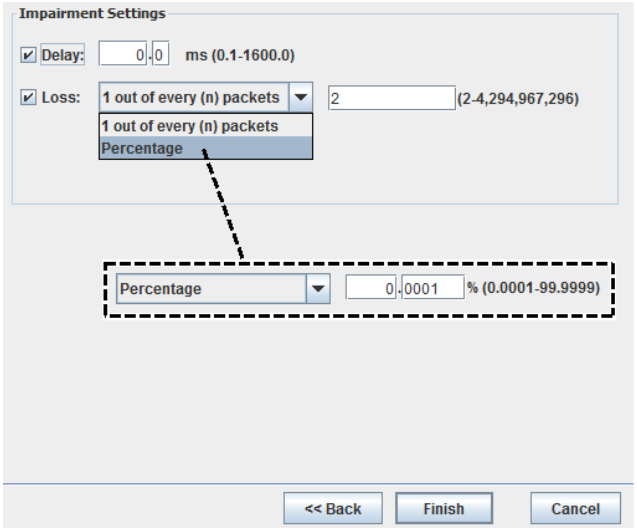
3 Select the Scope designation of the impairment:

- **Local (default) -** The new impairment is only available on the current topology.
- **Global -** The new impairment is available for use on multiple topologies / added to the list of Defined Impairments. Making a change to a global impairment's properties changes the properties of the impairment on all topologies the impairment is used.

4 Click **Next**.

5 On the Impairment Settings window, define (either one or both) the Delay and Loss settings:

- **Delay** - Enter a value from 0.1 to 1600.0 ms (0.0001 to 1.6 seconds)
- **Loss** - Select either:
  1 out of every (n) packets - Enter a value between 2 to 4,294,967,296
  - or -
  Percentage - Enter a value between 0.0001 to 99.9999

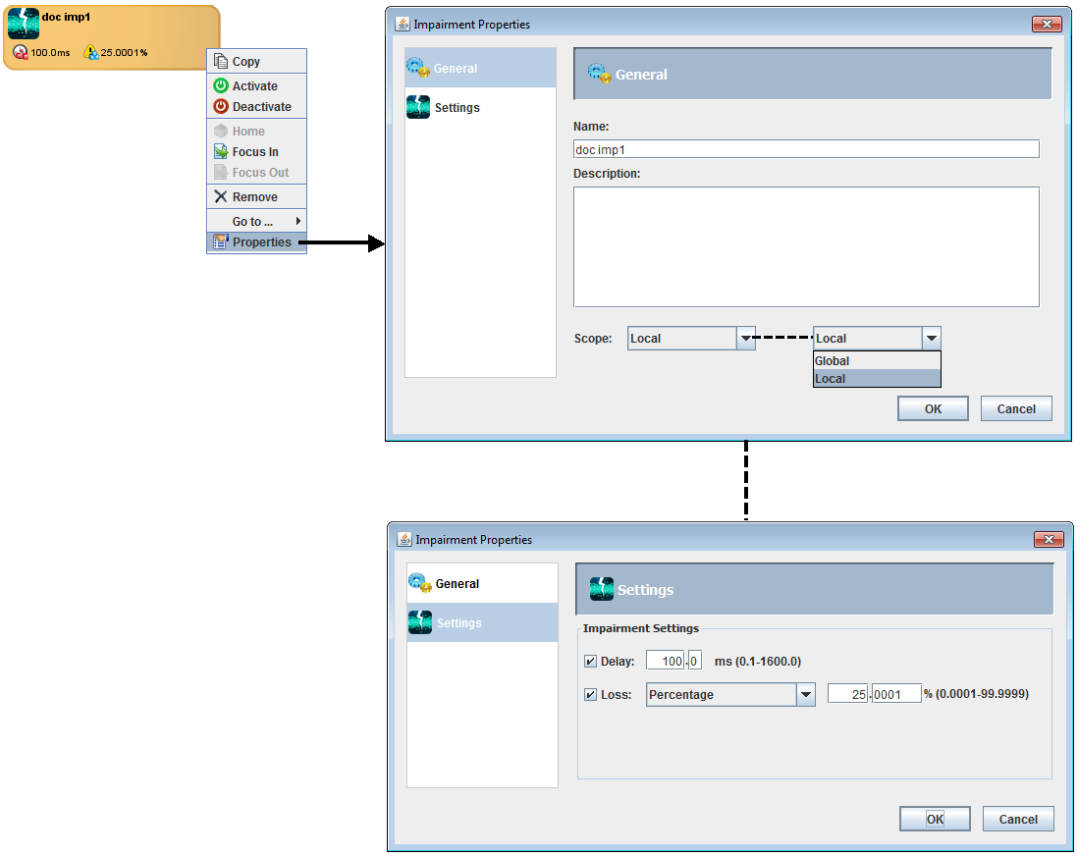


6 Click **Finish**. The new impairment file is created and displayed on the current topology manager screen. If the scope was set to Global, the new impairment also is added to the impairment tree.

Editing Impairment Properties

Local Impairments

1 Select the impairment on the topology manager screen, right-click and select **Properties**. The Impairment Properties window displays.



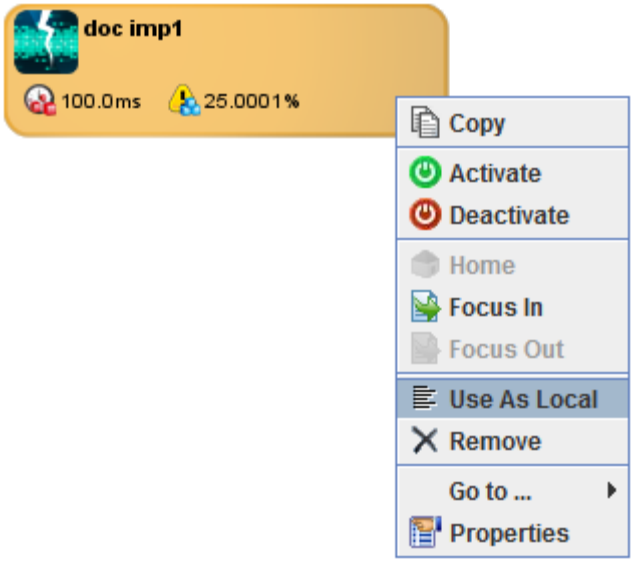
2 Update the impairment as required:

- **General**
  - Make any changes to either the Name or Description text fields.
  - Scope:
    - Local (default) - The new impairment is only available on the current topology.
    - Global - The new impairment is available for use on multiple topologies / added to the list of Defined Impairments. Making a change to a global impairment's properties changes the properties of the impairment on all topologies the impairment is used.
- **Settings** - Make any changes to either the Delay or Loss values.

3 Click **OK** to save the changes.

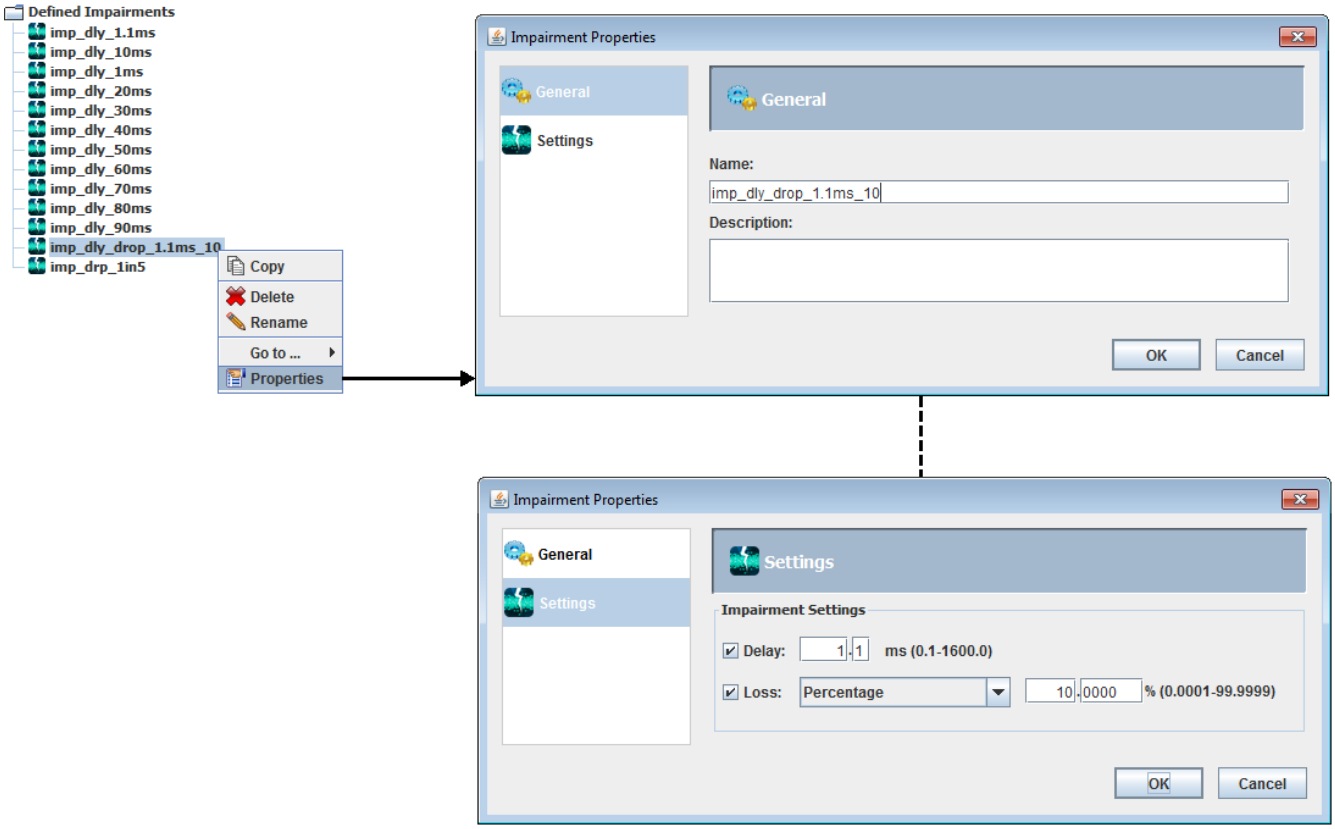
Use As Local

An impairment designated as Scope = Global can be converted to Scope = Local from the topology manager by right clicking and selecting **Use As Local** from the drop down menu. The impairment is removed from the list of Defined Impairments and only used in the current topology.



Global Impairments

1 Select and right-click on a defined impairment, then select **Properties**. The Impairment Properties window displays.



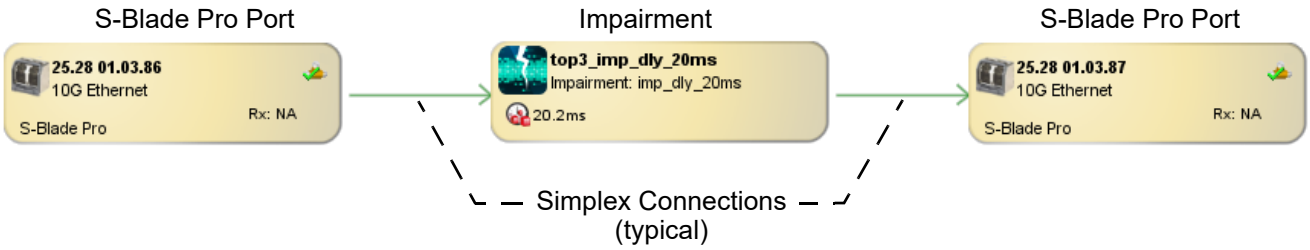
2 Update the impairment as required:

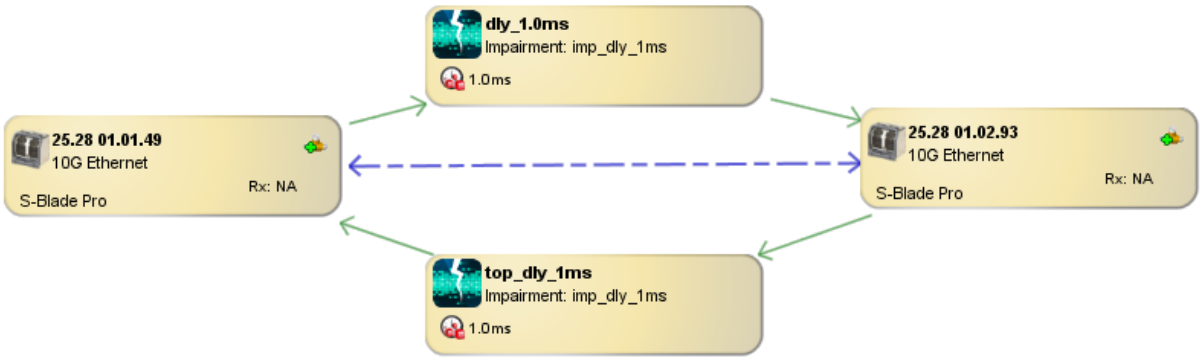
- **General** - Make any changes to either the Name or Description text fields.
- **Settings** - Make any changes to either the Delay or Loss values.

3 Click **OK** to save the changes.

Utilizing Impairments

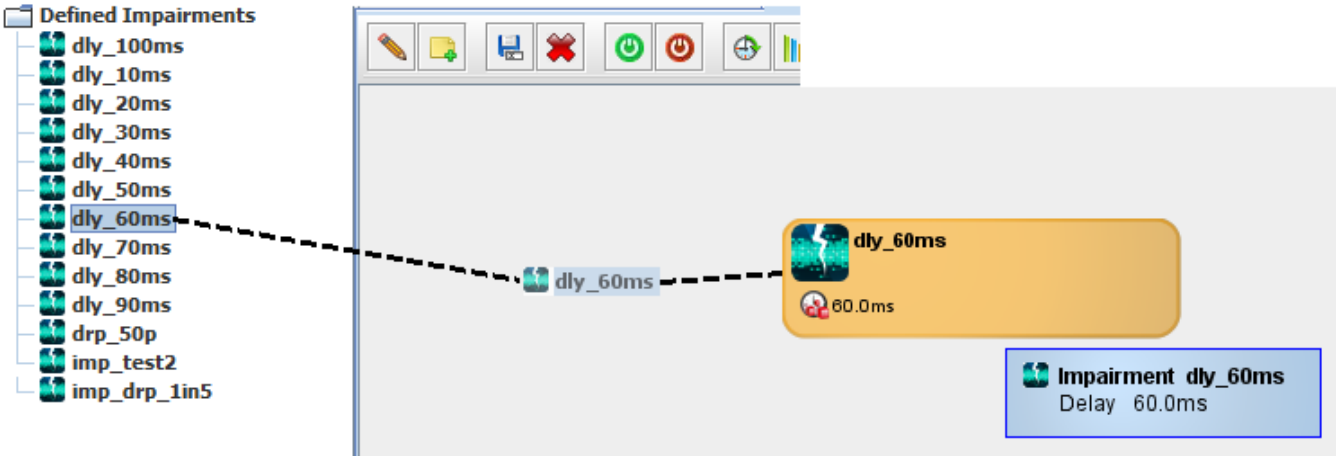
Impairments can be incorporated between any simplex connection using S-Blade Pro to S-Blade Pro SMART ports on the topology manager.





Adding Impairments to a Topology

1 Select the required defined impairment and drag (or copy/paste) to the topology manager. The impairment is now available on the topology manager.



Domain

Note: Usability of the Domain tab is determined by the TestStream Management server license key agreement settings. Unless Domain functionally is part of the purchased license key agreement, this tab is not accessible by the user.

Selecting the Domain tab allows defining a set of accessible ports, rules, and trunks under a unique user-defined name. This enables a user with Administrator privileges to assign a domain to a non-Administrator user limiting their access to ports that are in the assigned domain.

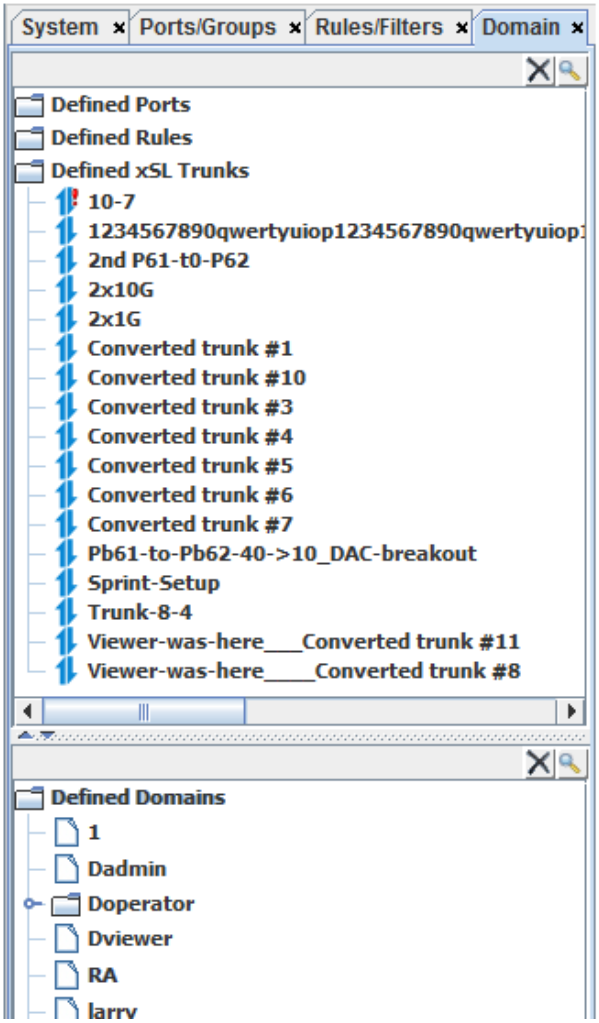
Note:
Defined Domain users cannot delete Topology and Groups containing ports that are not part of their domain.

Non-domain restricted users have access to all ports and trunks (assigned or not assigned to a domain).

Defined rules can be added (copy/paste) into a defined domain.

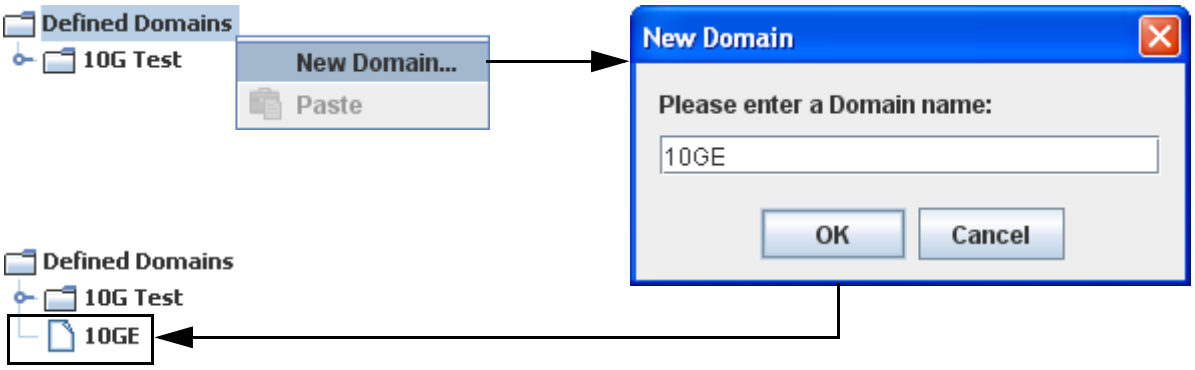
Defined filter rules that are not part of a user's domain cannot be activated, de-activated, or modified within a topology.

Refer to Associating Domains with xSL Trunks on page 3-112 on assigning trunks to defined domains.



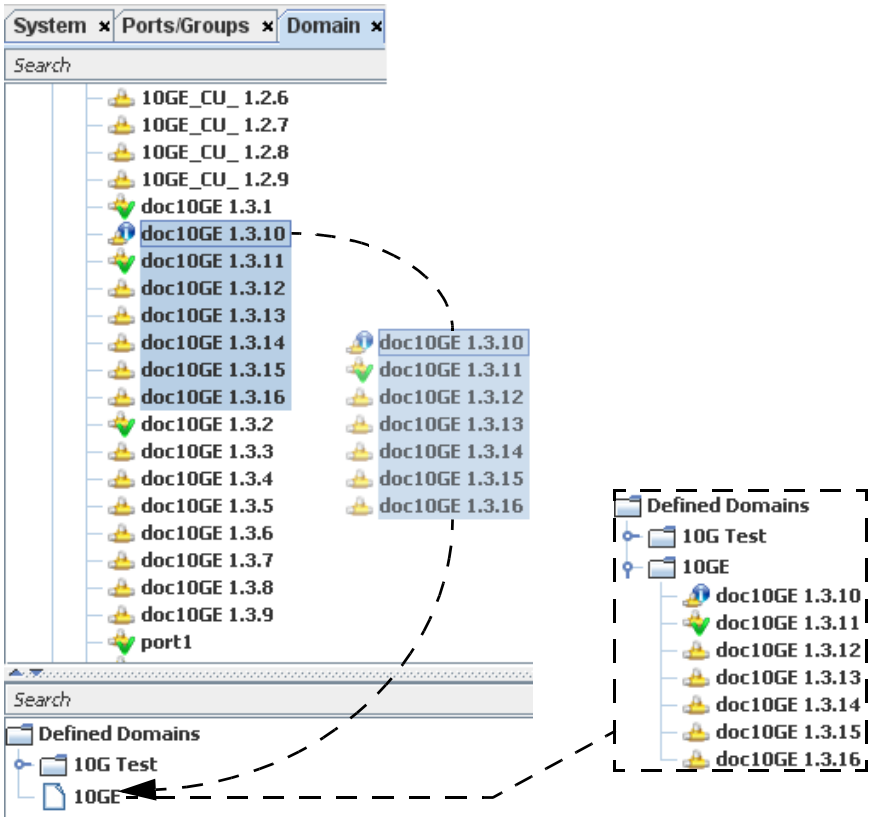
Create a Domain

1. Select the Domain tab.
2. Right click on the Defined Domains icon and select **New Domain**.
3. Enter a name for the domain and click **OK**. The new domain is listed under the Defined Domains icon



Assign Ports to the Domain

Select the required ports from the Defined Ports window listing all of the defined blade ports, and drag the selected ports to the new domain. The selected ports are now assigned to the domain.



Ports/Devices (TestStream Lab Manager Only)

The Ports/Devices tab, part of the TestStream Reservation feature, allows creating devices and then adding ports to the created devices. These devices and ports have attributes defined in name/value pairs.

Note:
Currently, the supported attributes are
Devices:
name
Ports:
name, protocol (ETH, FC, OC), speed (ETH: 1G,10G,25G,40G,50G,100G; FC: 1G,2G,4G,8G; OC: OC48,OC192)

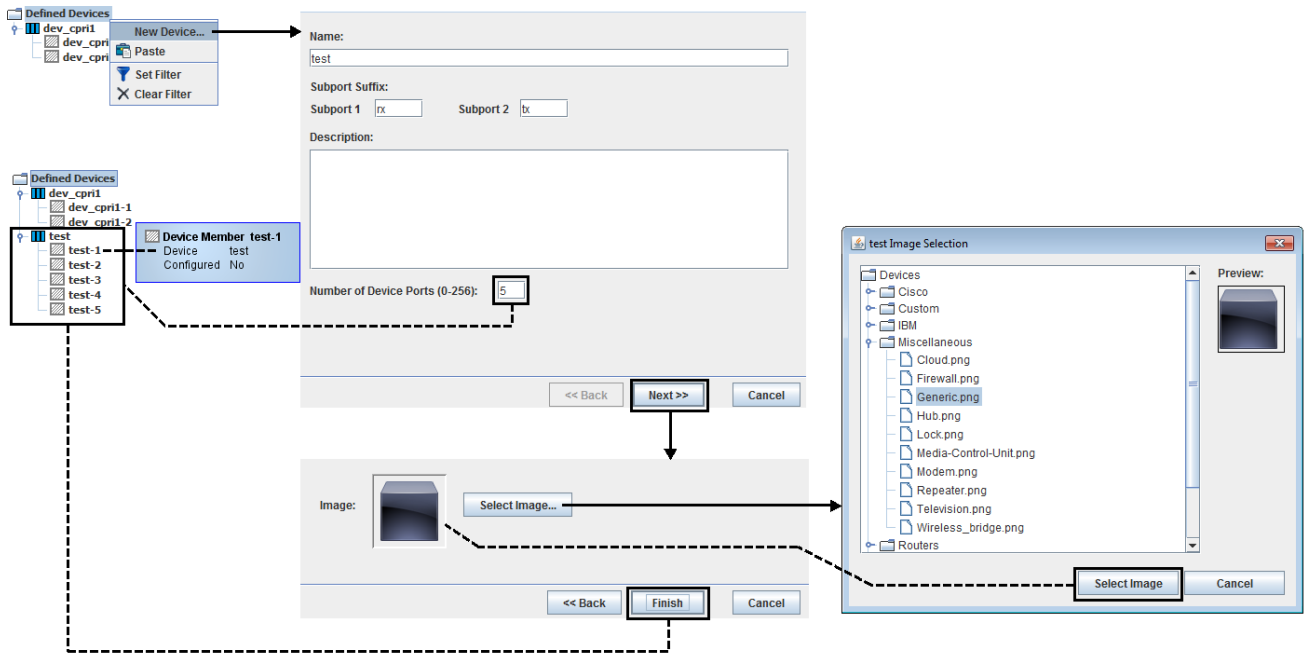
Reservation

The Reservation feature provides the following:

- Defines devices and their added ports.
- Maps port devices to OS-xx, 39xx and HS-3200 ports. Not all the port devices must be mapped to 39xx/HS-3200 ports. Unmapped ports can be reserved.
- Filters port devices per device name, port name, port speed, time availability using scheduler calendar.
- Uses a device topology to create connections between devices and to reserve port devices.
- Schedules the device topology. When the device topology is activated, connections are made. When the device topology is deactivated, connections are disconnected.
- Provides support for xSLs in reservations and any connections in a reservation needing an xSL will have one reserved.

Adding a New Device

To add a new device, right-click on **Defined Devices** and select **New Device**. The Device Configuration Wizard screen displays.



1 Enter a name for the device.

2 Under Subport Suffix, you can either use the default Subport 1/2 designations or enter your own designations.

3 Optionally, enter any description for the device.

4 Assign the number of Device Ports (range is 0 - 256 ports) required.

5 Click **Next**.

6 Finally, click **Select Image** to choose a graphic representing the device from the image library.

Note: You can add custom images to the image library (refer to Importing Custom Device Images on page 3-243).

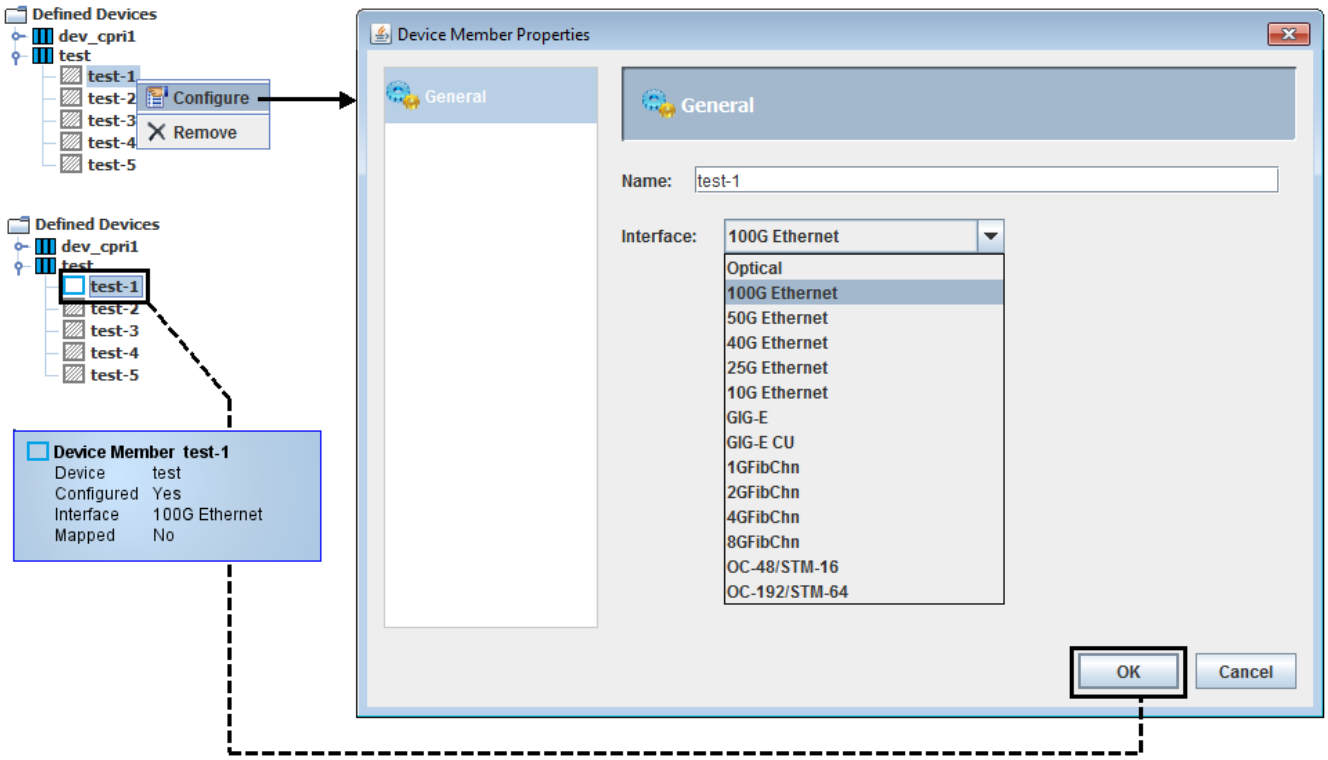
---

7 Click **Finish** to save the device.

Configure Device Ports

To configure properties on one or more device ports on a device:

1 From Defined Devices, select one or more ports on the device, then right-click and select **Configure**. The Device Member Properties screen displays.

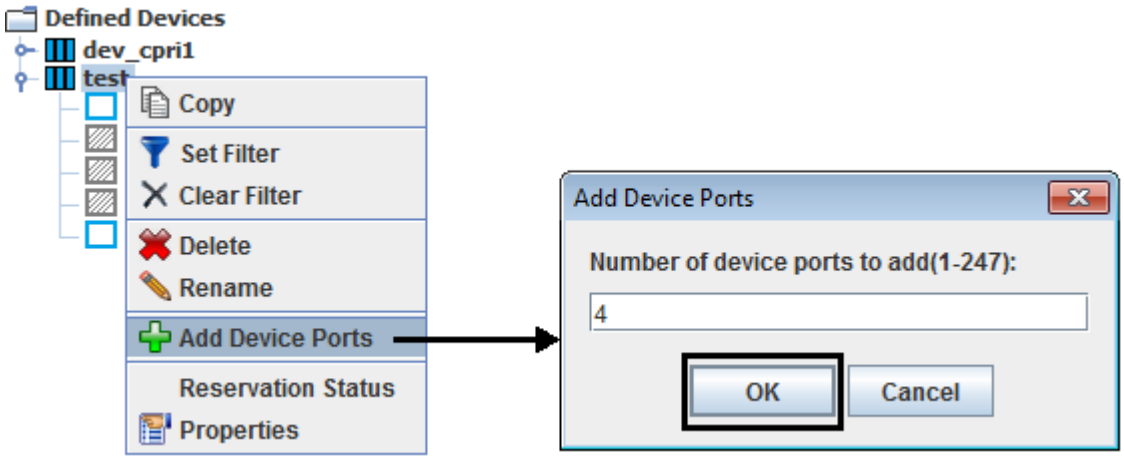


- The Name field allows updating the port name.
- The Interface drop-down menu allows selecting the required port interface.

2 Click **OK** to save the settings. The port icon changes to indicate a configured port. Hovering the cursor over the port displays the current port status.

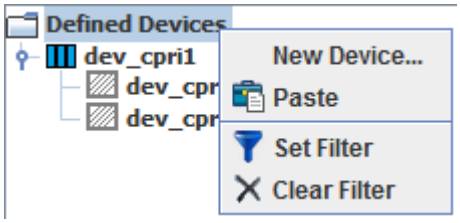
Adding Additional Device Ports

To add ports to a configured device, right-click on the device and select **Add Device Ports**. From the Add Device Ports screen, enter the number of ports to add (from 1 - 247) and click **OK**.



Defined Devices Menus

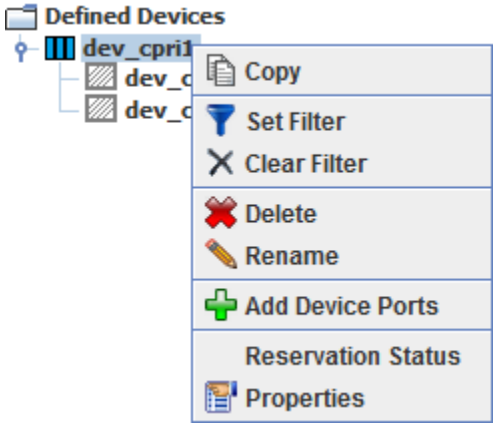
Select the Ports/Devices tab, then right-click on **Defined Devices**. The drop down menu displays the following selections:



- New Device - Create a new device (refer to Adding a New Device on page 3-239).
- Copy / Paste - Duplicate an already created device with its attributes.
- Set / Clear Filter - Define device filter settings (i.e., name, interface type, available reservation - start / end time and date); refer to Device Filtering on page 3-244).

Devices Sub-Menu

Right-clicking on a device displays the following drop down menu selections:

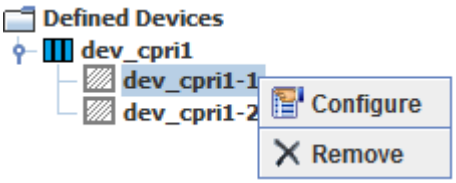


- Copy / Paste - Duplicate an already created device with its attributes.
- Set / Clear Filter - Define device filter settings (i.e., name, interface type, available reservation - start / end time and date); refer to Device Filtering on page 3-244).
- Delete - Remove the entire device.
- Rename - Change the device name.
- Add Device Ports - Add additional ports to device (refer to Adding Additional Device Ports on page 3-241).
- Reservation Status - Accesses the Reservation Status (refer to Reservation Status on page 3-256).
- Properties - View current / modify device property settings (device name, subport suffix, description, and image graphic).

Device Port Sub-Menus

Non-Configured Ports

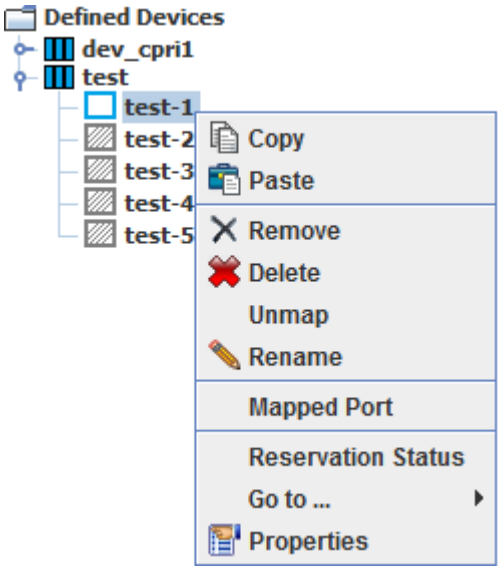
Right-clicking on an non-configured device port displays the following drop down menu selections:



- Configure - Assign port settings (refer to Configure Device Ports on page 3-240).
- Remove - Delete the port from the device.

Configured Ports

Right-clicking on a configured device port displays the following drop down menu selections:



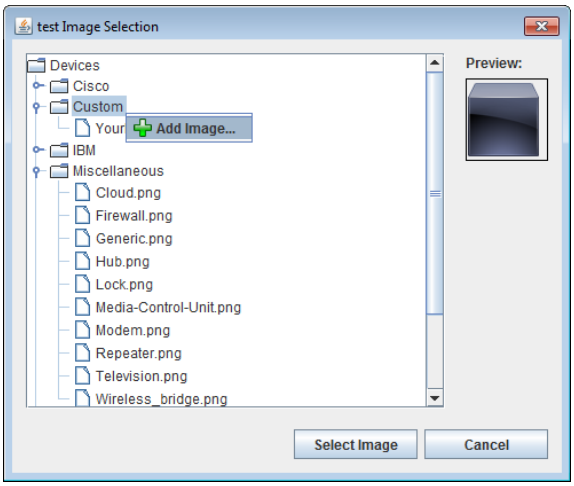
- Copy / Paste - Duplicate an already created port with its attributes.
- Remove - Removes the port from the device.
- Delete - Un-configures the device port.
- Unmap - Un-assign a TestStream port to a device port (refer to Port Mapping on page 3-245).
- Rename - Change the name of the device port.

- Mapped Port - View the properties of the TestStream port assigned to a device port (refer to Port Mapping on page 3-245).
- Reservation Status - Accesses the Reservation Status (refer to Reservation Status on page 3-256).
- Go To - Links to the following:
  - Topologies
- Properties - View current / modify port property settings (port name and interface type).

Importing Custom Device Images

Additional custom defined images can be added to the Image Selection listing. The image graphic must be no larger than 64 x 64 pixels and saved in .png file format. The file name for the new image must not contain spaces.

1 From the Image Selection screen right-click on the **Custom** folder and select **Add Image**.



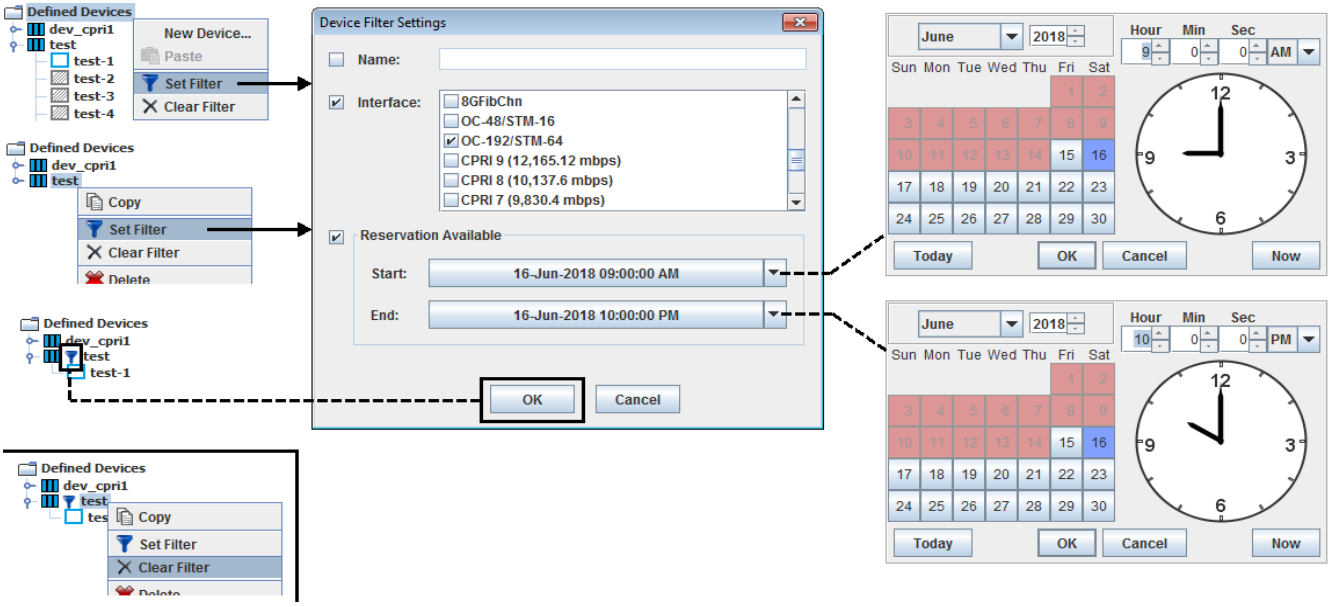
2 Select the .png file of the custom image to import. Once selected, the custom image icon will appear in the Image Selection listing under the Custom folder.

Device Filtering

Defined devices can be filtered based on time availability allowing the user to select a start and stop time with only the ports that are available in that time range being displayed.

Add a Filter

Right-click on either Defined Devices or a configured device and select **Set Filter**. The Device Filter Settings window displays.



1. Click on **Name** and enter the name of the device filter.
2. Click on **Interface** and select one or more interfaces.
3. Click on **Reservation Available** and set the Start and End times for the device.
4. Click **OK** to save the filter settings. A defined filter icon displays next to the defined device.

Remove a Filter

To remove a filter from a device (prior to the time the filter is active), right-click on the device and select **Clear Filter**.

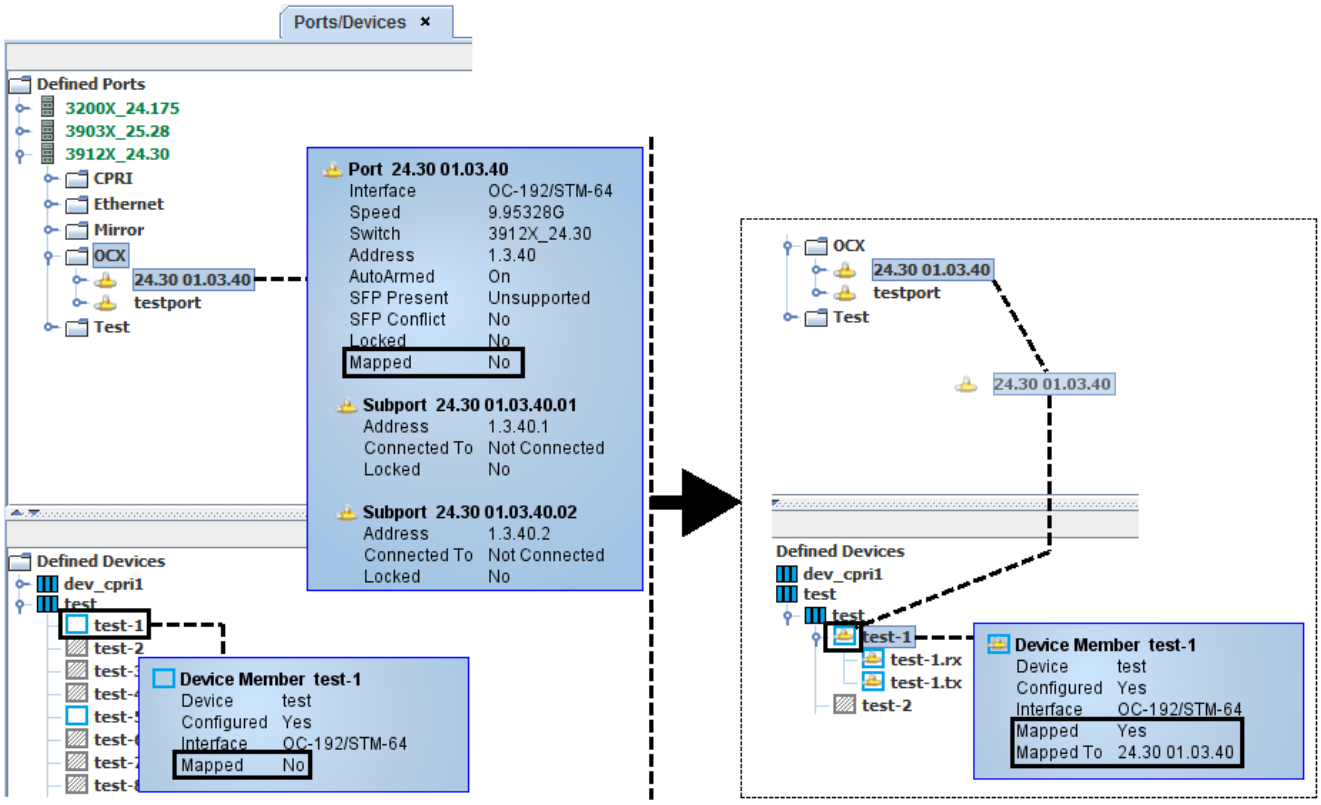
Port Mapping

Defined ports can be assigned (mapped) to configured device ports. The defined ports can be full duplex (i.e., 39xx and HS-3200) or full duplex / subport (i.e., OS-96 / OS-192); xSL ports can not be used for mapping.

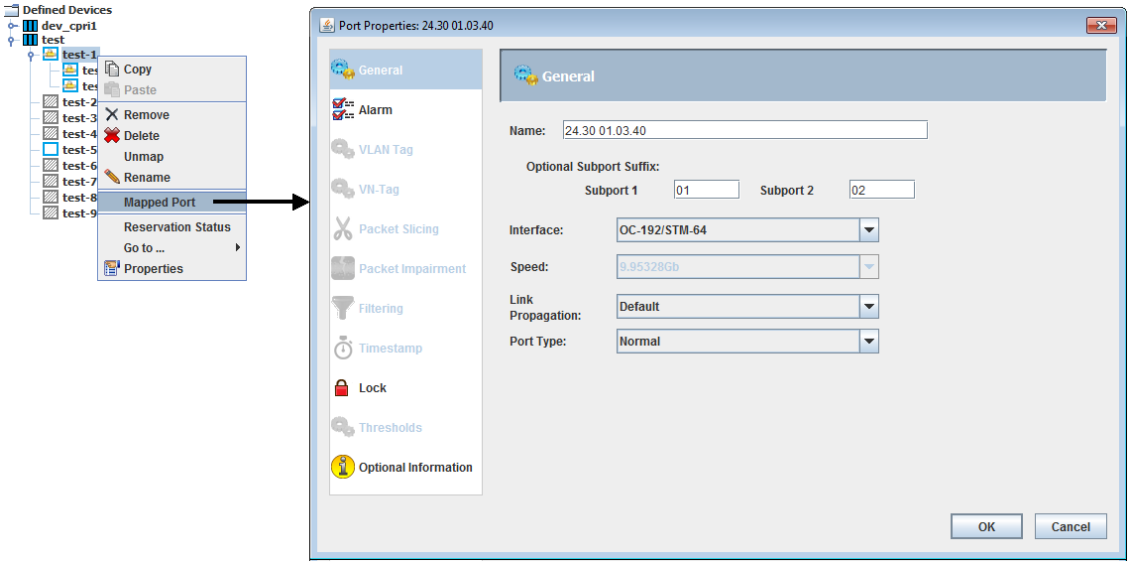
Important: Port and device port must have matching interfaces.

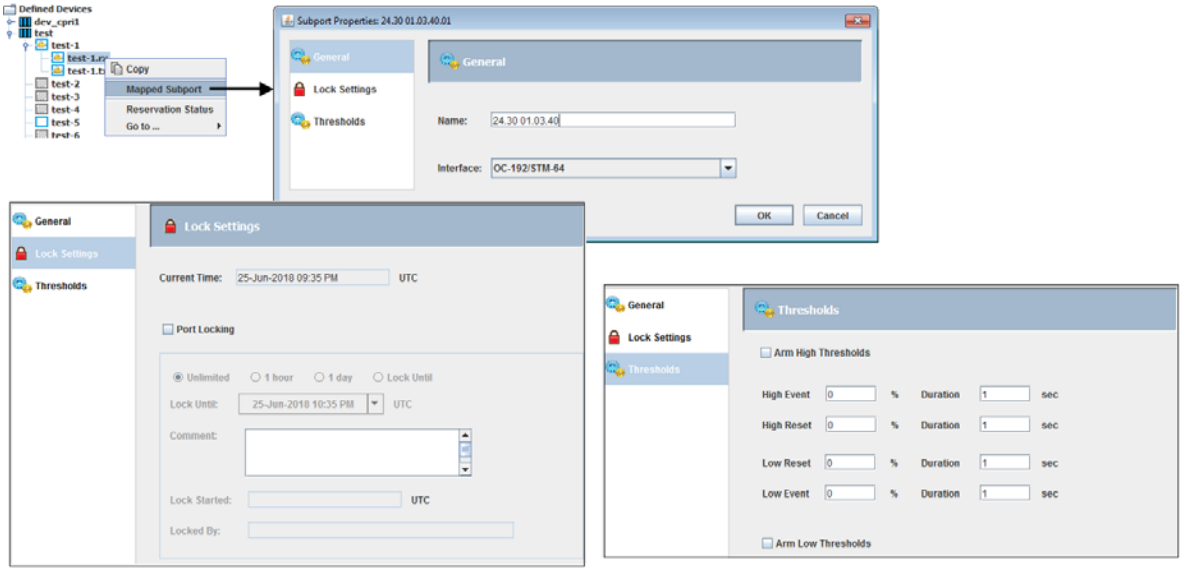
Mapping a Device

From Ports/Devices > Defined Ports, locate and click on the port to be assigned to the required device port. Drag the port to the defined device member under Defined Devices and release. A mapped port is identified by the Mapped Device Port icon (refer to Icon Legend Chart on page 2-45). The assigned port is removed from the list of available defined ports while mapped to the device port.



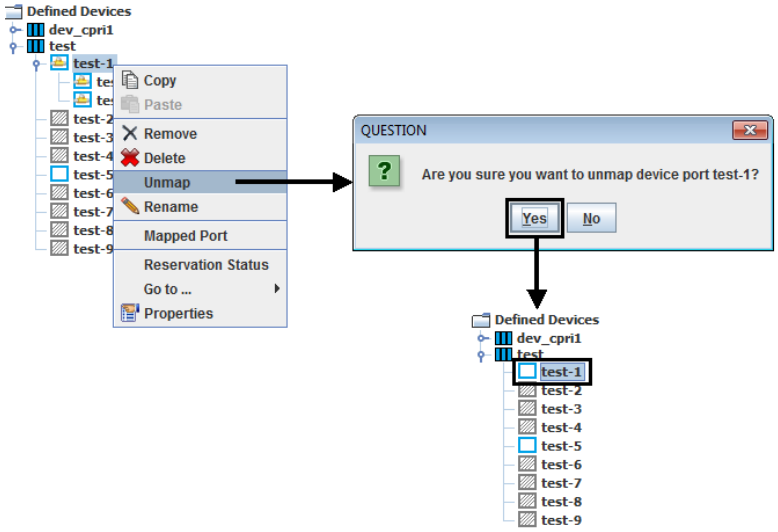
Right-clicking on either the mapped port (**Mapped Port**) or sub-ports (**Mapped Subport**) allows viewing it's port properties.





Unmaping a Device

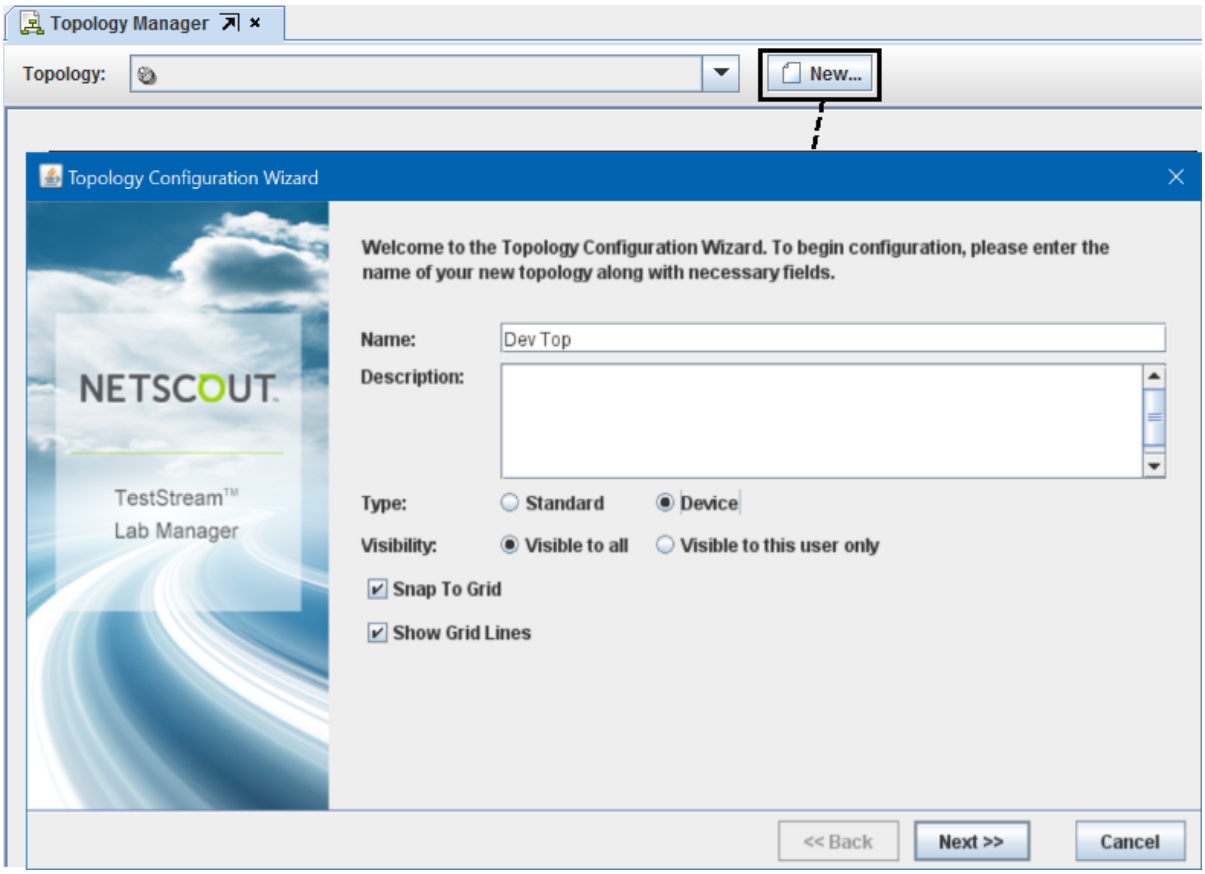
To un-assign (unmap) a defined port from a defined device port, right-click on the device port and select **Unmap**. Click **OK** to the confirmation question. The device port reverts to a defined device port (refer to Icon Legend Chart on page 2-45) with the removed defined port returned to the list of defined ports, available for later usage.



Creating Device Topologies

To create a Device Topology, from Topology Manager, click on **New**. From the Topology Configuration Wizard, enter a Name, optional Description, **Type: Device**, and select your visibility option. Click **Finish** to save your new device topology.

Device topologies are designated by a **(D)** next to the topology name.



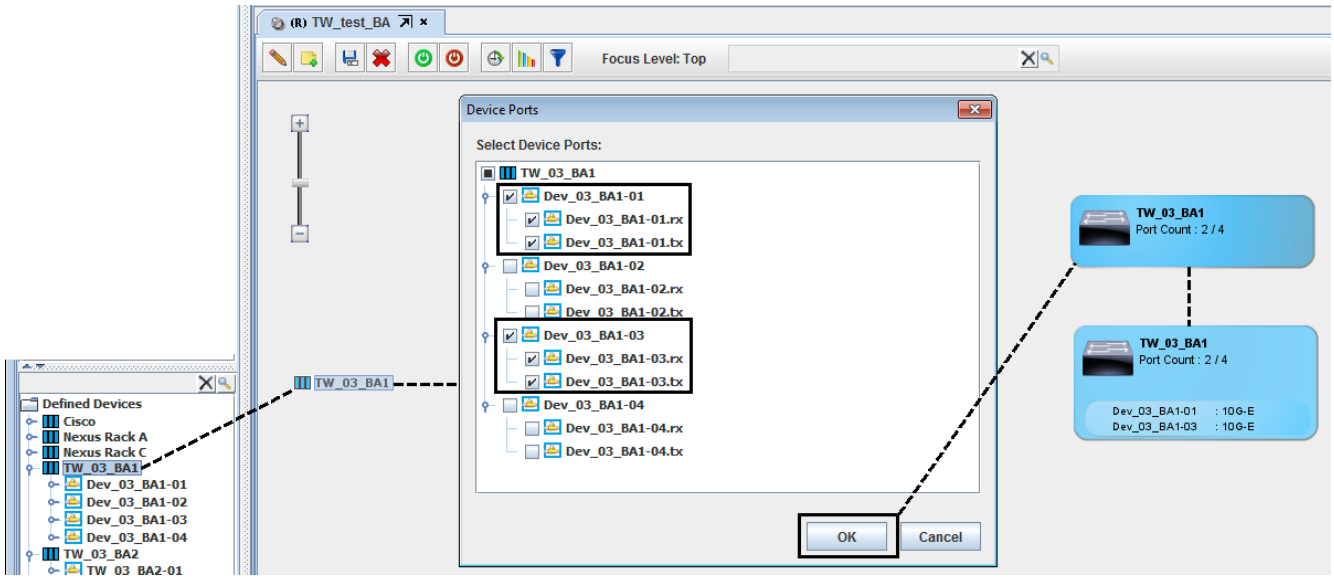
You can now drag and drop device ports into the device topology, then connect / activate / deactivate the ports as required (refer to Using Device Topologies on page 3-249).

Using Device Topologies

After creating a new device topology work screen (refer to Creating Device Topologies on page 3-248), you can now drag and drop defined devices / ports into the device topology.

Adding Devices / Ports

From Defined Devices, select a device and drag it into the topology - a Device Ports window displays listing the available ports in the device. Select the required ports in the device and click **OK**. The new device element is displayed in the topology screen. Double clicking on the element expands the view showing the selected ports.

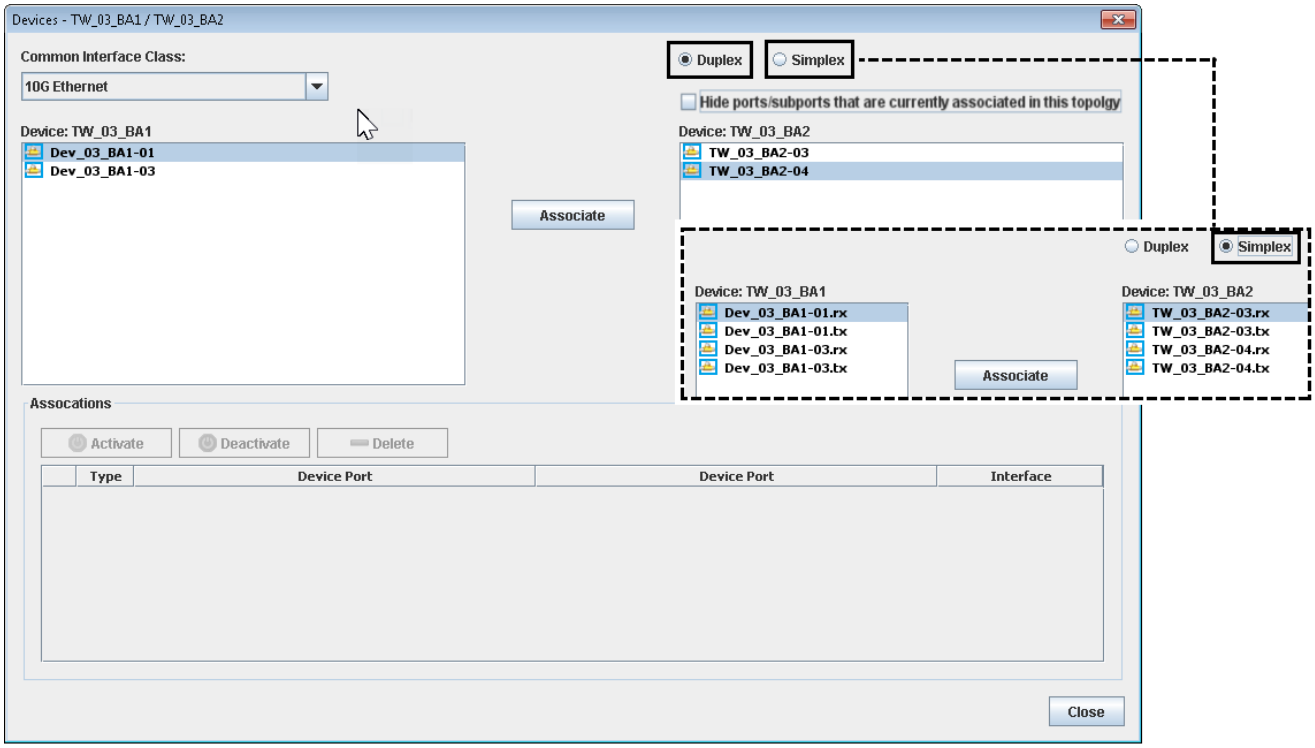


Associate Devices

To associate two devices, select the device elements and using the right mouse button drag a line between the two elements then release the button; an Association screen displays (refer to Association Screen on page 3-250).

Association Screen

The Association screen allows you to finalize the connections.

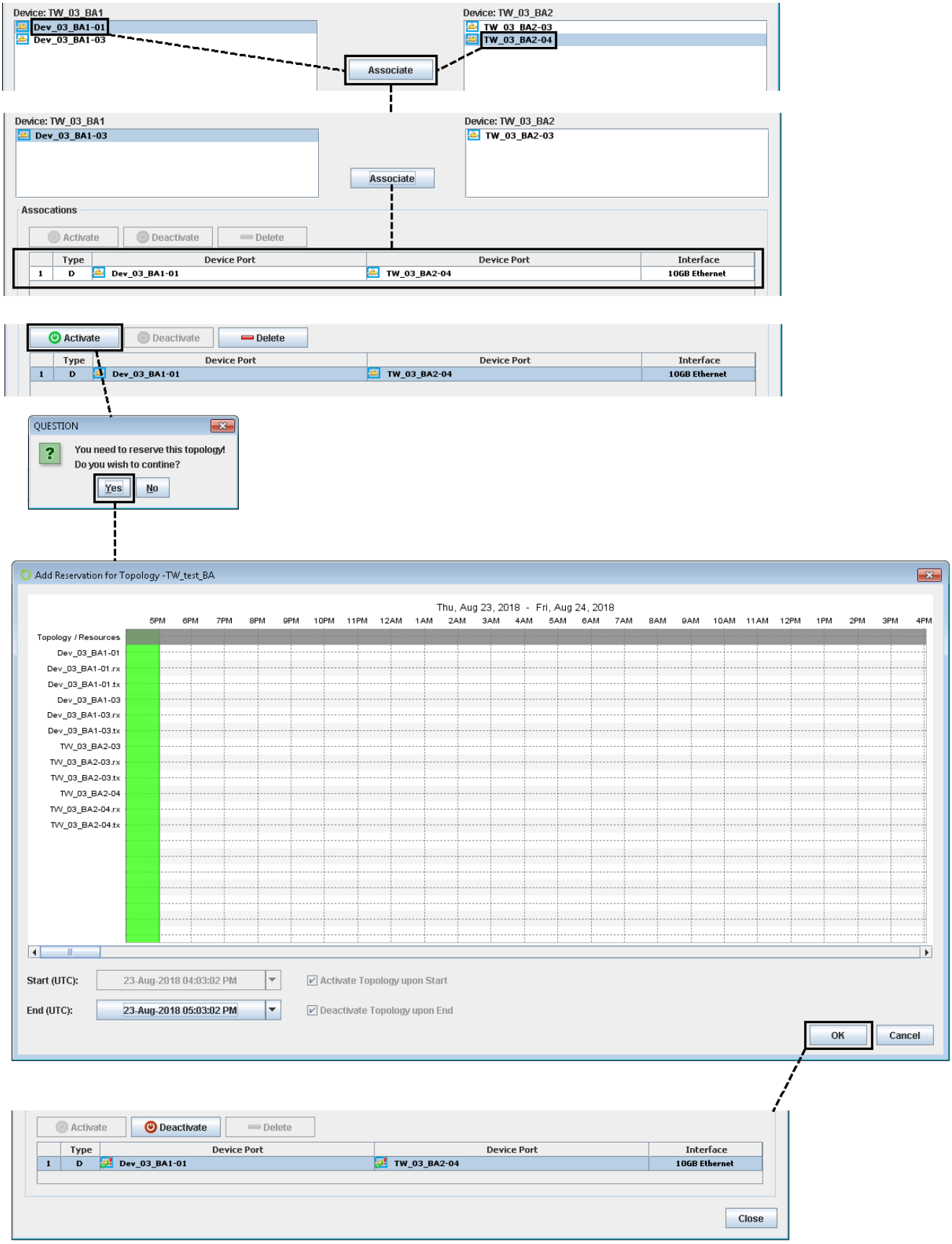


- Common Interface Class - Select the interface type between device ports.
- Device lists - select a port from both devices; if port type Duplex is selected, both Tx / Rx sub-ports are chosen; if Simplex is selected, you can select individual Tx or Rx sub-ports.
- Hide ports/subports that are currently associated in this topology - select to hide ports/subports that are already associated to another device in the topology.
- Associate button - Click Associate after selecting the device ports.
- Associations - Lists the associated device ports/sub-ports.
  - Activate - Start the selected association.
  - Deactivate - Shutdown the selected association.
  - Delete - Removes the selected association from the list and returns the devices to the device lists.

Select the device ports from the Device lists and click **Associate**. The selected device ports are moved to the Associations list. Click on **Activate** to complete the device connection.

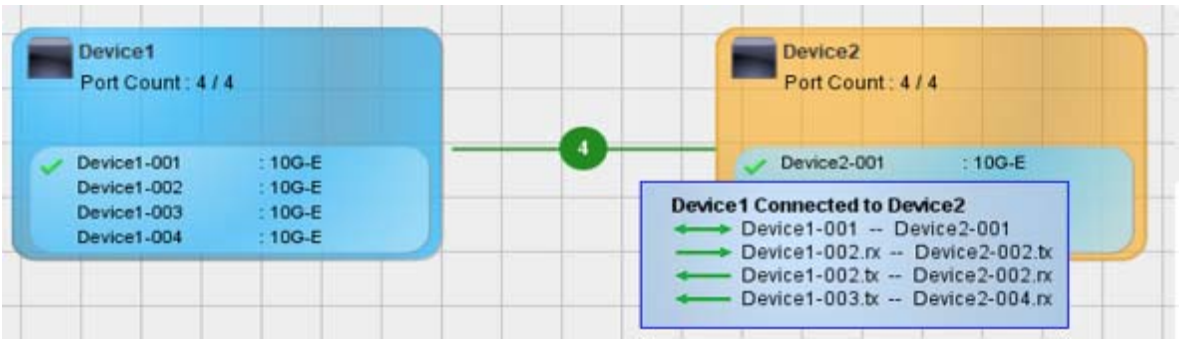
If there is no active reservation in the device topology (refer to Scheduling Device Topologies on page 3-254) and the Tools setting of Device Topologies is set to require a reservation, a prompt displays asking you to reserve this topology. Click **Yes** to continue. A reservation status displays showing the default (1 hr) reservation start and end time for the topology. The end time can be modified as required (refer to Scheduling Device Topologies on page 3-254). Click **OK** to save the reservation.

To end / remove the device connection prior to the reservation end time, click **Deactivate**.


Device: TW_03_BA1
Dev_03_BA1-01
Dev_03_BA1-03
Device: TW_03_BA2
TW_03_BA2-03
TW_03_BA2-04
Associate
Assocations
Activate
Deactivate
Delete
Type
Device Port
Interface
1
D
10GB Ethernet
QUESTION
You need to reserve this topology!
Do you wish to contine?
Yes
No
Add Reservation for Topology -TW_test_BA
Thu, Aug 23, 2018 - Fri, Aug 24, 2018
Topology / Resources
Start (UTC):
23-Aug-2018 04:03:02 PM
Activate Topology upon Start
End (UTC):
23-Aug-2018 05:03:02 PM
Deactivate Topology upon End
OK
Cancel
Close

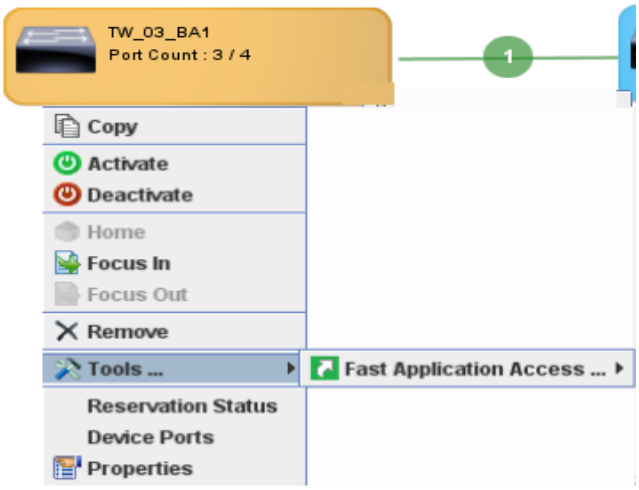
Activated devices are displayed with a solid line containing a numeric indicator of the activated associations.

A tool tip listing all active connections between devices is displayed by hovering over the association line between two devices.



Associated Device Menus

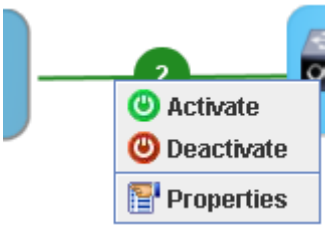
Right-clicking on an associated device displays the following menu selections:



- Copy / Paste - Duplicate an already created device with its attributes.
- Activate - Start the selected association.
- Deactivate - Shutdown the selected association.
- Home / Focus In / Focus Out - Allows removing from view (in a topology) all but a selected object with associated connections.
- Remove - Removes the device from the topology; only available on non-associated devices.
- Tools - Displays submenu with available tools, including Fast Application Access
- Reservation Status - Accesses the Reservation Status (refer to Reservation Status on page 3-256).
- Device Ports - Select available ports in the device.

- Properties - Accesses the device properties

Right clicking on the connection line displays the following menu selections:



- Activate - Start the selected association.
- Deactivate - Shutdown the selected association.
- Properties - Displays the Associations screen with the current device associations.

Scheduling Device Topologies

To schedule a device topology, click the schedule button. A window with the reservations for the device topology is displayed. In that window you can add, edit or delete reservations. Click on the add button to create a new reservation. A calendar displays showing the availability of the resources. Scheduling of a device topology is not allowed if one or more resources are not available for the selected time range. 'Add Reservation for Topology' window provides the following features:

- Selection of the duration of the reservation by dragging the vertical start and stop lines.
- Selection of the duration of the reservation by selecting the start and end times.
- Whether to automatically activate the topology when the reservation becomes active.
- When the reservation ends, the topology will be deactivated.

While a reservation is active the user that created it or an administrator can activate or deactivate the device topology and/or individual associations.

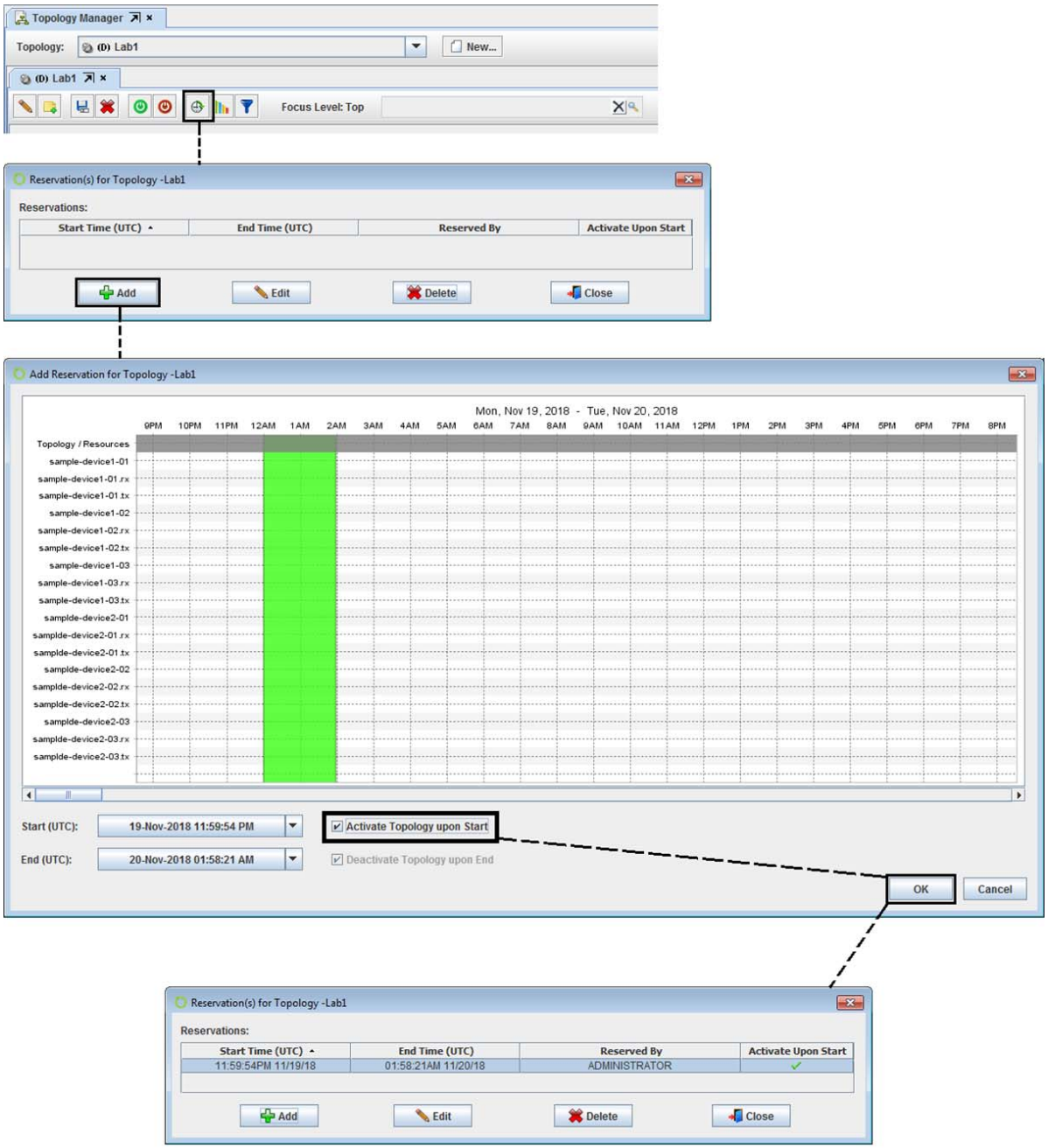
Note: When the reservation license is enabled, the device/device port/device topologies feature and reservations are available. By default, users must create a reservation to active/deactivate a device topology.

Without the reservation license, the device/device port/device topologies feature and reservations will not be available.

The reservation license will be checked at reservation time rather than at device mapping.

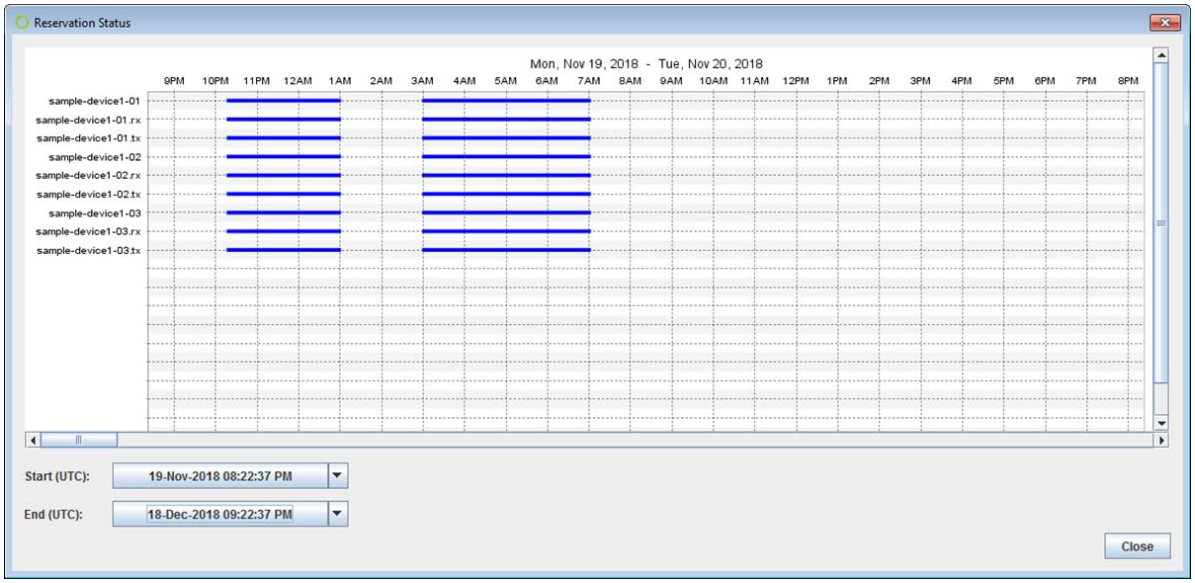
Note: For users that only want to use the device/device port/device topologies feature without reservations, a system setting (Tools => Configure => Device Topologies) will allow the customer to disable reservations. In this case, from an activation/deactivation point of view, the device topologies will behave like standard topologies.

A device topology can be reserved multiple times, using different date / time settings (e.g., Tuesday 1:00AM - 2:00PM, Wednesday 10:00 PM -11:00PM).



Reservation Status

The Reservation Status window displays an hourly calendar showing the time when device ports/sub-ports are reserved.



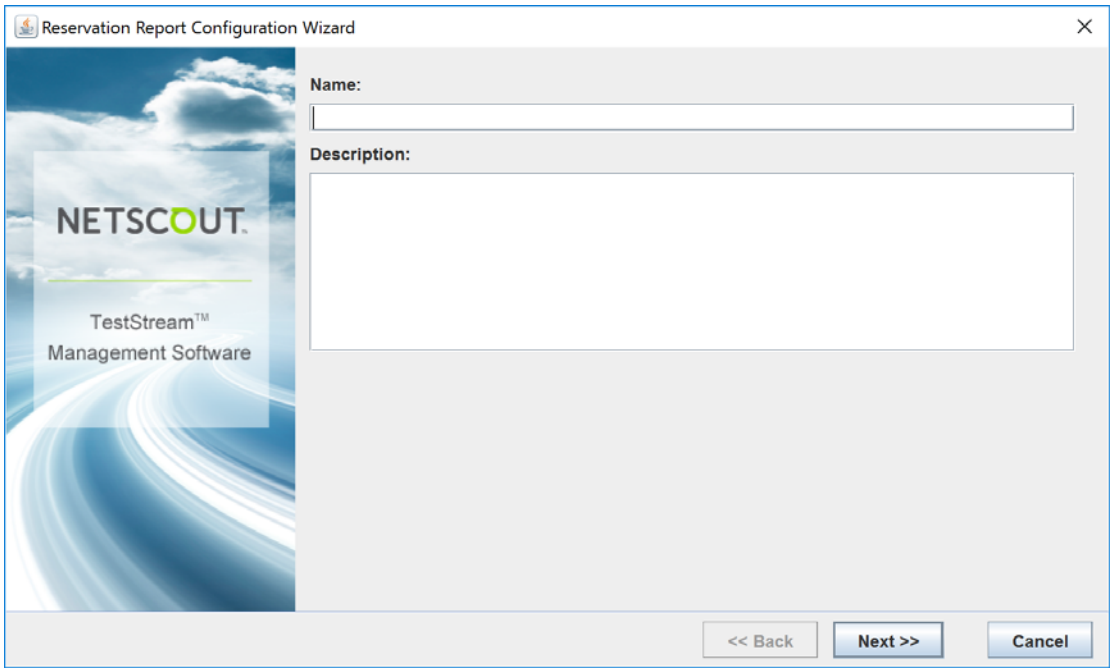
Reservation Reports

Reservation reports allow for a user to obtain reservation history for device ports. The history is displayed as a utilization percentage. A reservation report consists of the following components:

- Name - used to recall the report.
- Time Range - range can be 1 day, 1 month, 1 year or a custom range. The time range can exclude a daily range, as well as weekends.

A Reservation report can be edited, refreshed, copied (Save As), or deleted.

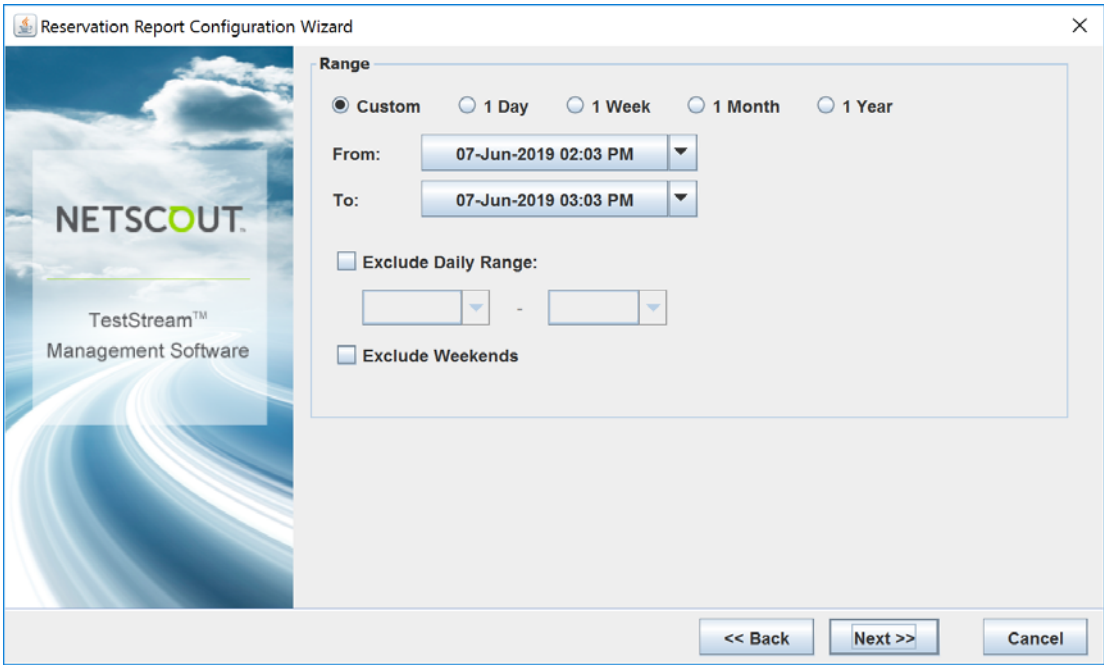
To access the Reservation Reports select **Tools > Statistics > Reservation Statistics** (or click the **Statistics** icon from the toolbar) and then click **New**. The Reservation Report Configuration Wizard is displayed.



Reservation Report Options:

- Enter the reservation report name
- Enter a description of the Reservation Report

Time Range



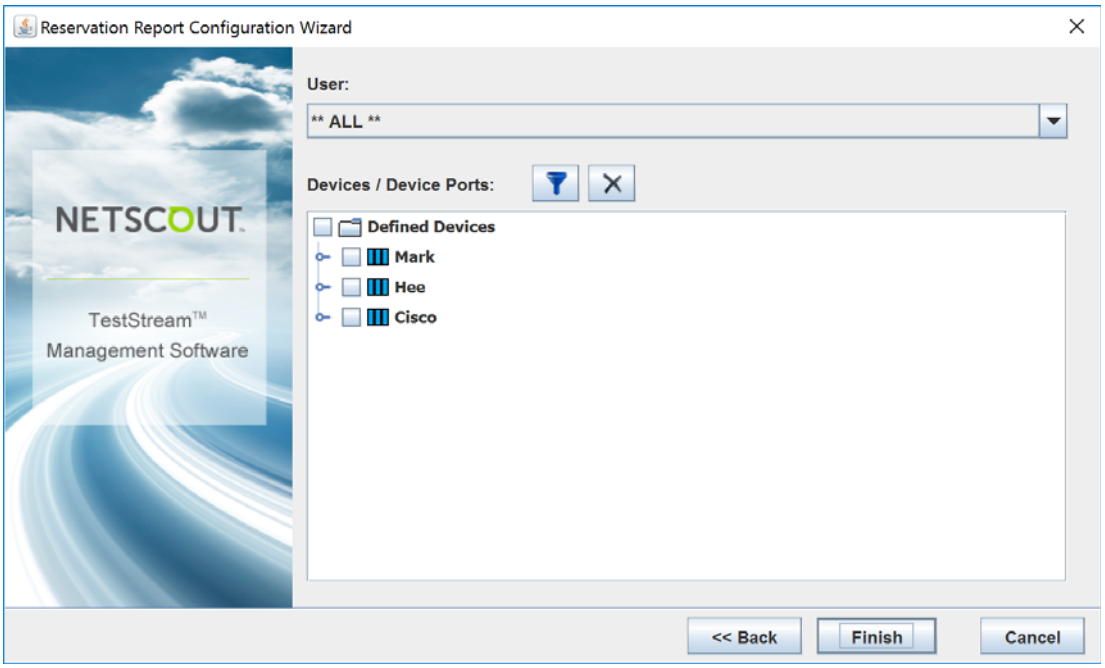
Time Range Options:

- Select the time range (Custom, 1 Day, 1 Week, 1 Month, 1 Year)

Note: If you select the Custom option, then you must enter the **From:** and **To:** ranges from the drop down menus.

- Select/De-select Exclude Daily Range (enter the time range to exclude)
- Select/De-select Exclude Weekends

Reservation Report Filtering



Reservation Report Filtering Options:

- Select a User from the drop down menu
- Select a Device/Device Port from the list of Defined Devices
- Configure the Device Filter Settings (enter a filter name and select the interface)
- Delete the Device Filter Settings

Chapter 4
Tools

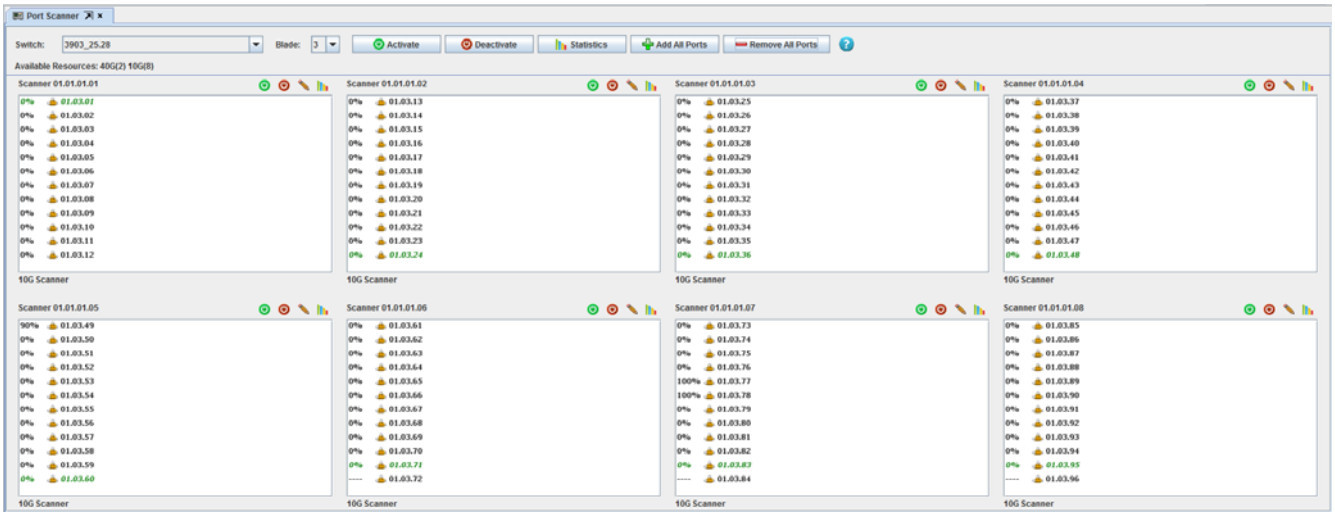
The Tools menu is comprised of the following:

Port Scanner (TestStream Lab Manager Only)

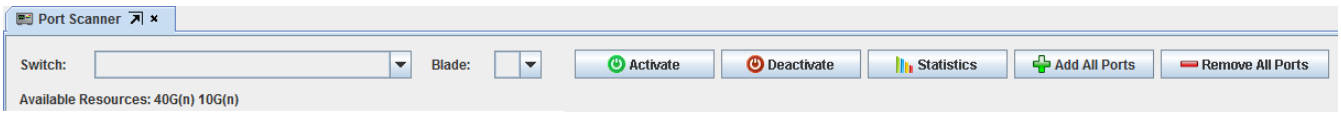
The Port Scanner provides the ability to configure / control a set of S-Blade Pro ports (scanners) to collect utilization statistics.

- Each defined scanner can contain up to 12 defined ports to rove over.
- Up to 8 scanners can be assigned to an S-Blade Pro.
- Port speeds can be intermixed in each scanner.
- Activation of a port scanner may be limited by system resources.
- When a scanner is running, the members display their last utilization collection.
- When a scanner is running, the member with the most recent collection is displayed in green italics.

From the toolbar, click on the Port Scanner icon, the Port Scanner screen displays.



At the top of the screen are the following functions:

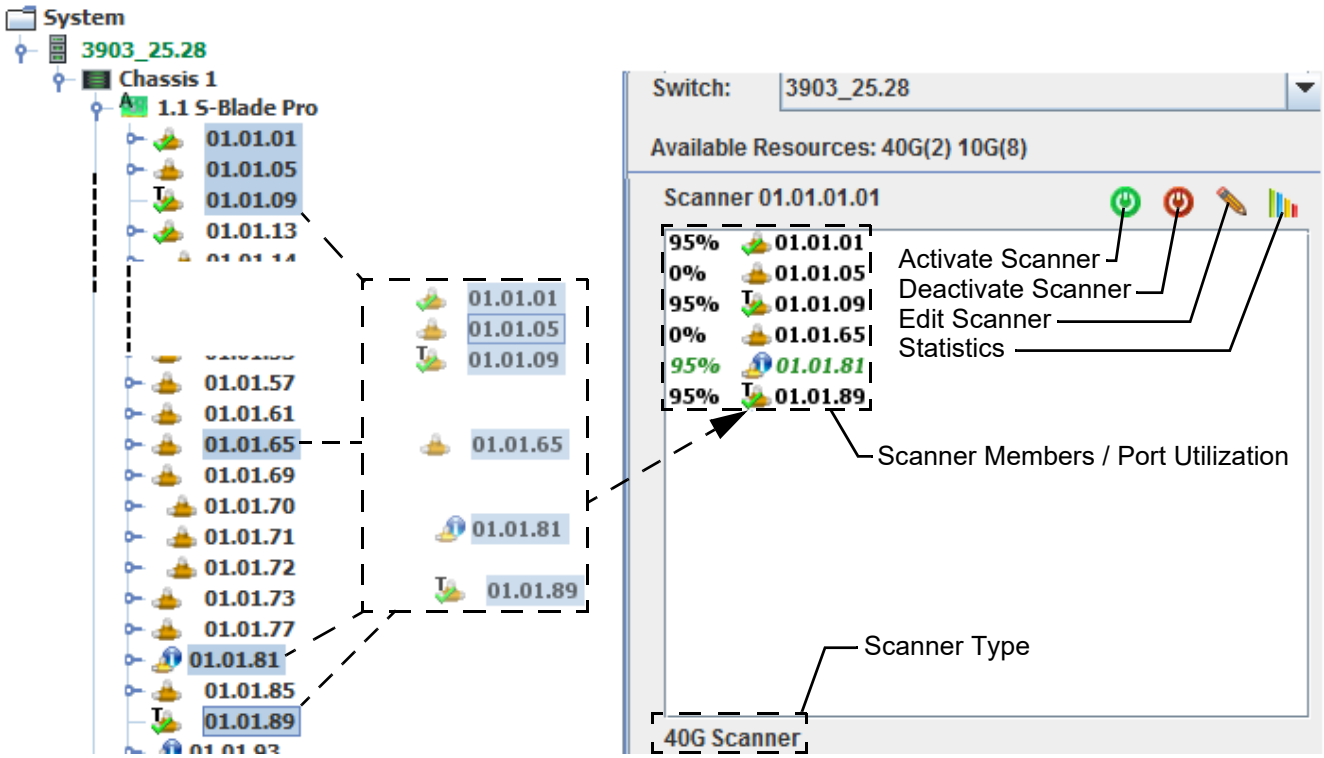


- Switch: List of all connected switches on the network; select required switch from the drop down menu.
- Blade: List of defined blades (by slot number) on a selected switch; select a blade from the drop down menu.
- Activate: Start all scanners on the selected blade.
- Deactivate: Stop all scanners on the selected blade.
- Statistics: Activate all scanners on the selected blade and begin viewing real time or historical statistics. Selecting Real Time Statistics displays a new window showing the current status of all activated scanners (refer to Scanner Real Time Statistics on page 4-5).
- Add All Ports: Selects all defined ports from a blade and adds them to the Port Scanners. All ports must be configured as either 10Gb or 40Gb with the S-Blade Pro set in Utilization Mode (refer to Step 3 of Adding a Switch on page 3-2).
- Remove All Ports: Deactivates all of the scanners then removes all of the ports from the scanners.
- Available Resources: Displays the type (e.g., 10Gb, 40Gb) and number of current defined ports available on the selected blade.

Assigning Ports to a Scanner

1. Select the switch from the Switch menu, then the blade from the Blade menu.
2. From either System or Ports/Groups, select one or more defined ports from the same blade with the same port type (e.g, Blade 1, 40Gb ports) then drag and drop the ports into a Scanner window. The selected ports are displayed with the scanner type indicated in the lower left of the window.

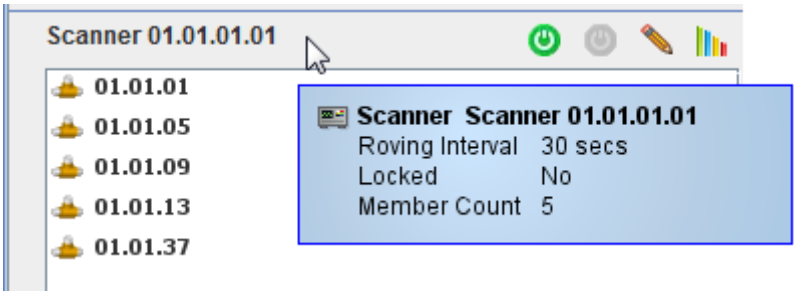
Note: Selecting one port for a scanner results in stationary statistics, selecting more than one port for a scanner allows roving statistics.



- Activate Scanner: Allow the scanner to begin collecting utilization statistics.
- Deactivate Scanner: Ends the collection of utilization statistics from this scanner.
- Edit Scanner Properties: Refer to Scanner Properties on page 4-4.
- Statistics: Allows viewing real time (refer to Scanner Real Time Statistics on page 4-5) or historical statistics (refer to Port Historical Statistics on page 4-12) of the selected active scanner.

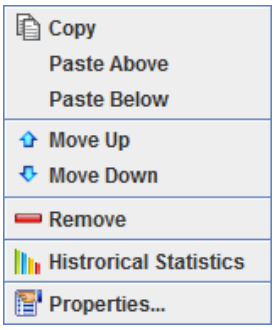
Scanner Properties Tooltip

Hovering near a scanner name area will display a tooltip with the selected scanners properties (refer to Scanner Properties on page 4-4) and number of attached member ports.



Scanner Member Menu

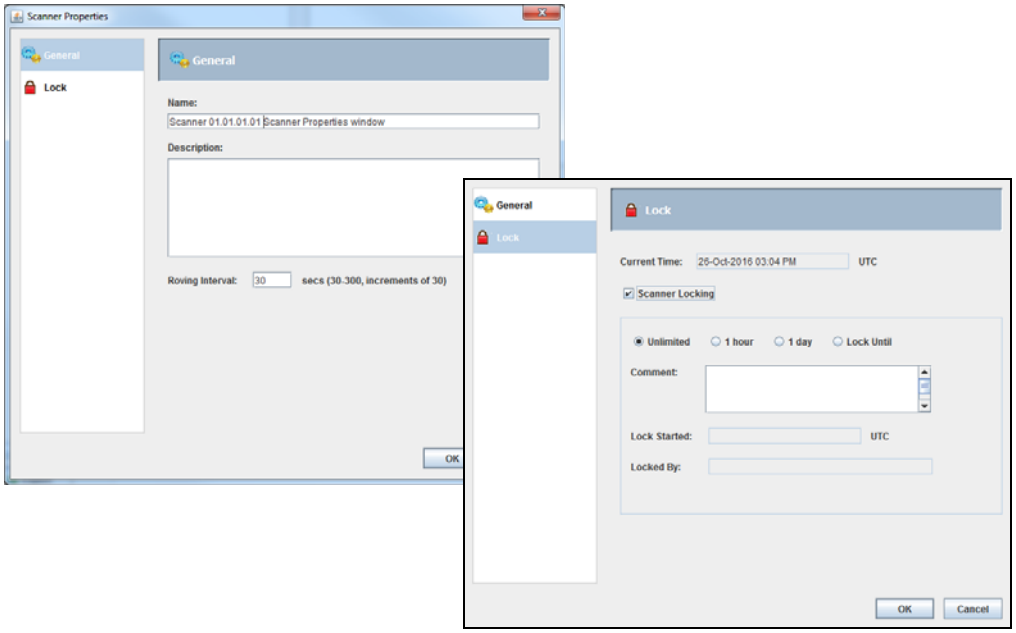
Right clicking on a scanner member displays the following sub-menu.



- Copy - Duplicate (with a new defined name) a selected port.
- Paste Above / Below - Insert a copied port into the scanner member group at a specified position.
- Move Up / Down - Reposition a port in a group.
- Remove - Eliminate the port member from the scanner.
- Historical Statistics - Places selected port members in the Port Historical Statistics name column (refer to Port Historical Statistics on page 4-12).
- Properties - View port configuration information (Refer to Port Properties on page 3-170.)

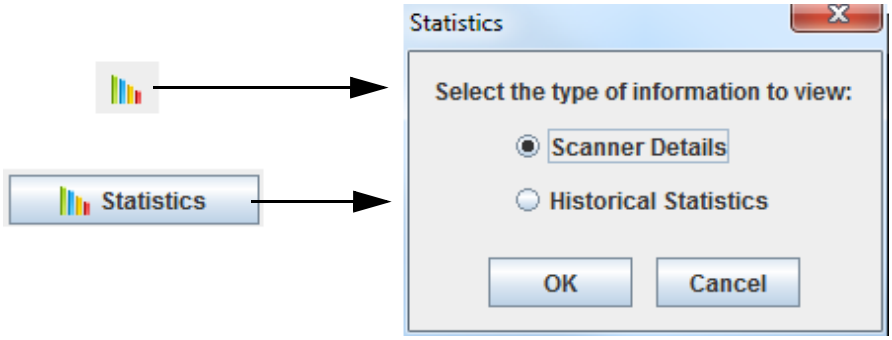
Scanner Properties

Clicking on the Edit Scanner icon of a scanner opens a Scanner Properties window allowing changing the scanner name, adding description information, setting the roving interval time (from 30 to 300 seconds; default = 30 seconds), and optionally setting scanner locking (similar to port locking, refer to Port Lock Settings on page 3-98) of the group of ports in the scanner.



Scanner Real Time Statistics

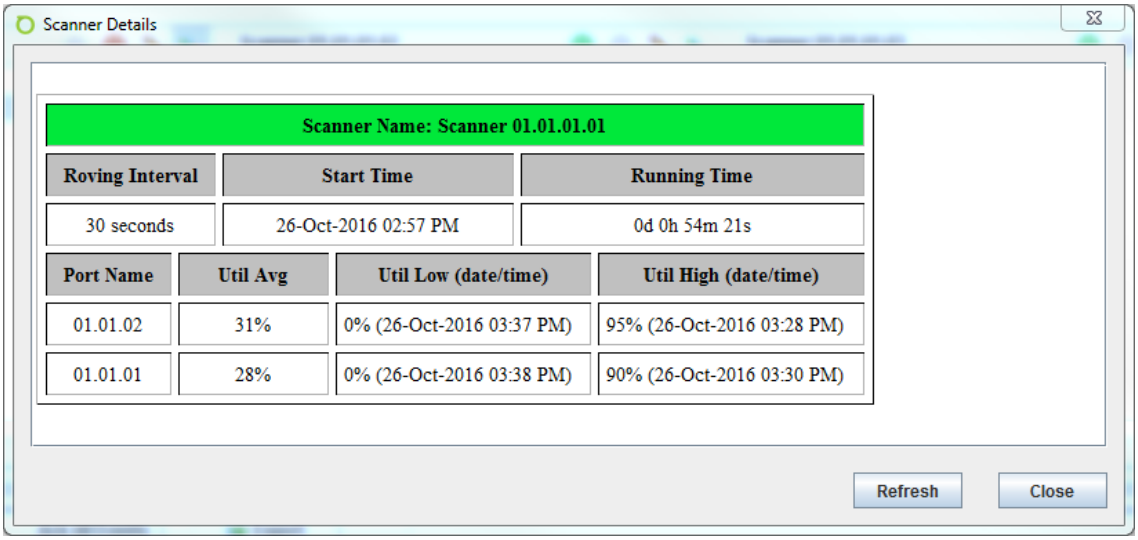
Clicking on either the Statistics icon for an individual scanner or the Statistics button activates a selection screen.



Selecting Historical Statistics takes you to the Port Historical Statistics screen (refer to Port Historical Statistics on page 4-12).

Selecting Scanner Details will display one of two Scanner Detail screens:

- Scanner Details (Individual Scanner)



Click **Refresh** to update Scanner Details to the current results.

- Scanner Details (All Activated Scanners)

Scanner Details

Scanner Name: Scanner 01.01.01.01		
Roving Interval	Start Time	Running Time
30 seconds	26-Oct-2016 07:03 PM	0d 1h 52m 45s

Port Name	Util Avg	Util Low (date/time)	Util High (date/time)
01.01.01	80%	0% (07-Sep-2016 08:03 PM)	95% (07-Sep-2016 08:06 PM)
01.01.05	0%	0% (07-Sep-2016 08:02 PM)	0% (07-Sep-2016 08:02 PM)
01.01.09	94%	81% (07-Sep-2016 09:34 PM)	95% (07-Sep-2016 08:02 PM)
01.01.13	0%	0% (07-Sep-2016 08:02 PM)	0% (07-Sep-2016 08:02 PM)
01.01.37	95%	95% (07-Sep-2016 08:02 PM)	95% (07-Sep-2016 08:02 PM)
01.01.38	88%	53% (07-Sep-2016 08:02 PM)	95% (07-Sep-2016 08:05 PM)

Scanner Name: Scanner 01.01.01.02		
Roving Interval	Start Time	Running Time
30 seconds	26-Oct-2016 07:03 PM	0d 1h 53m 45s

Port Name	Util Avg	Util Low (date/time)	Util High (date/time)
01.01.18	70%	0% (07-Sep-2016 08:02 PM)	80% (07-Sep-2016 08:02 PM)
01.01.19	66%	0% (07-Sep-2016 08:03 PM)	80% (07-Sep-2016 08:02 PM)
01.01.20	0%	0% (07-Sep-2016 08:02 PM)	0% (07-Sep-2016 08:02 PM)
01.01.21	80%	80% (07-Sep-2016 08:02 PM)	80% (07-Sep-2016 08:02 PM)
01.01.22	95%	0% (30-Nov-1979 12:00 AM)	0% (30-Nov-1979 12:00 AM)
01.01.23	88%	0% (30-Nov-1979 12:00 AM)	0% (30-Nov-1979 12:00 AM)

Refresh Close

Click **Refresh** to update Scanner Details to the current results.

Statistics

Select **Tools > Statistics**, or from the toolbar, select the **Statistics** icon, or from the keyboard **Alt+F6**. The Statistics screen displays. The following selections are available:

- System Statistics on page 4-7
- Port Real Time Statistics on page 4-8
- Port Historical Statistics on page 4-12

System Statistics

System statistics displays an overview of the system utilization on each switch on the system. The total defined count on a switch is based on the physical number of ports in the switch and on the blade types installed in the switch.

Port / Sub-Port Statistics

Indicates the total number of ports currently in the switch, defined ports, connected ports, and alarmed ports.

Port Statistics Options

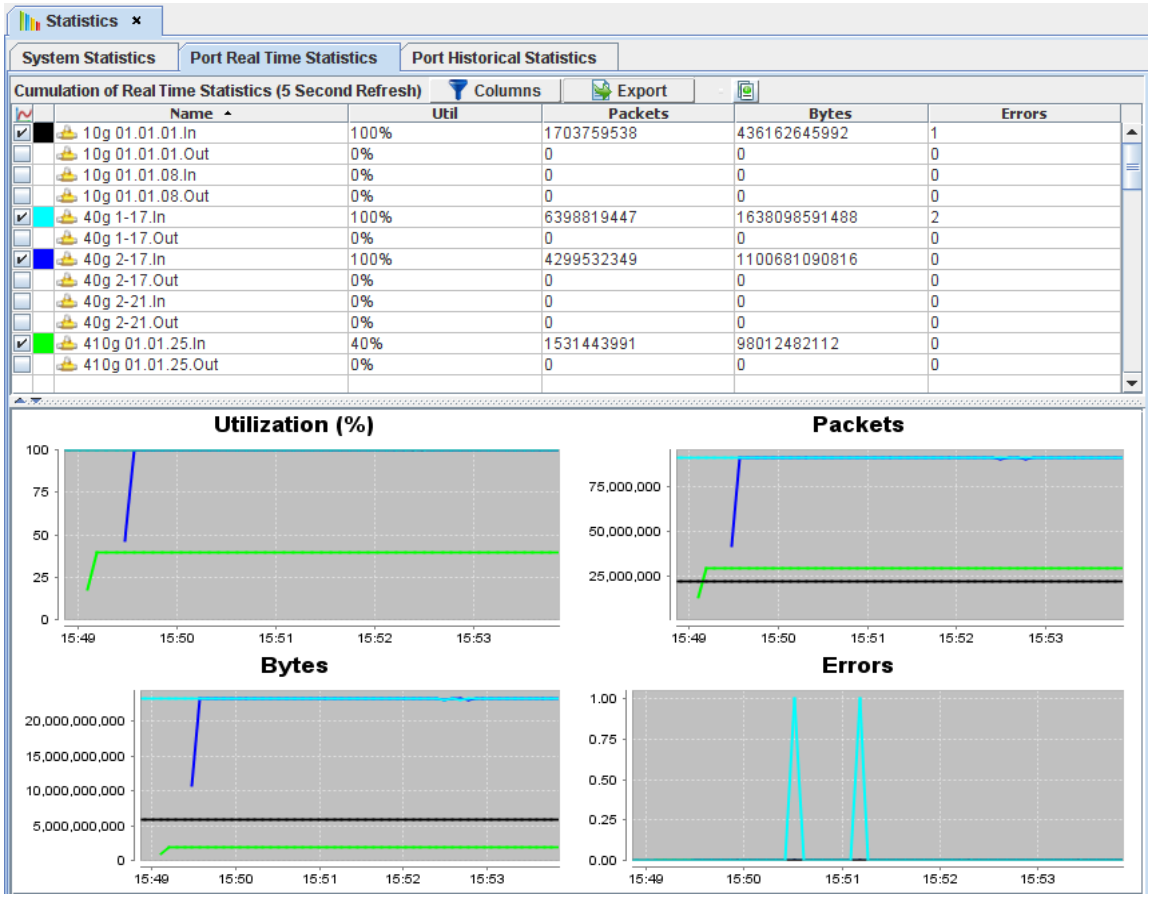
Right-click onto a Port / Sub-Port Statistics graph to display a sub-menu for the selected switch:

- Save As - Save the Port Statistics graph in a PNG format.
- Print - Sends the Port Statistics graph to the users printer.

Port Real Time Statistics

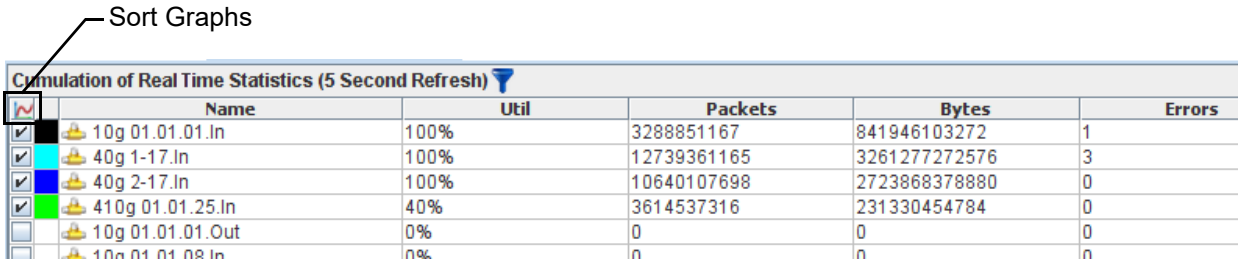
Selecting **Port Real Time Statistics** displays cumulative real time statistics on selected ports/subports (connected and un-connected) every 5 seconds in tabular and graphical formats.

Select and drag (or Copy / Paste) the blade ports/subports to the Name column. Click up to 12 ports in the first column (graph) to display graphical results. The checked ports are displayed using different colors and are updated on a 5 second refresh rate.



Name	Util	Packets	Bytes	Errors
10g 01.01.01.In	100%	1703759538	436162645992	1
10g 01.01.01.Out	0%	0	0	0
10g 01.01.08.In	0%	0	0	0
10g 01.01.08.Out	0%	0	0	0
40g 1-17.In	100%	6398819447	1638098591488	2
40g 1-17.Out	0%	0	0	0
40g 2-17.In	100%	4299532349	1100681090816	0
40g 2-17.Out	0%	0	0	0
40g 2-21.In	0%	0	0	0
40g 2-21.Out	0%	0	0	0
410g 01.01.25.In	40%	1531443991	98012482112	0
410g 01.01.25.Out	0%	0	0	0

Clicking on the Sort Graphs icon sorts all checked ports / subports together.



Name	Util	Packets	Bytes	Errors
10g 01.01.01.In	100%	3288851167	841946103272	1
40g 1-17.In	100%	12739361165	3261277272576	3
40g 2-17.In	100%	10640107698	2723868378880	0
410g 01.01.25.In	40%	3614537316	231330454784	0
10g 01.01.01.Out	0%	0	0	0
10g 01.01.08.In	0%	0	0	0

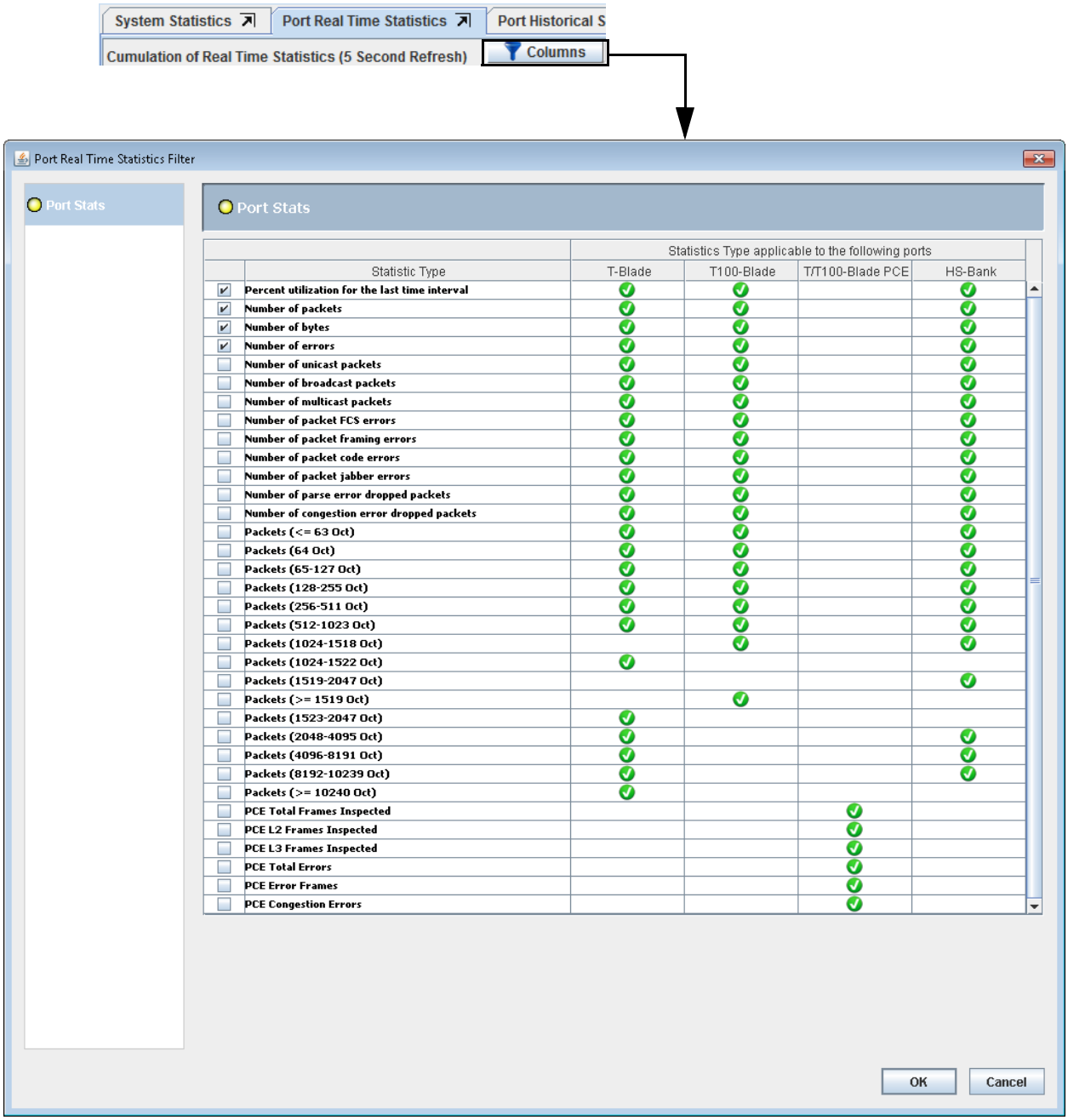
Refer to Port Properties - Threshold Settings on page 3-148 to set port threshold alarms.

Click on the **Historical Report** icon (refer to Historical Report on page 4-14) to define usability settings to record statistics for the last 60 minutes.

Port Real Time Statistics Field Filtering

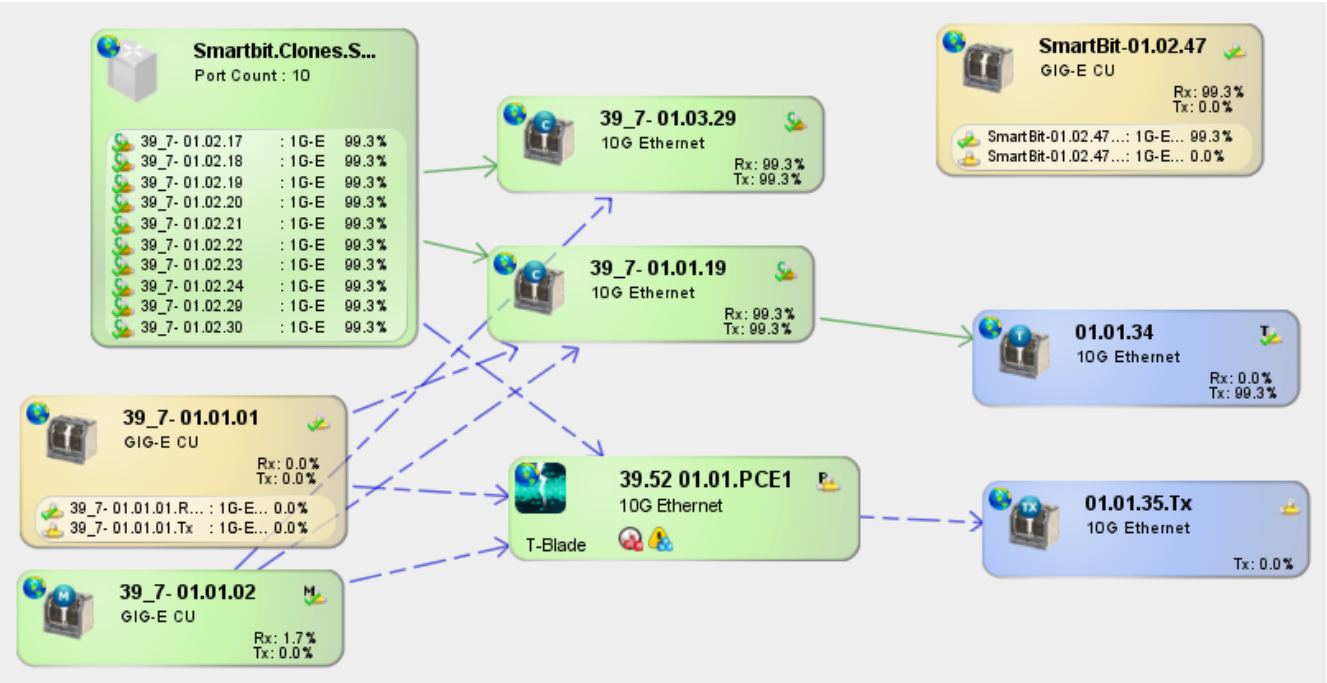
Note:
Utilization (%) Display: 1Gb Source traffic at 0.1% displays as 0.1% utilization on 10Gb Destination Ports.

Click on the Filter Columns icon to display a selectable listing of the statistics fields. From this list, the user can enable / disable the display of any of the statistics type entries. The port columns indicate which type of ports the statistics type is valid. Select/unselect the required fields, then click **OK**.



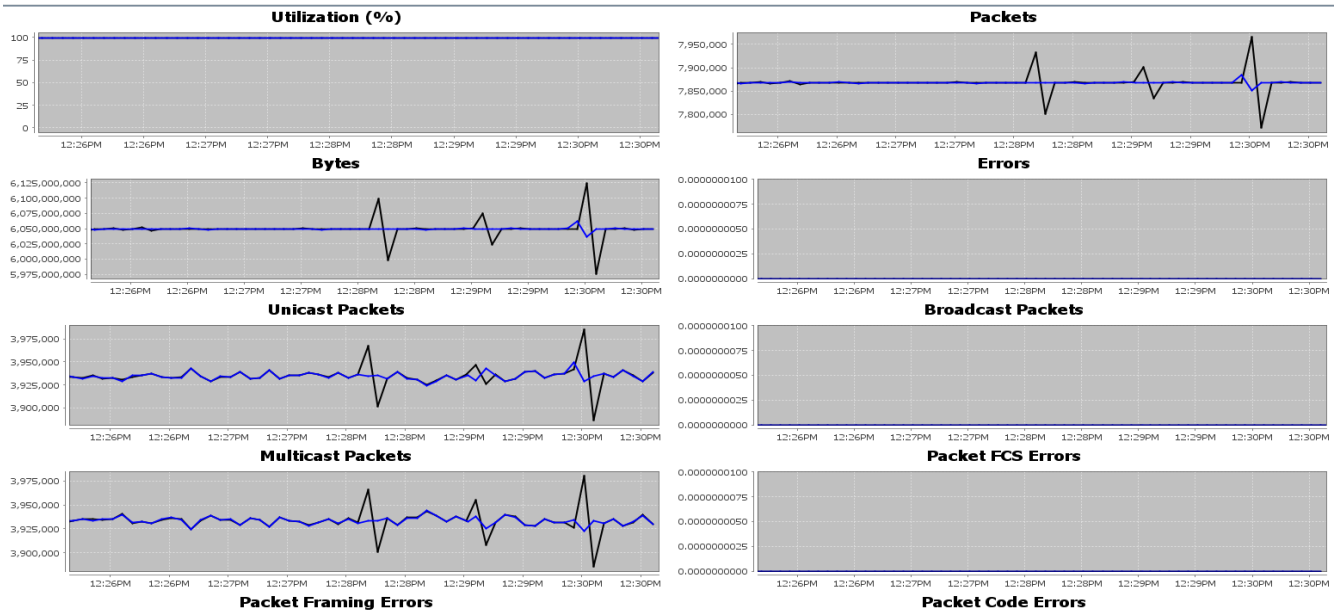
Interpreting Clone Port Real Time Statistics

Test case example: Clone ports from different blades are cloning the same traffic; the source traffic is coming from one blade with clone ports from two other blades as the destination.



When viewing the Port Real Time Statistics screen, it is important to understand how the counters are gathered in order to interpret the data displayed in table view or graph view correctly.

The counter values are collected from the ports every 5 seconds. The timing of this interval is very precise, but can deviate by small fractions of a second, usually much less than 1 millisecond (.001 second). This deviation can affect the values displayed in two consecutive intervals for a single port (i.e., if one interval is extended by a fraction of a millisecond, the next interval will generally be reduced by about the same amount), although the correction can be spread across more than two intervals.



To observe the effect of this behavior, graph the packet and byte counts and the utilization (%) for one port that is receiving data at a constant rate (a traffic generator may be required to get a constant data rate, as the variable data rate of “real” network traffic hides the effect of the variations in counter collection). You may see occasional spikes (both up and down) in the packet and byte count graphs. The utilization (%) graph shows a straight line because the utilization calculation accounts for any variation in the time intervals.

When viewing counters from multiple ports that are receiving and/or transmitting the exact same packet flow, you may see different values in table view or different graphs in graph view. This can occur as the collection is done serially, one port at a time, so the counters from different ports represent 5 second intervals that are slightly offset from each other. The counters will differ by the number of packets that are sent or received during that time interval.

Port Historical Statistics

Selecting **Port Historical Statistics** displays a current view of selected port/subport statistics in tabular and graphical formats. Utilization, Congestion Errors, and Total Errors statistics / graphs can be set to display selected time ranges from the previous hour out to the past 30 days.

To enable a configured port to begin collecting historical statistics, from the Port Properties dialog box (refer to Configuring Blade Ports on page 3-57), select **Link Admin UP / Always Collect Rx Stats** or select another port in the connection. To halt historical statistics on a port, un-select the **Link Admin UP / Always Collect Rx Stats** check box.

Note: Connected ports can be assumed to be collecting historical statistics data; viewing the port properties of an individual port can be used to verify the status of the port.

Historical Statistics - Tabular Display

The statistics filter allows selecting the displayed statistic fields.

Select and drag (or Copy / Paste) blade ports or subports to the **Name** column.
Click (up to 12) check boxes next to each port/subport to graph on the chart; each selected port/subport is assigned a color (port legend) for visual tracking on the Historical Stats display. Statistic results for the ports are immediately displayed and updated on a user selected refresh rate.

Click on the **Filter Columns** icon to select the columns to display.

Select from the **Timeframe** drop down menu the time frame from which statistics are calculated in the statistics table (up to 30 days).

Clicking on the **Historical Report** icon (refer to Historical Report on page 4-14) allows setting usability settings to record statistics for the last 60 minutes.

Select from the **Refresh Rate** drop down menu the time interval (1 / 5 / 10 minutes, or disabled) to update the statistics data.

Clicking on the **Sort Graphs** icon sorts all checked ports / subports together.

The **Downloading Data** column indicates, using a moving hourglass icon, when data about the port is being loaded from the TestStream server to the tabular display.

Port Historical Statistics Field Descriptions

- Name - Port/Subport identifier
- Utilization (High/Average/Low) - Percent utilization for the last time interval
- Congestion Errors (Sum) - Number of congestion error dropped packets
- Total Errors (Sum) - Number of packet errors - uses the number of packet FCS errors, packet framing errors, packet jabber errors, parse error dropped packets, and congestion error dropped packets to determine the error count. Refer to Port Properties - Threshold Settings on page 3-148 to set port threshold alarms.

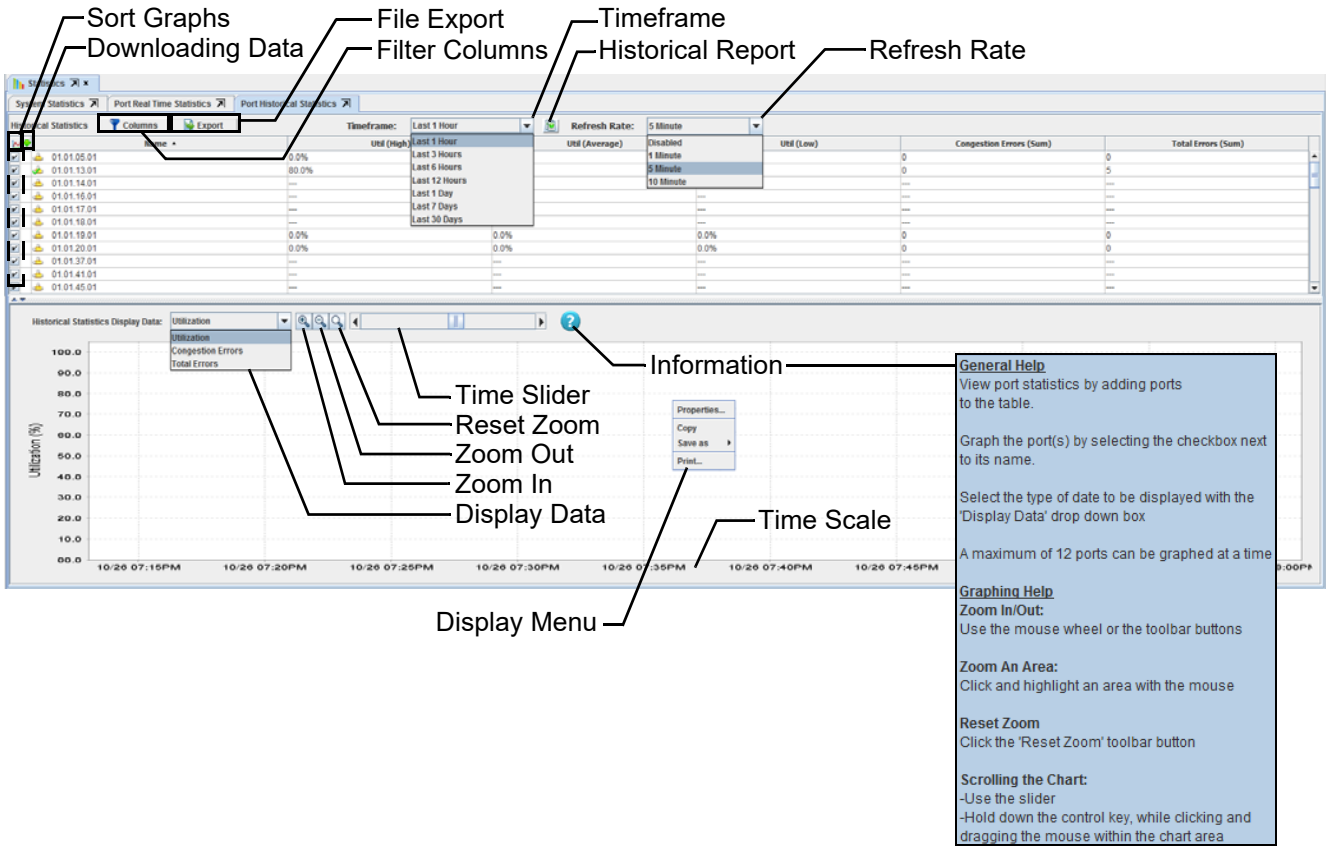
Historical Statistics - Graphical Display

For the Historical Statistics graphical display, select the following:

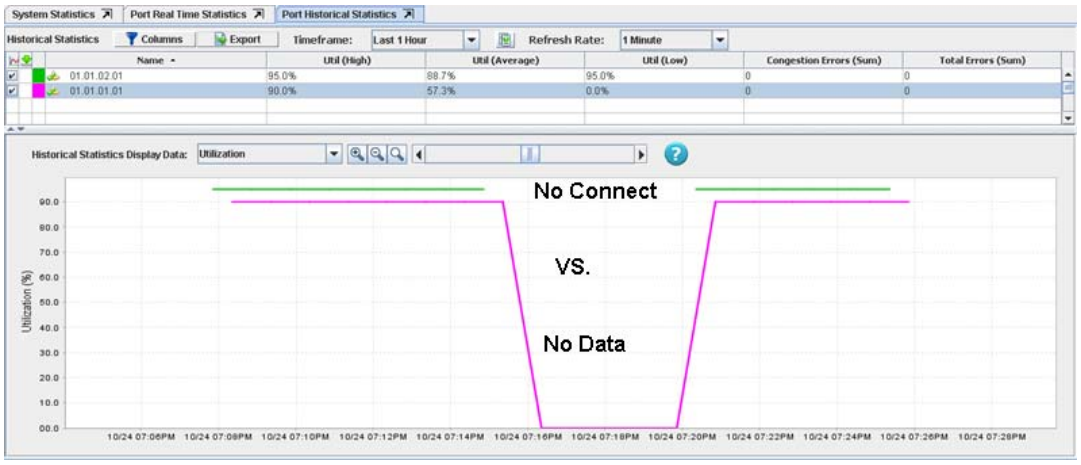
- Display Data Menu: Utilization, Congestion Errors, or Total Errors
- Time Scale: 1/3/6/12/24 hour, 3/7 day, or manual setting

Historical Stats Chart Controls:

- To manually zoom in / out of the screen: use the mouse wheel or click the **Zoom In / Out** buttons
- To manually zoom into an area: click and highlight an area using the mouse
- To reset the chart zoom level, click the **Reset Zoom** button
- Scroll the chart: hold down the control key then click and drag the mouse within the chart area
  - or -
  use the time slider control



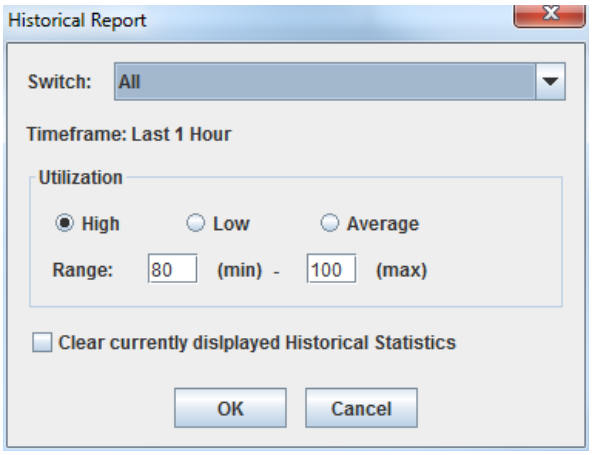
Note: Port Historical Statistics displays if a selected port in a scanner is not connected or if it is connected but no data is passing through the port.



For example, the green line shows a gap indicating there was no connection at the shown time frame; the magenta line shows 0% indicating there was a connection but no data was passing through the port at the shown time frame.

Historical Report

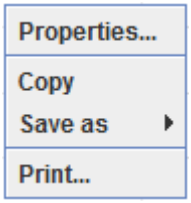
Clicking on the Historical Report icon displays the following window.



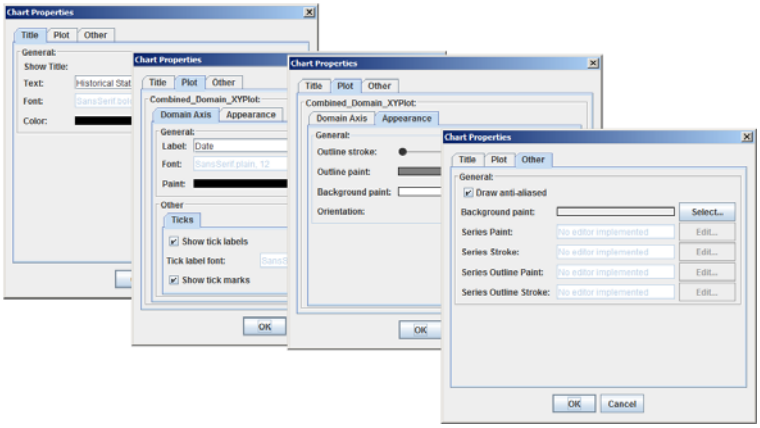
- Switch - Drop down listing of all network-connected switches; select all or individual switches.
- Utilization - Select a time range:
  - High: From 80 to 100 minutes maximum
  - Low: From 0 to 20 minutes max
  - Average: From 20 to 80 minutes max
- Click on **Clear** to remove all currently displayed historical statistics.

Historical Statistics Display Menu

Right clicking anywhere in the Historical Statistics graphical display brings up the following menu:



- Properties: Customize the statistics chart appearance.



- Copy: Copy the current statistics chart for inserting (paste) into another document.
- Save as: Save the current statistics chart in .png graphic format.
- Print: Print (or save as a PDF file) the current statistics chart.

Statistics Report

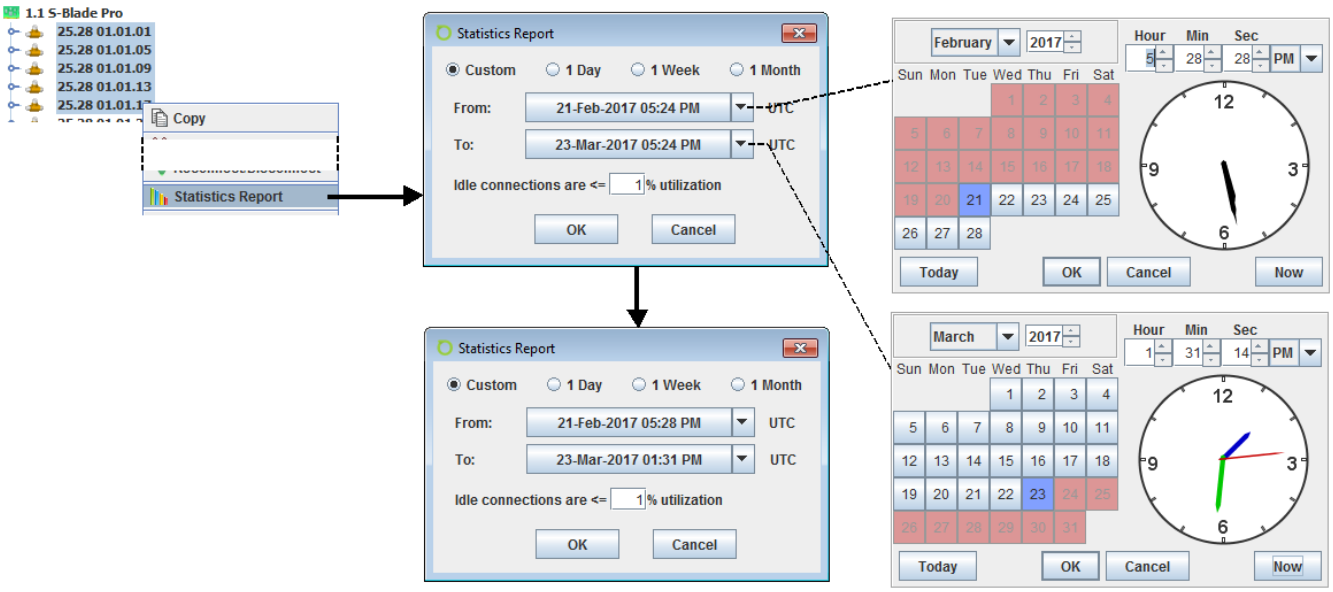
Statistics Report allows creating custom reports of historical statistics covering a specified time frame for S-Blade Pro ports consisting of:

- Percentage of time a port was disconnected
- Percentage of time a port was either idle or in use while connected
- A plot-line graph showing the data of the specified time frame

1 Select one or more ports, right-click and select **Statistics Report** from the drop down menu.

2 Select the time frame you wish to run the report:

- Custom - select a time frame within the last 30 days



- 1 Day - select the current 24 hour period
- 1 Week - select the past 7 days
- 1 Month - select the past 30 days

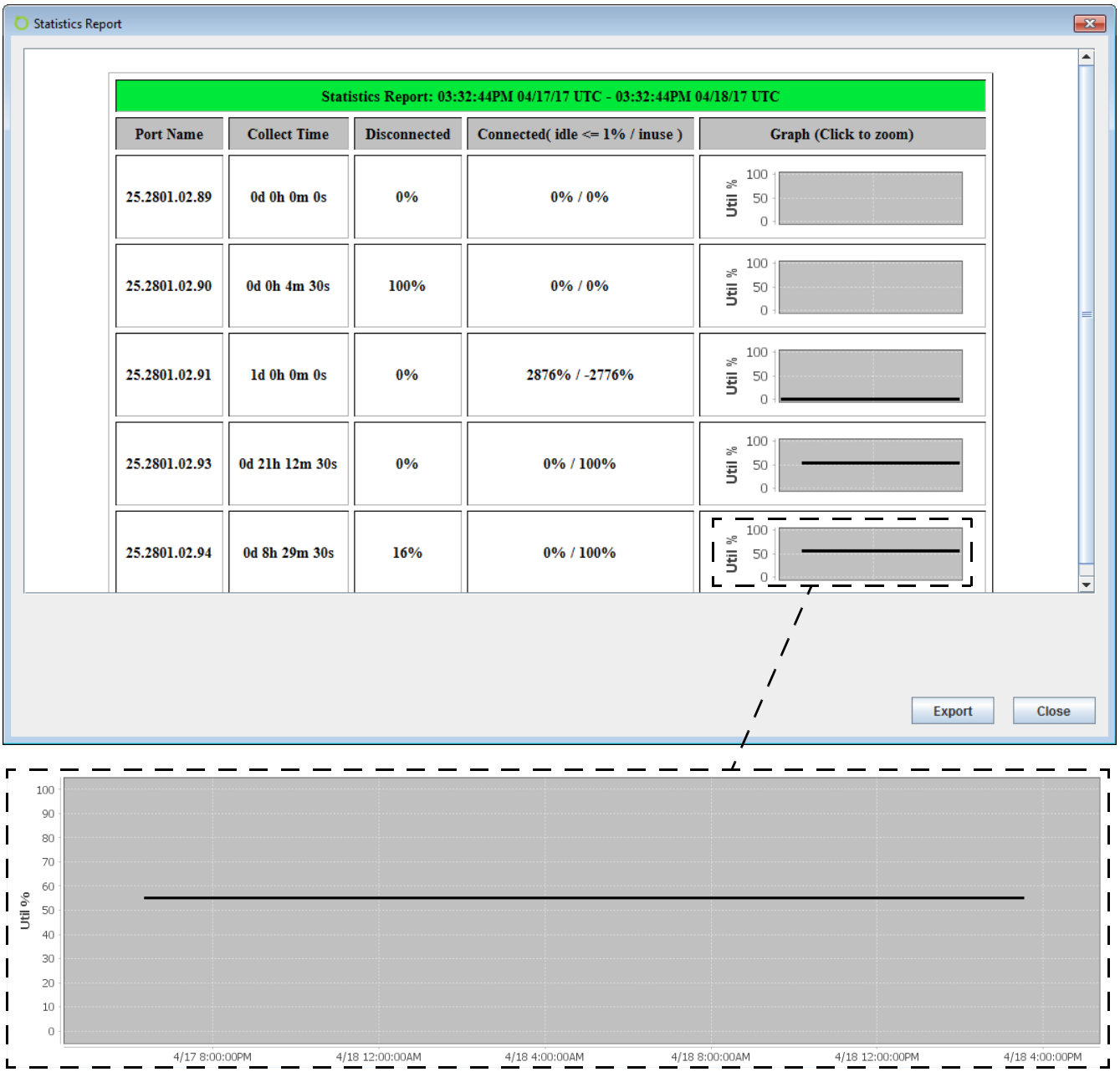
3 For **Idle Connections are <= n% Utilization**, specify the data traffic idle threshold (default = 1%).

4 Click **OK** to generate the report. The Statistics Report window displays showing the selected ports with their separate statistic reports. Clicking on a graph image displays a detailed graphic (in png format) of the selected graph.

Note: To view the detailed graphics, please associate the resulting (png format) graphic with a graphics program (e.g., Windows Photo Viewer).

---

5 Click **Export** to save the results to a csv file for displaying in spreadsheet format.


Statistics Report
Statistics Report: 03:32:44PM 04/17/17 UTC - 03:32:44PM 04/18/17 UTC
Port Name
Collect Time
Disconnected
Connected(idle <= 1% / inuse)
Graph (Click to zoom)
25.2801.02.89
0d 0h 0m 0s
0%
0% / 0%
25.2801.02.90
0d 0h 4m 30s
100%
0% / 0%
25.2801.02.91
1d 0h 0m 0s
0%
2876% / -2776%
25.2801.02.93
0d 21h 12m 30s
0%
0% / 100%
25.2801.02.94
0d 8h 29m 30s
16%
0% / 100%
Util %
100
50
0
Export
Close

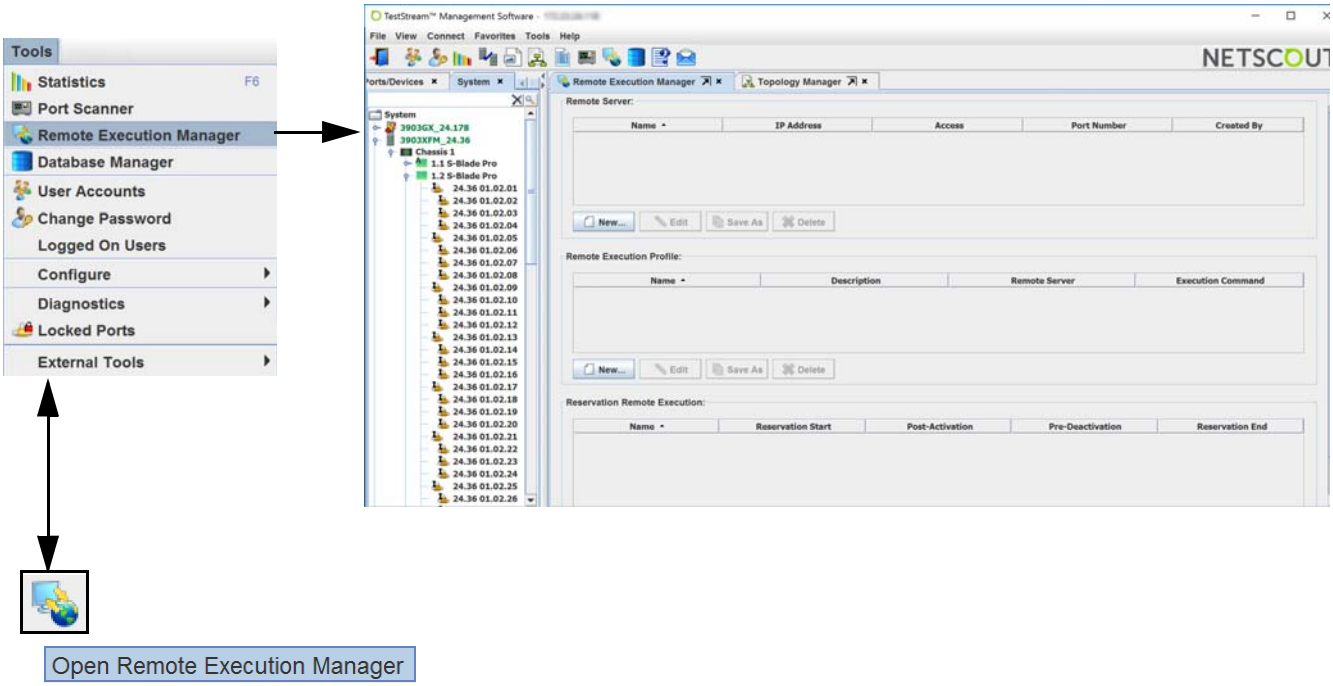
Util %
100
90
80
70
60
50
40
30
20
10
0
4/17 8:00:00PM
4/18 12:00:00AM
4/18 4:00:00AM
4/18 8:00:00AM
4/18 12:00:00PM
4/18 4:00:00PM

Remote Execution Manager (TestStream Lab Manager Only)

The Remote Execution Manager provides the ability to configure remote execution profiles. When adding or editing a reservation, you can add or edit up to four remote command execution configurations, corresponding to the following stages:

- Reservation start before activation: typical use case is the configuration of user equipment
- Reservation start after activation (if 'Activate Topology upon Start' is selected): typical use case is starting test equipment
- Reservation end before deactivation: typical use case is stopping test equipment and gather results
- Reservation end after deactivation: typical use case is clean up configuration of user equipment

To access the Remote Execution Manager, select **Tools > Remote Execution Manager**, or from the toolbar, select the **Remote Execution Manager** icon. The Remote Execution Manager screen displays.

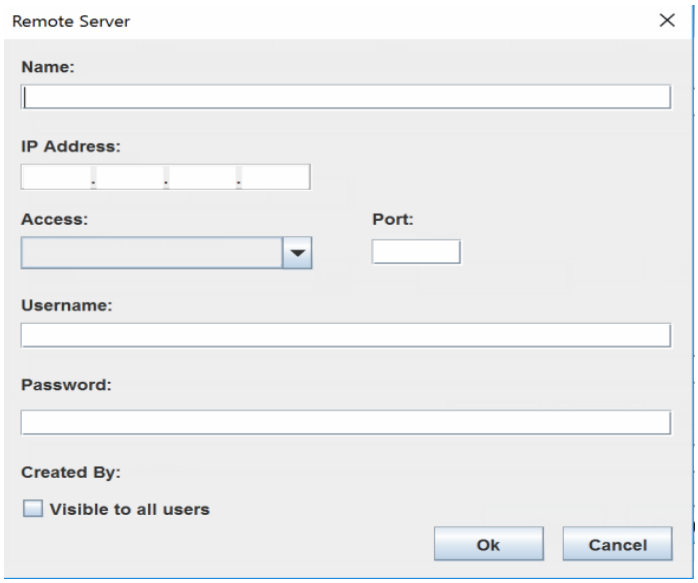


The following selections are available:

- Remote Server
- Remote Execution Profile
- Reservation Remote Execution

Remote Server

When adding, editing, or copying (Save As) a Remote Server, the Remote Server window is displayed.

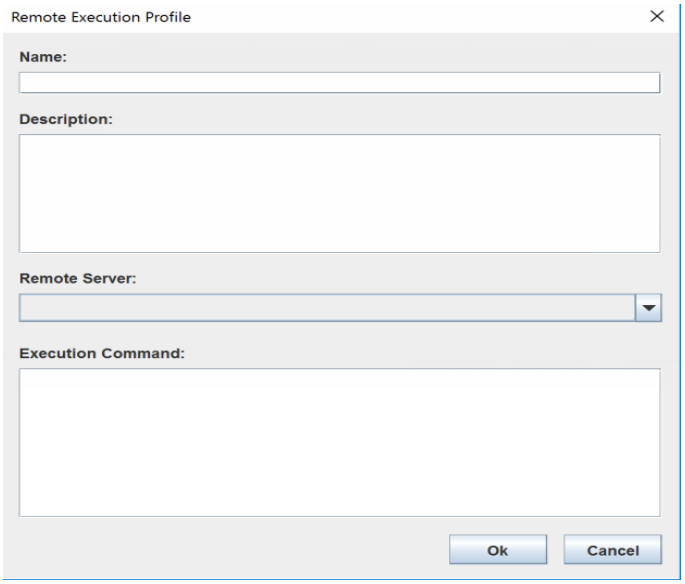


Remote Server Options:

- Enter the server name
- Enter the IP address
- Select the access protocol (Telnet or SSH)
- Enter the port number
- Enter the user name
- Enter the password
- Select/Deselect Visible to all users

Remote Execution Profile

When adding, editing, or copying (Save As) a Remote Execution Profile, the Remote Execution Profile window is displayed.

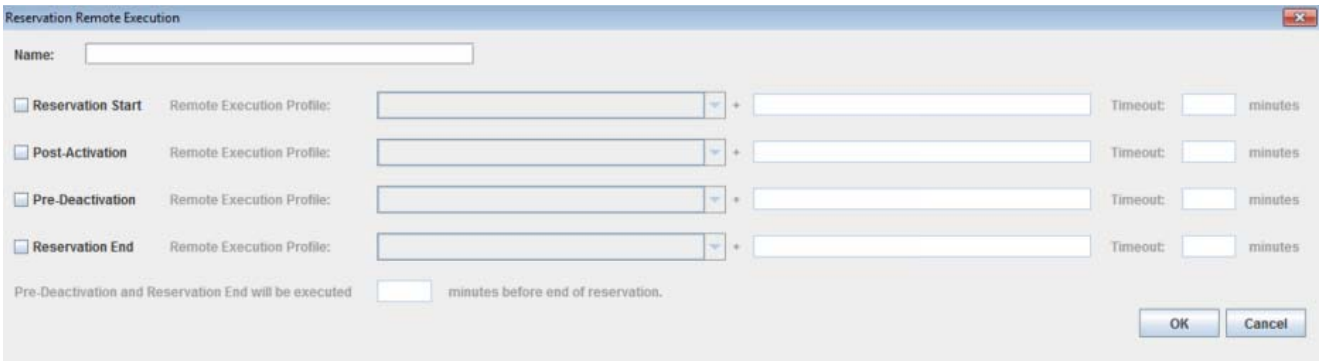


Remote Execution Profile Options:

- Enter the server name
- Enter a description of the profile
- Select the remote server
- Enter the execution command (character string of up to 512 characters)

Reservation Remote Execution

When adding, editing, or copying (Save As) a Reservation Remote Execution, the Reservation Remote Execution window is displayed.



Reservation Remote Execution Options:

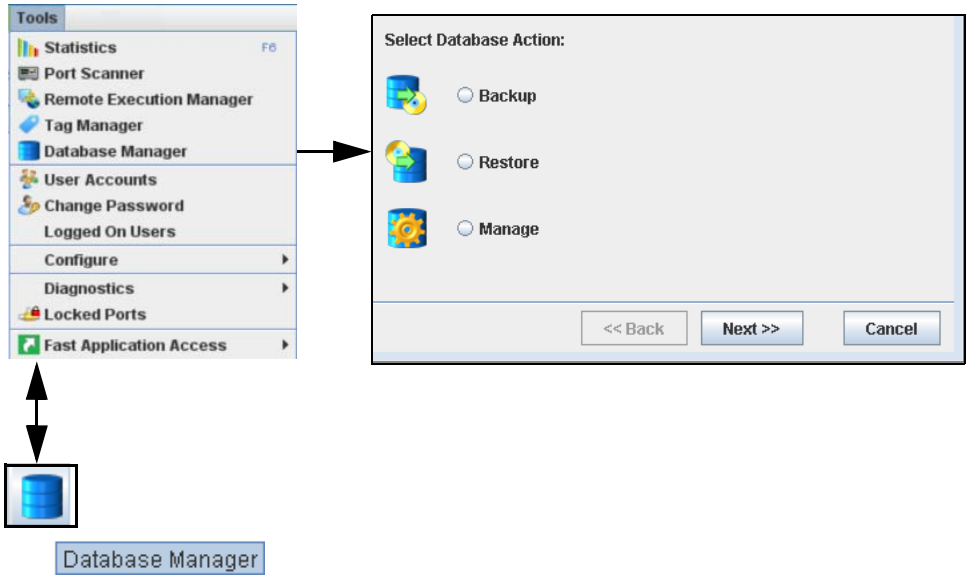
- Enter the reservation name
- Select the stage for the reservation remote execution
- Select the remote execution profile for the selected stage
- Enter an optional append string (character string of up to 512 characters) for the selected remote execution profile
- Enter a time out value

Database Manager

Database utilities are available to manage the TestStream Management application, performing off-line database maintenance functions, and ensuring the integrity of the TestStream Management server database. The applications are:

- Backup on page 4-21
- Restore on page 4-21
- Manage on page 4-22

To access the database utilities, select **Tools > Database Manager**, or from the toolbar, select the **Database Manager** icon. The Database Manager screen displays.



Backup

Allows compiling and saving up to 10 connection databases for the switch. The connection files are saved to the TestStream Management server or to an external storage location.

1 Select **Backup** from the Database Manager main screen, then click **Next**.

2 Enter a name and file description for the backup file.

> **Note:** The following characters must not be included in the backup file name: **\ ( ) \\ % /**

3 If saving the connection file to an external location, click **Export Upon Completion**, then select the directory and file location.

> **Note:** Exported backups should not be stored on the TestStream Management Server.

4 If saving the debug logs of the switches and servers to an external location, click **Backup Debug Logs**, then select the directory and file location.

> **Note:** The Backup Debug Logs option is only available if Export Upon Completion is selected.
>
> The debug logs should only be saved if it is necessary to send these logs to customer service to help in troubleshooting an issue.

5 Click **Next**. A second screen confirming the Backup Name, Description, and Export location (if required) is displayed.

6 Click **Finish**. The database file is saved.

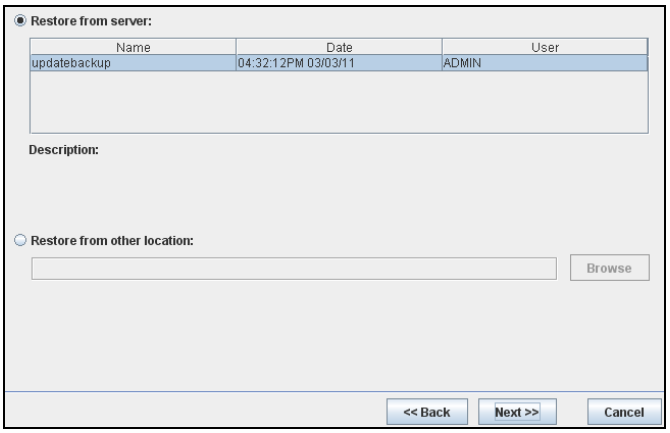
Restore

Allows retrieving and loading the existing connection database to the switch or a replaced nGenius 3900 series switch blade.

1 Select **Restore** from the Database Manager main screen, then click **Next**.

2 **If restoring the database from TestStream Management Server:** Click Restore from server: then select the backup file from the listing. Enter a name and file description for the backup file.
If restoring the database from another source: Click Restore from other location: then click the Browse button to find the location and filename of the backup database.

3 Click **Next**.



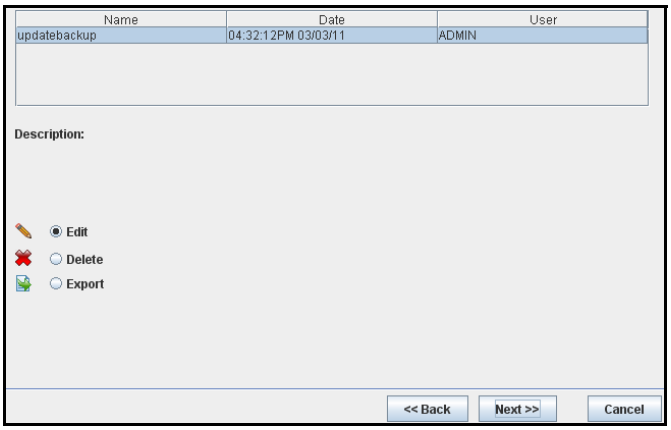
Important: After restoring a connection database, the current connection manager database is automatically synchronized with the restored database.

After a database restore, each switch on the network receives a automatic reconcile while reconnecting to the TestStream Management server. Initial re-login to TestStream Management can take a long time depending on the number of switches in the database.

Manage

Allows editing, deleting, or exporting a selected connection database.

1. Select **Manage** from the Database Manager main screen, then click **Next**.
2. **If editing a database:** Select a database file from the file listing. Select **Edit**.
   If deleting a database: Select a database file from the file listing. Select **Delete**.
   If exporting a database: Select a database file from the file listing. Select **Export**.
3. Click **Next**.



User Accounts

Refer to User Accounts on page 2-30.

Change Password

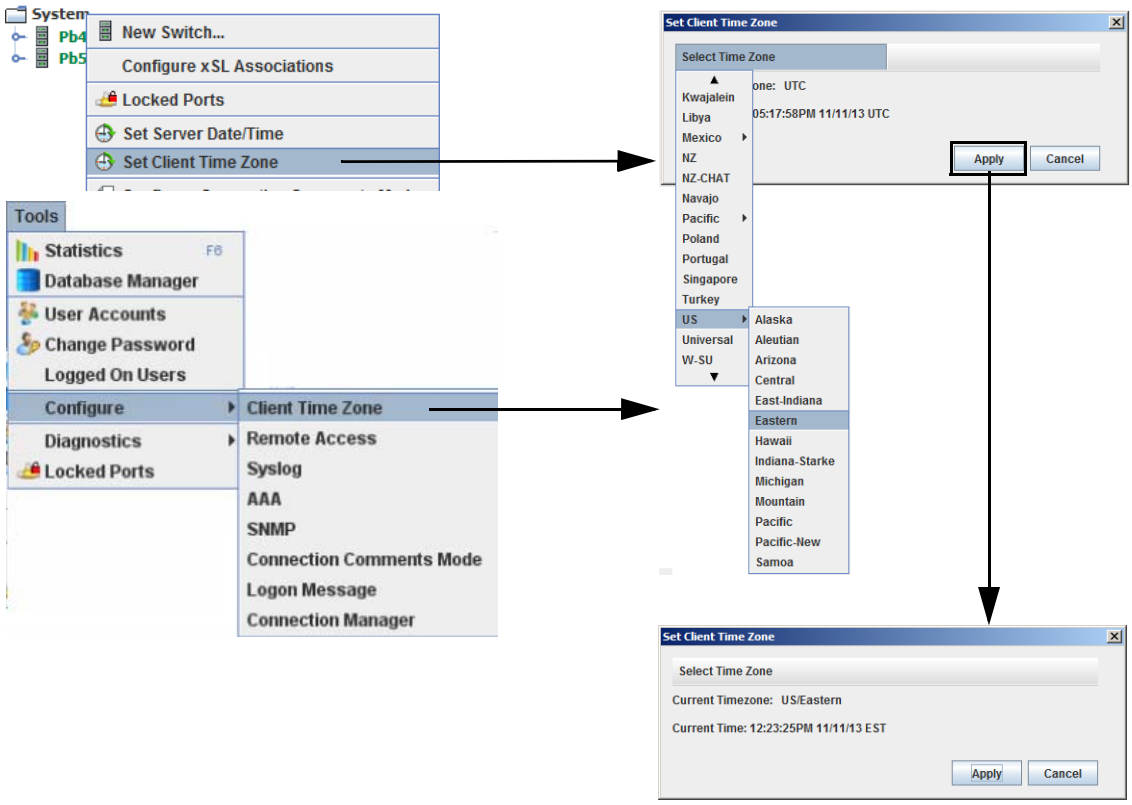
Refer to Change Password on page 2-37.

Logged On Users

Refer to Logged On Users on page 2-38.

Client Time Zone

Client Time Zone allows setting the time zone to correlate with the local TestStream Client user's geographic location.



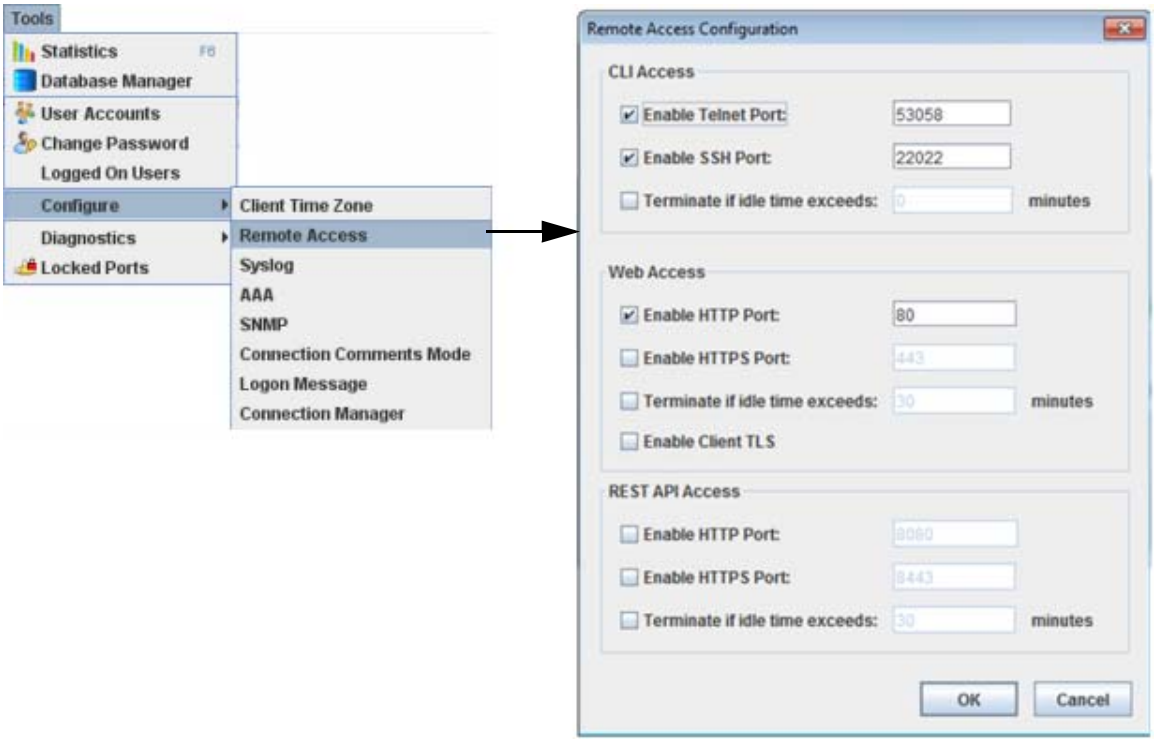
1. From the System tab, right-click on the System icon and select **Set Client Time Zone**
   - or -
   Select **Tools > Configure > Client Time Zone**. The Set Client Time Zone screen displays.
2. Click on **Select Time Zone**. A drop down listing of time zone locations displays.
3. Select the time zone appropriate to your area, then click **Apply**. The current (selected) time zone is displayed with the current local time.

Configure Remote Access

Note: Refer to Appendix A for a description of the Command Line Interface (CLI) specification and commands.

Configure Remote Access allows setting the port and address assignments for accessing the TestStream Management Command Line Interface (CLI) and GUI interfaces utilizing Telnet, HTTP, HTTPS, and SSH protocols (Refer to CLI Access to the TestStream Management Server on page 2-13 and CLI Access using an nGenius 3900 Series Blade Console Port on page 2-13).

1 From the administrator user lever, select **Tools > Configure > Remote Access**. The Remote Access Configuration screen displays.



2 **CLI Access Options:**

- **Setting CLI Access - Telnet**: Select **Enable Telnet Port** and enter a valid TCP port number (default: 53058) in the Telnet Port number field.
- **Setting CLI Access - SSH**: Select **Enable SSH Port** and enter the TCP port (default: 22022) to be used by the TestStream Management server in the SSH Port number field.
- **Terminate Session On Idle Time**: select **Terminate if idle time exceeds** and enter a numeric value in minutes (where x = idle time; 0 is default).

Web Access Options:

- **HTTP**: Select **Enable HTTP Port** and enter a valid the HTTP port number (default: 80) in the HTTP Port number field.
- **HTTPS**: Select **Enable HTTPS Port** and enter a valid the HTTPS port number (default: 443) in the HTTPS Port number field.
- **Terminate Session On Idle Time**: select **Terminate if idle time exceeds** and enter a numeric value in minutes (where x = idle time; 30 is default).
- **Client TLS:** Select **Enable Client TLS** to utilize the TLS Secure Server Communication component installed on TestStream Management.

Rest API Access Options:

Note: Rest API is not supported when the TestStream Management Server runs in an S-Blade (embedded server).

- **HTTP**: Select **Enable HTTP Port** and enter a valid the HTTP port number (default: 8080) in the HTTP Port number field.
- **HTTPS**: Select **Enable HTTPS Port** and enter a valid the HTTPS port number (default: 8443) in the HTTPS Port number field.
- **Terminate Session On Idle Time**: select **Terminate if idle time exceeds** and enter a numeric value in minutes (where x = idle time; 30 is default).

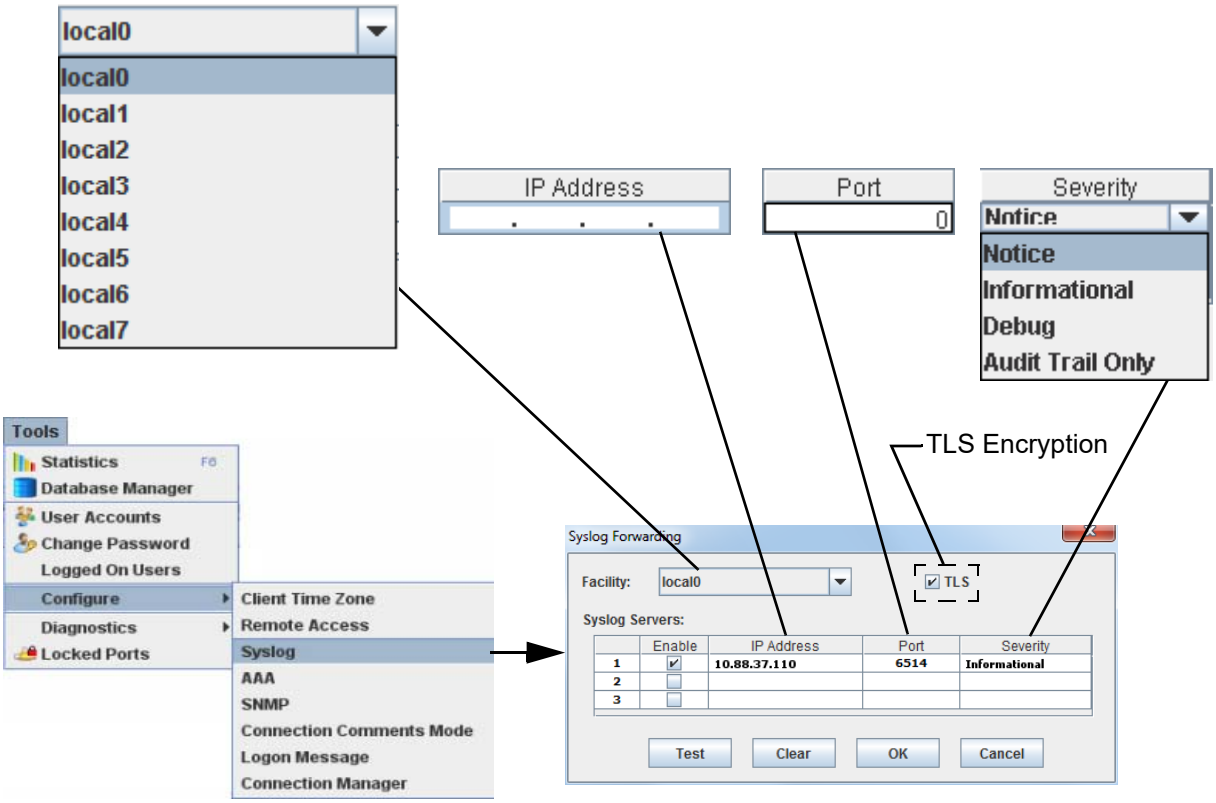
3 Click **OK** to save the changes.

Note: Allow 2 minutes to let TestStream Management finalize the new configuration settings prior to utilizing the new remote access settings.

Configure Syslog

This feature allows forwarding TestStream Management audit trails and alarms to up to three TestStream Management servers connected to the TestStream Management network.

Select **Tools > Configure > Syslog**. The SysLog Forwarding screen displays.



Up to three servers, each with an individual IP address, port number, and severity level are displayed. Clicking **Enable** allows forwarding syslog messages to the selected server(s).

Set Syslog Server Settings

From the **Facility** drop-down menu, select (from local0 through local7) a storage location that will be used by TestStream Management when accessing all system log events. Click on the IP Address and Port fields to enter the server IP addresses / port numbers. To filter the type of messages received by a syslog server, click on the Severity field to access a drop-down menu and select the required security level (refer to Severity Levels on page 4-27). Selecting **Clear** removes the information in a selected row. Selecting **Test** pings the IP address of the selected syslog server. Select **Cancel** to ignore any changes to the syslog settings.

Click **OK** to save the syslog configuration settings.

Severity Levels

Each syslog server can be set with the required security level.

Four security levels are selectable:

- Notice - System / Port Alarms only.
- Informational - Audit Trail information messages; Audit Trail and System / Port Alarms.
- Debug - Audit Trail and System / Port Alarms.
- Audit Trail Only - Audit Trail messages only.

TLS Encryption

TLS Syslog requires proper certificates to secure communication between the client and server. TestStream Management contains a self-signed certificate allowing TLS Syslog installation; however, a self-signed certificate is not a recommended method for TLS Syslog and should only be used during initial test setup. One the setup is validated, the self-signed certificate should be replaced with a proper certificate from Certificate Authority (CA).

From the Syslog Forwarding screen, click on **TLS** to use the self-signed certificate; un-click in order to assign a CA certificate.

Certificate Location

All certificates and encryption keys are stored in the */etc/ssl/rsyslog* directory:

- **PFS-ca-key.key** - Certificate Authority (CA) private key
- **PFS-ca-self-sign.pem** - Self-signed CA certificate
- **PFS-ca.pfx** - Combined CA private key and CA certificate for Windows environment; password is required (default = netscout)
- **PFS-syslog.key** - TestStream Server private key
- **PFS-syslog.pem** - TestStream Server certificate signed with CA certificate

Configure AAA

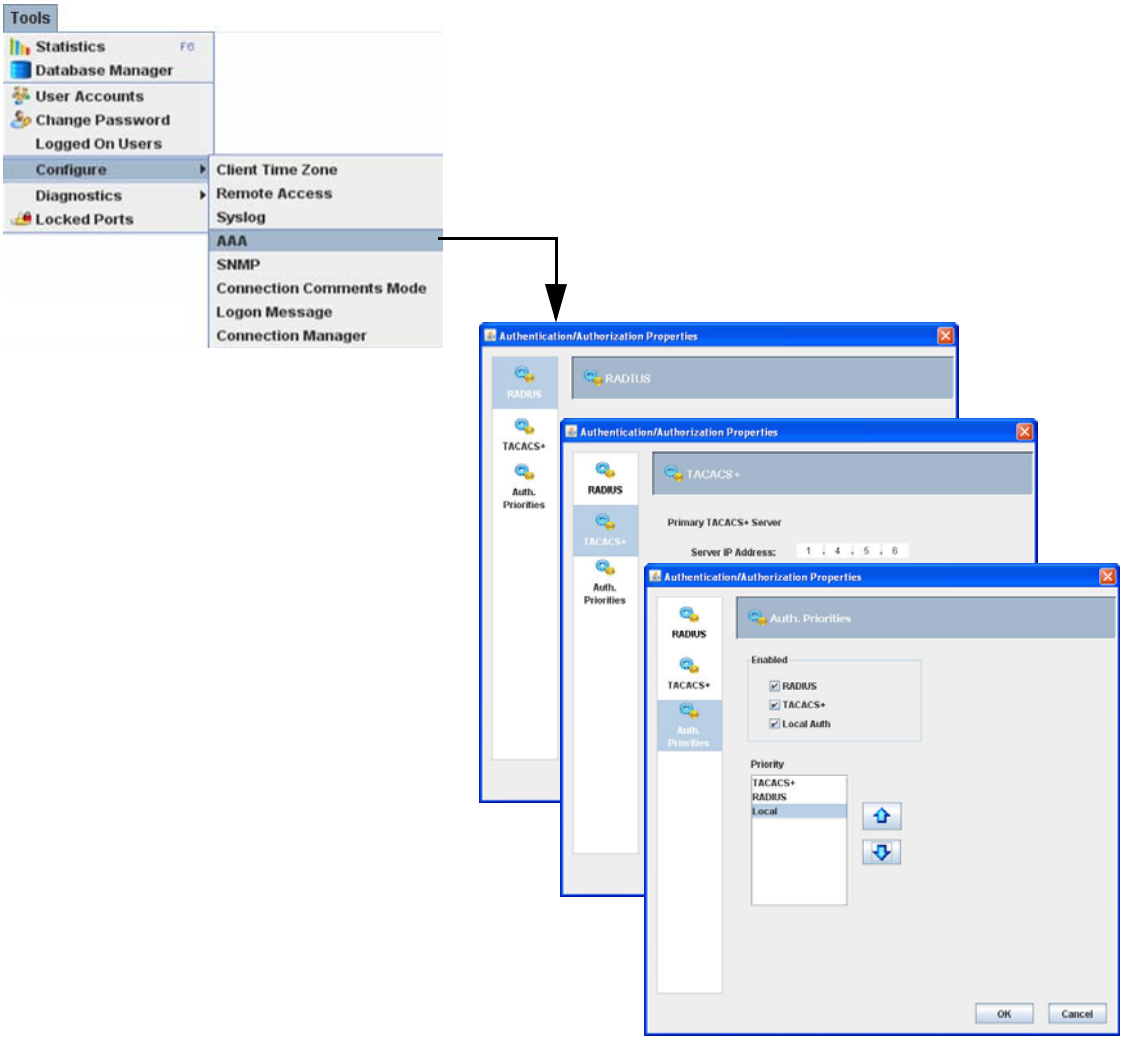
TestStream Management provides support for the Authentication, Authorization, and Accounting (AAA) VPN infrastructure for RADIUS (Remote Authentication Dial In User Service), TACACS+ (Terminal Access Controller Access-Control System Plus) and Active Directory.

Note: Accounting feature is not currently supported; however, audit trail entries are available from Syslog (refer to Configure Syslog on page 4-27) for capturing accounting-style entries.

Note: TACACS+ / RADIUS Administrator users cannot edit user accounts authenticated from a TACACS+ / RADIUS server.

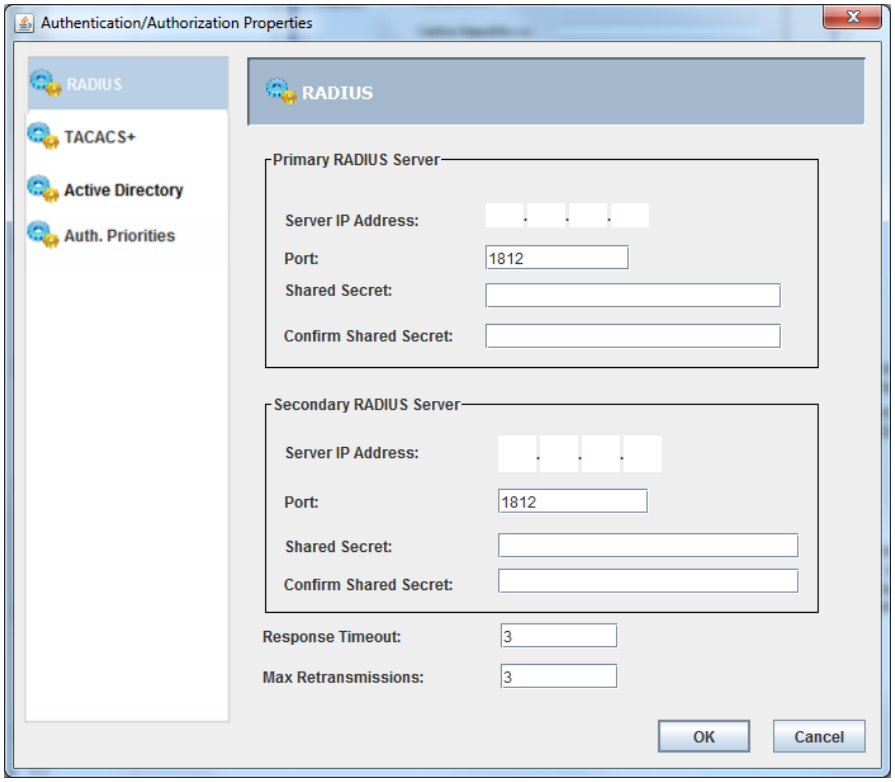
Each approved TestStream Management user can be assigned more than one authentication method. If more than one method is assigned, the methods are prioritized, i.e., the highest priority is first used and if unsuccessful, the next method until the first successful method. If all selected methods fail, the user is not logged into TestStream Management.

Select **Tools > Configure > AAA**. The Authentication/Authorization Properties screen displays.



RADIUS

The RADIUS screen allows the user to configure two servers (primary / secondary) using the RADIUS protocol.



1. **Primary RADIUS Server** - Enter the IP address, port number (default is 1812), and password (between 8 - 64 characters). Re-enter the password in the **Confirm Shared Secret:** text field.
2. **Secondary RADIUS Server** - Enter the IP address, port number (default is 1812), and password (same as Primary, between 8 - 64 characters). Re-enter the password in the **Confirm Shared Secret:** text field.
3. Enter the Response Timeout (in seconds); default is 7.
4. Enter the number of Maximum Retransmissions; default is 5.
5. Click **OK** to save the settings.

When using RADIUS, TestStream Management will attempt to access the first server, then after the maximum number of retransmissions, will attempt accessing the secondary server. If after the maximum number of retransmissions on the secondary server is reached, TestStream Management determines the RADIUS logon a failure and attempts to logon using the next lowest authentication method or until the Local AUTH method is accessed.

Utilizing TestStream Management with RADIUS Servers

TestStream Management provides a dictionary file for RADIUS that contains the NETSCOUT vendor id:

```
VENDOR    netscout    38692
```

Note: The VENDOR number can be overwritten from the ONPATH CONF file: **RADIUS=xxx** where **xxx** is the required vendor ID number.

If this number is changed, the TestStream Management server must be rebooted.

Vendor Specific Attributes (VSA) and attribute value name to number mapping (string to integer):

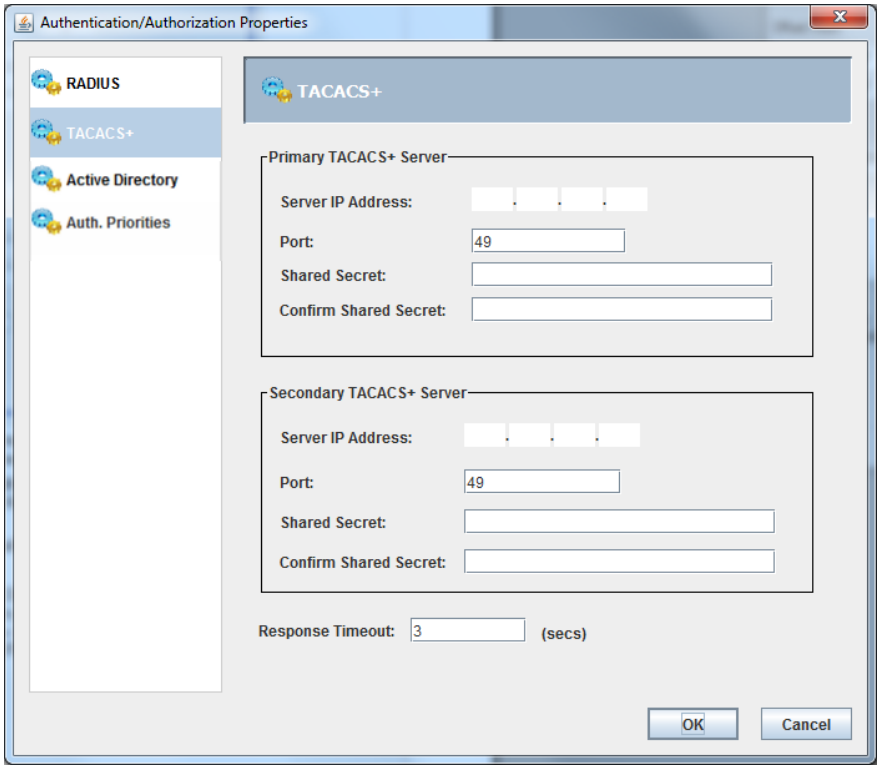
```
BEGIN-VENDOR   netscout
ATTRIBUTE   netscout-User-Access-Level    1    integer
# Access level definition
VALUE netscout-User-Access-Level    Administrator  1
VALUE netscout-User-Access-Level    Operator    2
VALUE netscout-User-Access-Level    Viewer    3
VALUE netscout-User-Access-Level    Custom1    4
VALUE netscout-User-Access-Level    Custom2    5
VALUE netscout-User-Access-Level    Custom3    6
VALUE netscout-User-Access-Level    Custom4    7
VALUE netscout-User-Access-Level    Custom5    8
VALUE netscout-User-Access-Level    Diagnostics    9

END-VENDOR  netscout
```

Customers must add this dictionary file to their RADIUS server. When configuring a user, customers add the attribute **netscout-User-Access-Level** to the user profile then set it to a value between 1 and 9 or use the translation table included in the dictionary file.
For example, when using a Linux RADIUS server, the file **/etc/raddb/users** contains the configured users. The user **username** has its password set to **userpassword** and the TestStream Management user level set to **Administrator** (which is translated to 1 when sent to the RADIUS client):

```
# TestStream Management Users
username Cleartext-Password := userpassword
netscout-User-Access-Level = Administrator
```

TACACS+

The TACACS+ screen allows the user to configure two servers (primary / secondary) using the TACACS+ protocol.



1. **Primary TACACS+ Server** - Enter the IP address, port number (default is 49), and password (between 8 - 64 characters). Re-enter the password in the **Confirm Shared Secret:** text field.
2. **Secondary TACACS+ Server** - Enter the IP address, port number (default is 49), and password (same as Primary, between 8 - 64 characters). Re-enter the password in the **Confirm Shared Secret:** text field.
3. Enter the Response Timeout (in seconds); default is 3.
4. Click **OK** to save the settings.

When using TACACS+, TestStream Management will attempt to access the first server, then if a timeout occurs, will attempt accessing the secondary server. If a timeout on the secondary server occurs, TestStream Management determines the TACACS+ logon a failure and attempts to logon using the next lowest authentication method or until the Local AUTH method is accessed.

TACACS+ Authentication Levels

TACACS+ server returns an attribute-value pair **priv-lvl** set to the desired level as shown below.

For example, as administrator:
TACACS AVPAIRS:: priv-lvl=15

TACACS+ level 15 maps to level 1 in TestStream (administrator)

TACACS+ level 14 maps to level 2 in TestStream (operator)

TACACS+ level 13 maps to level 3 in TestStream (viewer)

TACACS+ level 12 maps to level 4 in TestStream (custom1)

TACACS+ level 11 maps to level 5 in TestStream (custom2)

TACACS+ level 10 maps to level 6 in TestStream (custom3)

TACACS+ level 9 maps to level 7 in TestStream (custom4)

TACACS+ level 8 maps to level 8 in TestStream (custom5)

TACACS+ level 7 maps to level 9 in TestStream (diagnostic)

TACACS+ levels 6-0 map to level 3 in TestStream (viewer)

Assigning User Domains from the TACACS Server

When an nGenius 3900 series switch is configured to use TACACS+ as the primary source to AAA, all user domain assignments must be assigned from the TACACS server. Domains are still created, modified, and deleted locally from TestStream Client by Administrator users, however, domain assignments must be assigned from TACACS.
To assign domain users via the TACACS server:

From TestStream Management:

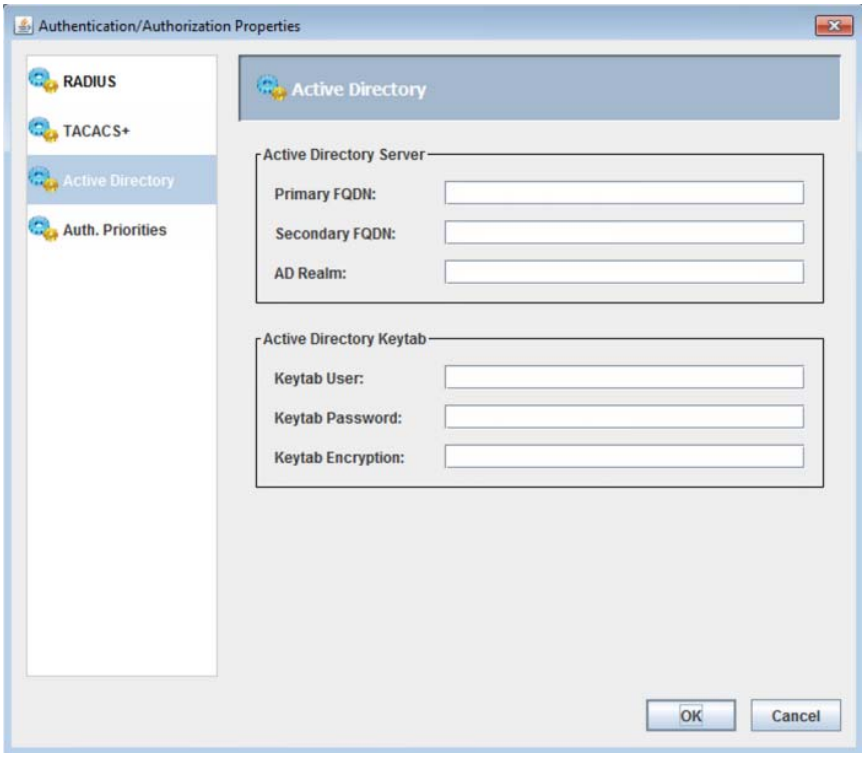
- Create a domain
- Add ports to the domain

From TACACS Server:

- Assign users to a domain using the attribute ***Domain = DomainName***
- Login as a domain user; user authentication is now defined

Active Directory

The TACACS+ screen allows the user to configure two servers (primary / secondary) using the TACACS+ protocol.



1. **Active Directory Server** - Enter the Primary and Secondary FQDN names of the Active Directory Domain Controller and the AD Realm name (which specifies the user account information location).
2. **Active Directory Keytab**- Enter the Keytab User, Password, and Encryption for the existing Active Directory user.
3. Click **OK** to save the settings.

Active Directory Security Access Levels

TestStream Management AAA supports various access levels for each user including Administrator, Operator, Viewer, Diagnostics, and five custom levels. The following table lists the group names for each security level.

Table 4-1

TestStream Security Level	Active Directory Group Name
Administrator	TESTSTREAM_ADMIN
Operator	TESTSTREAM_OPER
Viewer	TESTSTREAM_VIEWER
Custom 1	TESTSTREAM_CUSTOM1
Custom 2	TESTSTREAM_CUSTOM2
Custom 3	TESTSTREAM_CUSTOM3
Custom 4	TESTSTREAM_CUSTOM4
Custom 5	TESTSTREAM_CUSTOM5
Diagnostic	TESTSTREAM_DIAG

Note: A user may be part of multiple groups in the Active Directory environment. If a user does not belong to any of the Active Directory groups, they will not be allowed to log on to the TestStream Managment.

Assigning User Domains from the TACACS Server

When an nGenius 3900 series switch is configured to use TACACS+ as the primary source to AAA, all user domain assignments must be assigned from the TACACS server. Domains are still created, modified, and deleted locally from TestStream Client by Administrator users, however, domain assignments must be assigned from TACACS.
To assign domain users via the TACACS server:

From TestStream Management:

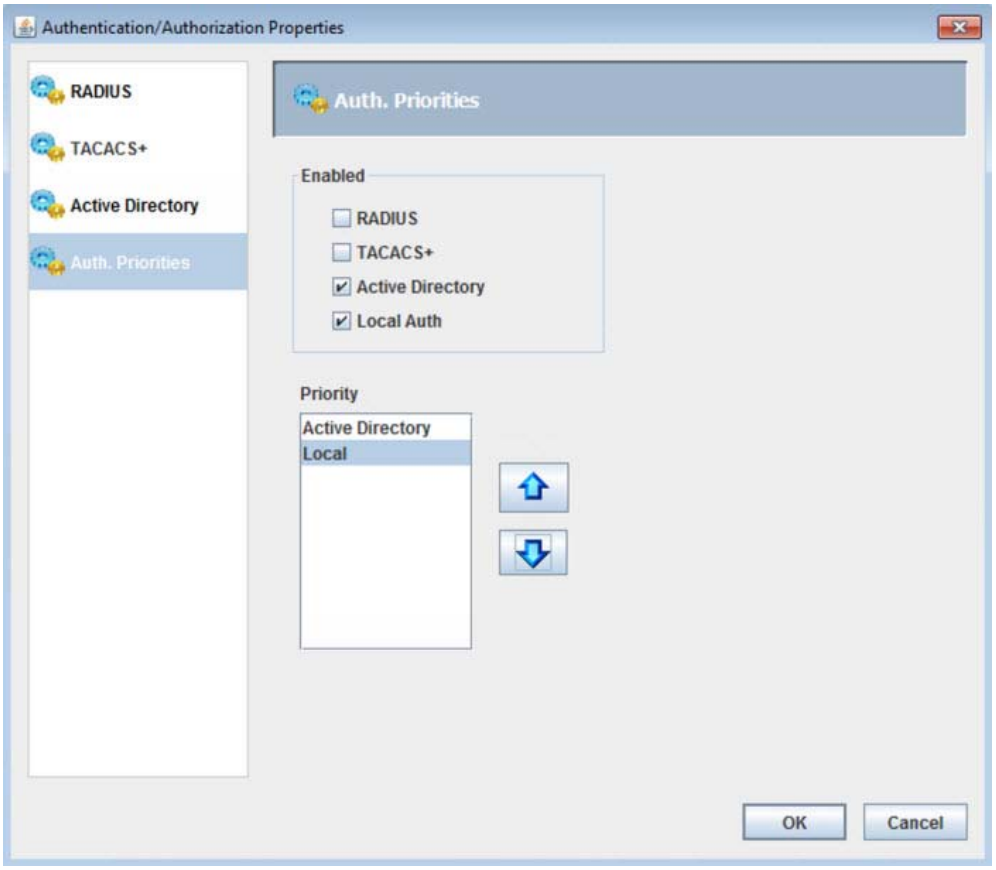
- Create a domain
- Add ports to the domain

From TACACS Server:

- Assign users to a domain using the attribute ***Domain = DomainName***
- Login as a domain user; user authentication is now defined

AUTH Priorities

From the AUTH Priorities screen, the authentication methods used and order of priority are defined.



- The Enabled section displays the available selected methods. Click the check boxes to select the required methods. The selected enabled priorities are displayed in the Priority listing.
- The Priority section is used to set the order of the selected (enabled) authentication priorities. Click on a method then the up/down buttons to move the selection.

Note: Local Auth should always be selected (enabled) and set to the lowest priority to ensure that if the other methods fail, users will still have a way into TestStream Management.

- Click **OK** to save the settings.

Configure Server Redundancy

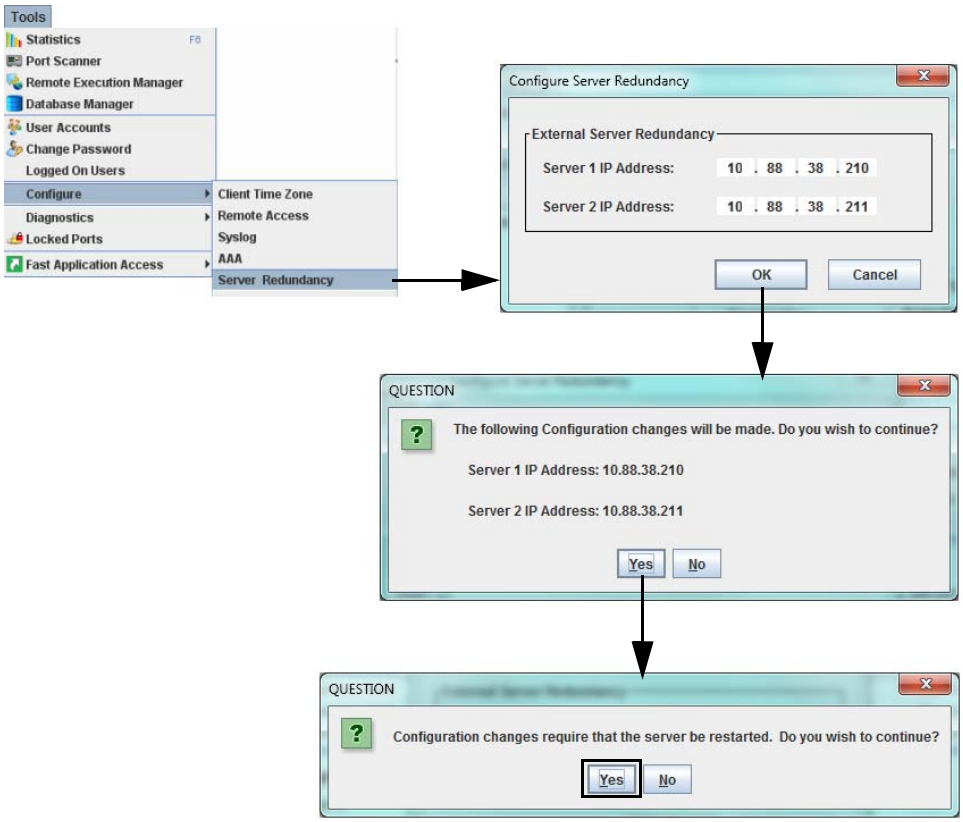
Note: The Server Redundancy option only displays in the menu when External TestStream Management server(s) are connected to the TestStream Management network.

This option allows pairing redundant servers to accommodate changing network requirements. It does not configure the actual IP addresses of the servers.

Note: IP Address Range Notice
The following range of IP addresses are NETSCOUT reserved for the nGenius 3900 series switches and must not be assigned to your TestStream Management network:
172.16.0.0/24 or **192.168.0.0/24**.

Important: Do not assign an IP address for an External TestStream Management server unless a TestStream Management server is physically connected and operational in the TestStream Management network.

1 From the toolbar, select **Tools > Configure > Server Redundancy**. The Configure Server Redundancy window displays, showing the currently assigned IP addresses of the TestStream Management servers.



2 In the Configure Server Redundancy section, modify the following configuration information for your network:

- Server 1 IP Address
  and if required,
- Server 2 IP Address

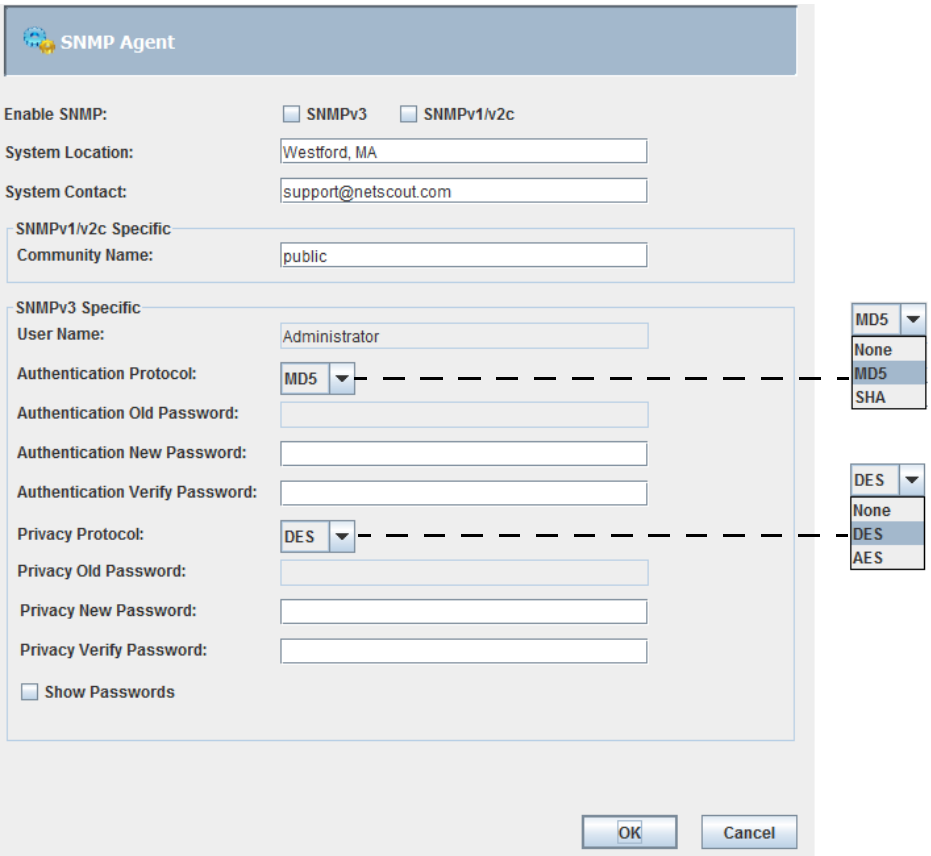
3 Click **OK** - a confirmation change screen displays - click **Yes**. Click **Yes** to the next configuration screen to save the settings. TestStream Management performs an automatic restart of the server(s) to apply the new IP address settings.

Configure SNMP

Configure SNMP (Simple Network Management Protocol) provides the ability to define SNMP v1/v2c/v3 alarm trap destinations.

SNMP Agent

1 Select **Tools > Configure > SNMP** then select **SNMP Agent**. The SNMP Agent screen displays.



2 At Enable SNMP, select the required SNMP protocol version (v1/v2c, v3, or both).

3 Enter in the System Location field the physical location of the nGenius 3900 series switch (default: Westford, MA; maximum character size is 255, no invalid characters).

4 Enter in System Contact the email / phone number for any nGenius 3900 series switch issues (default:support@netscout.com; maximum character size is 255, no invalid characters).

5 **SNMP v1/v2c Specific**:

   a Enter in the Community Name field the name used to query the nGenius 3900 series switch using SNMP v1/v2c messaging (default: public; maximum character size is 255, no invalid characters).

6 **SNMP v3 Specific**:

   a The User Name field is fixed with the default of Administrator.

   b Select the Authorization Protocol (to retrieve information from the nGenius 3900 series switch) from the drop-down list:

   – None

   – MD5 (default)

   – SHA

c Authentication Old Password displays the current / default password (default: netscout1). To change the password, enter a new password (minimum 8 characters, maximum 255, no invalid characters) in the Authentication New Password field. Reenter the new password in the Authentication Verify Password field.

d Select the Privacy Protocol (to retrieve information from the nGenius 3900 series switch) from the drop-down list:

– None

– DES (default)

– AES

e Privacy Old Password displays the current / default password (default: netscout1). To change the password, enter a new password (minimum 8 characters, maximum 255, no invalid characters) in the Privacy New Password field. Reenter the new password in the Privacy Verify Password field.

f Click **Show Passwords** to view the password text entered in step c and step e. If Show Password is not selected, dots are displayed when entering the text.

Supported SNMP MIBs

TestStream Management supports the following MIBs:

- MIB-2 System Table
- RFC 2863
  - ifTable - List of interface entries. The number of entries is given by the value of ifNumber.
  - ifXTable - List of interface entries. The number of entries is given by the value of ifNumber. This table contains additional objects for the interface table.
- RFC 2819 (RMON1)
  - etherStatsTable - List of Ethernet statistics entries.
- RFC 3273 (HCRMON)
  - etherStatsHighCapacityTable - Contains the High Capacity RMON extensions to the RMON-1 etherStatsTable.
  - hcRMONCapabilities (BITS) - An indication of the High Capacity RMON MIB groups supported on at least one interface by this probe.
- RFC 4502 (RMON2)
  - probeCapabilities (BITS) - An indication of the RMON MIB groups supported on at least one interface by this probe.

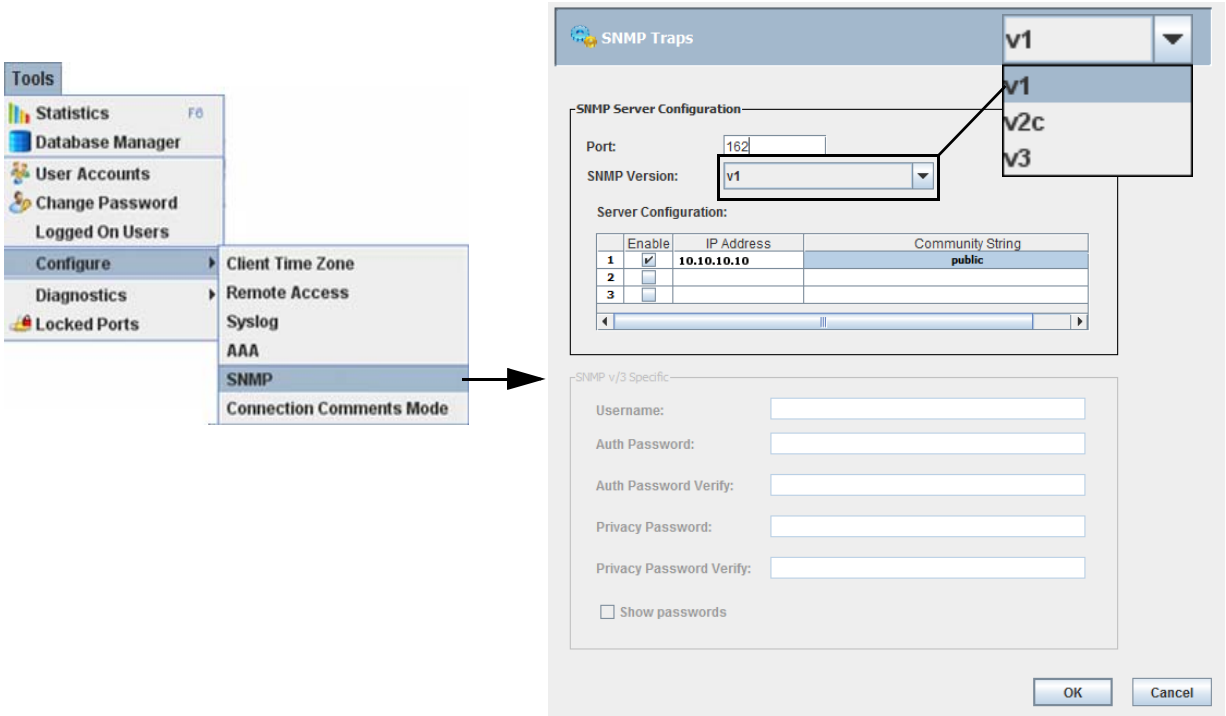
CLI Commands

SNMP traps can also be set using the following CLI commands (refer to CLI Commands, Standard Commands - TestStream Lab Manager and TestStream Controller on page A-31):

- **CONF**igure **SNMP** {**ENA**ble|**DIS**able} {v3|v1_v2|all} [**GLO**bal]
- **CONF**igure **SNMP SYSC**ontact systemcontact [**SYSL**ocation systemlocation] [**GLO**bal]
- **CONF**igure **SNMP SYSL**ocation systemlocation [**SYSC**ontact systemcontact] [**GLO**bal]
- **CONF**igure **SNMP ROCO**mmunity readonlycommunityname
- **CONF**igure **SNMP AUTH**entication {**NON**e|**MD5**|**SHA**} [**PRIV**acy {**NON**e|**DES**|**AES**}] [**GLO**bal]
- **CONF**igure **SNMP PRIV**acy {**NON**e|**DES**|**AES**} [**AUTH**entication {**NON**e|**MD5**|**SHA**}] [**GLO**bal]
- **CONF**igure **SNMP PWAU**thentication newauthpassword verifyauthpassword [**GLO**bal]
- **CONF**igure **SNMP PWPR**ivacy newprivacypassword verifyprivacypassword [**GLO**bal]
- **SHO**w **SNMP**

SNMP Traps

1 Select **Tools > Configure > SNMP**, then **SNMP Traps**. The SNMP Traps screen displays.



2 Enter the port number of the SNMP manager (default:162).

3 Select the SNMP protocol version (v1, v2c, or v3) from the drop-down menu.

4 From Server Configuration, select **Enable** to activate the SNMP trap feature on the selected server.

- Enter the Server IP address of the SNMP manager.
- Enter the community identifier. The default name is **`public`**; the character string can be up to 255 characters.

Note: Do not enter more than 255 characters in the community identifier window otherwise the SNMP Traps screen freezes. If this occurs, close the SNMP screen (click the **X**) then restart the SNMP setup session.

The following special characters can be used in the community identifier:
`~!@^_+-={}[]:,./`

---

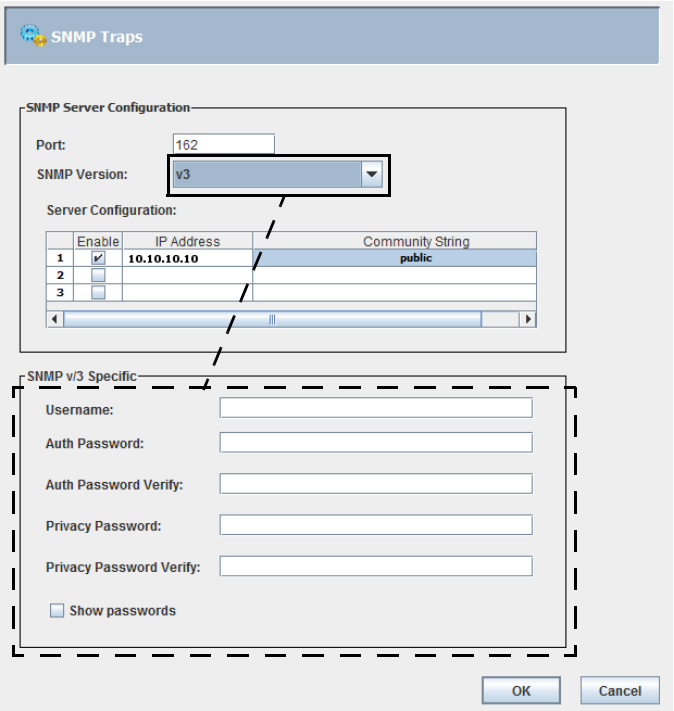
5 If SNMP v3 is selected, the SNMP v3 Specific section becomes active:

a Enter the Username for SNMP v3 authentication.

b Click **Show Passwords** to view the password text entered in step c and step d. If Show Password is not selected, dots are displayed when entering the text.

c Enter a user Authentication Password (HMAC-SHA-96 protocol; 8 to 64 characters) then re-enter to verify the password.

d Enter a Privacy Password (CFB-AES-128 encryption; 8 to 64 characters) for SNMP v3 encryption then re-enter to verify the password.



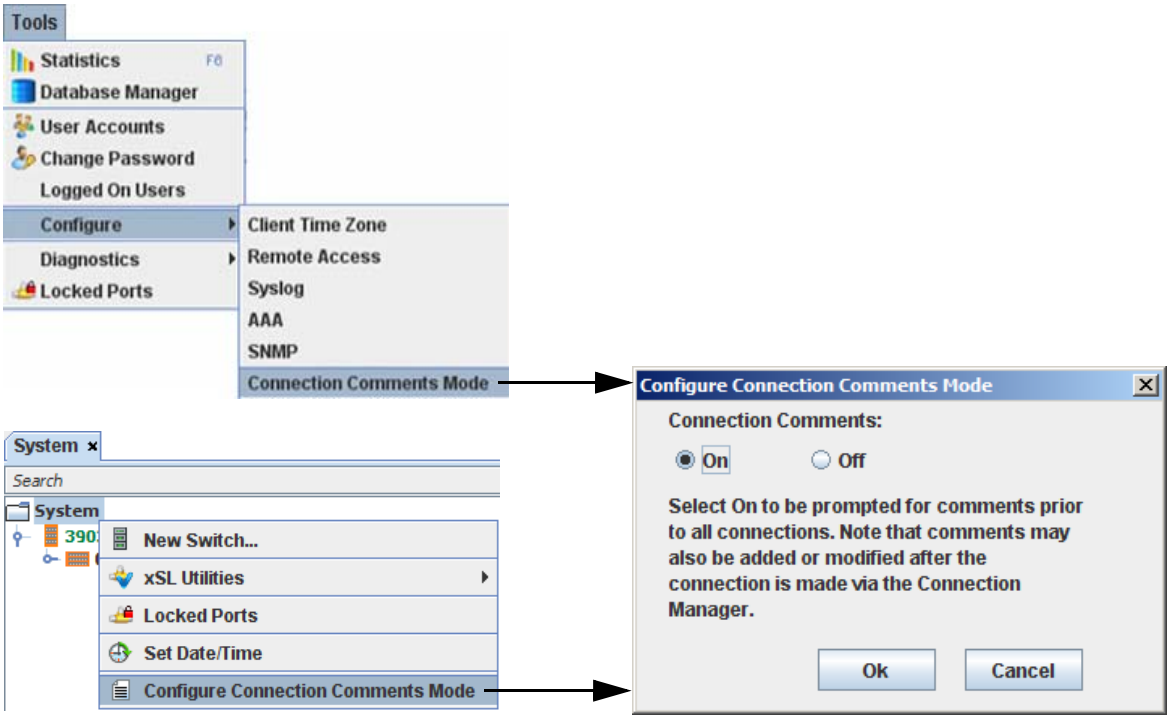
6 Click **Cancel** to end the SNMP configuration without saving the entered settings. Click **Ok** to save the SNMP settings.

Connection Comments Mode

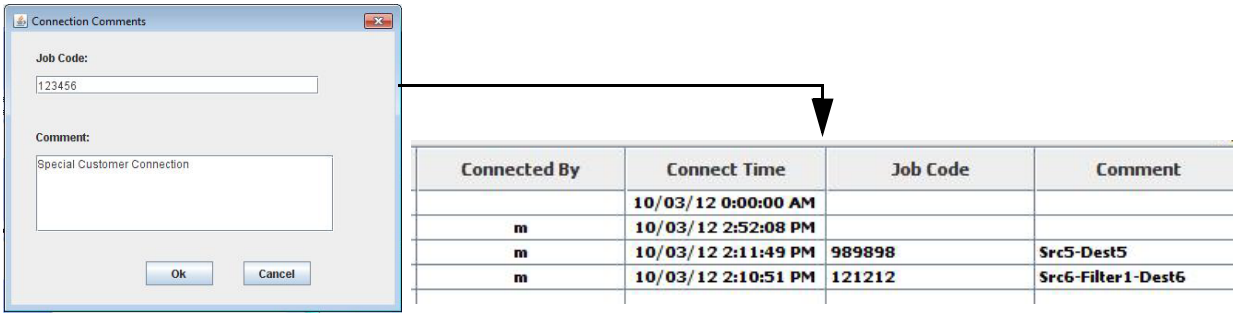
Connection Comments Mode allows adding annotations to connections, made from the Topology Manager, and displayed in the Connection Manager.

1 Select **Tools > Configure > Connection Comments Mode** or from the System tab, right-click on System and select **Configure Connection Comments Mode**. The Configure Connection Comments Mode screen displays.

2 Select **On** then click **OK**.



With Connection Comments set to **On**, whenever a packet/port connection is defined for connection in the Topology Manager, a Connection Comments screen is displayed. Enter information in the Job Code / Comments columns pertaining to the connection, then click **OK**. The connection is completed in the Topology Manager with the connection and comments displayed in the Connection Manager fields. Updates to the Job Code and Comment fields can also be made by clicking on the respective fields and entering the information.

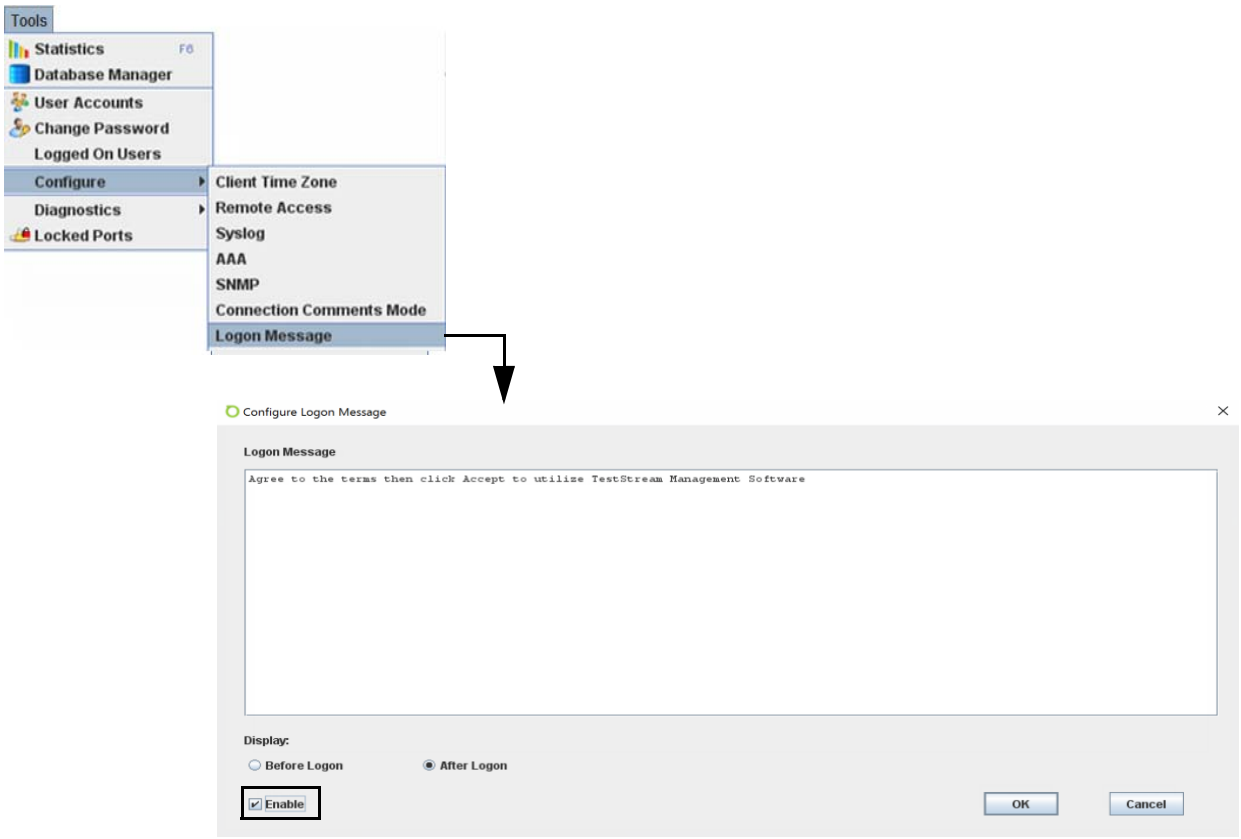


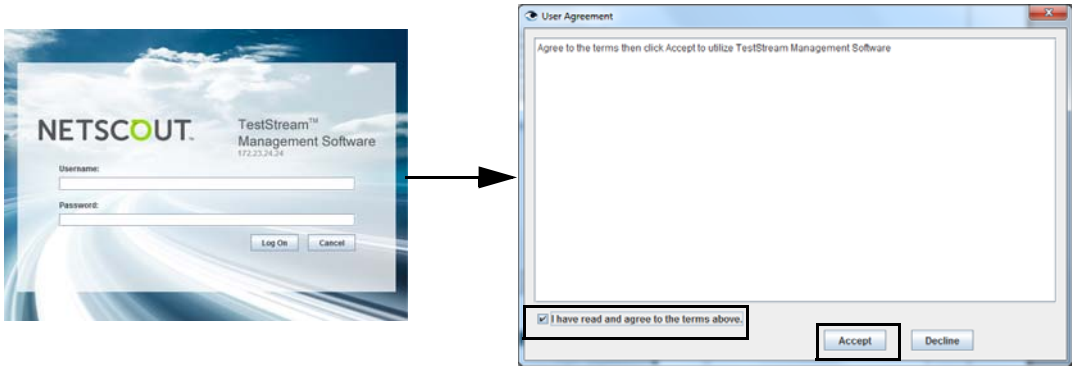
Connected By	Connect Time	Job Code	Comment
	10/03/12 0:00:00 AM		
m	10/03/12 2:52:08 PM		
m	10/03/12 2:11:49 PM	989898	Src5-Dest5
m	10/03/12 2:10:51 PM	121212	Src6-Filter1-Dest6

Configure Logon Message

Logon Message provides the ability to display a message, similar to the message of the day (MOTD) to users before or after logging on to the TestStream Management GUI or from a CLI user logon. When this message appears, users must select **Accept** to proceed. If **Decline** is selected, the session ends. The login message can display legal disclaimers or any message an administrator wishes to share with other TestStream Management users. REST API supports displaying the after logon message. The message is returned as part of the login response.

1 Select **Tools > Configure > Logon Message**. The Configure Logon Message screen displays.





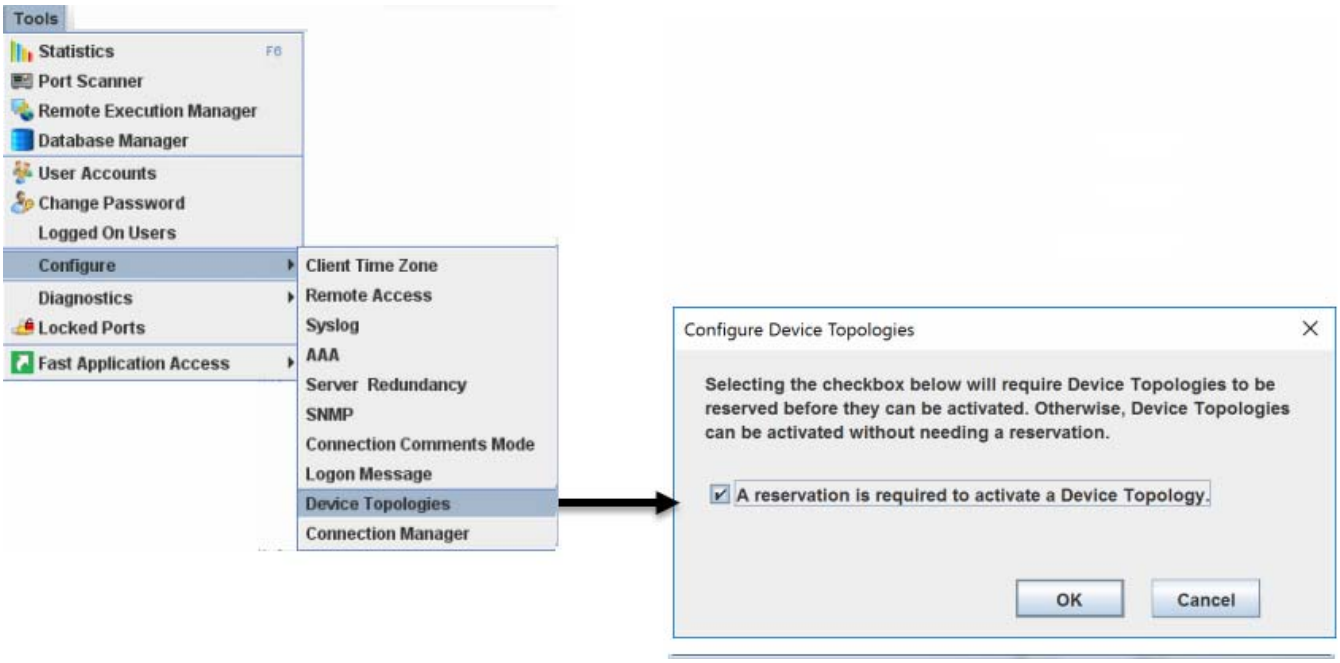
2 In the Logon Message field, enter the required text (up to 10,000 characters) to be displayed after the TestStream Management GUI logon.

3 Select **Before Logon** or **After Logon**, then select **Enable** to activate the message display, then **OK** to save the message. To turn off the logon message display, unselect Enable, then OK to save the changes. The message remains in the text field for future use or editing as required.

Configure Device Topologies (TestStream Lab Manager Only)

For users that only want to use the device/device port/device topologies feature without reservations, a system setting (Tools => Configure => Device Topologies) will allow the customer to disable reservations. In this case, from an activation/deactivation point of view, the device topologies will behave like standard topologies.

1 Select **Tools > Configure > Device Topologies**. The Configure Device Topologies screen displays.



2 By selecting the checkbox, Device Topologies need to be reserved before they can be activated. If the checkbox is left unselected, then Device Topologies can be activated without needing a reservation.

3 Click on **OK** to save the selection.

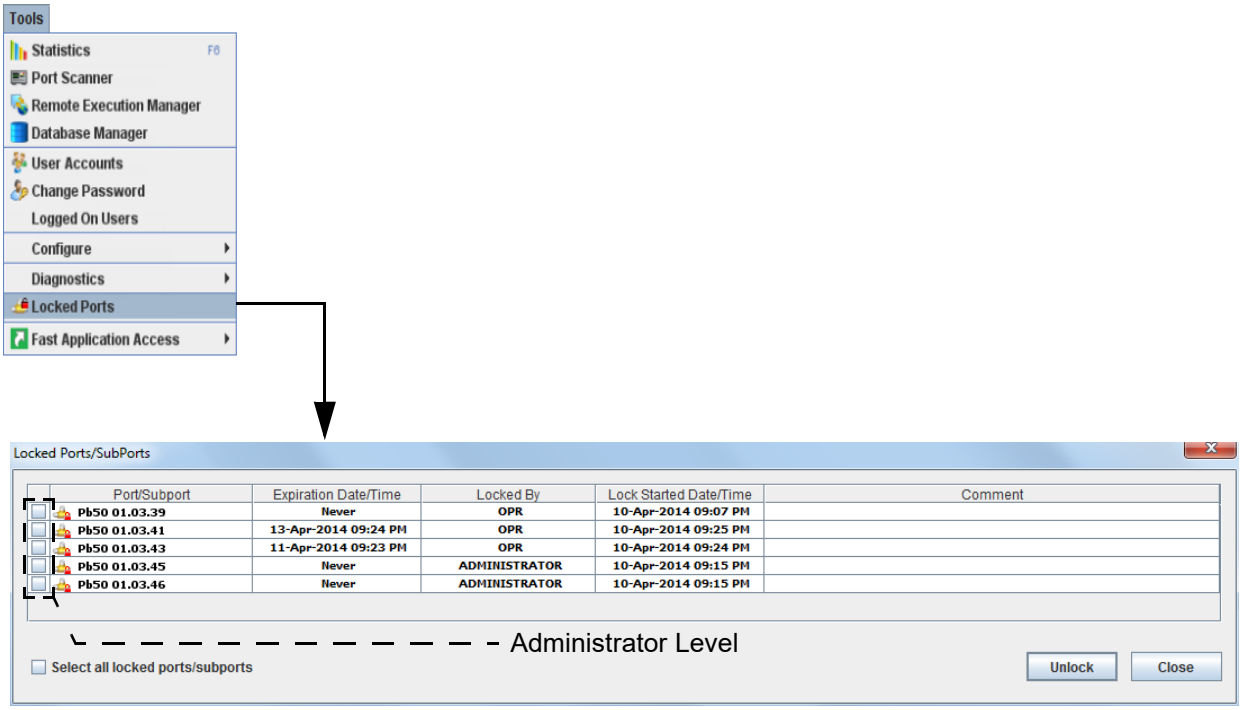
Diagnostics

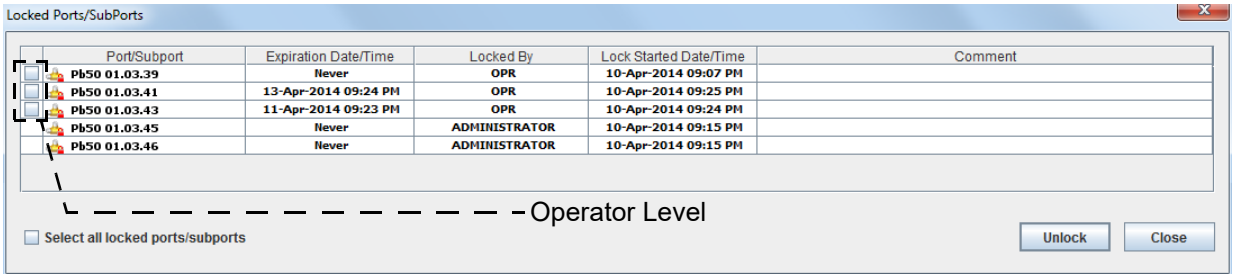
Refer to Diagnostics and System Tests on page 7-1.

Locked Ports

The locked ports screen displays all assigned locked ports / subports (refer to Port Lock Settings on page 3-98).

Select **Tools > Locked Ports**. The Locked Ports screen displays.





The screen shows the locked ports, date/time locking ends, the users who initiated different port locks, the date/time the locks started, and comments entered.

Note: If port lock setting Unlimited is selected for a port, the Expiration Date/Time field for that port displays **Never**.

Individual locked ports, assigned by the logged-in user, can be selected, for unlocking or click **Select all locked ports** to unlock all of the ports at once.

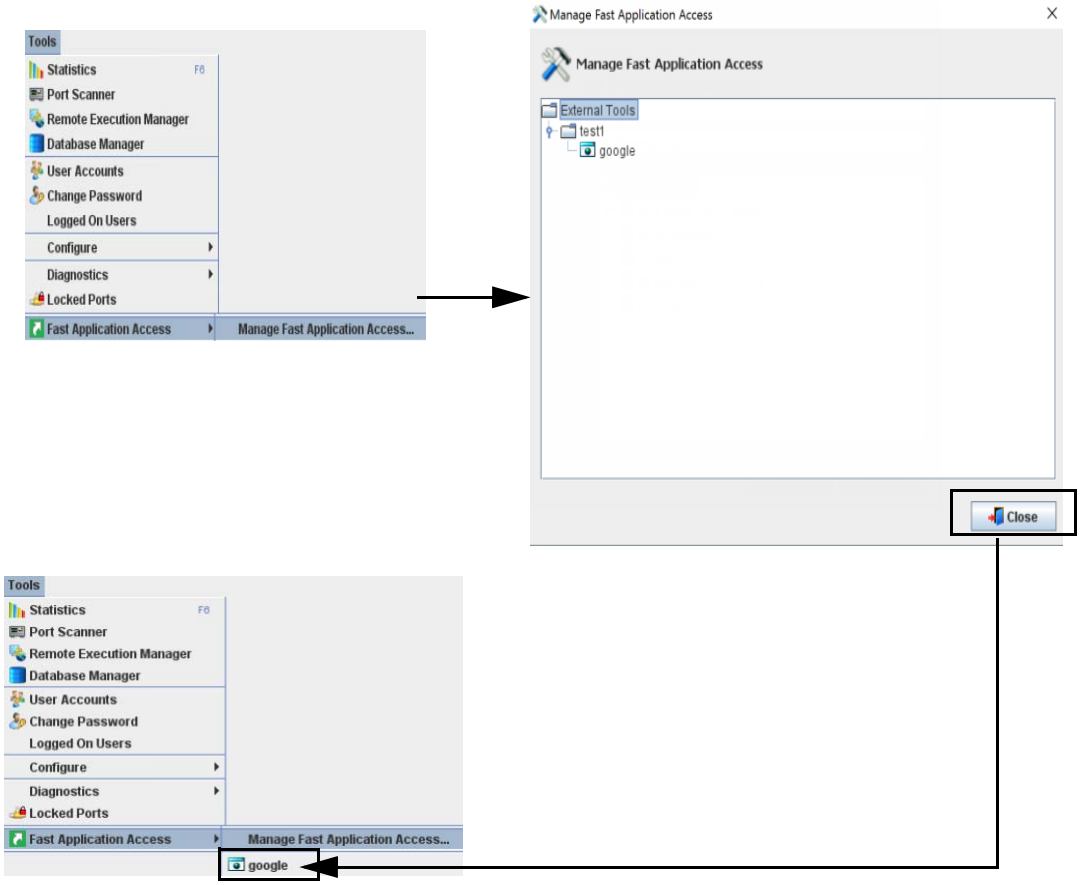
Note: Users with administrator level access can select, regardless of port ownership, any of the listed ports for unlocking.

Fast Application Access (TestStream Lab Manager Only)

The Fast Application feature is used for accessing an external application or resource to control test equipment or start third-party management applications.

Add an Application

1 From the Tools menu, select **Fast Application Access> Manage Fast Application Access**. The Manage Fast Application screen displays.



2 To add an application or folder, right-click the External Tools folder and select from the following:

- Folder - enter a New Folder name
- Remote Desktop - enter a name for the tool, computer name/IP address, username/password, and select if you want to make the application visible to all users
- Local CMD - enter a name for the tool, a command line, select if you want to wait for the command to finish before the GUI closes the window (you can also enter a specific timeout), and select if you want to make the application visible to all users
- SSH CMD - enter a name for the tool, the IP address/port, username/password, a command line, select if you want to wait for the command to finish before the GUI closes the window (you can also enter a specific timeout), and select if you want to make the application visible to all users
- URL - enter a name for the tool, the URL, and select if you want to make the application visible to all users

Note: If the "Visible to all users" option is selected, all users will be able to access, modify, or delete this tool. If it is not selected, then only the creator and an admin level user will be able to do so.

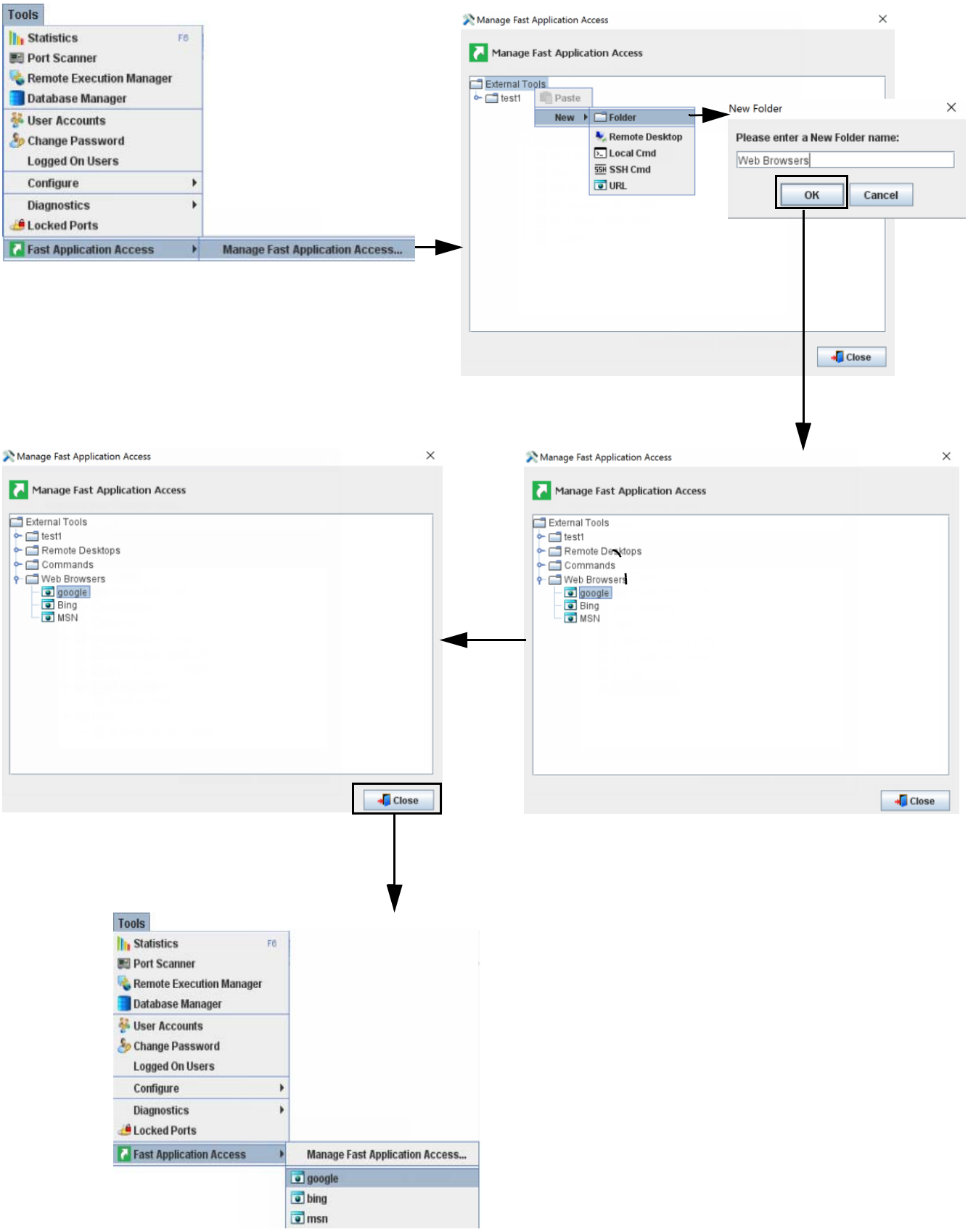
3. After you have configured your new application, click **OK**. The new link is displayed in the Fast Application Access menu.

Organize Applications

The list of saved tools can be moved to self-defined sets of folders, similar to Internet favorite folders, for ease in locating a particular tool.

1. Select **Tools > Fast Application Access> Manage Fast Application Access**. The Manage Fast Application Access screen displays.
2. Right-click on the External Tools folder and select **New Folder**. Enter the new folder name and click **OK**. The new folder is added to the tree listing. Click **Close** to save the updates.
3. Repeat step 2 as required for any additional folders.
4. From the Manage Fast Application Access screen, the individual tool links can now be moved to the new defined folders by dragging the link names to the folders.

   You can also copy applications from one folder to another, but when you paste the application in the new folder you must enter a new name for the application.

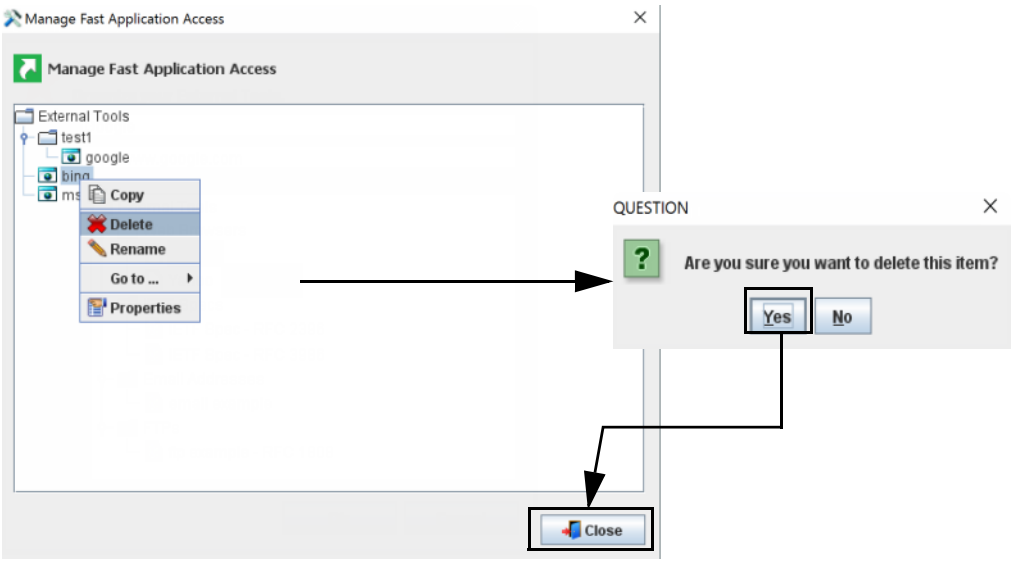

Tools
Statistics F8
Port Scanner
Remote Execution Manager
Database Manager
User Accounts
Change Password
Logged On Users
Configure
Diagnostics
Locked Ports
Fast Application Access
Manage Fast Application Access...
Manage Fast Application Access
Manage Fast Application Access
External Tools
test1
Paste
New
Folder
Remote Desktop
Local Cmd
SSH Cmd
URL
New Folder
Please enter a New Folder name:
Web Browsers
OK
Cancel
Close
Manage Fast Application Access
Manage Fast Application Access
External Tools
test1
Remote Desktops
Commands
Web Browsers
google
Bing
MSN
Close
Manage Fast Application Access
Manage Fast Application Access
External Tools
test1
Remote Desktops
Commands
Web Browsers
google
Bing
MSN
Close
Tools
Statistics F8
Port Scanner
Remote Execution Manager
Database Manager
User Accounts
Change Password
Logged On Users
Configure
Diagnostics
Locked Ports
Fast Application Access
Manage Fast Application Access...
google
bing
msn

Delete an Application

External Tool links can be removed as necessary.

1 Right-click on the tool name and select **Delete**.

2 Click **Yes** to the confirmation question, then click **Close.**

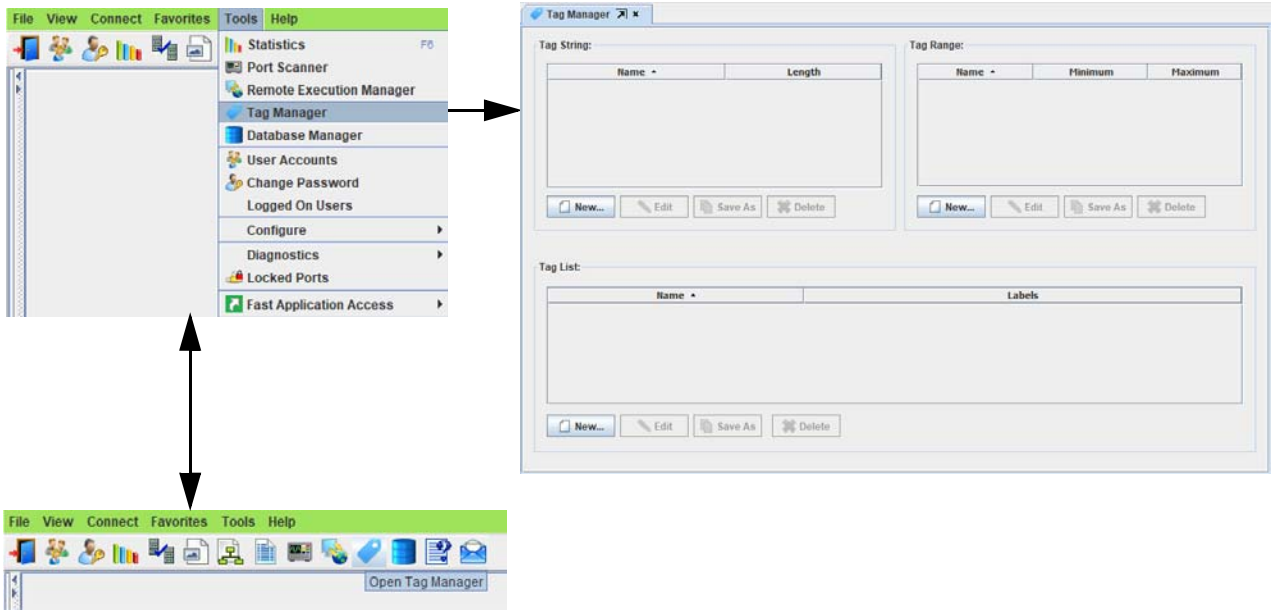


Tag Manager

Tag Manager utilities are available to manage user defined tags. The utilities are:

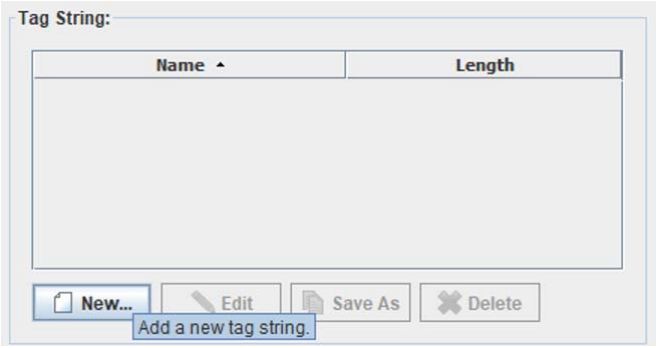
- Tag String on page 4-50
- Tag Range on page 4-51
- Tag List on page 4-53

To access the Tag Manager utilities, select **Tools > Tag Manager**, or from the toolbar, select the **Tag Manager** icon. The Tag Manager screen displays.

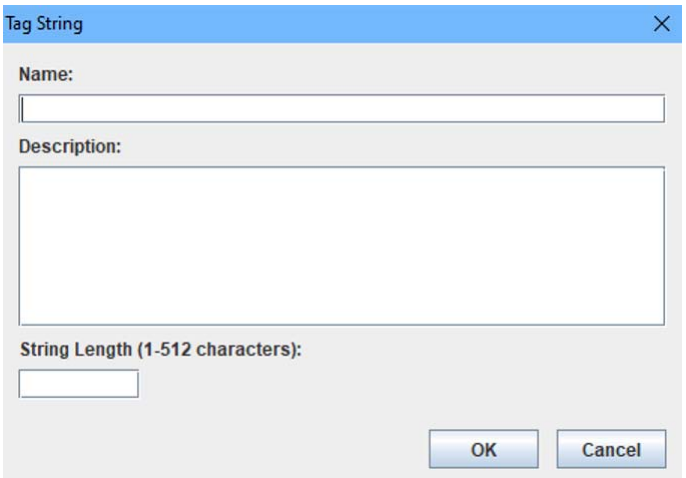


Tag String

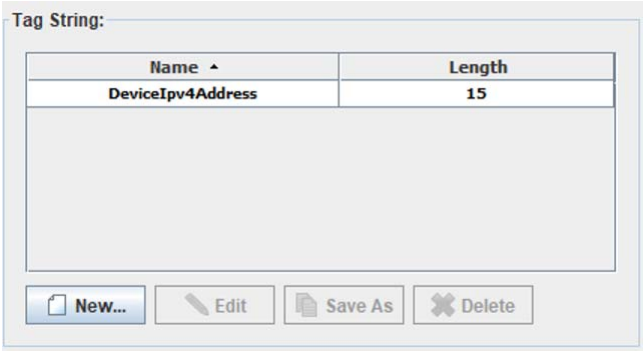
To add a new tag string, click the **New...** button in the **Tag String:** section.



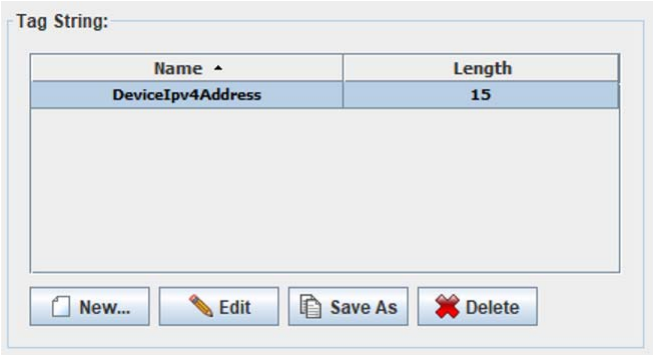
In the **Tag String:** window, fill in the **Name:**, **Description:** (optional), and **String Length** fields. The **Description** field will be displayed as help in the device and topology tag instances window.



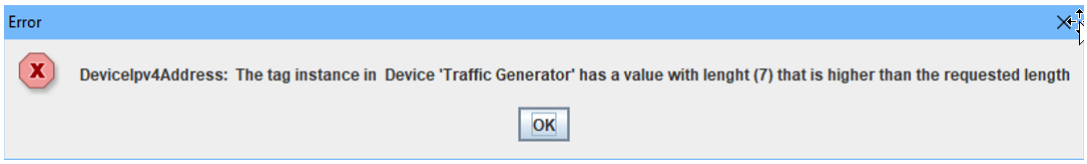
After the fields are filled in, click the **OK** button.



Selecting a tag string will enable the **Edit**, **Save As**, and **Delete** buttons.

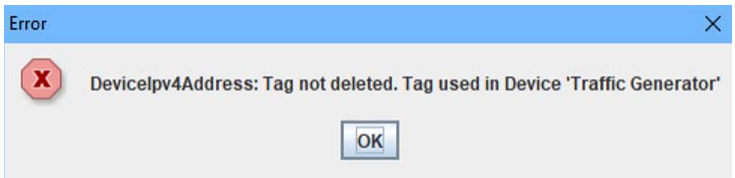


Clicking the **Edit** button displays the **Tag String** window where the fields **Name:**, **Description:**, and **String Length** can be modified. When done click the **OK** button. If the **String Length** field decreases in value and there are tag instances of this user defined tag with a length bigger then the new value, then the edit will be rejected, and an error window will be displayed.



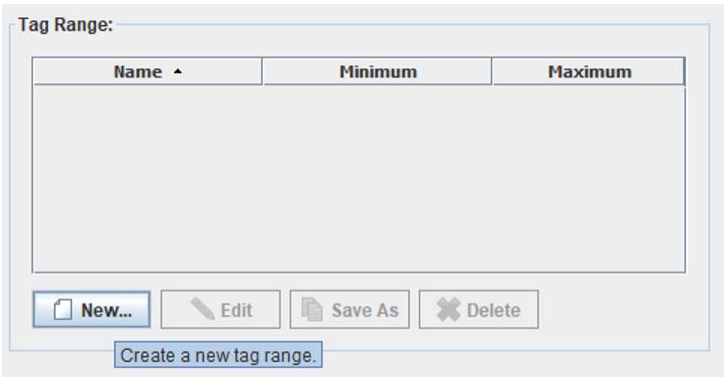
Clicking the **Save As** button displays the **Tag String** window with the current values for the **Name:**, **Description:**, and **String Length** fields. Once the desired changes are made click the **OK** button and a new tag is created (the **Name** field must be updated before clicking the **OK** button).

Clicking the **Delete** button will remove the tag from the system. If a device or a topology has an instance of the user defined tag to be deleted, the deletion will fail and an error window will be displayed, identifying the devices and topologies that have a tag instance of the user defined tag to delete.

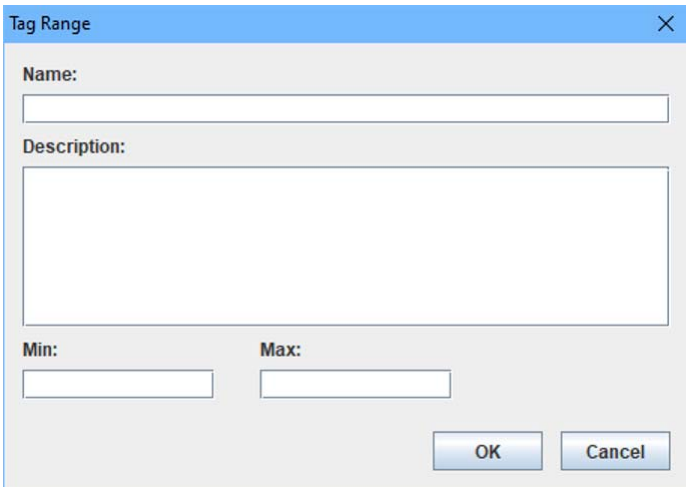


Tag Range

To add a new tag range, click the **New...** button in the **Tag Range:** section.

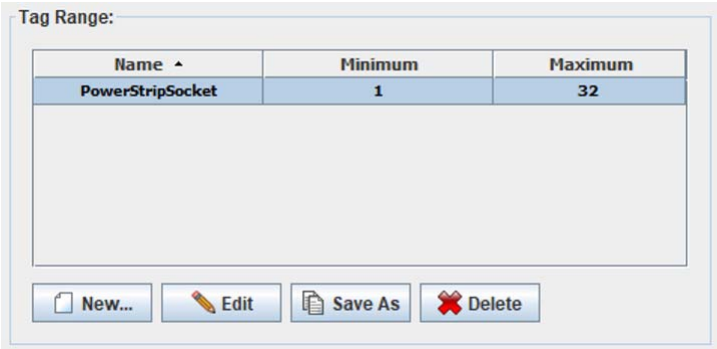


In the **Tag Range** window, fill in the **Name:**, **Description:** (optional), **Min:**, and **Max:** fields. The **Description** field will be displayed as help in the device and topology tag instances window.

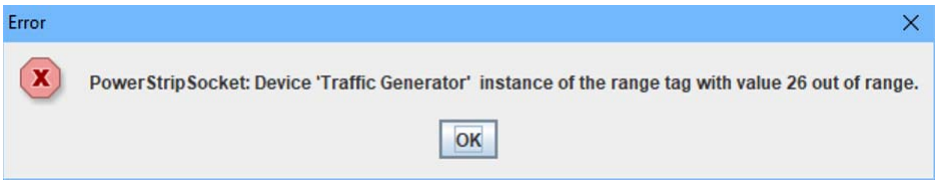


After the fields are filled in, click the **OK** button.

Selecting a tag range will enable the **Edit**, **Save As**, and **Delete** buttons.

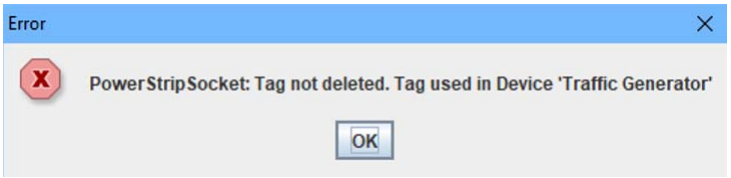


Clicking the **Edit** button displays the **Tag Range** window where the fields **Name:**, **Description:**, **Min:** and **Max:** can be modified. When you are done, click the **OK** button. If the **Min:** or **Max:** fields were modified and there are tag instances of this user defined tag with value that will be outside the updated range, then the edit will be rejected, and an error window will be displayed.



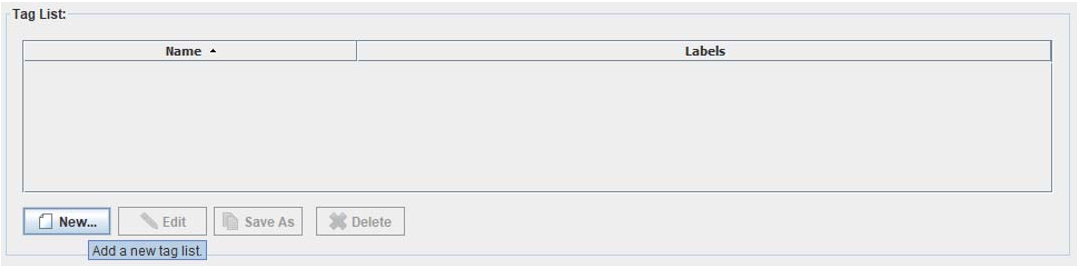
Clicking the **Save As** button displays the **Tag Range** window with the current values for the **Name:**, **Description:**, **Min:**, and **Max:** fields. Once the desired changes are made click the **OK** button and a new tag is created (the **Name** field must be updated before clicking the **OK** button).

Clicking the **Delete** button will remove the tag from the system. If a device or a topology has an instance of the user defined tag to be deleted, the deletion will fail, and an error window will be displayed identifying the devices and topologies that have a tag instance of the user defined tag to delete.

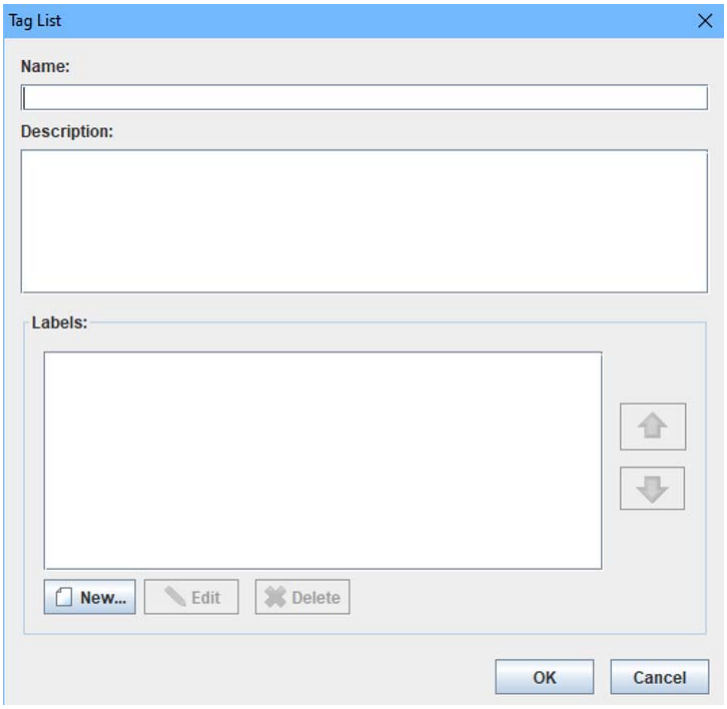


Tag List

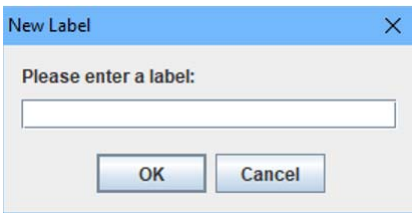
To add a new tag list, click the **New...** button in the **Tag List:** section.



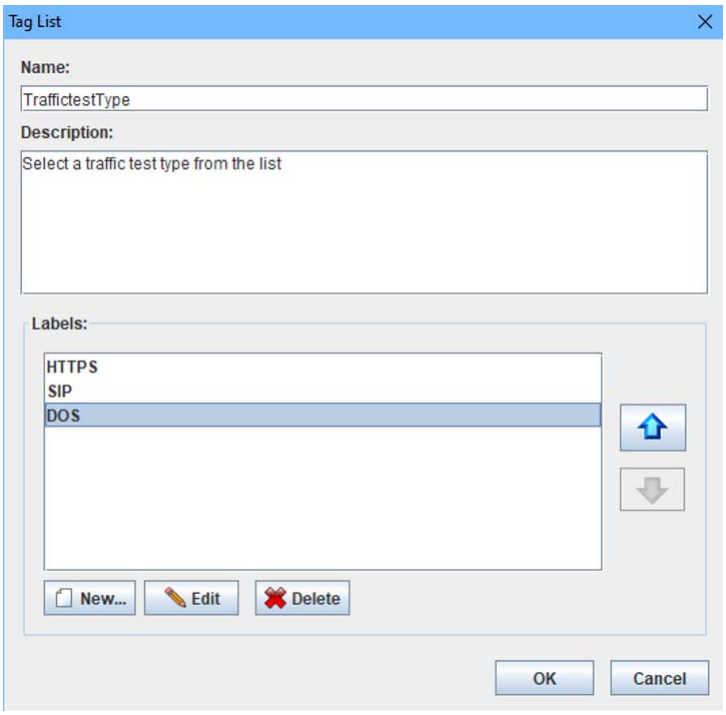
In the **Tag List** window, fill in the **Name:** and **Description:** (optional) fields. The **Description** field will be displayed as help in the device and topology tag instances window.



Then add the desired labels by clicking the **New** button in the **Labels:** section.

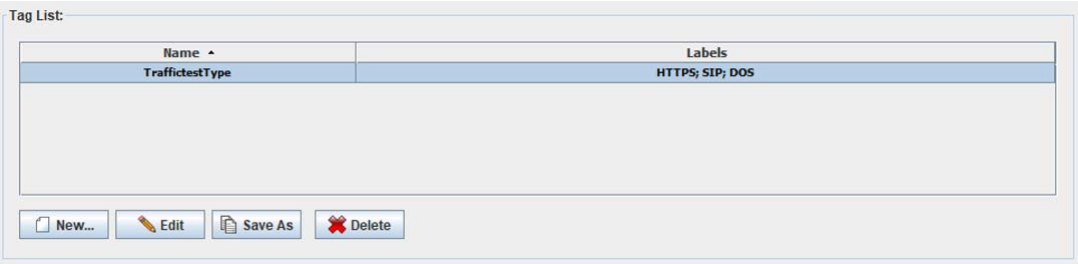


After labels are added, the **Edit** and **Delete** buttons of the **Labels** section are enabled. Labels positions can be changed with the **Up** and **Down** buttons.

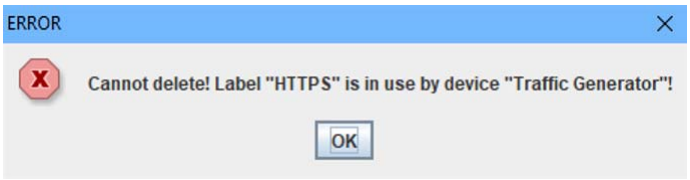


After the fields are filled in, click the **OK** button.

Selecting a tag list will enable the **Edit**, **Save As**, and **Delete** buttons.



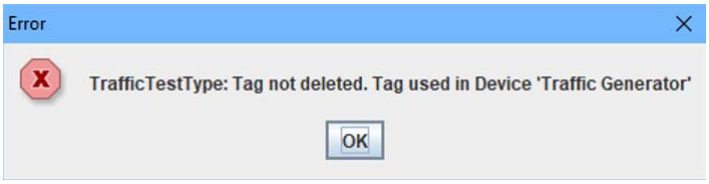
Clicking the **Edit** button displays the **Tag List** window where the fields **Name:**, **Description:**, and **Labels:** can be modified. Deleting a label that is used by tag instances of this user defined tag will be rejected, and an error window will be displayed.



When done click the **OK** button.

Clicking on the **Save As** button displays the **Tag List** window with the current values for the **Name:**, **Description:**, and **Labels:** fields. Once the desired changes are made click the **OK** button and a new tag is created (the **Name** field must be updated before clicking the **OK** button).

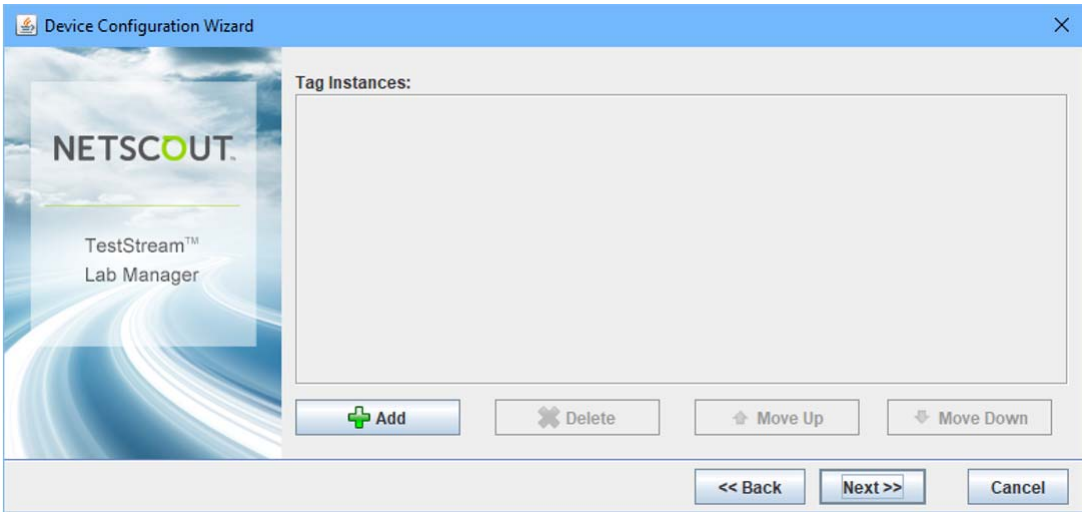
Clicking the **Delete** button will remove the tag from the system. If a device or a topology has an instance of the user defined tag to be deleted, the deletion will fail, and an error window will be displayed identifying the devices and topologies that have a tag instance of the user defined tag to delete.

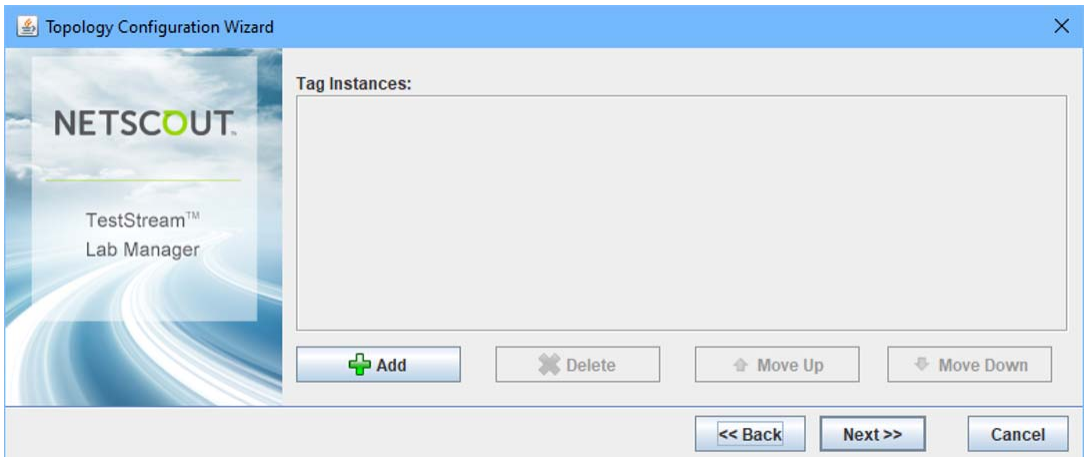


Tag Instances

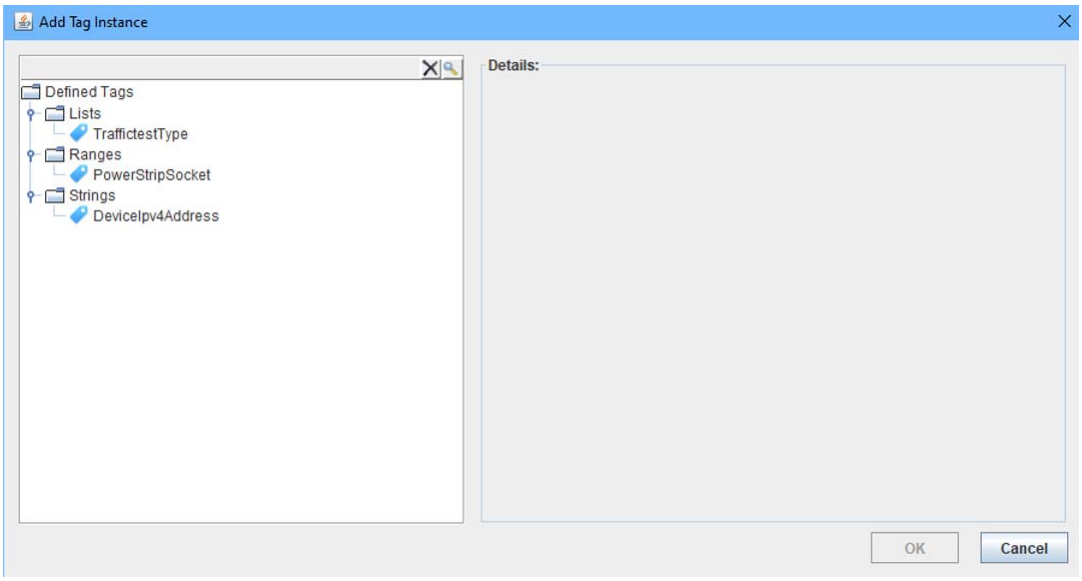
User defined tags can be given values by creating instances in devices and topologies. These instances can be added at the time that a device or topology is created or at the time it is revised.

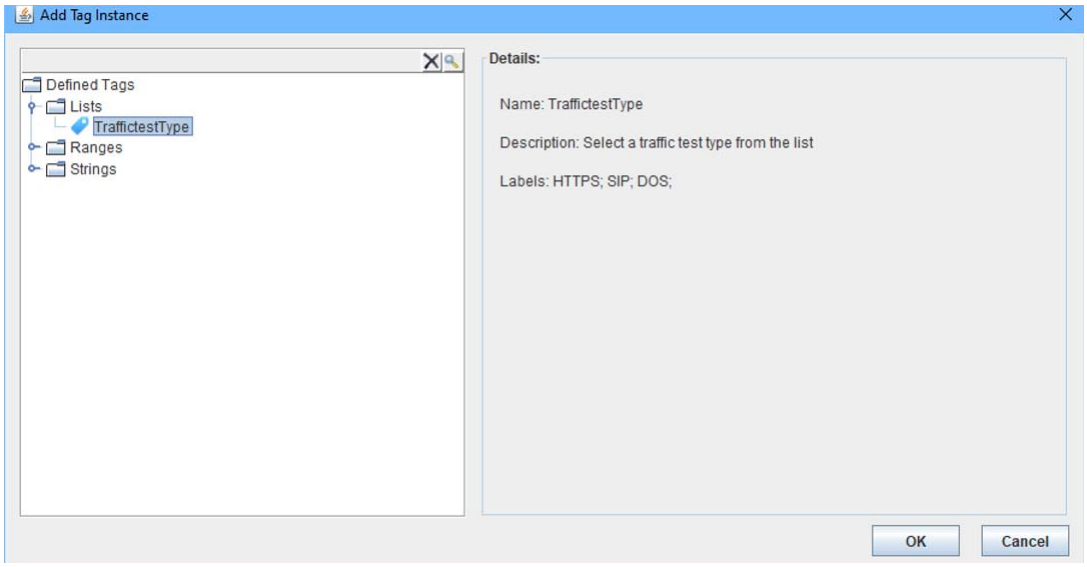
The **Device Configuration Wizard** and the **Topology Configuration Wizard** will have a new step before the **Fast Application Access** step, where tag instances can be added.



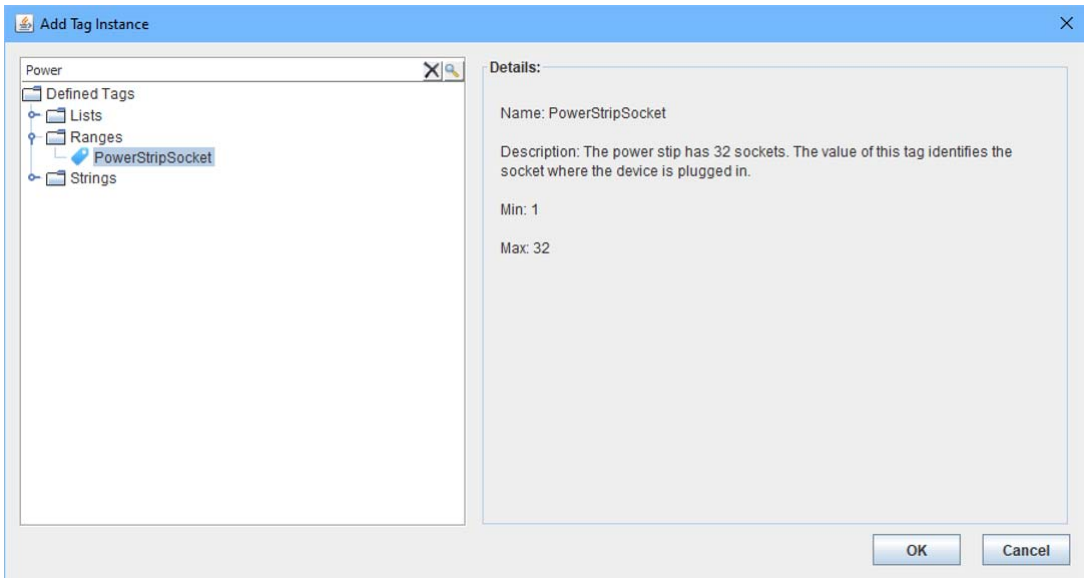

Topology Configuration Wizard
NETSCOUT
TestStream™
Lab Manager
Tag Instances:
Add
Delete
Move Up
Move Down
<< Back
Next >>
Cancel

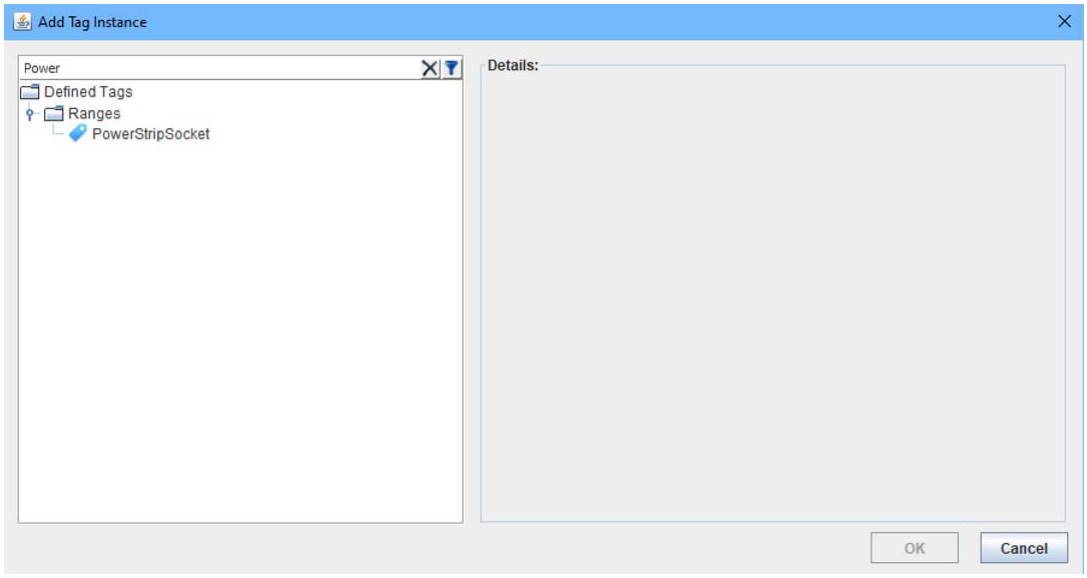
Clicking the **Add** button displays the **Add Tag Instance** window. In this window, the left pane shows the user defined tags in a tree like structure with folders for each user defined tag type. These folders can be expanded and compacted. When expanded it will show all the user defined tags of the corresponding type. The **Details:** pane on the right displays a user defined tag detail when the user defined tag is selected (clicked on) in the left pane.



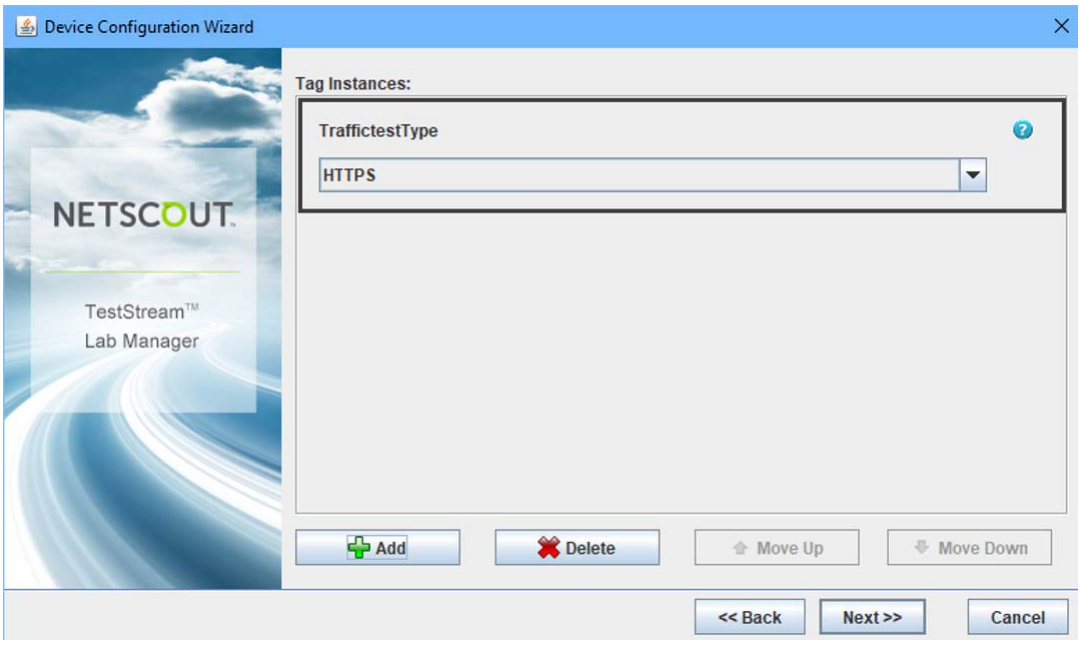


The tree of user defined tags can also be searched or filtered.

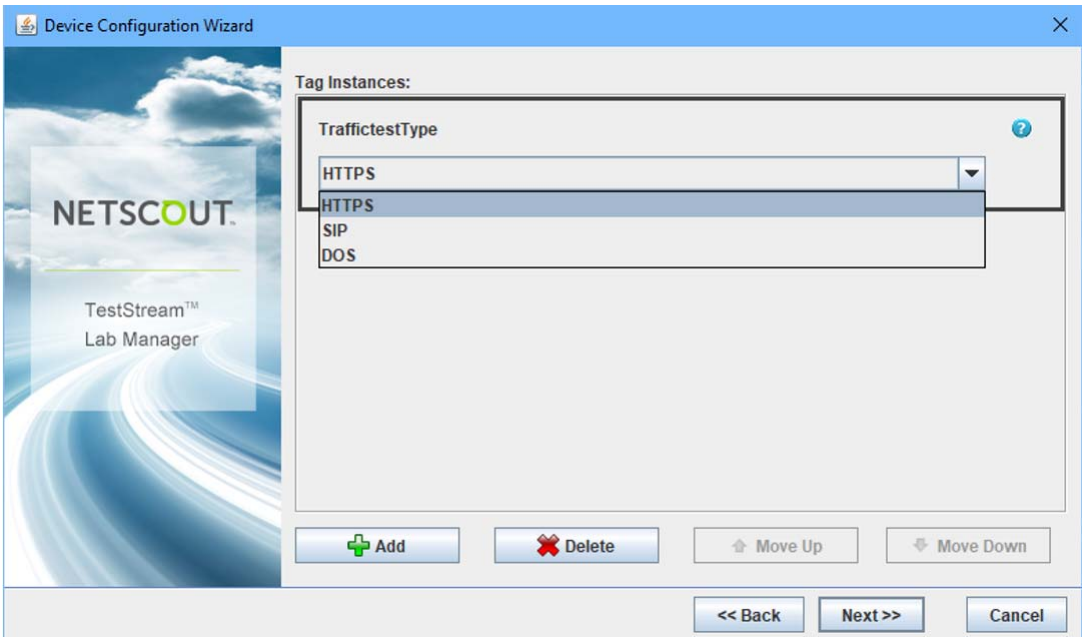




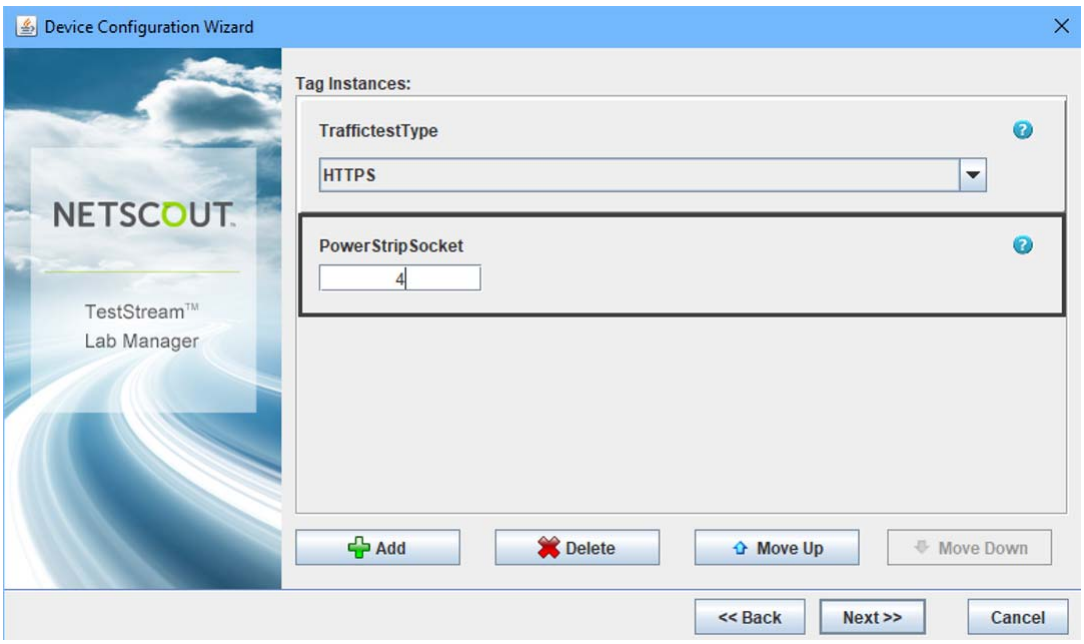
After the desired user defined tag is found, select it by clicking on it and then click the **OK** button. The added user defined tag will be displayed in the configuration wizard **Tag Instances** window.



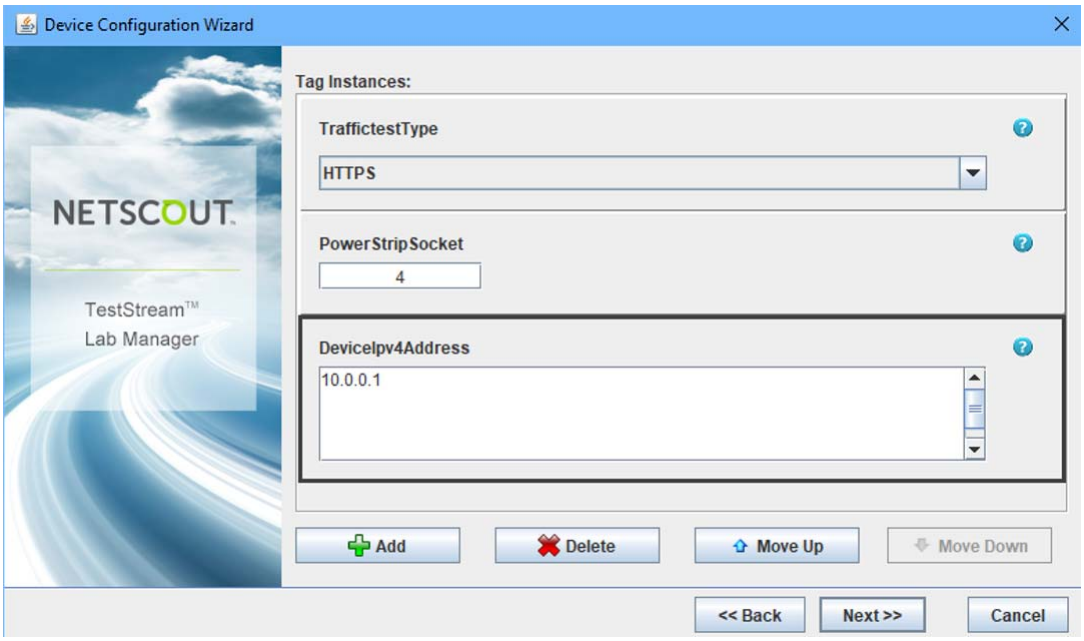
Once added, the user can change the value of the instance of the user defined tag. For list tags, select a value from the drop-down list.



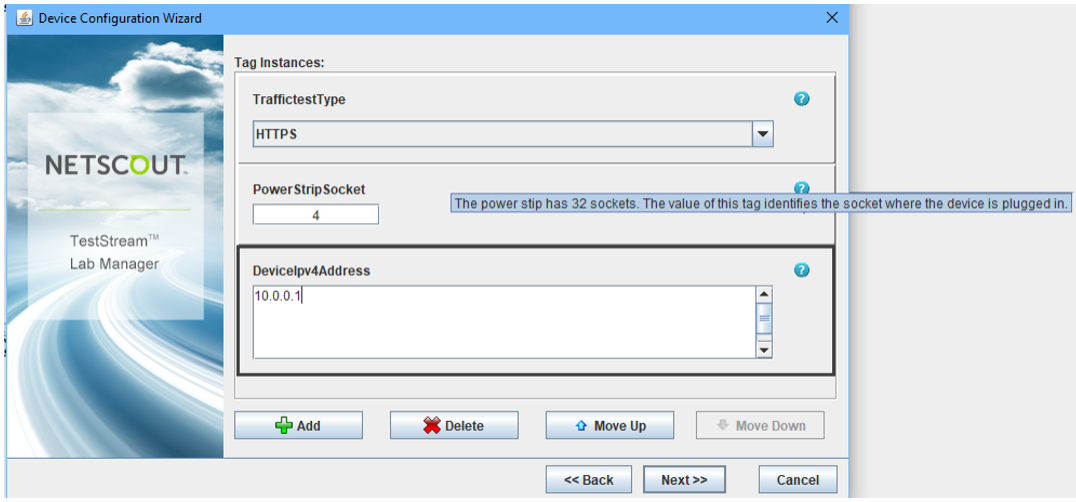
For range tags, type the desired value within the range tag min. and max. value.



For string tags, type the desired characters up to a max. number of characters define by the string tag.



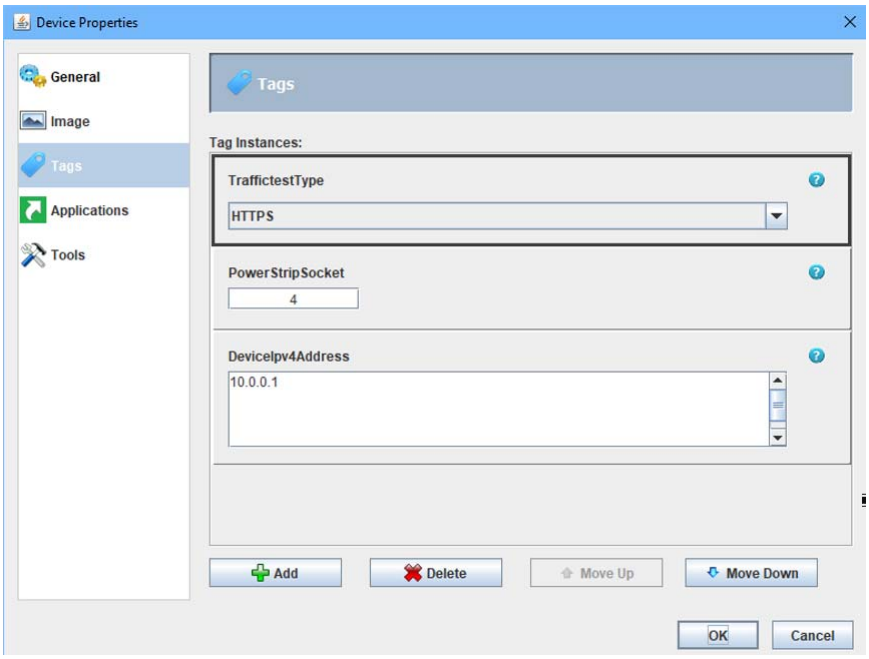
Placing the mouse pointer on a help icon displays the description of the user defined tag as a tooltip.



Tag instances can be deleted. Select a tag instance by clicking it (its border will be shown in bold line) and then click the **Delete** button.

The tag instances order can be modified using the **Move Up** and **Move Down** buttons (select a tag instance by clicking it and then use these buttons to move the tag instance up or down). The order selected is the order in which the tag instances will be displayed in the device and topology properties window. When done configuring the tag instances, click the **Next** button.

The tag instances of a device or topology can be revised by accessing the properties window. When the **Device Properties** or **Topology Properties** window is open, select **Tags** on the left pane.



Select the desired tag instance by clicking it and then edit its value. As with the configuration wizard, tag instances can be added, moved up/down and deleted. When done click the **OK** button.

System Tags

System tags are identified by their unique name and start with the string **ts-**.

The following system tags are supported (tag names listed):

- ts-server-ipv4-address

  This tag value is the IPv4 address of the active server. This tag is available in FAAs or local tools. This tag is available in REMs.

- ts-topology-name

  This tag is available if the FAA or local tool was invoked from a topology. This tag value is the name of the topology in whose context the FAA, local tool or REM has been invoked. This tag is available in REM.

- ts-device-name

  This tag is available if the FAA or local tool was called from a device or a device port. This tag value is the name of the device in whose context the FAA, or local tool has been invoked.

- ts-username

  This tag is available in FAAs or local tools. This tag value is the username of the user that invoked the FAA or local tool. This tag is available in REMs and its value is the username that scheduled the reservation using REM.

If an FAA or local tool is called from a context that does not support a system tag, the call is rejected and the error message identifies the system tag that is invalid in the calling context.

TestStream Management Software supports using system tags in FAAs or local tools. TestStream Management Software supports using system tags in REMs. The user uses the name of a system tag in between @@ characters (2 @ at the beginning and 2 @ at the end) in the same fields that support the user defined tags feature. At the time of invocation, the system tag shall be replaced by its value.

On Demand Tag Value Selection

In local tools or FAA entries, if a user defined tag name is used in between ^ ^ (2 ^ at the beginning and 2 ^ at the end), instead of being replaced by its value, the user is prompted to select a value at the time the local tool or FAA entry is invoked.

FAA and Local Tools

When an FAA is associated to a device or a topology, TestStream SW does not check whether the FAA uses user defined tags or system tags. At the time an FAA that uses user defined tags is invoked and the device or topology does not have an instance of all the user defined tags used, the FAA call is rejected and an error message is sent to the user as a response. This error message provides a list of the user defined tags that the device or topology does not have instances of.

At the time an FAA that uses system tags is invoked and the device or topology does not support the system tags used, the FAA call is rejected and an error message is sent to the user as a response. This error message provides a list of system tags that the device or topology does not support.

When a local tool is defined, TestStream SW does not check whether the local tool uses user defined tags or system tags. At the time a local tool that uses user defined tags is invoked and the device or topology does not have an instance of all the user defined tags used, the local tool call is rejected and an error message is sent to the user as a response. This error message provides a list of user defined tags that the device or topology does not have instances of.

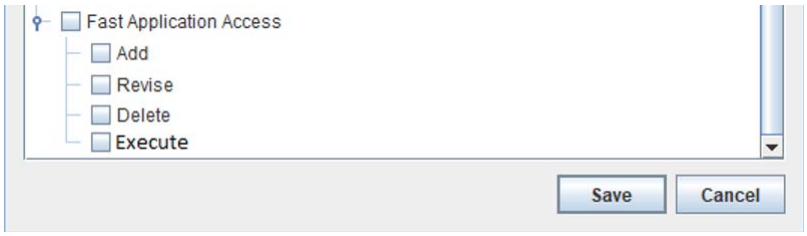
At the time a local tool that uses system tags is invoked and the device or topology does not support the system tags used, the local tool call is rejected and an error message is sent to the user as a response. This error message provides a list of system tags that the device or topology does not support.

Domains

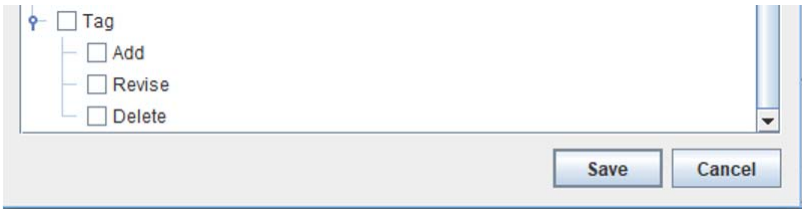
Tags are available to all users and all the devices/device ports. Users can set the tag value of a device/device port only if the device is in their domain.

Security

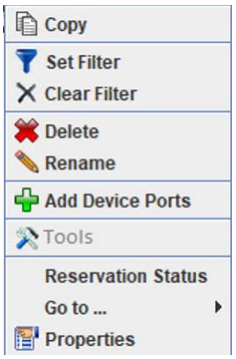
By default, the administrator, operator and diagnostics users have the rights to execute FAAs. Viewer users are not able to execute FAAs. Custom users can be configured to have rights to execute FAAs.



A new security entry is added to the security levels configuration: **Tags** with option to **Add**, **Revise** and **Delete**. Administrator, operator and diagnostics levels have these items checked. These items allow a user to manage user defined tags. The assignment of tags to devices or topologies is part of the device and topology security settings (add/revise/delete item).

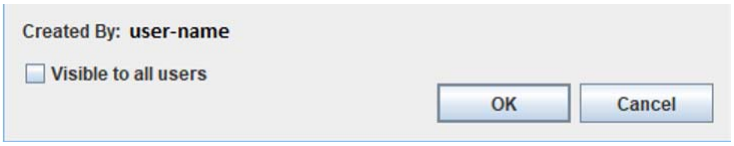


The Java Client grays out the **Tools** entry in the context sensitive menu for topologies, device and device ports if the user does not have the rights to execute FAAs. For example, for the device context sensitive menu (RMC):



Visibility

At the time an FAA or local tools is created the user selects its visibility.



To run an FAA or local tool, the user has to have visibility to access it and have rights to execute FAAs.

Auto-completion

When configuring an FAA or local tool (or possibly Remote Execution Profile or Reservation Remote Execution) the user types the start of a tag delimiter "@@.. " or "^ ^.. " and the system provides auto-complete (the GUI displays a list of tags that match the characters already typed like in IDEs).

Export and import of tags

The system supports exporting and importing tags. The main use case is to facilitate users to edit tags outside the GUI. The file used for import/export follows a well specified syntax (for example, XML based with specific elements) and a document is provided to users describing it.

Importing a file does not remove any tag that is not listed in the imported file. This allows users to have a library of tag files and import the desired one without having to do an export, modify and import.

At the time a file is imported, the system verifies that:

- existing tags were included if their types were not modified.

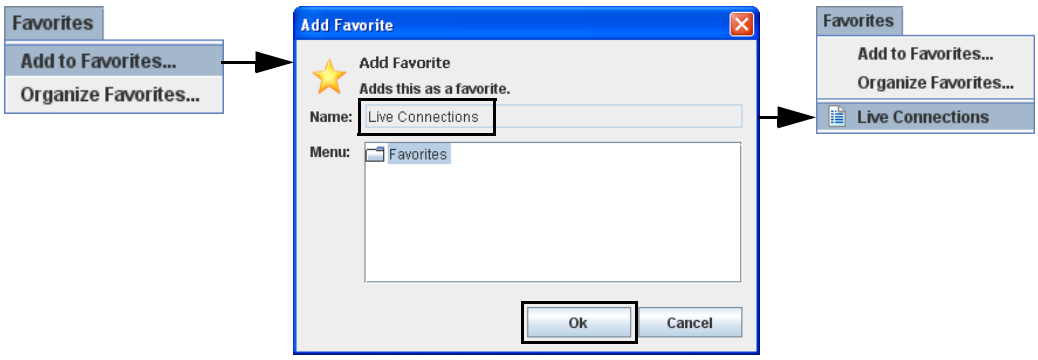
- the changes will not invalidate any existing device/device port configuration.

Chapter 5
Favorites

Favorites provides quick access links to saved connection sets in Connection Manager or saved network diagrams in Topology Manager. By saving a link, similar to saving an Internet URL address for later access, a library of connection sets / network diagrams can be generated.

Add Favorites

1. Open an application (i.e., Connection Manager, Topology Manager) and access the required connection set or topology layout.
2. To add the accessed connection set or topology layout to the Favorites list, select **Favorites > Add to Favorites**. The Add Favorite screen displays. The name of the accessed connection set or topology layout is automatically displayed in the **Name:** field. Click **OK** to save the link. The new access link is now listed in the Favorites menu.



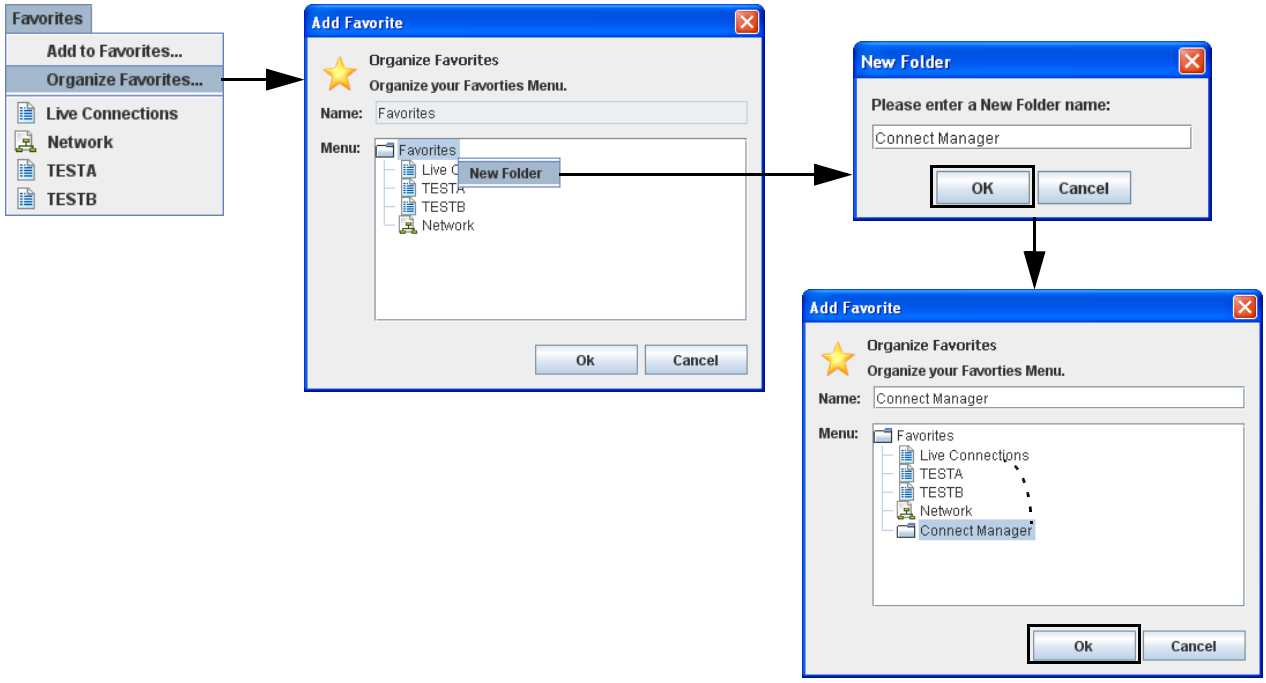
Organize Favorites

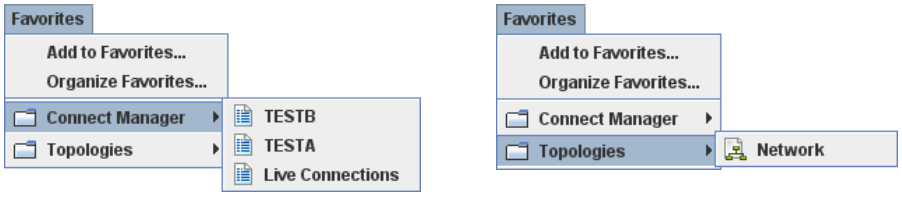
The list of saved favorites can be moved to self-defined sets of folders, similar to Internet favorite folders, for ease in locating a particular access link.

Add Folders

1. Select **Favorites > Organize Favorites**. The Add Favorite screen displays.
2. Right-click on Favorites and select **New Folder**. Enter the new folder name and click **OK**. The new folder is added to the tree listing and to the Favorites main menu. Click **OK** to save the updates.
3. Repeat step 2 as required for any additional folders.

From the Add Favorite screen, the individual favorite links can now be moved to the new defined folders by dragging the link names to the folders.

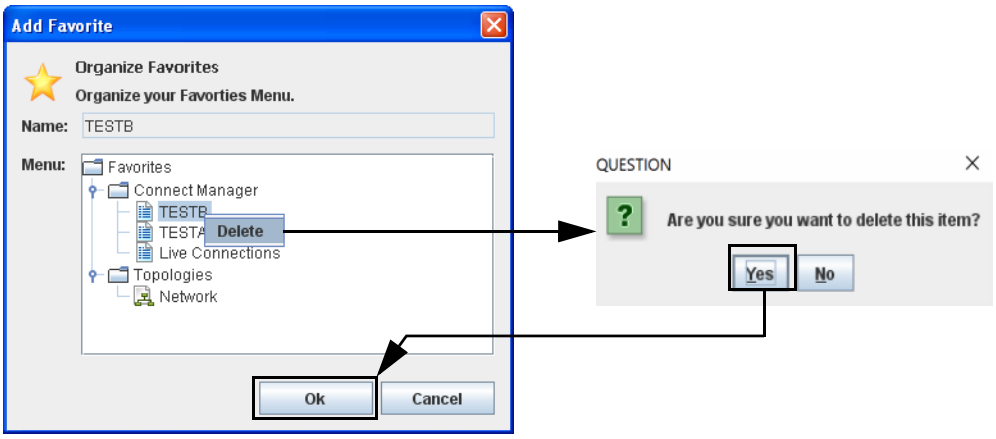




Delete Favorites

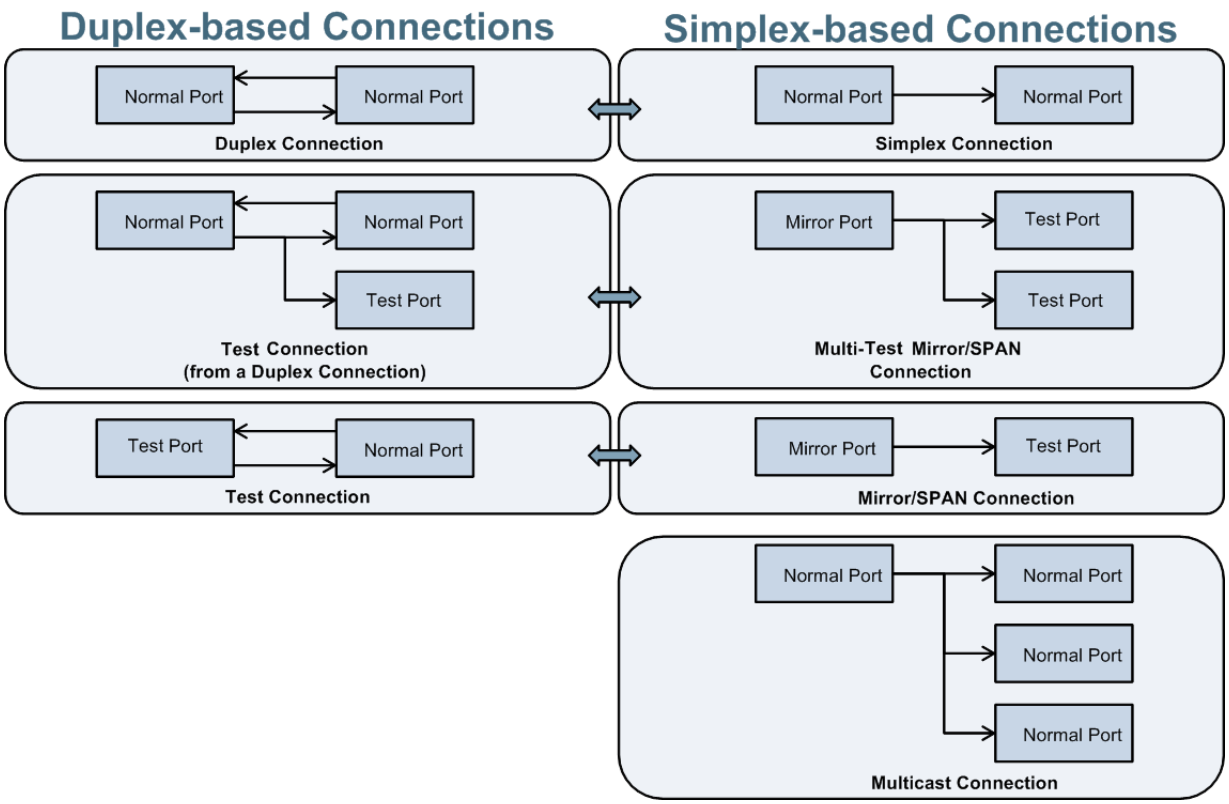
Favorites can be removed as necessary.

1. Right-click on the favorite name and select **Delete**.
2. Click **Yes** to the confirmation question, then click **OK**.



Chapter 6
Connectivity

TestStream Management supports the following connectivity configurations:



Port connectivity / status is accomplished using the following Connect menu functions:

- Switch Graphic on page 6-2
- Topology Manager on page 6-2
- Connection Manager on page 6-34

Switch Graphic

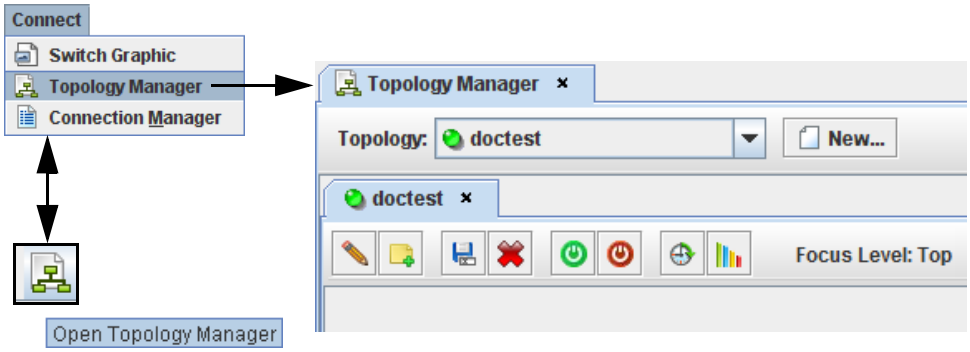
Refer to Viewing Switch Details on page 3-13.

Topology Manager

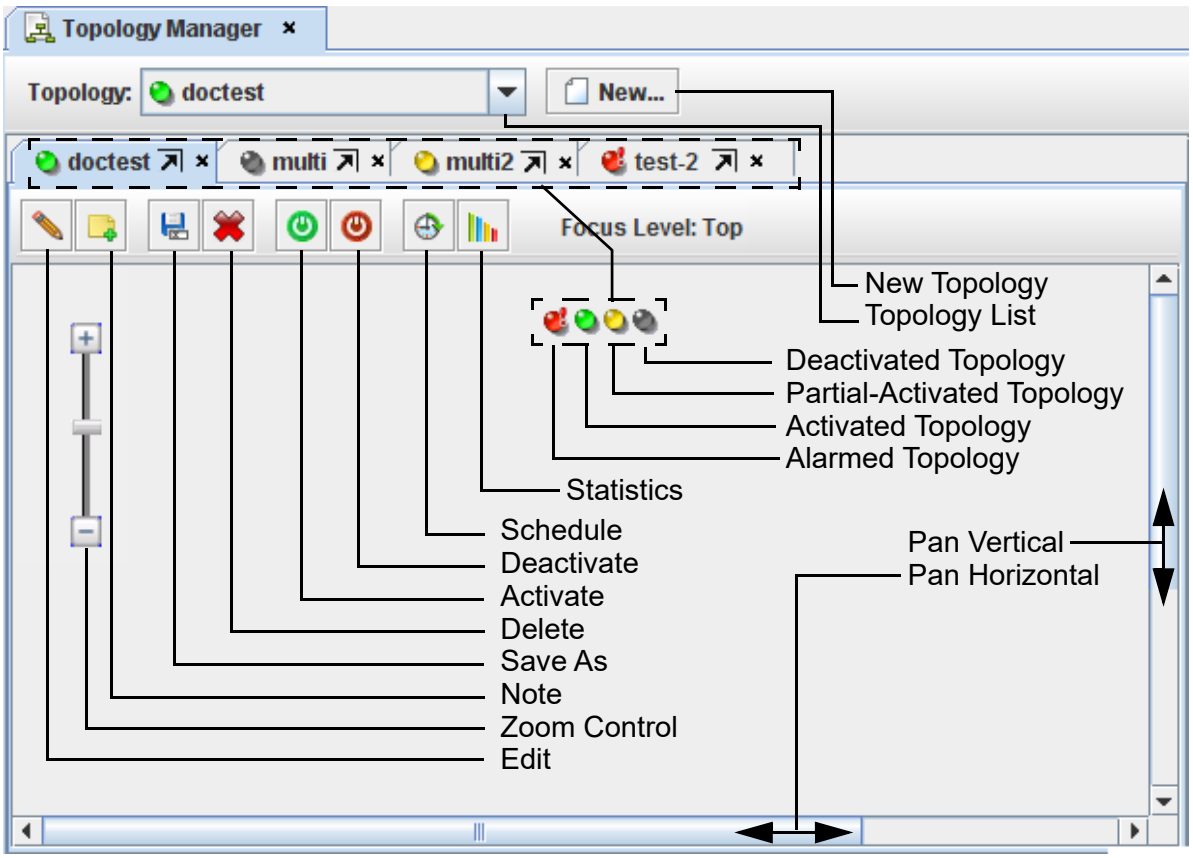
The Topology Manager allows the user to graphically connect ports, packets, and associated filter objects.

Starting Topology Manager

Select **Connect > Topology Manager**, or from the toolbar, select the **Topology Manager** icon, or from the keyboard **Alt+F8**. The Topology Manager screen displays.



Topology Manager Controls



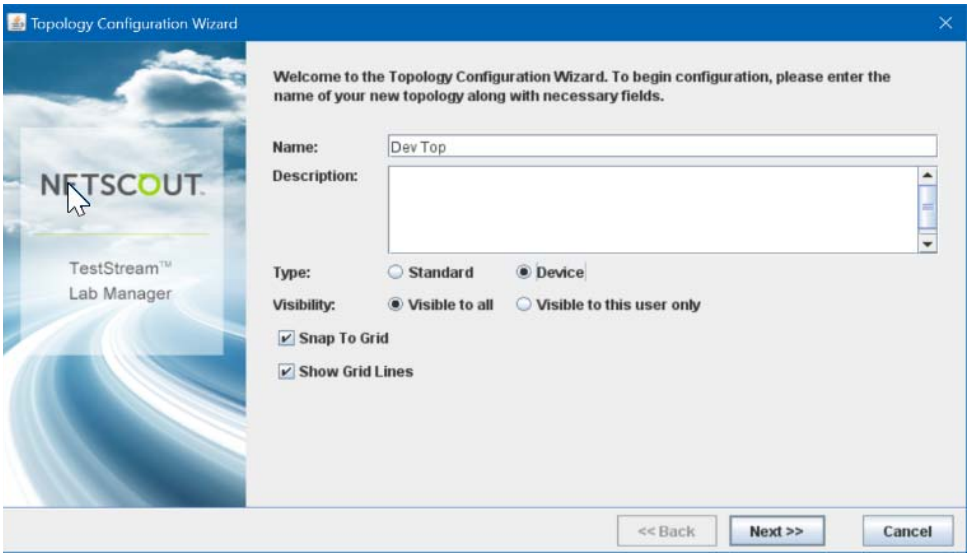
- Topology - List of named topologies
- New - Starts Topology Configuration Wizard to create a new topology
- Statistics - View statistics for all of the ports on the topology
- Schedule - Assign activation / deactivation times for selected topology
- Deactivate - Removes active connection; places connection in standby
- Activate - Completes connection of all associations on the current topology
- Delete - Remove the current topology
- Save As - Save currently selected topology as another topology with all of the original objects
- Note - Add a note to the topology
- Zoom Control - Slider bar/buttons for zooming in (+) or out (-) in the topology screen. Optionally, the mouse scroll wheel also zooms in and out.
- Edit - Change topology attributes
- Pan Vertical / Horizontal - Allows manual panning of the topology screen

Create a New Topology

From the Topology Manager, click **New**. The Topology Configuration Wizard screen displays.

- Enter a name for the topology connection set in the **Name** field.
- Enter additional information (optional) in the **Description** field.
- Select the type of topology required: Standard or Device (refer to Scheduling Device Topologies on page 3-254).
- Select if this topology set is visible to all TestStream Management users (default) or just to the logged-in user (yourself). Click **Finish**.
- Select **Snap to Grid** to have newly placed objects or moved objects snap to the grid.
- Select **Show Grid Lines** to have the topology show grid lines.

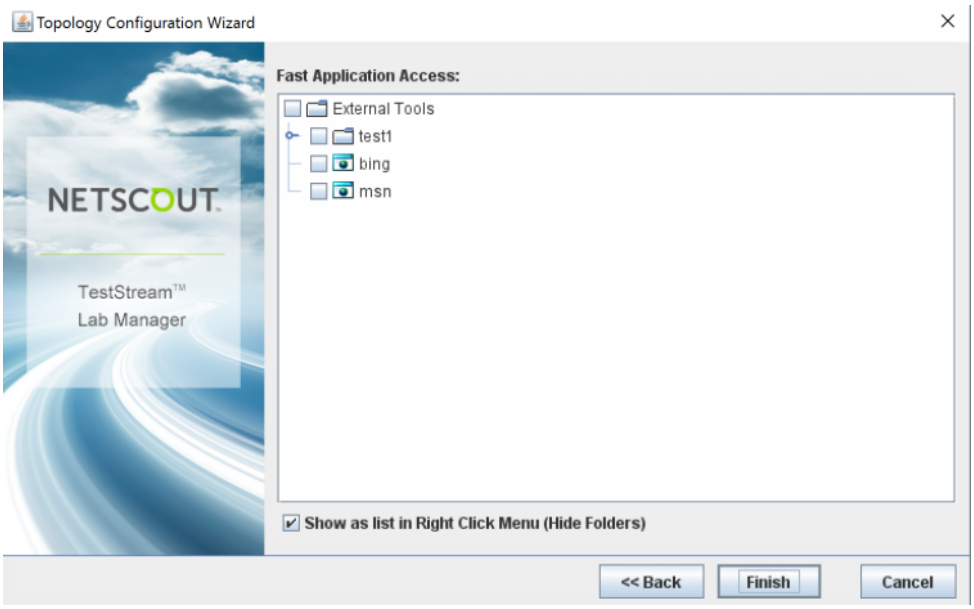
Note: When a new topology is created, the Snap to Grid and Show Grid Lines options are selected by default.



Note: Administrator level allows viewing of all created topologies. Non-Administrator level users can view global and defined topologies visible only to the user from the Topology Manager and the GO To... menu option. However, the GO To... menu option is disabled if none of the topologies are either global or user defined topologies visible only to the user.

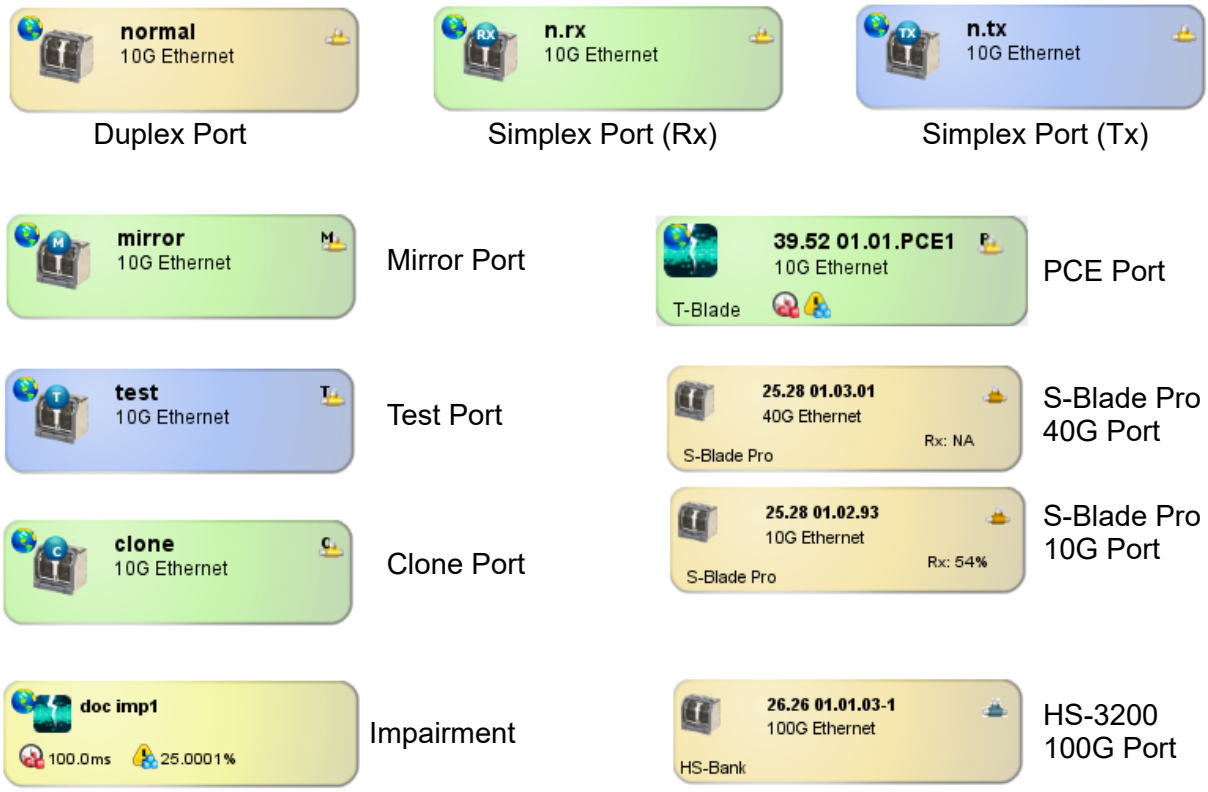
For Test Stream Lab Manager only, after you click **Next**, a second screen appears. On this screen, the user can associate an external application or resource to the new topology. Select the desired folder or external application/resource and then click **OK**.

Note: You can also choose to list the external applications/resources as a flat list, without their folder location, by selecting **Show as list in Right Click Menu (Hide Folders)**.



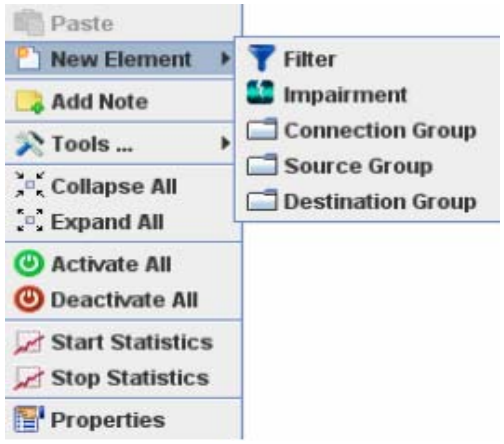
Topology Connection Objects

The following shows the various topology connection objects.



Topology Manager Screen Sub Menus

Right clicking on an open area of the topology manager screen displays the following menu:



- Paste - Place a copy of selected objects (Source Group, Filter, Destination Group, Connection Group) into another topology set
- New Element - Places a new undefined packet object into the currently selected topology set
- Add Note - Add an information note to the topology
- Tools - Displays submenu with available tools, including Fast Application Access
- Collapse All - Hide from view all associated ports/sub-ports within an object
- Expand All - View all associated ports/sub-ports within an object

- Activate - Completes all non-activated packet connections
- Deactivate - Removes all activated packet connections; places connections in standby
- Start Statistics - Begin statistics recording
- Stop Statistics - End statistics recording
- Properties - Displays the selected topology's general properties

Test Blade Connectivity

General Descriptions

- **Source Groups** are used to pass traffic from multiple source ports through the same routing, filtering, and packet processing.
- **Destination Groups** are used to multicast or load balance an outgoing traffic stream to multiple destination ports.
- **Connection Groups** provide a mechanism to activate a number of port-to-port, subport-to-subport, or port-to-subport connections. The same functionality can be obtained using functionally identical associations. A Connection Group can only be connected to a single other Connection Group. Both Connection Groups must have the same number of members. If a Connection Group member is a subport and the associated Connection Group has a subport in the corresponding location, the two subports must be complimentary (i.e., an Rx subport connected to a Tx subport or vice-versa).
- Port-to-port connections provide a full duplex data path.
- Subport-to-subport connections provide a simplex data path.
- Port-to-subport connections provide a simplex data path.

Locked Ports

When a source or destination group contains a port which has been locked by another user:

- If the group has any active connections, no ports or sub-ports, locked or otherwise, can be added to the group.
- If the group has any active connections, no ports or sub-ports, locked or otherwise, can be removed from the group.
- When locked ports are added to a group, no connections from that group can be activated.
- No connections can be activated to or from the group.
- No connections can be deactivated to or from the group.
- Ports or sub-ports cannot be added to any groups with an active connection to or from the group.
- Ports or sub-ports cannot be removed from any groups with an active connection to or from the group.

When a connection group contains a port which has been locked by another user:

- When locked ports are added to a group, the user should be warned that no connections from that group can be activated.
- No connections can be activated to the connection group.
- No connections can be deactivated to from the connection group.
- No ports can be added to or removed from any connection group with an active connection, regardless of locked ports.

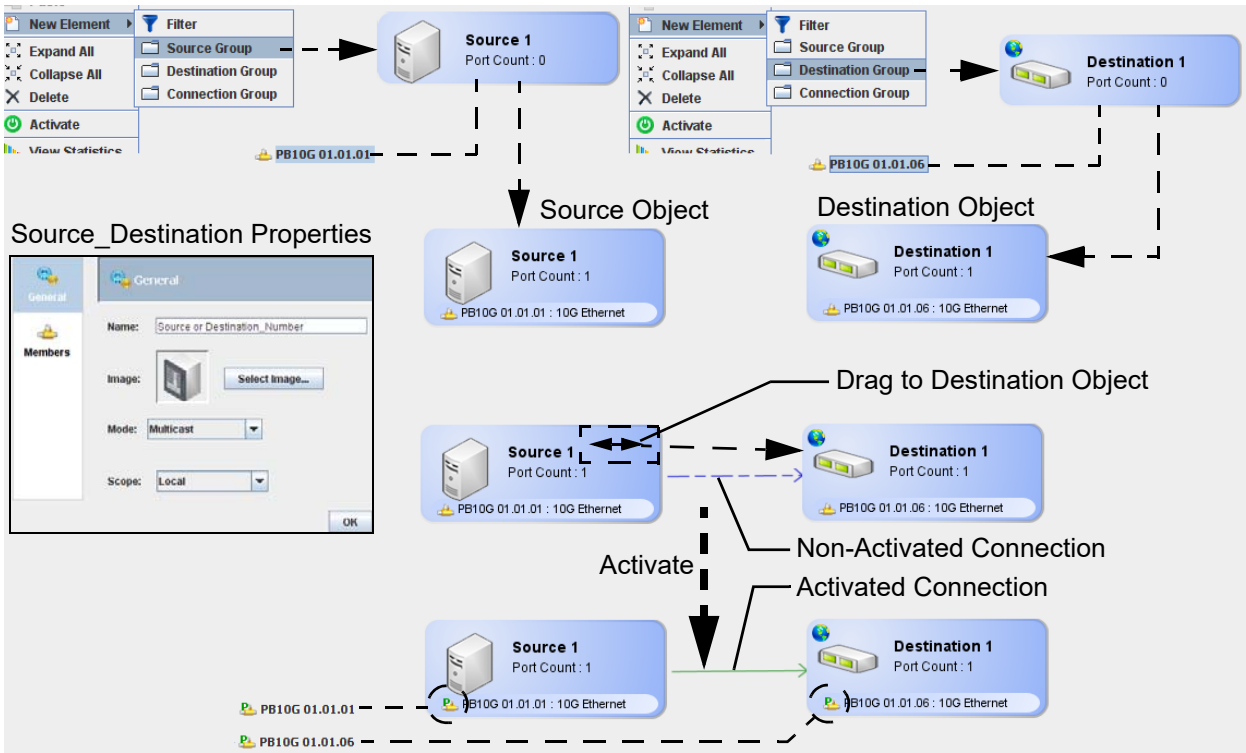
Port-to-Port Packet (Duplex) Connectivity

Select a topology from the Topology drop down list.

Source Object: Right-click in the topology screen and select **New Element > Source Group**. A properties screen displays allowing customizing (e.g., Name, Image, Scope; refer to Port Group Creation on page 6-22) of the object. Click **OK** to save any changes. An empty (port count = 0) source object displays. From the System tab, select a port and drag it over to the source object; the object now displays the port number and interface type (refer to Source Group Objects on page 6-26). If required, double-click on the source object to display the port information.

Destination Object: Right-click in the topology screen and select **New Element > Destination Group**. A properties screen displays allowing customizing (e.g., Name, Image, Mode, Scope; refer to Port Group Creation on page 6-22) of the object. Click **OK** to save any changes. An empty (port count = 0) destination object displays. From the System tab, select a port and drag it over to the destination object; the object now displays the port number and interface type (refer to Destination Group Objects on page 6-27). If required, double-click on the destination object to display the port information.

Right-click on the inside of the source object - a double-arrow line indicator displays. Drag the double-arrow line over to the destination object. A blue dotted line (indicating a non-activated packet connection) displays between the objects. Click **Activate** to complete the packet connection (the connection line becomes a solid green, a green check-mark icon displays next to each connected port in the object and the connection listings in System and Ports/Groups).



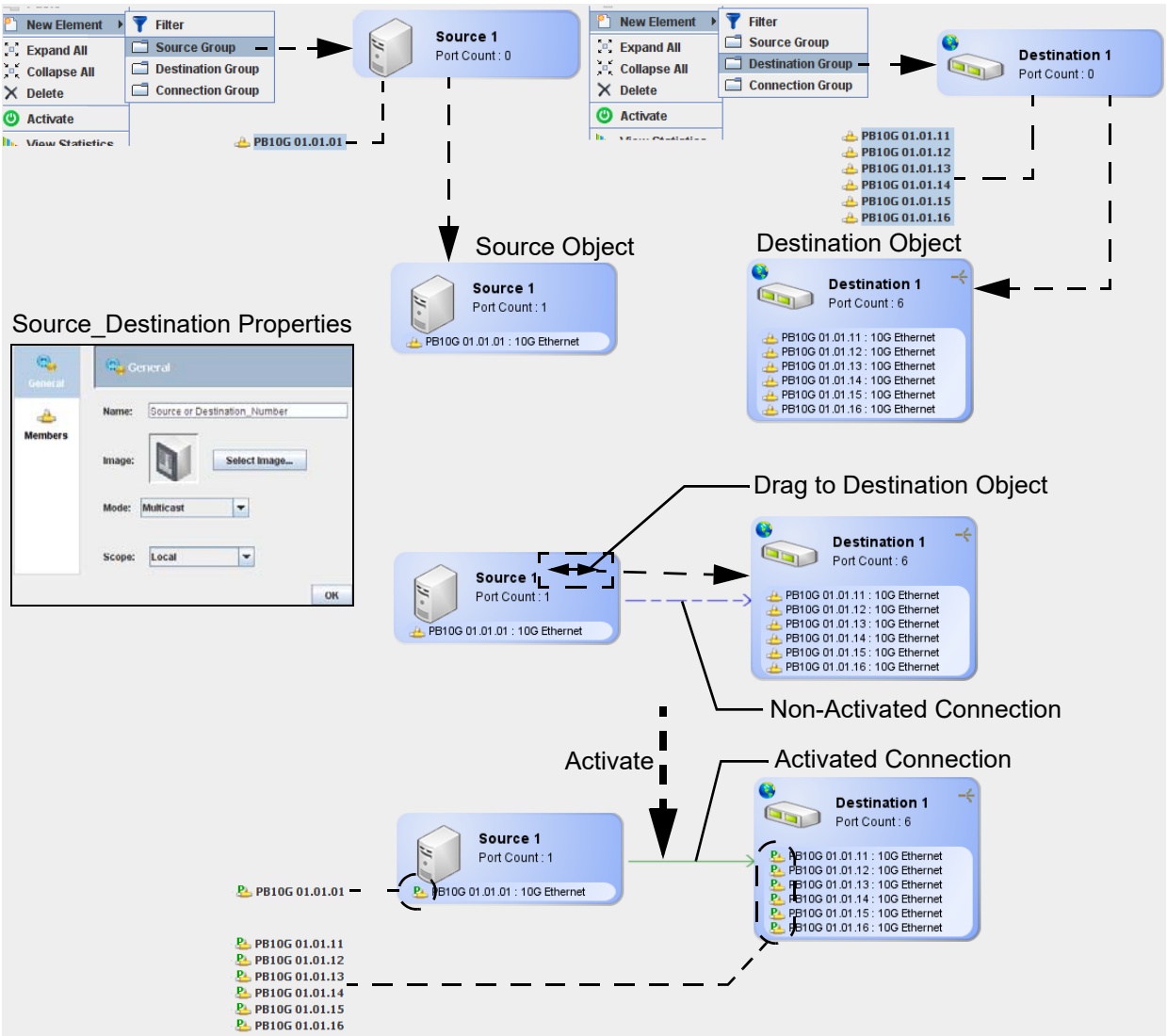
Port-to-Multiple Ports Packet (Duplex) Connectivity

Select a packet set from the Topology drop down list.

Source Object: Right-click in the topology screen and select **New Element > Source Group**. A properties screen displays allowing customizing (e.g., Name, Image, Scope; refer to Port Group Creation on page 6-22) of the object. Click **OK** to save any changes. An empty (port count = 0) source object displays. From the System tab, select a port and drag it over to the source object; the object now displays the port number and interface type (refer to Source Group Objects on page 6-26). If required, double-click on the source object to display the port information.

Destination Object: Right-click in the topology screen and select **New Element > Destination Group**. A properties screen displays allowing customizing (e.g., Name, Image, Mode, Scope; refer to Port Group Creation on page 6-22) of the object. Click **OK** to save any changes. An empty (port count = 0) destination object displays. From the System tab, select two or more ports and drag them over to the destination object; the object now displays the port numbers, interface types, and if in multicast or load balance mode (refer to Destination Group Objects on page 6-27). If required, double-click on the destination object to display the port information. The individual ports can be repositioned in the destination object by selecting, right-clicking, and select either **Move Up/Down** as necessary.

Right-click on the inside of the source object - a double-arrow line indicator displays. Drag the double-arrow line over to the destination object. A blue dotted line (indicating a non-activated packet connection) displays between the objects. Click **Activate** to complete the packet connection (the connection line becomes a solid green, a green check-mark icon displays next to each connected port in the object and the connection listings in System and Ports/Groups).

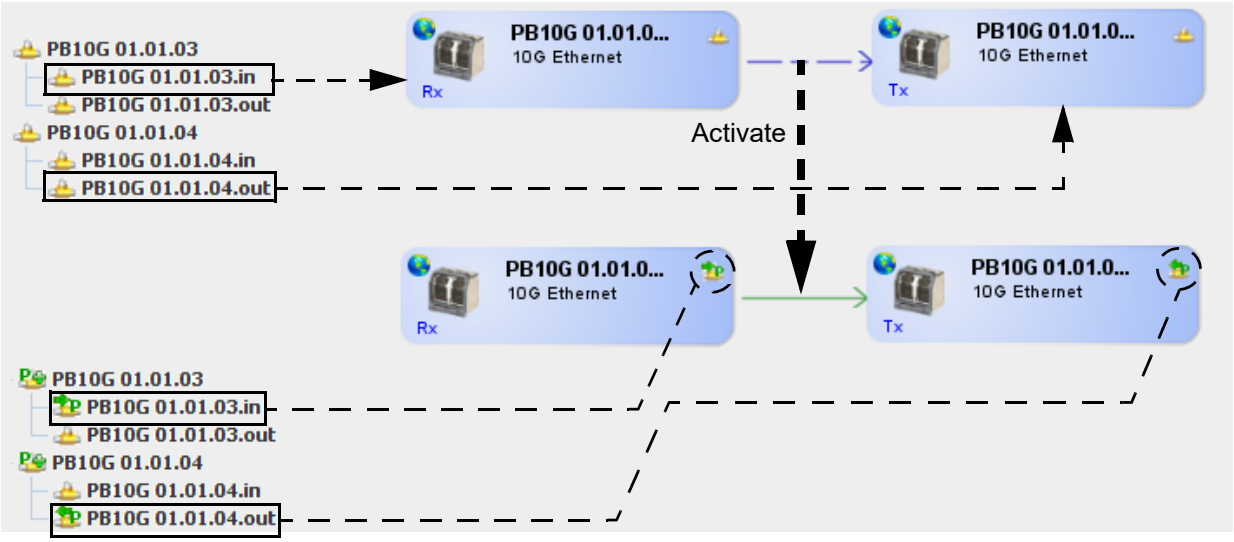


Subport-to-Subport Packet (Simplex) Connectivity

From the System tab, select a T-Blade sub-port and drag it over to the topology screen. A sub-port object displays showing the port number, interface type, and sub-port type (Rx or Tx).

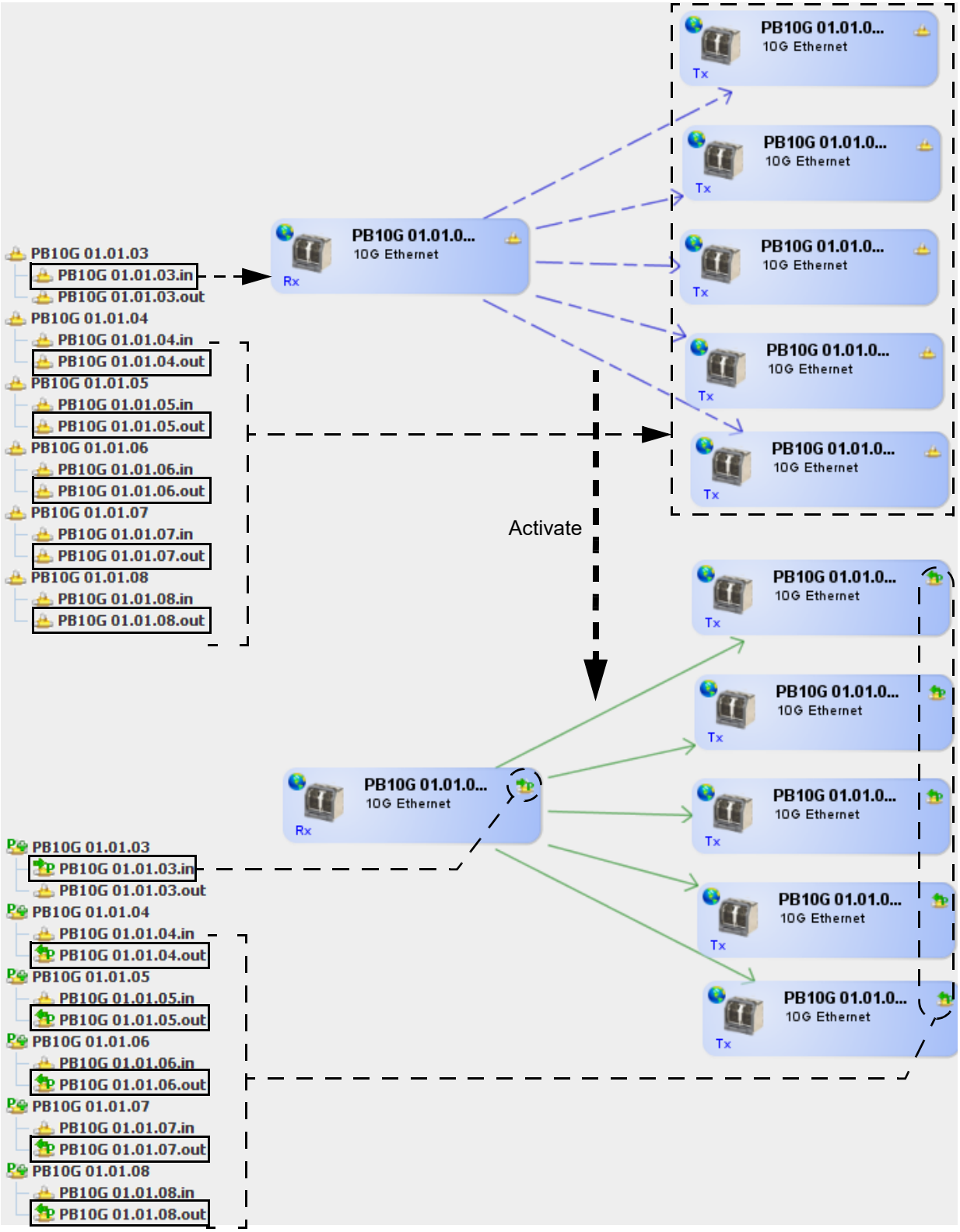
Simplex Port Connections: Select a second sub-port (of the opposite port type) and drag it over to the topology screen. A sub-port object displays showing port number, interface type, and sub-port type (Rx or Tx).

Right-click on the inside of the first sub-port object - a double-arrow line indicator displays. Drag the double-arrow line over to the sub-port object. A blue dotted line (indicating a non-activated connection) displays between the objects. Click **Activate** to complete the connection (the connection line becomes a solid green, a Connected Simplex Port (Rx or Tx) icon displays next to each connected port in the object and the connection listings in System and Ports/Groups).



Simplex Multicast Connections: Select the required sub-ports (of the opposite port type) and drag them over to the topology screen. Each sub-port object displays the port number, interface type, and sub-port type (Rx or Tx).

Right-click on the inside of the first sub-port object - a double-arrow line indicator displays. Drag the double-arrow line over to the group sub-port object. A blue dotted line (indicating a non-activated connection) displays between the objects. Click **Activate** to complete the connection (the connection line becomes a solid green, a Connected Simplex Port (Rx or Tx) icon displays next to each connected port in the object and the connection listings in System and Ports/Groups).


PB10G 01.01.03
PB10G 01.01.03.in
PB10G 01.01.03.out
PB10G 01.01.04
PB10G 01.01.04.in
PB10G 01.01.04.out
PB10G 01.01.05
PB10G 01.01.05.in
PB10G 01.01.05.out
PB10G 01.01.06
PB10G 01.01.06.in
PB10G 01.01.06.out
PB10G 01.01.07
PB10G 01.01.07.in
PB10G 01.01.07.out
PB10G 01.01.08
PB10G 01.01.08.in
PB10G 01.01.08.out
PB10G 01.01.0...
10G Ethernet
Rx
Tx
Activate

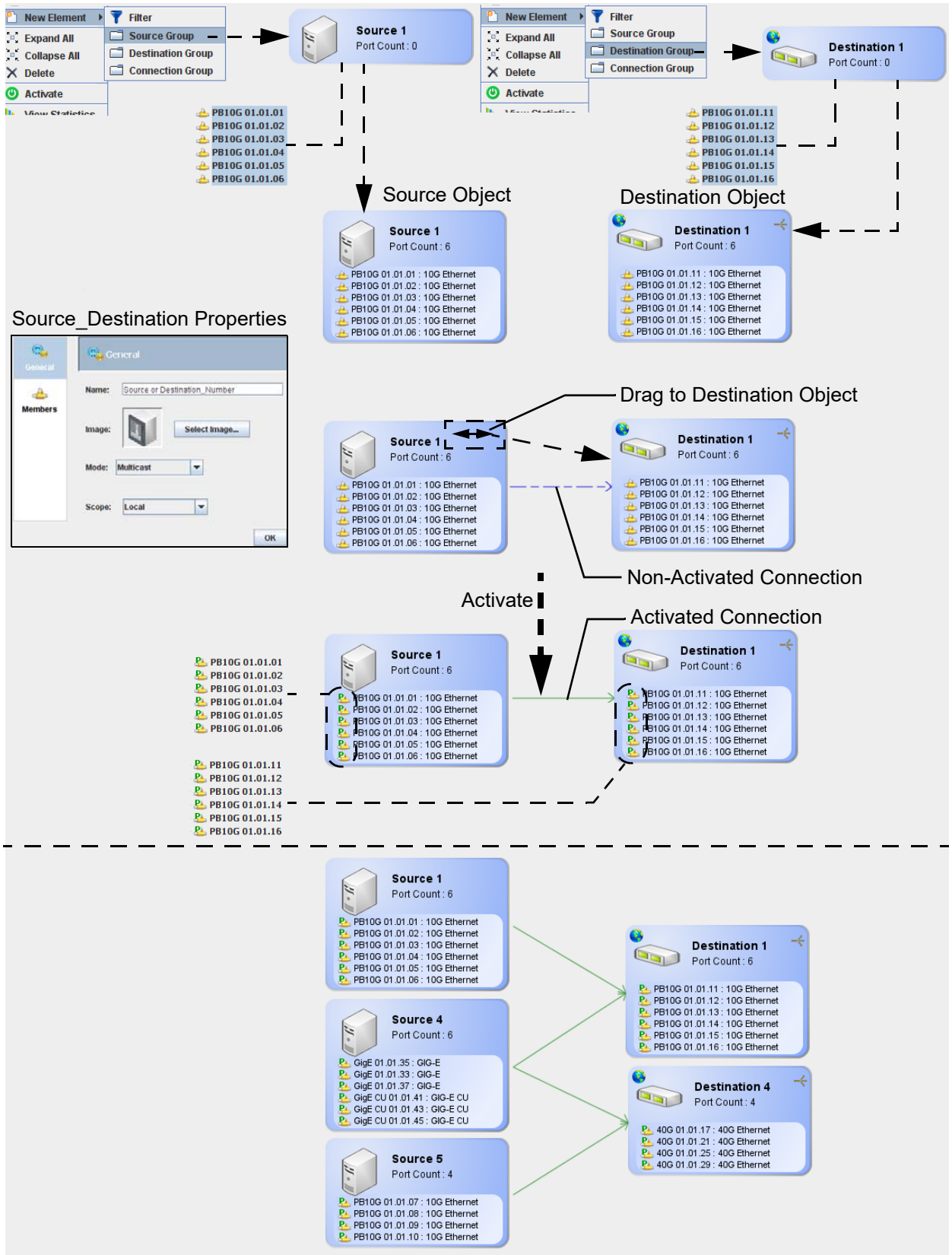
Multiple to Multiple Packet Connectivity

Select a packet set from the Topology drop down list.

Source Object: Right-click in the topology screen and select **New Element > Source Group**. A properties screen displays allowing customizing (e.g., Name, Image, Scope; refer to Port Group Creation on page 6-22) of the object. Click **OK** to save any changes. An empty (port count = 0) source object displays. From the System tab, select two or more ports and drag them over to the source object; the object now displays the port numbers and interface types (refer to Source Group Objects on page 6-26). If required, double-click on the source object to display the port information. The individual ports can be repositioned in the source object by selecting, right-clicking, and select either **Move Up/Down** as necessary.

Destination Object: Right-click in the topology screen and select **New Element > Destination Group**. A properties screen displays allowing customizing (e.g., Name, Image, Mode, Scope; refer to Port Group Creation on page 6-22) of the object. Click **OK** to save any changes. An empty (port count = 0) destination object displays. From the System tab, select two or more ports and drag them over to the destination object; the object now displays the port numbers, interface types, and if in multicast or load balance mode (refer to Destination Group Objects on page 6-27). If required, double-click on the destination object to display the port information. The individual ports can be repositioned in the destination object by selecting, right-clicking, and select either **Move Up/Down** as necessary.

Right-click on the inside of the source object - a double-arrow line indicator displays. Drag the double-arrow line over to the destination object. A blue dotted line (indicating a non-activated packet connection) displays between the objects. Click **Activate** to complete the packet connection (the connection line becomes a solid green, a green check-mark icon displays next to each connected port in the object and the connection listings in System and Ports/Groups).


New Element
Expand All
Collapse All
Delete
Activate
Filter
Source Group
Destination Group
Connection Group
Source 1
Port Count : 0
Destination 1
Port Count : 0
PB10G 01.01.01
PB10G 01.01.02
PB10G 01.01.03
PB10G 01.01.04
PB10G 01.01.05
PB10G 01.01.06
PB10G 01.01.11
PB10G 01.01.12
PB10G 01.01.13
PB10G 01.01.14
PB10G 01.01.15
PB10G 01.01.16
Source Object
Destination Object
Source 1
Port Count : 6
PB10G 01.01.01 : 10G Ethernet
PB10G 01.01.02 : 10G Ethernet
PB10G 01.01.03 : 10G Ethernet
PB10G 01.01.04 : 10G Ethernet
PB10G 01.01.05 : 10G Ethernet
PB10G 01.01.06 : 10G Ethernet
Destination 1
Port Count : 6
PB10G 01.01.11 : 10G Ethernet
PB10G 01.01.12 : 10G Ethernet
PB10G 01.01.13 : 10G Ethernet
PB10G 01.01.14 : 10G Ethernet
PB10G 01.01.15 : 10G Ethernet
PB10G 01.01.16 : 10G Ethernet
Source_Destination Properties
General
Members
Name:
Source or Destination_Number
Image:
Select Image...
Mode:
Multicast
Scope:
Local
OK
Drag to Destination Object
Non-Activated Connection
Activate
Activated Connection
Source 4
Port Count : 6
GigE 01.01.35 : GIG-E
GigE 01.01.33 : GIG-E
GigE 01.01.37 : GIG-E
GigE CU 01.01.41 : GIG-E CU
GigE CU 01.01.43 : GIG-E CU
GigE CU 01.01.45 : GIG-E CU
Source 5
Port Count : 4
PB10G 01.01.07 : 10G Ethernet
PB10G 01.01.08 : 10G Ethernet
PB10G 01.01.09 : 10G Ethernet
PB10G 01.01.10 : 10G Ethernet
Destination 4
Port Count : 4
40G 01.01.17 : 40G Ethernet
40G 01.01.21 : 40G Ethernet
40G 01.01.25 : 40G Ethernet
40G 01.01.29 : 40G Ethernet

Group to Group Packet (Duplex) Connectivity

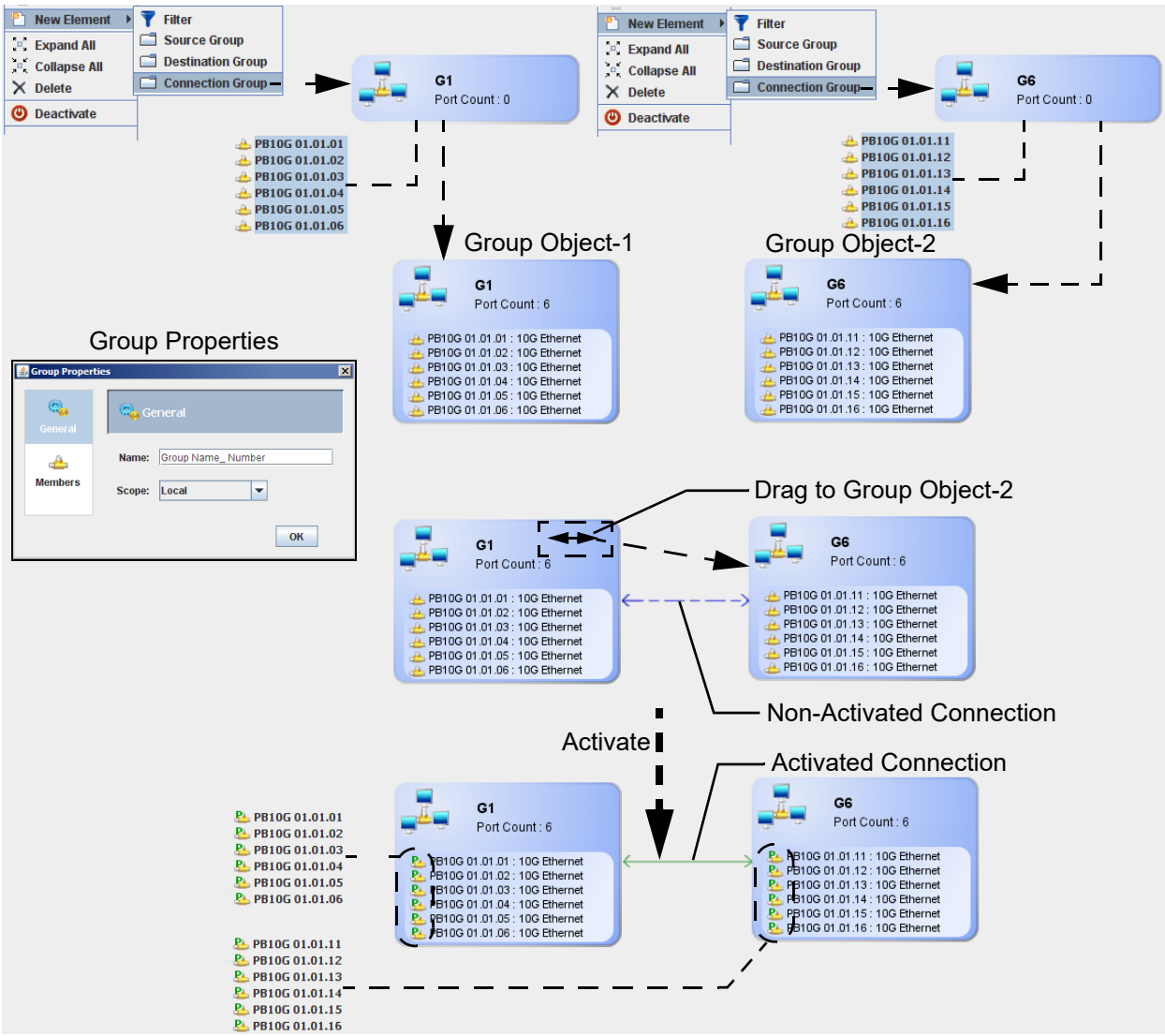
Note: Groups must contain the same number of port items (e.g., 2 <-> 2, 3 <-> 3, 10 <-> 10).

Select a packet set from the Topology drop down list.

Group Object - 1: Right-click in the topology screen and select **New Element > Connection Group**. A group properties screen displays allowing customizing (e.g., Name, Scope; refer to Port Group Creation on page 6-22) of the object. Click **OK** to save any changes. An empty (port count = 0) group object displays. From the System tab, select two or more ports and drag them over to the group object; the object now displays the port numbers and interface types. If required, double-click on the group object to display the port information. The individual ports can be repositioned in the group object by selecting, right-clicking, and select either **Move Up/Down** as necessary.

Group Object - 2: Right-click in the topology screen and select **New Element > Connection Group**. A group properties screen displays allowing customizing (e.g., Name, Scope; refer to Port Group Creation on page 6-22) of the object. Click **OK** to save any changes. An empty (port count = 0) group object displays. From the System tab, select two or more ports and drag them over to the group object; the object now displays the port numbers and interface types. If required, double-click on the group object to display the port information. The individual ports can be repositioned in the destination object by selecting, right-clicking, and select either **Move Up/Down** as necessary.

Right-click on the inside of the first group object - a double-arrow line indicator displays. Drag the double-arrow line over to the second group object. A double-arrow blue dotted line (indicating a non-activated duplex packet connection) displays between the objects. Click **Activate** to complete the packet connection (the connection line becomes a double-arrow solid green, a green check-mark icon displays next to each connected duplex port in the object and the connection listings in System and Ports/Groups).


New Element
Expand All
Collapse All
Delete
Deactivate
Filter
Source Group
Destination Group
Connection Group
G1
Port Count : 0
G6
Port Count : 0
PB10G 01.01.01
PB10G 01.01.02
PB10G 01.01.03
PB10G 01.01.04
PB10G 01.01.05
PB10G 01.01.06
PB10G 01.01.11
PB10G 01.01.12
PB10G 01.01.13
PB10G 01.01.14
PB10G 01.01.15
PB10G 01.01.16
Group Object-1
Group Object-2
Port Count : 6
PB10G 01.01.01 : 10G Ethernet
PB10G 01.01.02 : 10G Ethernet
PB10G 01.01.03 : 10G Ethernet
PB10G 01.01.04 : 10G Ethernet
PB10G 01.01.05 : 10G Ethernet
PB10G 01.01.06 : 10G Ethernet
PB10G 01.01.11 : 10G Ethernet
PB10G 01.01.12 : 10G Ethernet
PB10G 01.01.13 : 10G Ethernet
PB10G 01.01.14 : 10G Ethernet
PB10G 01.01.15 : 10G Ethernet
PB10G 01.01.16 : 10G Ethernet
Group Properties
General
Members
Name:
Group Name_ Number
Scope:
Local
OK
Drag to Group Object-2
Non-Activated Connection
Activate
Activated Connection

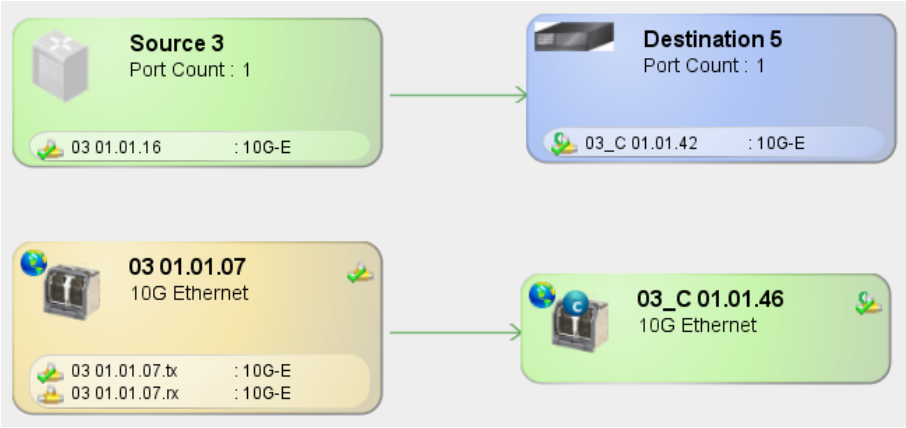
Clone Ports

To clone a port, the port must be linked to a defined clone port. To link a clone port with a source port, place the source port on a topology (as a port or in a source group). Place the clone port on the same topology (matching the source port as a port or as a destination group). Create an association by right clicking on the source port (or source group), dragging the mouse to the clone port (or destination group) and releasing the right button. Activate the association - a simplex connection is made.

Using Clone Ports with Independent Filtering

Linking Clone Ports

A clone port can also be linked (as part of a destination group) to a source group with more than one port.

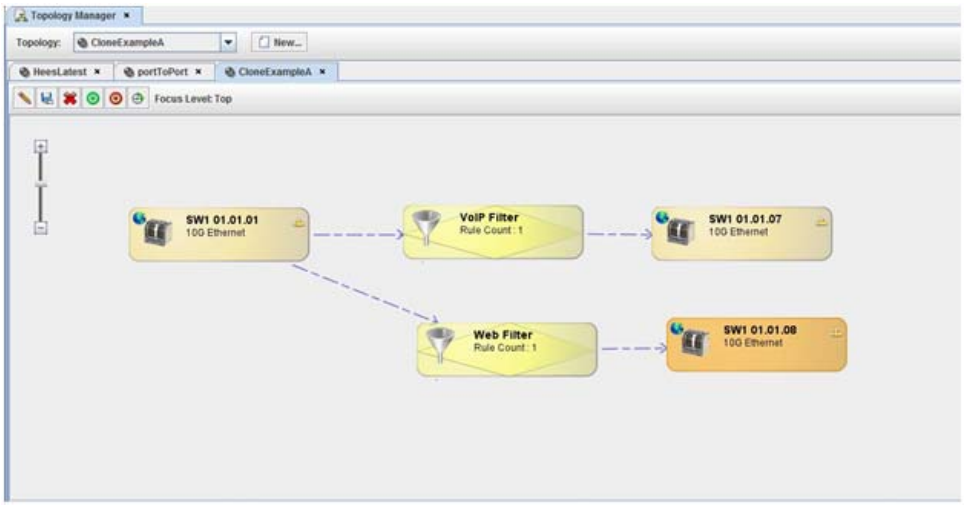


Clone Ports Usage Examples

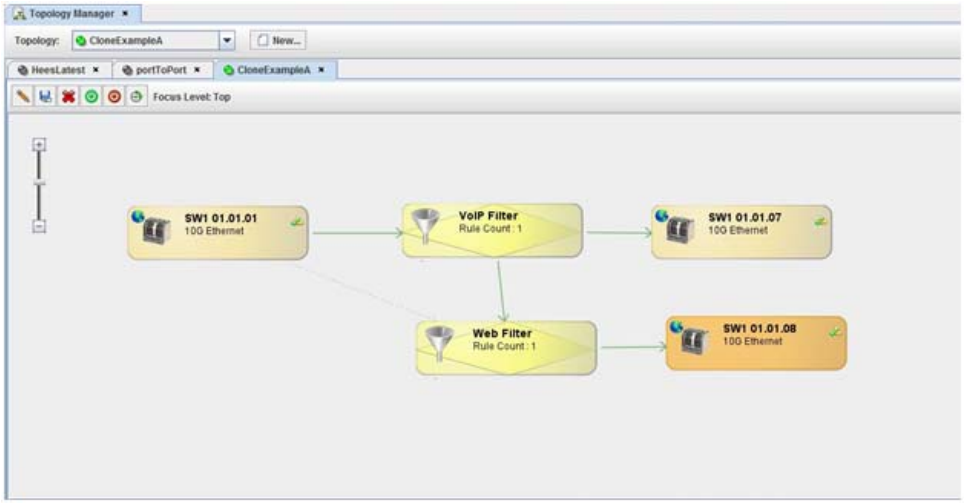
The following describes typical configuration examples when utilizing clone ports.

Independent Filtering of Source Port Datastream

Clone ports provide a way to apply additional independent processing to a source port traffic stream. In Example 1, port “SW1 01.01.01” is associated with two filters. When activated, port “SW1 01.01.07” will receive all data that passes the VoIP Filter, but port “SW1 01.01.08” will only receive the data that does not pass the VoIP Filter and also passes the Web Filter (Example 2). This may not be the desirable affect.



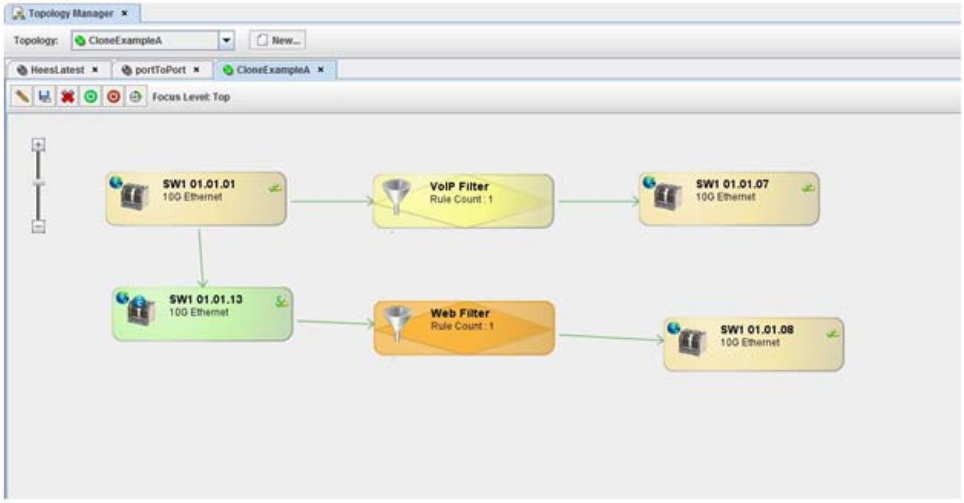
Example 1 - Multiple Filters on a Port



Example 2 - Filter Precedence/Overlap Problem with Multiple Filters on a Port

Clone ports provide a workaround for this filter precedence/overlap problem described above. Using clone ports, a user can apply filters to a source port stream without concern for how other users are filtering the data.

In Example 3, port “SW1 01.01.017” receives all the data from port “SW1 01.01.01” that passes the VoIP Filter, and port “SW1 01.01.08” will receive all the data from port “SW1 01.01.01” that passes the Web Filter, not just that data that did not pass the VoIP Filter but passed the Web Filter.

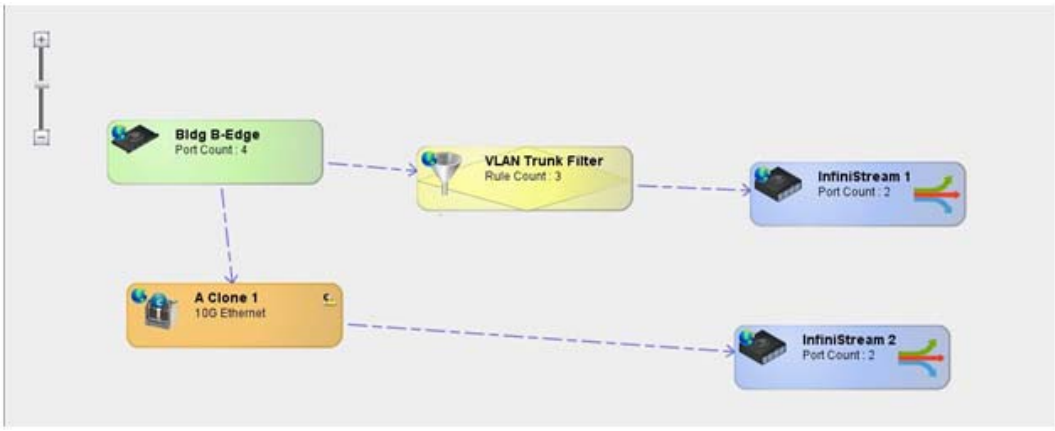


Example 3 - Independent Filter Using Clone Ports

Packet Modifiers

Clone ports provide a workaround for packet modifiers like the VLAN modify feature where all downstream ports receive the modified packet. By using a clone port, the original stream is still available in the cloned port

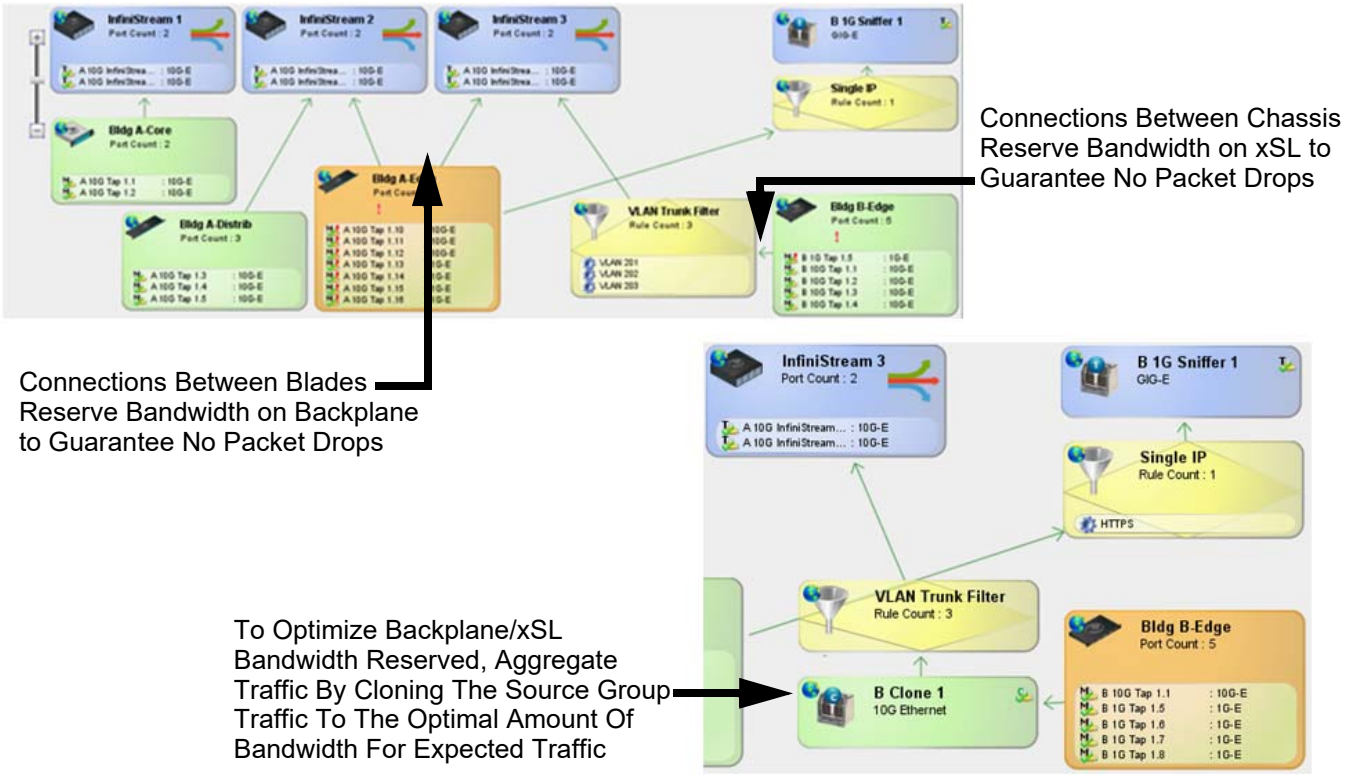
In Example 4, the original data minus the VLAN tag can be sent to an alternate destination by using a clone port.



Example 4 - Using Clone Ports with VLAN Modify

Backplane/xSL Bandwidth Optimization

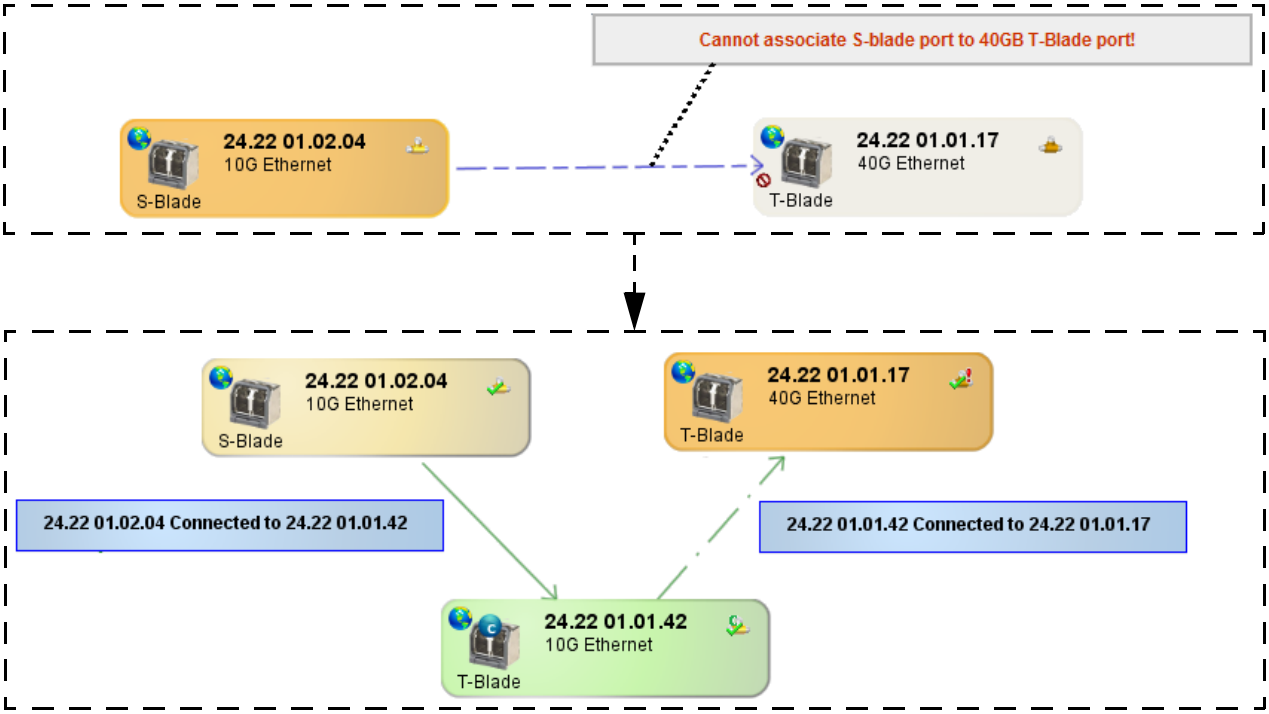
Example 5 shows how the clone port “B Clone 1 “can be used to minimize the backplane bandwidth used. When the expected traffic is less than 10G, the backplane bandwidth can be optimized by using “B Clone 1” to clone the source group “Bldg B Edge”. This configuration uses only 10G of bandwidth versus 50G that would be used if “Bldg B Edge” was connected directly to the “VLAN Trunk Filter”.



Example 5 - Clone Ports to Optimize Backplane Bandwidth

S-Blade to T-Blade Connectivity

When connecting a 10GbE S-Blade port to a 40GbE T-Blade port, the S-Blade port must be routed through a 10GbE T-Blade Clone Port to the 40GbE T-Blade port for proper connectivity.

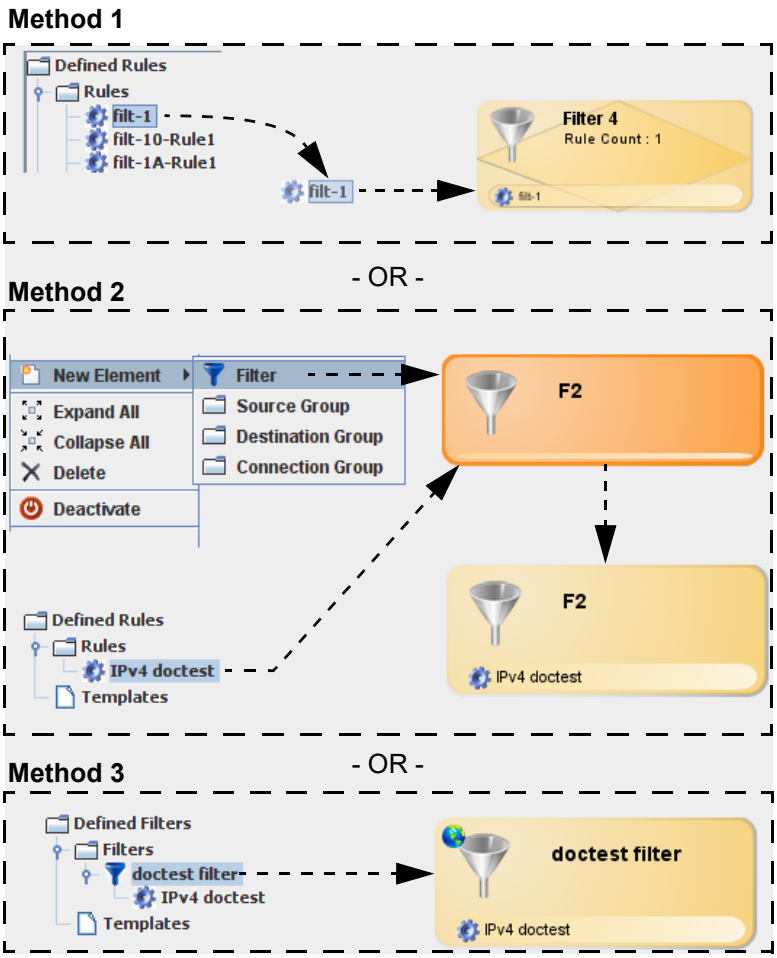


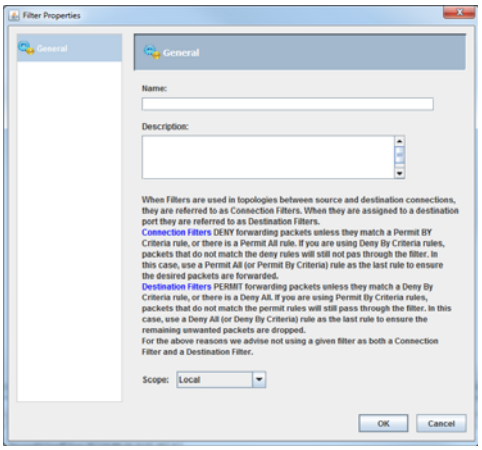
Adding Filters

Method 1: From the Rules/Filters tab, select a defined rule (refer to Rules/Filters on page 3-188) and drag it over to the topology screen. A properties screen displays allowing customizing (e.g., Name, Description, Scope; refer to Port Group Creation on page 6-22) of the filter. Click OK to save any changes. A filter object containing the defined rule displays.

Method 2: Right-click in the topology screen and select **New Element > Filter**. A properties screen displays allowing customizing (e.g., Name, Description, Scope; refer to Port Group Creation on page 6-22) of the filter. Click **OK** to save any changes. An empty filter object displays. From the Rules/Filters tab, select a defined rule (refer to Rules/Filters on page 3-188) and drag it over to the filter object.

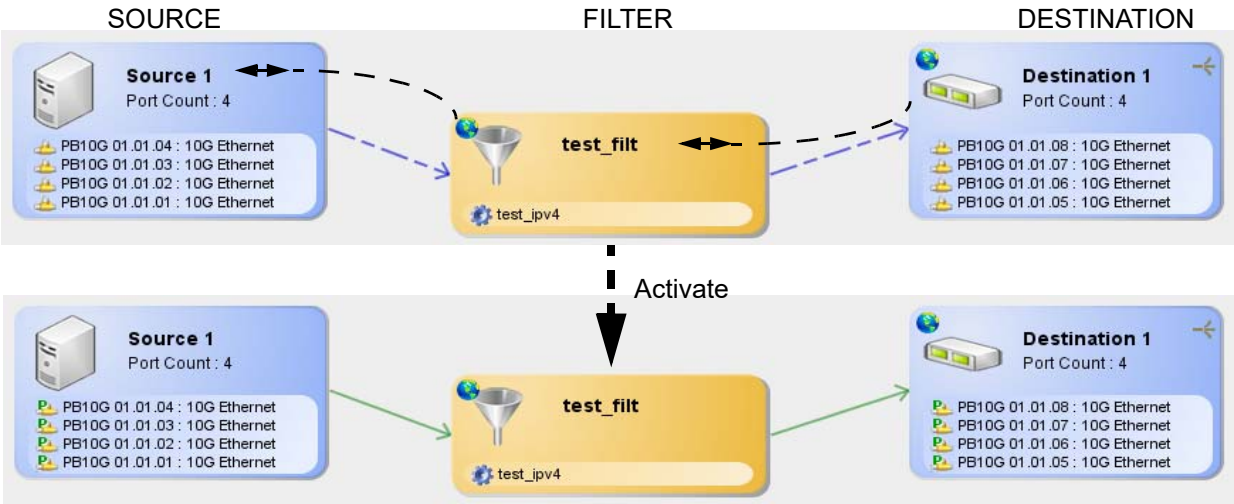
Method 3: From the Rules/Filters tab, select a defined filter (refer to Rules/Filters on page 3-188) and drag it over to the topology screen. A filter object containing the defined filter displays.





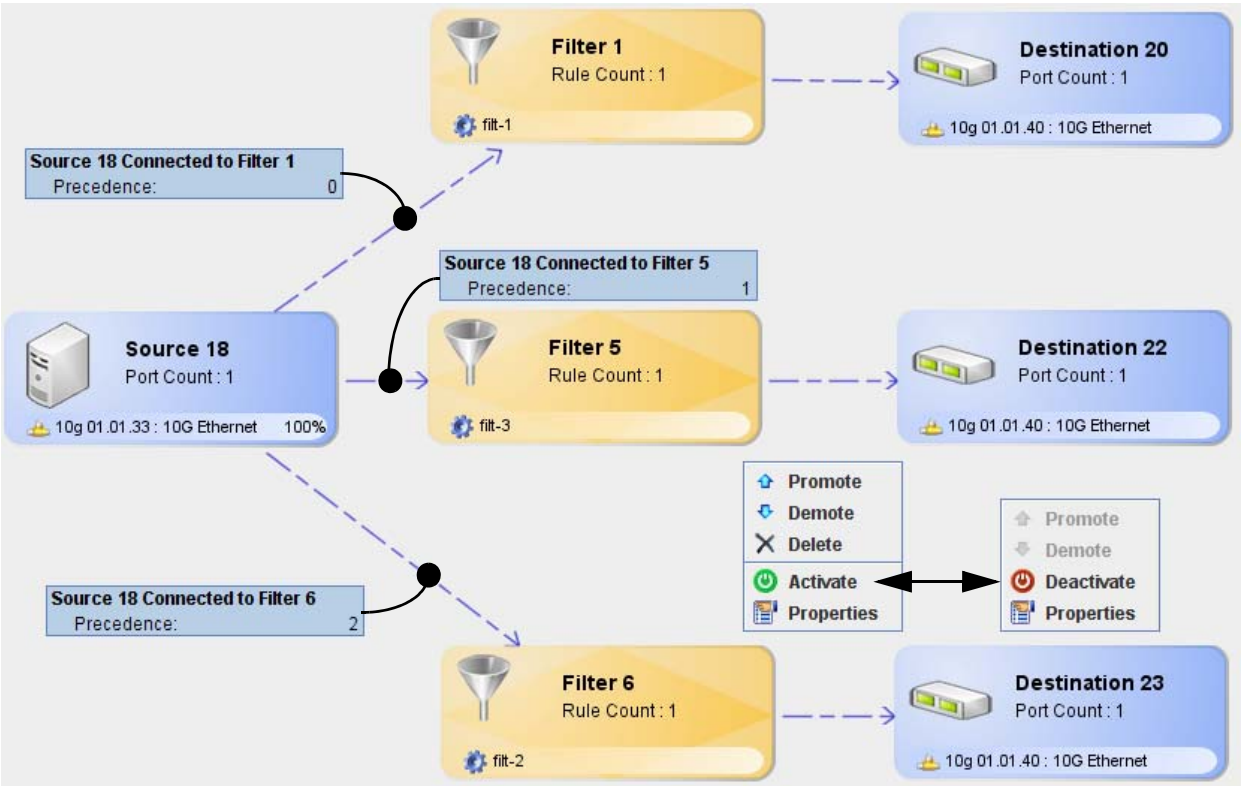
Note: All Source - to - Filter - to - Destination connections are Simplex connections.

To add the filter to a packet connection, select (or right click) the current packet connection then disconnect and remove the connection between the source/destination objects. Right-click on the inside of the source object until a double-arrow line indicator displays. Drag the double-arrow line over to the filter - a blue dotted line displays. Right-click on the inside of the filter object until a double-arrow line indicator displays. Drag the double-arrow line over to the destination object. Click **Activate** to complete the filtered packet connection (the connection lines become solid green, a green check-mark icon displays next to each connected port in the objects and the connection listings in System and Ports/Groups).



Filter Precedence

Filter precedence is used to establish a sequence in which TestStream Management examines incoming traffic and applies a policy rule. TestStream Management automatically sorts policies from the most detailed (highest precedence) to the most basic (lowest precedence), comparing the information in the packet to the list of defined rules in the first policy. The first rule in the list to match the conditions of the packet is applied to the packet. The precedence levels can be modified (Promote / Demote) from the topology manager prior to activation; the precedence order can be changed any time the displayed topology set is deactivated.

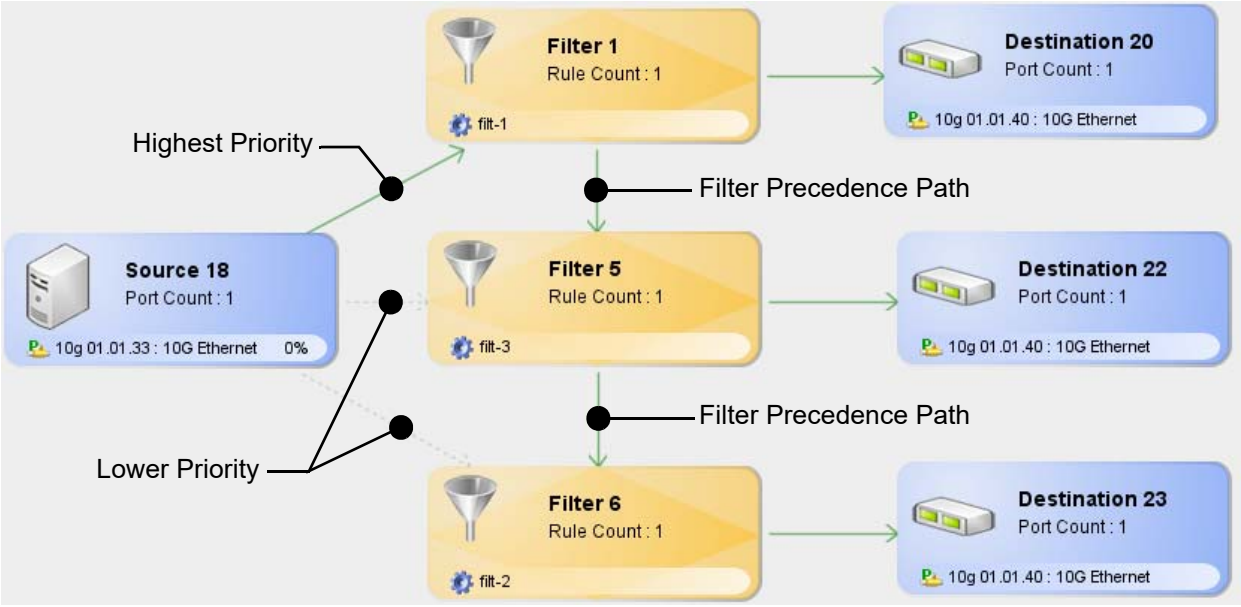


Upon activation of the topology set, the current defined filter precedence paths are displayed:

- Highest priority (Precedence 0) - Solid green line
- All lower precedence (1, 2, etc.) - Dotted light green lines

The current defined filter precedence path is indicated by the flow indicators between the filter objects (for example):

- Filter 1 Connected to Filter 5: Filter 9 only receives traffic that does not match Filter 1's rules
- Filter 5 Connected to Filter 6: Filter 6 only receives traffic that does not match Filter 5's rules



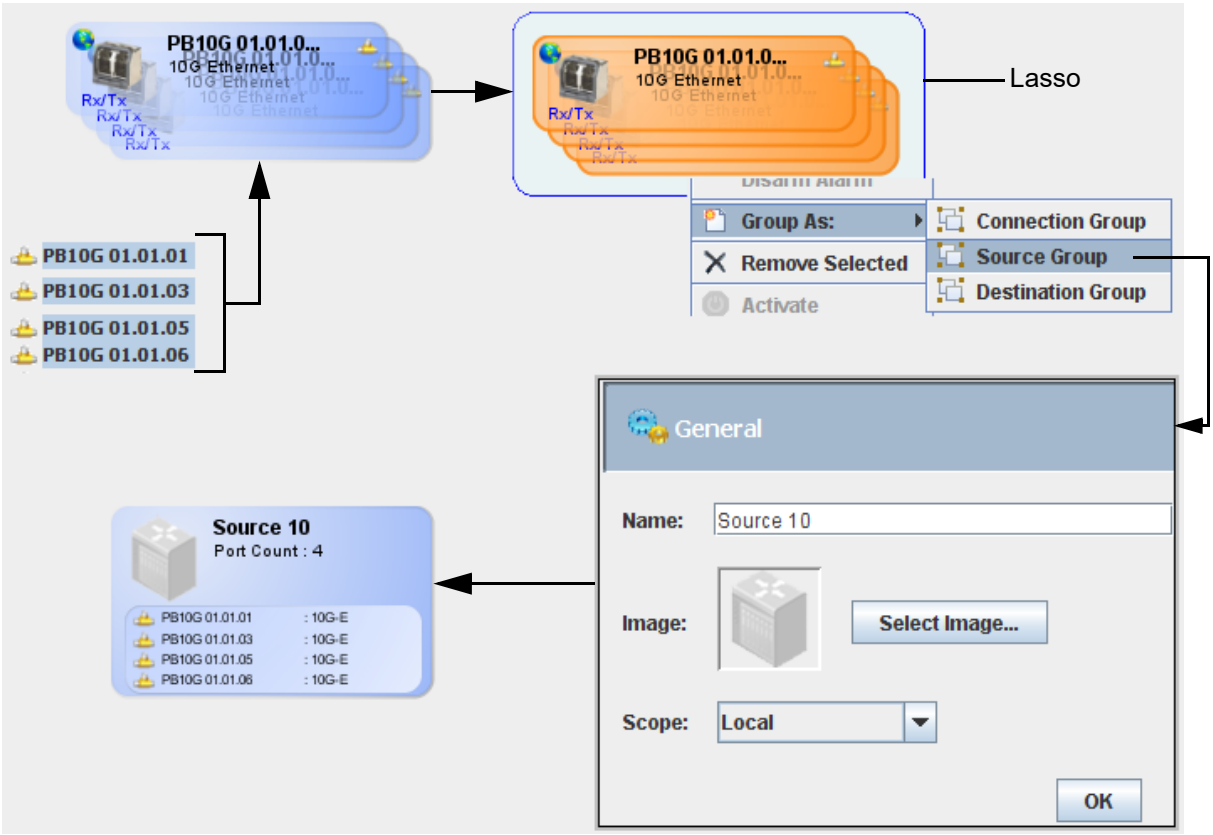
Lasso Feature

The lasso feature allows selecting objects on the topology screen for group (e.g., source, destination, connection) creation or for group deletion.

Port Group Creation

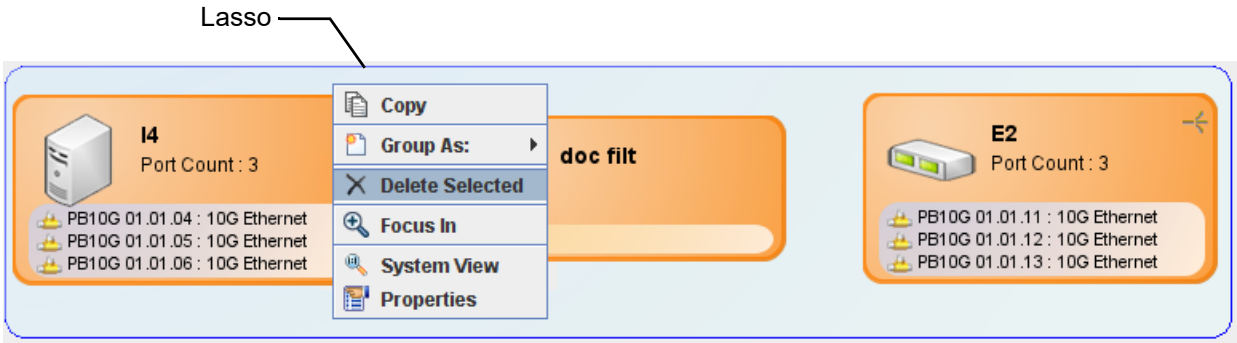
To merge individual ports / subports into groups, select the required ports and drag then over to the topology screen - a set of individual port objects are displayed. Left-click, hold, and drag the cursor to create a lasso area around the port objects. Right-click on one of the selected objects and select **Group As:** then the group type (e.g. Source Group for this example) from the drop down menu. A properties screen displays allowing customizing of the group:

- **Name:** Use the default system name or rename as necessary
- **Image** (Source / Destination Objects): Use the default image or click **Select Image** to choose a different image from the graphic library (refer to Selecting an Object Image on page 6-25)
- **Mode** (Destination Object): Multicast (default) - allows data to be sent over multiple destination ports or Load Balance - distributes data across destination ports
- **Scope:**
  - Local (default) - changes made only to the selected object
  - Global - changes are made to all global-assigned packet objects



Delete Selected Objects

To remove multiple objects all at once from a topology set (instead of clicking on individual objects and selecting Remove), left-click, hold, and drag the cursor to create a lasso area around the objects to delete - each selected object is highlighted. Right-click on one of the selected objects and select **Delete Selected** from the drop down menu.



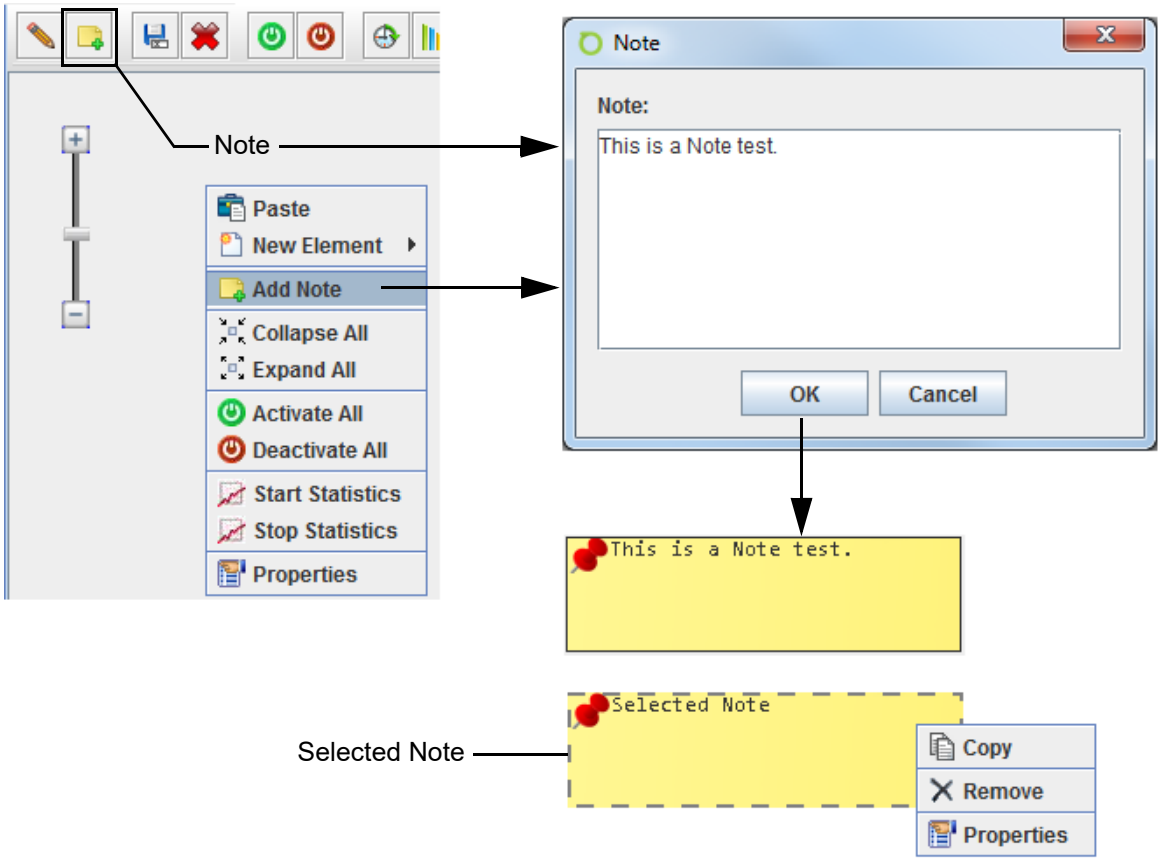
Note: As a shortcut in selecting all of the objects on the topology screen for removal, use **Ctrl + A**, then use the **Delete Selected** menu option.

Note Feature

The note feature allows adding information notes (e.g., user note relating to a defined set of connections) to a selected topology.

1. From the topology screen, right click and select **Add Note** from the menu or click on the Note icon on the topology manager toolbar. The note editing window displays.
2. Enter your text in the Note text field (249 characters max) and click **OK**. The note is displayed on the topology screen. Click and hold on a note to drag it around the screen for positioning as necessary.

Note: A selected note is identified with a dashed border around the note. Click outside of the note to unselect the note.

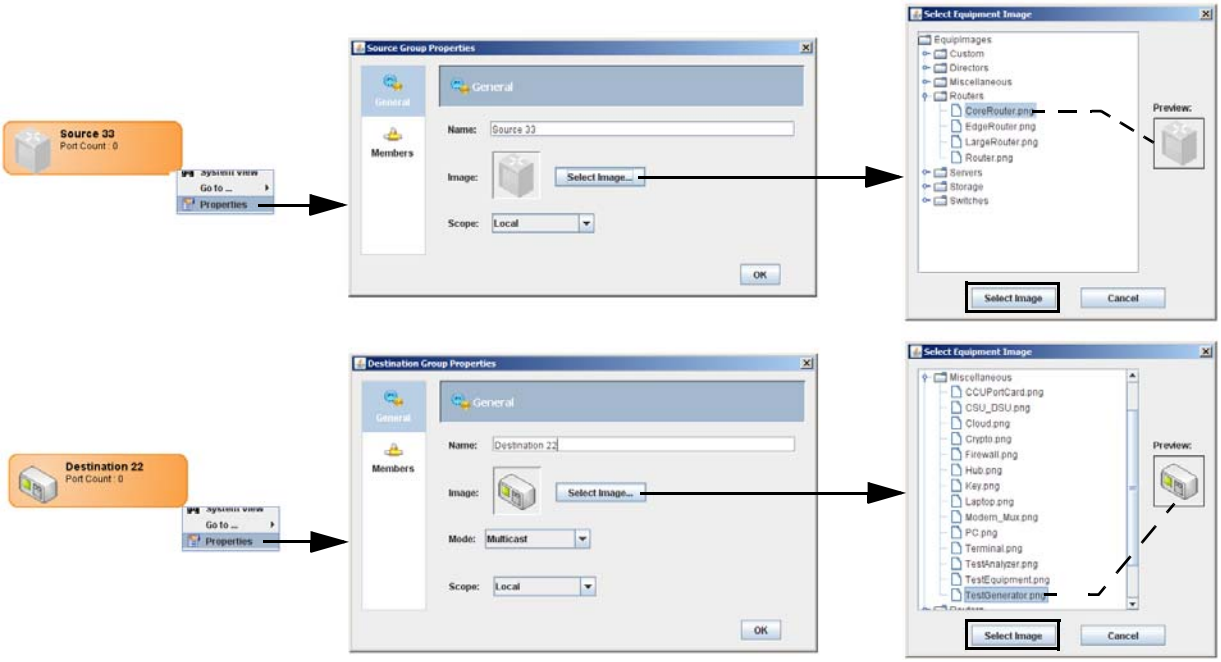


Right click on the note to access the note menu:

- **Copy -** Duplicate the note to the same or a different topology screen.
- **Remove -** Delete the note from the current topology screen.
- **Properties -** Displays the note editing window for making text changes to the selected note.

Selecting an Object Image

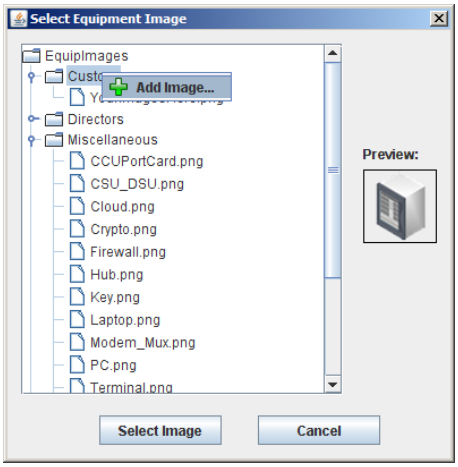
To change the default object image of a source or destination object, select the object, right-click and select **Properties**. From the object properties screen, select **Select Image** to choose a graphic representing the object. Once the image is selected, click **Select Image**. The selected image now displays on the properties screen. Click **OK**. The selected image is now displayed on the object.



Importing Custom Object Images

Additional custom defined images can be added to the TestStream Management image file. The image graphic must be no larger than **64 x 64 pixels** and saved in **.png** file format. The file name for the new image <u>must not</u> contain spaces.

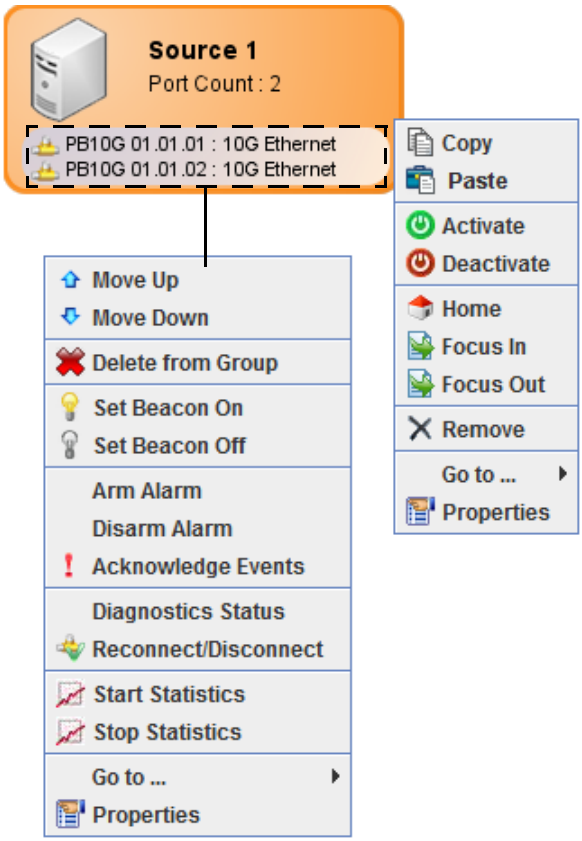
From the object properties screen, click **Select Image**. Right click on the Custom folder and select **Add Image**. A file browser displays. Select the **.png** file of the custom image to import. Once selected, the new image icon appears in the Custom folder.



Topology Objects Sub Menus

Right clicking on a defined topology object (i.e., source, destination, connection, filter) displays the following sub menus:

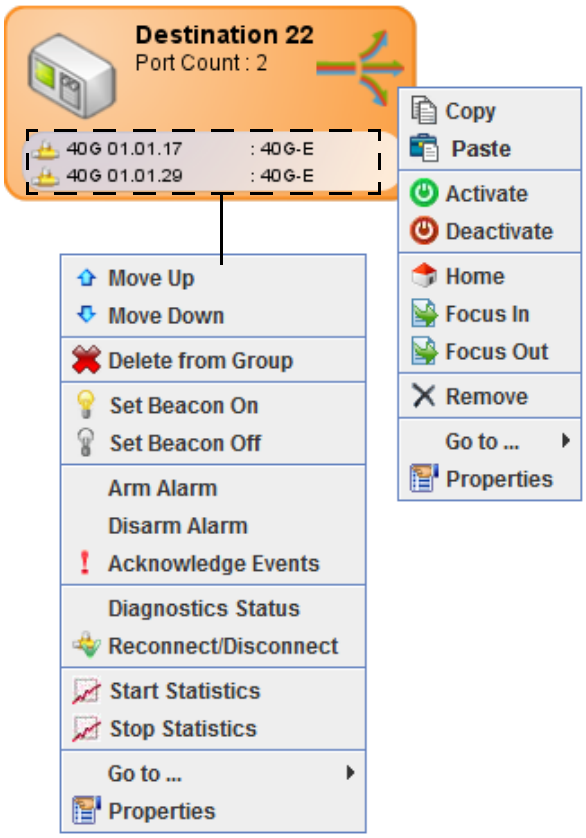
Source Group Objects

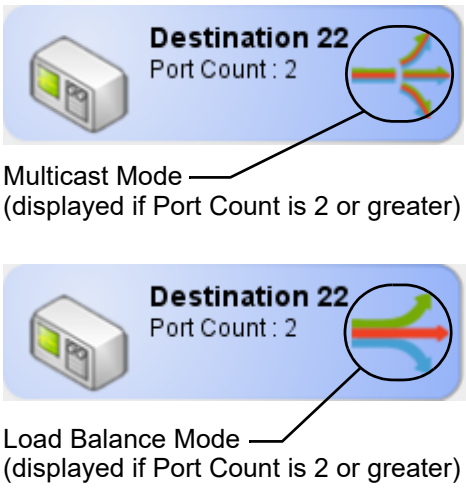


- Move Up / Move Down - Change numeric sequence of ports in the object (this menu function is displayed when port count is 2 or greater)
- Delete from Group - Remove port(s) from source group object
- Set Beacon On / Off - Activates green and yellow pair of LED indicators on the blade to visually locate a blade port in a chassis for maintenance or troubleshooting.
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.
- Reconnect/Disconnect - Reconciles the connections of a selected port
- Copy / Paste (source) - Make a duplicate for placement into the topology set
- Arm / Disarm Alarm - Activate / deactivate port alarms
- Acknowledge Events - Acknowledge port events on a specified port
- Remove (X)- Remove source object from packet set
- Activate - Completes all non-activated packet connections
- Deactivate - Removes all activated packet connections; places connections in standby
- Home / Focus In / Focus Out - Allows removing from view (in a packet set) all but a selected object with associated packet connections
- Start Statistics - Begin statistics recording
- Stop Statistics - End statistics recording

- Go to ... - Links to the following:
  - Switch Graphic
  - Connection Manager
  - Topologies
- Properties (port) - Display / edit source port property settings. Refer to Port Properties on page 3-170.
- Properties (source) - Display / edit source properties (general information, members). Refer to Object Properties on page 6-30.

Destination Group Objects

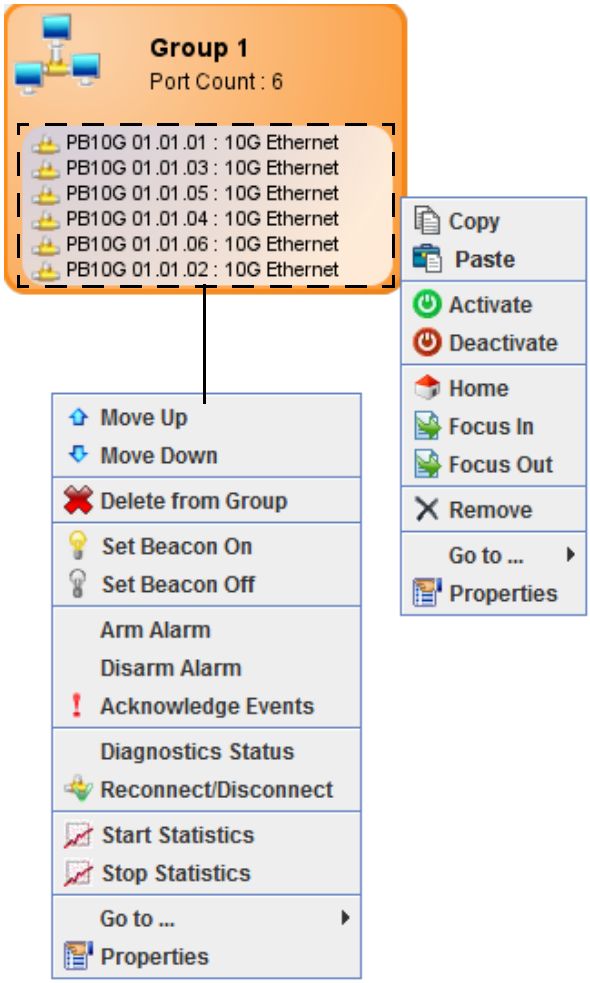




- Move Up / Move Down - Change numeric sequence of ports in the object (this menu function is displayed when port count is 2 or greater)
- Delete from Group - Remove port(s) from destination group object
- Set Beacon On / Off - Activates green and yellow pair of LED indicators on the blade to visually locate a blade port in a chassis for maintenance or troubleshooting.
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.
- Reconnect/Disconnect - Reconciles the connections of a selected port
- Copy / Paste - Make a duplicate for placement into the topology set
- Arm / Disarm Alarm - Activate / deactivate port alarms
- Acknowledge Events - Acknowledge port events on a specified port
- Remove (X) - Remove destination object from packet set
- Activate - Completes all non-activated packet connections
- Deactivate - Removes all activated packet connections; places connections in standby
- Home / Focus In / Focus Out - Allows removing from view (in a packet set) all but a selected object with associated packet connections

- Start Statistics - Begin statistics recording
- Stop Statistics - End statistics recording
- Go to ... - Links to the following:
  - Switch Graphic
  - Connection Manager
  - Topologies
- Properties (port) - Display / edit destination port property settings. Refer to Port Properties on page 3-170
- Properties (destination) - Display / edit destination properties (general information, members). Refer to Object Properties on page 6-30.

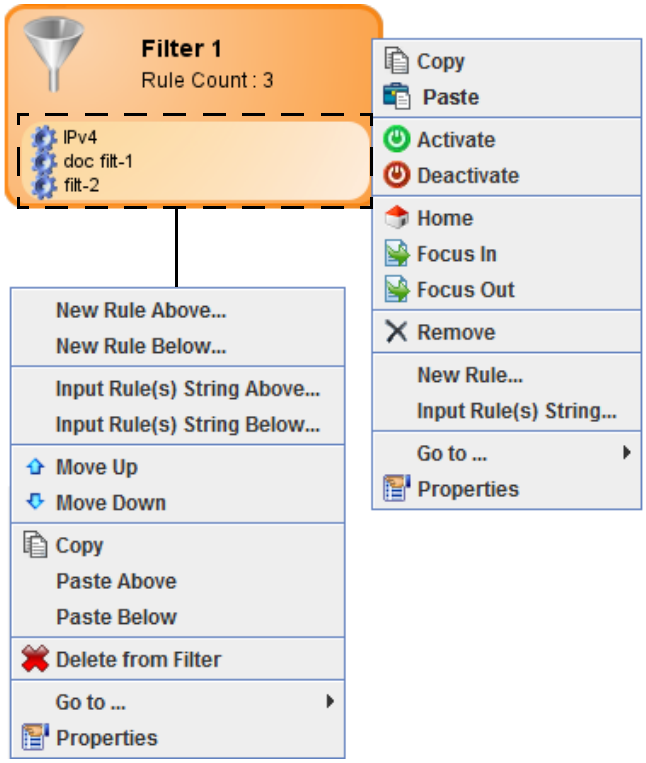
Connection Group Objects



- Move Up / Move Down - Change numeric sequence of ports in the object (this menu function is displayed when port count is 2 or greater)
- Delete from Group - Remove port(s) from connection group object
- Set Beacon On / Off - Activates green and yellow pair of LED indicators on the blade to visually locate a blade port in a chassis for maintenance or troubleshooting.
- Diagnostics Status - Refer to Diagnostics Status on page 7-1.
- Reconnect/Disconnect - Reconciles the connections of a selected port
- Copy / Paste - Make a duplicate for placement into the topology set
- Arm / Disarm Alarm - Activate / deactivate port alarms

- Acknowledge Events - Acknowledge port events on a specified port
- Remove (X) - Remove connection group object from packet set
- Activate - Completes all non-activated packet connections
- Deactivate - Removes all activated packet connections; places connections in standby
- Home / Focus In / Focus Out - Allows removing from view (in a packet set) all but a selected object with associated packet connections
- Start Statistics - Begin statistics recording
- Stop Statistics - End statistics recording
- Go to ... - Links to the following:
  - Switch Graphic
  - Connection Manager
  - Topologies
- Properties (port) - Display / edit connection group port property settings. Refer to Port Properties on page 3-170
- Properties (connection group) - Display / edit connection group properties (general information, members). Refer to Object Properties on page 6-30.

Filter Objects



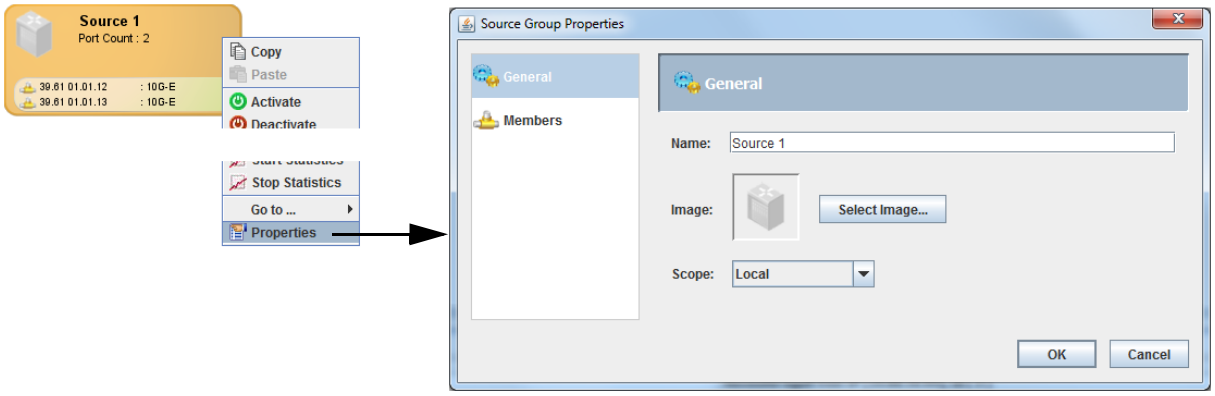
- New Rule Above / Below - Create a new rule and position the rule at a particular order in the filter; refer to Defining Rules on page 3-190
- Input Rule(s) String Above / Below - Create a new rule string and position the rule string at a particular order in the filter; refer to Defining Rules on page 3-190
- Move Up / Move Down - Change numeric sequence of filters in the object (this menu function is displayed when filter count is 2 or greater)
- Delete from Filter - Remove rule from filter object
- Copy / Paste - Make a duplicate for placement into the topology set
- Paste Above / Below - Place a rule from the rules list into the filter at a particular order in the filter

- Remove (X) - Remove connection group object from packet set
- Activate - Completes all non-activated packet connections
- Deactivate - Removes all activated packet connections; places connections in standby
- Home / Focus In / Focus Out - Allows removing from view (in a packet set) all but a selected object with associated packet connections
- Remove (X) - Remove filter object from topology set
- New Rule - Add a new rule; refer to Defining Rules on page 3-190
- Input Rule(s) String - Add a new rule string; refer to Rule Strings on page 3-198
- Go to ... - Links to the following:
  - Switch Graphic
  - Connection Manager
  - Topologies
- Properties (rule) - Display / edit rule settings. Refer to Defining Rules on page 3-190.
- Properties (filter) - Displays filter properties (general information). Refer to Object Properties on page 6-30.

Object Properties

Right clicking on a defined packet set object (i.e., source, destination, connection, filter) and selecting **Properties** displays the properties screen of the selected object.

Source Group

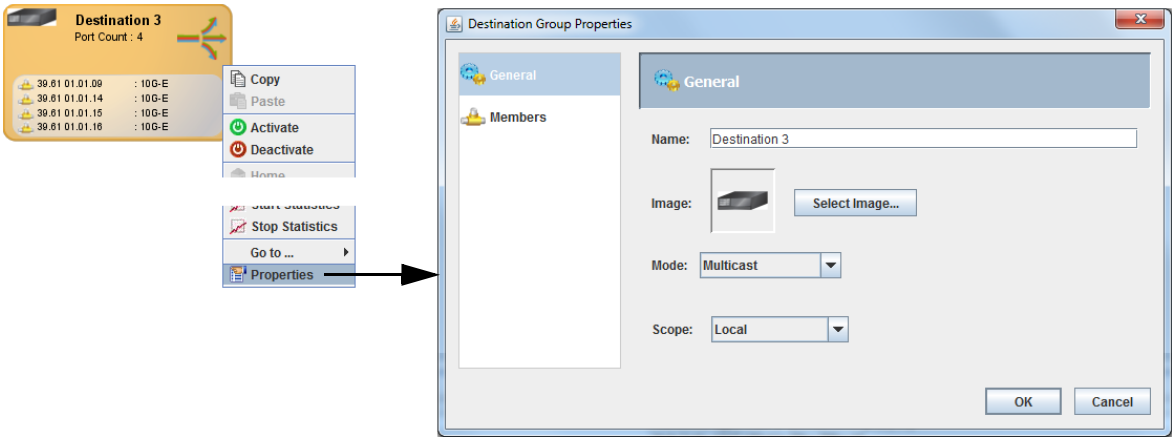


General:

- Name - Title of the source group; use the default name or rename as necessary
- Image - Use the default image or click **Select Image** to choose a different image from the graphic library (refer to Selecting an Object Image on page 6-25)
- Scope:
  - Local (default) - changes made only to the selected object
  - Global - changes are made to all global-assigned packet objects

Members: Lists all ports associated to the source group

Destination Group

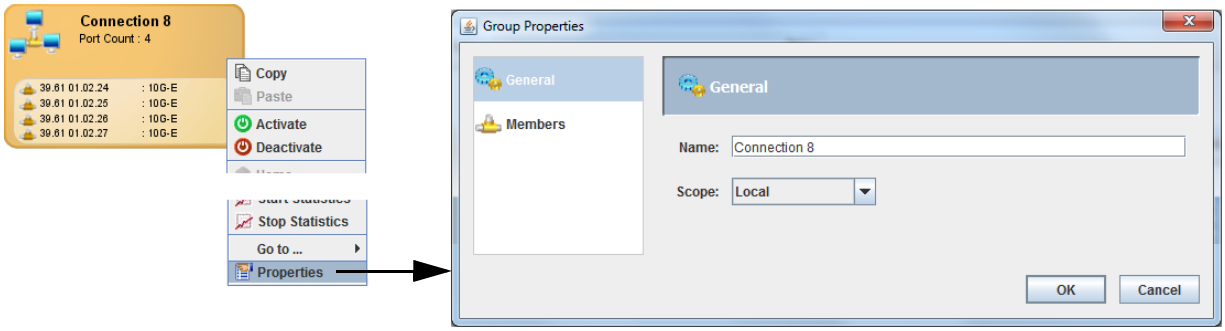


General:

- Name - Title of the destination group; use the default name or rename as necessary
- Image - Use the default image or click **Select Image** to choose a different image from the graphic library (refer to Selecting an Object Image on page 6-25)
- Mode - Multicast - allows data to be sent over multiple destination ports; Load Balance (default) distributes data across destination ports
- Scope:
  - Local (default) - changes made only to the selected object
  - Global - changes are made to all global-assigned packet objects

Members: Lists all ports associated to the destination group

Connection Group

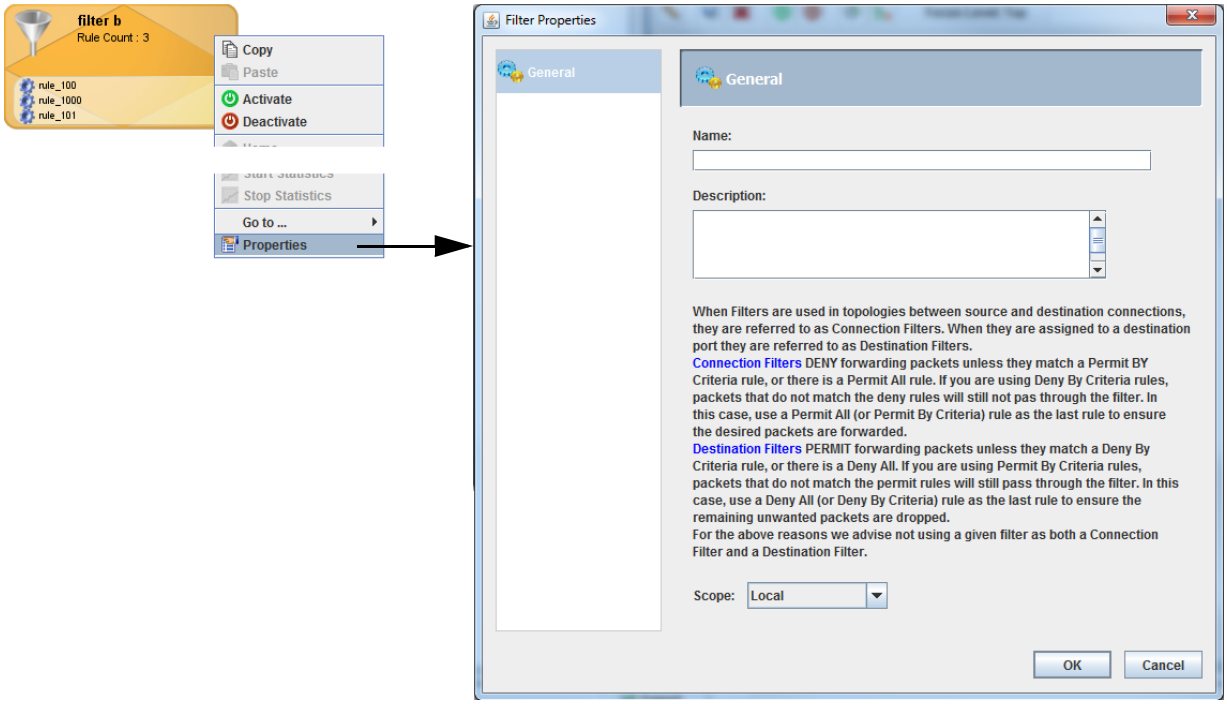


General:

- Name - Title of the connection group; use the default name or rename as necessary
- Scope:
  - Local (default) - changes made only to the selected object
  - Global - changes are made to all global-assigned packet objects

Members: Lists all ports associated to the connection group

Filter



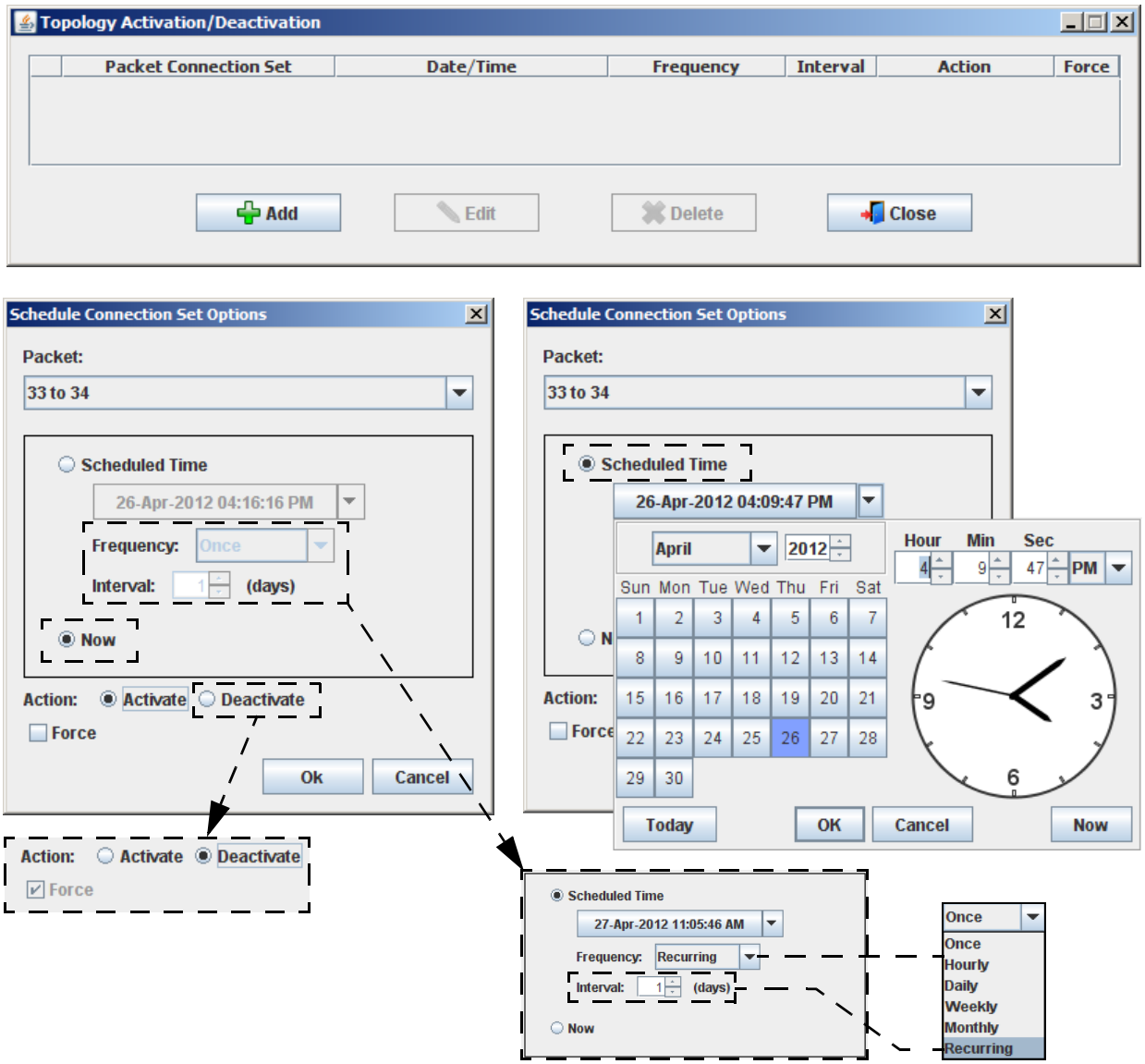
General:

- Name - Title of the filter; use the default name or rename as necessary
- Description - Add information describing filter function / usage
- Scope:
  - Local (default) - changes made only to the selected filter
  - Global - changes are made to all global-assigned packet filters

Topology Connection Scheduler

Topology Connection Scheduler allows assigning activation / deactivation times for selected connection sets.

1. Select a connection set from the topology drop down menu, then click on the Packet Set Scheduler icon. The Topology Activation/Deactivation screen displays.
2. Click **Add**. A Schedule Connections Set Options screen displays. Select a packet set from the **Packet** drop down menu.
3. Set time setting: Click **Now** (default) to set an immediate action. Select **Scheduled Time** to set an action for a particular time / date. The **Frequency** drop down menu is used to set either a single or recurring activation / deactivation (if Frequency = Recurring is selected, the time interval, in days, can be set from 1 to 31).
4. Select the required Action: **Activate** the packet set; Force activation is optional.
   or
   Deactivate (Force is automatically selected for deactivation).
5. Click **OK** to save the settings. The timed packet set is displayed in the Topology Activation/Deactivation screen showing the assigned settings. To modify a timed packet set, click on the packet set and click **Edit**. To remove a timed packet set, click on the packet set and click **Delete**. Click **Close** to end the session.



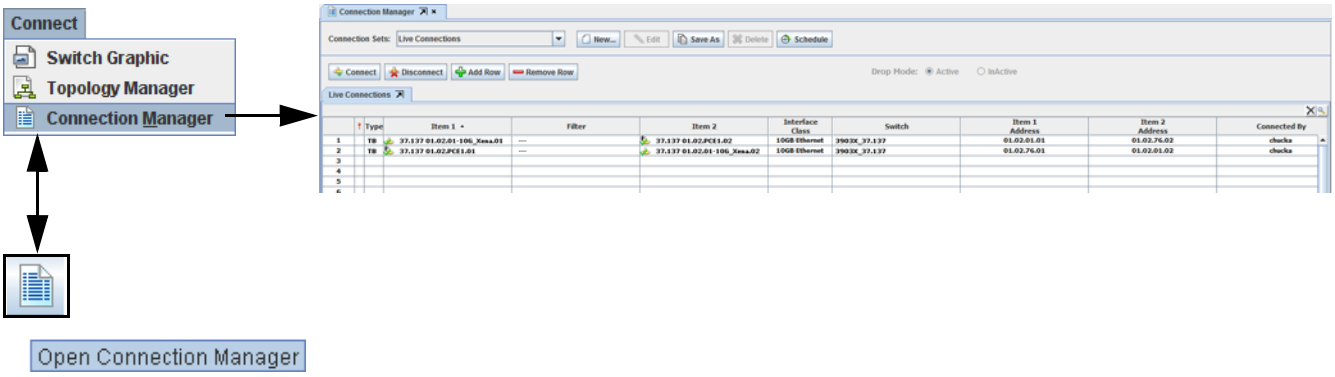
Connection Manager

The Connection Manager provides port connection functionally, displaying live connections and currently defined connection sets.

> **Note:** T-Blade, HS-3200, and HS-6400 connectivity from the Connection Manager is not supported, however packet connections are displayed. Refer to Test Blade Connectivity on page 6-35.

Connection sets and the live connections table will span multiple switches if they exist.

1 Select **Connect > Connection Manager**, or from the toolbar, select the **Connection Manager** icon, or from the keyboard **Alt+F7**. The Connection Manager screen displays.



The following columns are displayed:

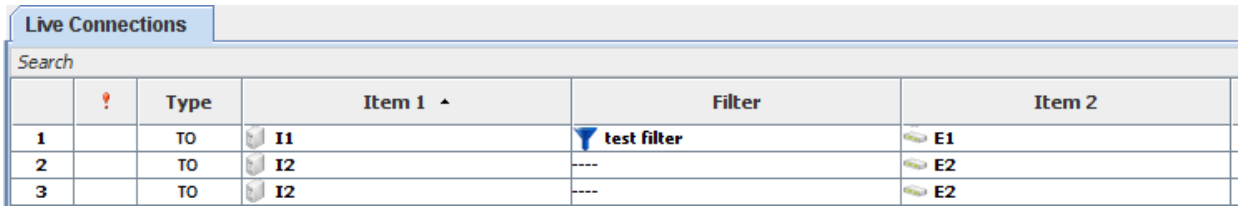
- Alarmed **(!)** – Indicates that at least one of the ports in the connection is alarmed. Clicking on the icon sorts and displays all information-marked lines together.
- Type – P (port connection - duplex), sP (simplex port connection - 39xx series only), MT (mirror/test connection), T (test connection), G (group connection - duplex), sM (simplex multicast - 39xx series only), TO (Topology Only).
- Item 1 / Item 2 – displays the connection path. Sortable by name (click on either Item 1 or Item 2).
- Connection Filter - displays a connected defined filter.
- Connection Impairment - displays a connected defined impairment.
- Interface Class – displays the blade class.
- Switch – displays the switch name where connections are live. Clicking on Switch sorts the switches by type.
- Item 1 Address / Item 2 Address– displays the physical port path location (chassis.blade.port) of the connection.
- Connected By - displays the login name of the user who made the connection.
- Connect Time - displays the date / time the connection was made.
- Job Code - optional user-entered information (refer to Connection Comments Mode on page 4-42)
- Comment - optional user-entered information refer to Connection Comments Mode on page 4-42)

> **Note:** The displayed columns can be user selected using the Connection Table Filter > Display Columns option.

Right-clicking on the **Live Connections** tab allows selective filtering and printing the list of connections. Filter by switch, domain security, connection type, interface, option to turn on / off display columns (switch and or physical port path). The list of connections can be saved / exported to a CSV file for use in an Excel spreadsheet or other application.

Test Blade Connectivity

Packet connections created in the topology manager (refer to Topology Manager on page 6-2) are displayed in the connection manager.



The following fields are displayed:

- **!** – Information: Indicates that at least one of the ports in the connection is alarmed. Clicking on the icon sorts and displays all information-marked lines together.
- Type – TO (Topology Only)
- Item 1 (source) / Item 2 (destination) – displays the connection path.

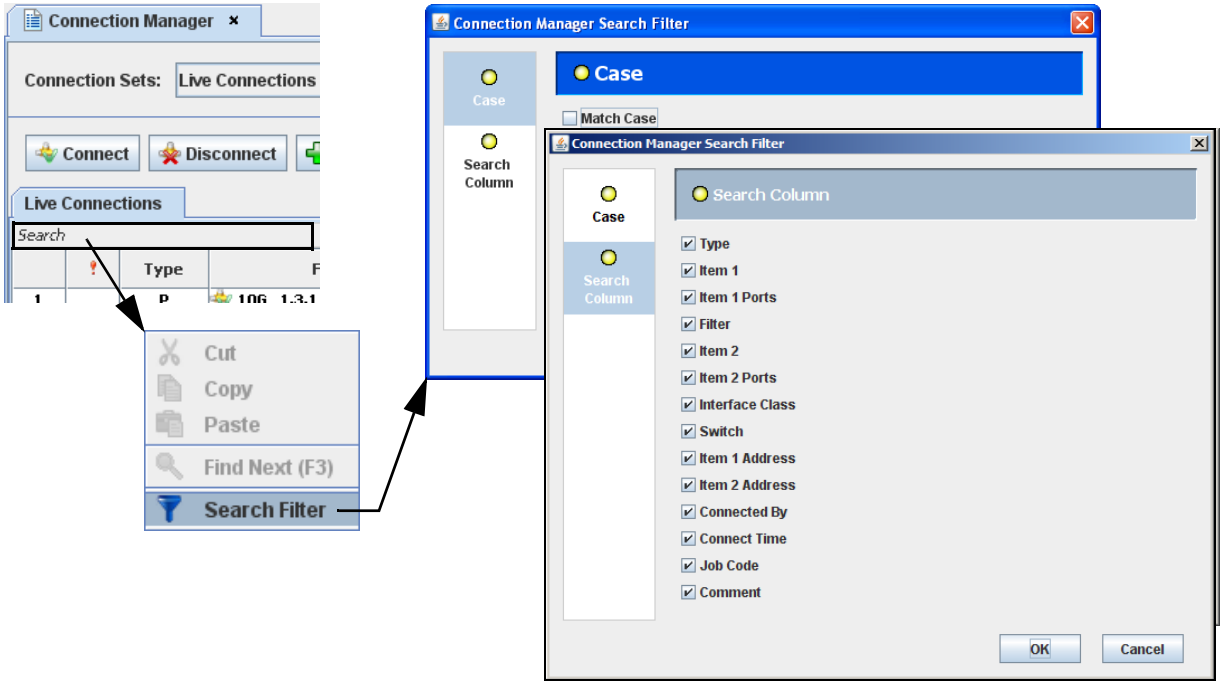
> **Note:** Test blade live connections are sortable from the Item 1 (source) column only.

- Filter - displays associated filter (if used in packet connection)

Connection Manager Search

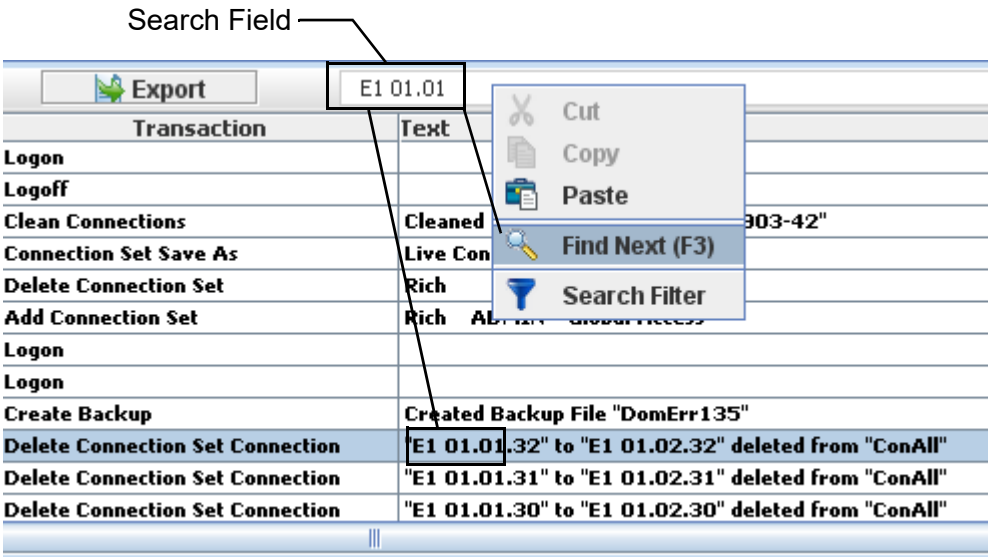
The search function allows the user to define the search parameters for a particular switch based on selected column fields.

From the Connection Manager screen, right-click on the **Search** field. Select **Search Filter**. The connection Manager Search Filter displays. From the Case and Search Column screens, click to select / unselect the fields required for the search query.



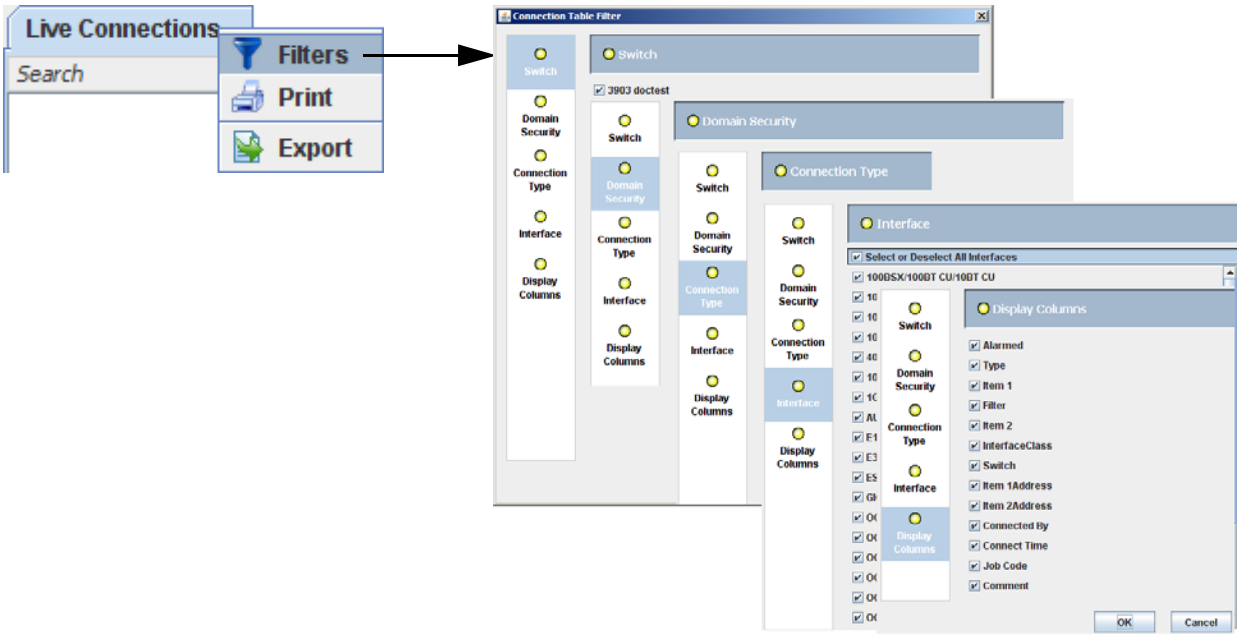
Find Next (F3)

From the Search field, enter a variable port name (e.g., E1 01.01) to locate all occurrences starting with the port name. The first occurrence of the variable will be located. To locate additional occurrences of the same variable name, right-click on the search name and select **Find Next (F3)** or use the **F3** key. Continue using the F3 key to find all occurrences as required.



Connection Table Filters

Right-clicking on a connection set tab allows defining the display properties of the connection table.



- Switch - lists all connected switches (selected by default); unselect to remove from displayed listing
- Domain Security - select all ports (default) or only ports accessible in Domain Security.
- Connection Type - select the type of connections to list.
- Interface - select the type of interfaces to list.
- Display Columns - select which columns to display.

Chapter 7
Diagnostics and System Tests

This chapter describes the TestStream Management diagnostics status and test features for the nGenius 3900 switch.

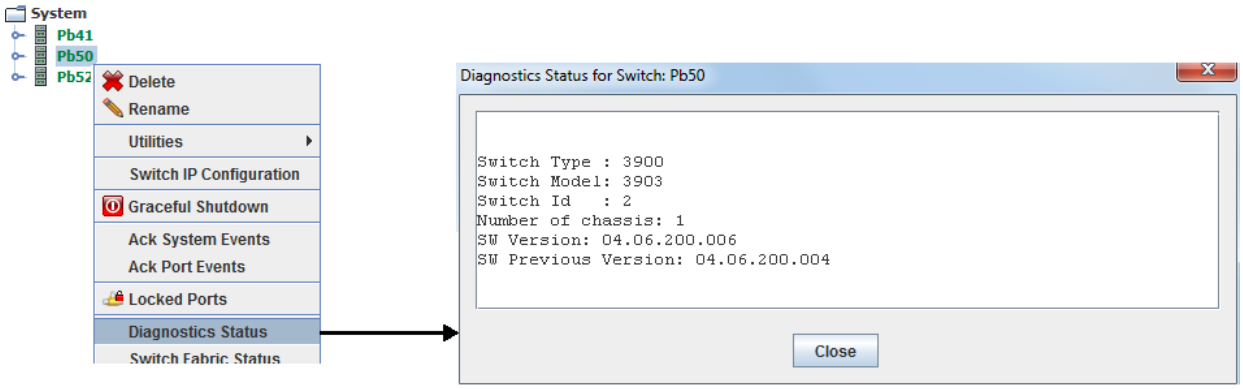
Diagnostics Status

Operational status of the nGenius 3900 series switch is displayed for the following:

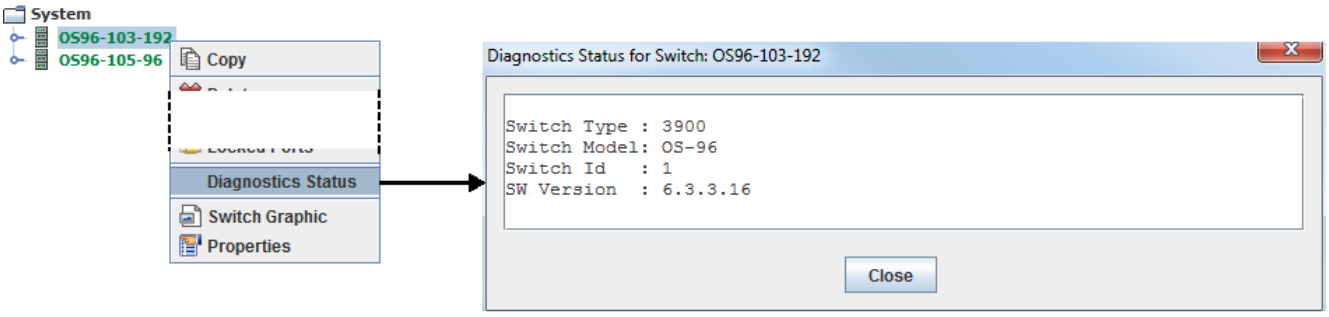
- Switch
- Chassis
- Blade
- Port

Switch

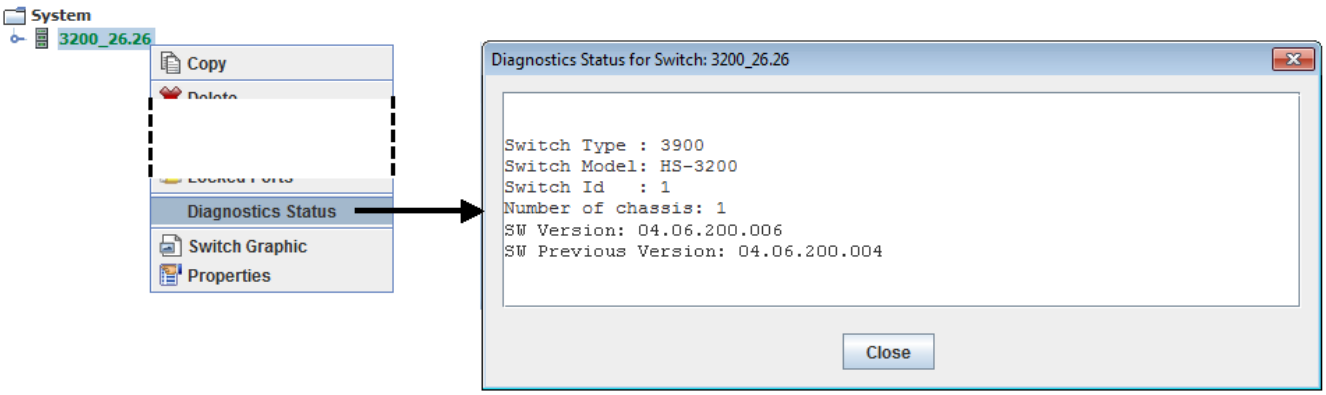
Click on the **System** tab. From the switch level, right-click on the switch name then select **Diagnostics Status** from the drop-down menu. A screen displays the switch type / model, number of chassis in the switch, and currently / previously installed TestStream Management software versions.



For the OS-16, OS-96, and OS-192 optical switches, Diagnostics displays the switch type / model, switch identifier, and firmware version installed in the switch.



For the HS-3200 switch, Diagnostics displays the switch type / model, number of chassis in the switch, and currently / previously installed TestStream Management software version.s

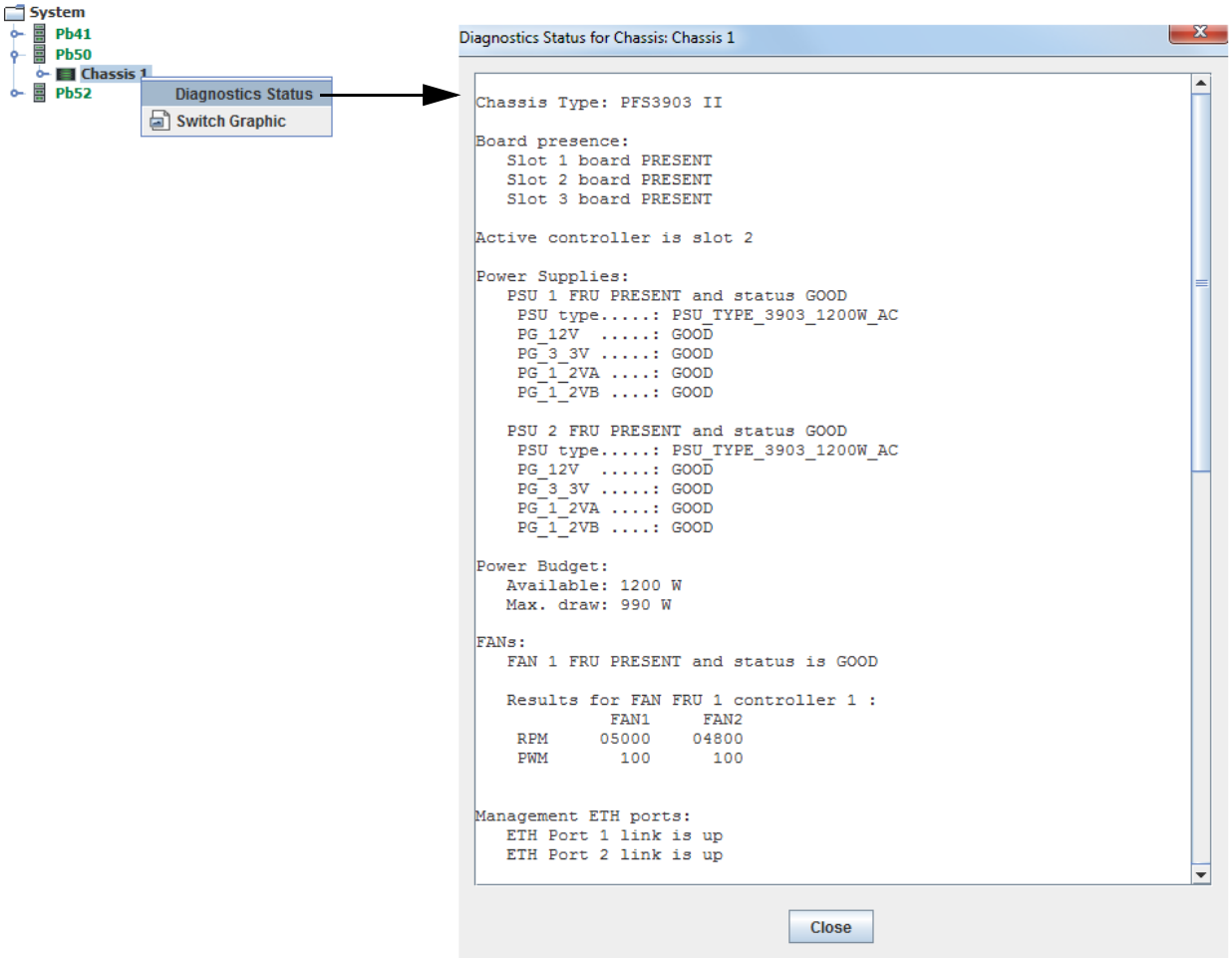


Chassis

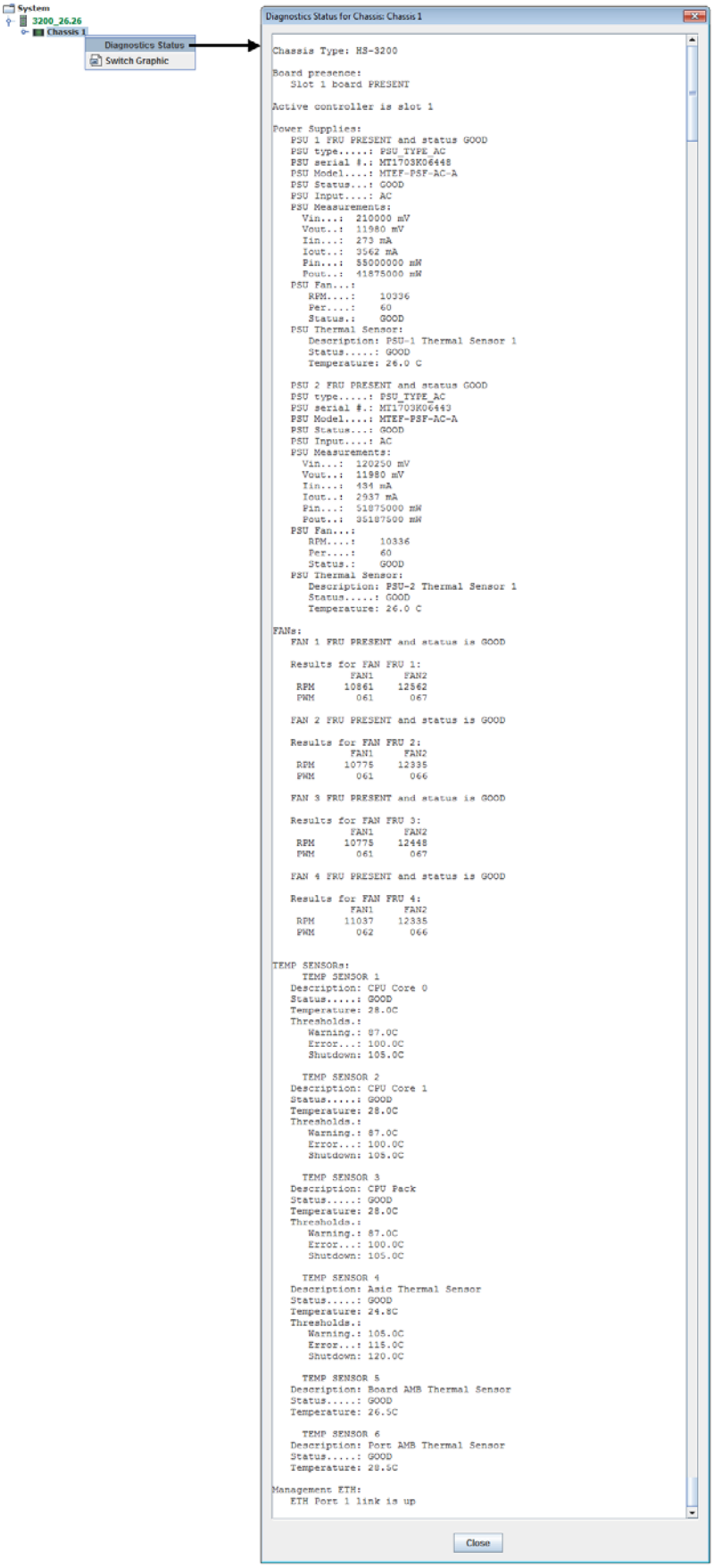
Click on the **System** tab. From the chassis level, right-click on the chassis name then select **Diagnostics Status** from the drop-down menu. A screen displays the current status of the chassis including slot locations of blades installed in chassis, power supply status, fan status, fan controller status, and slot location of active chassis controller.

Note: Diagnostics Status for Chassis is not supported on OS-16, OS-96, and OS-192 switches.

nGenius 3900 Switches (typical)



HS-3200 Switches (typical)

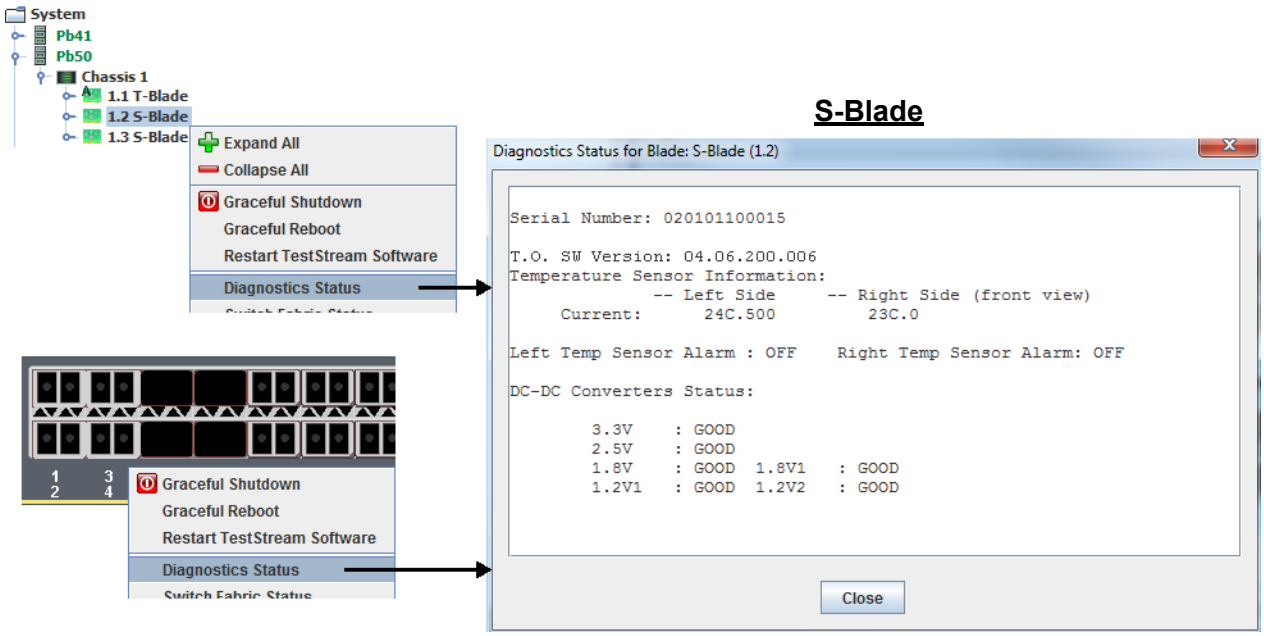


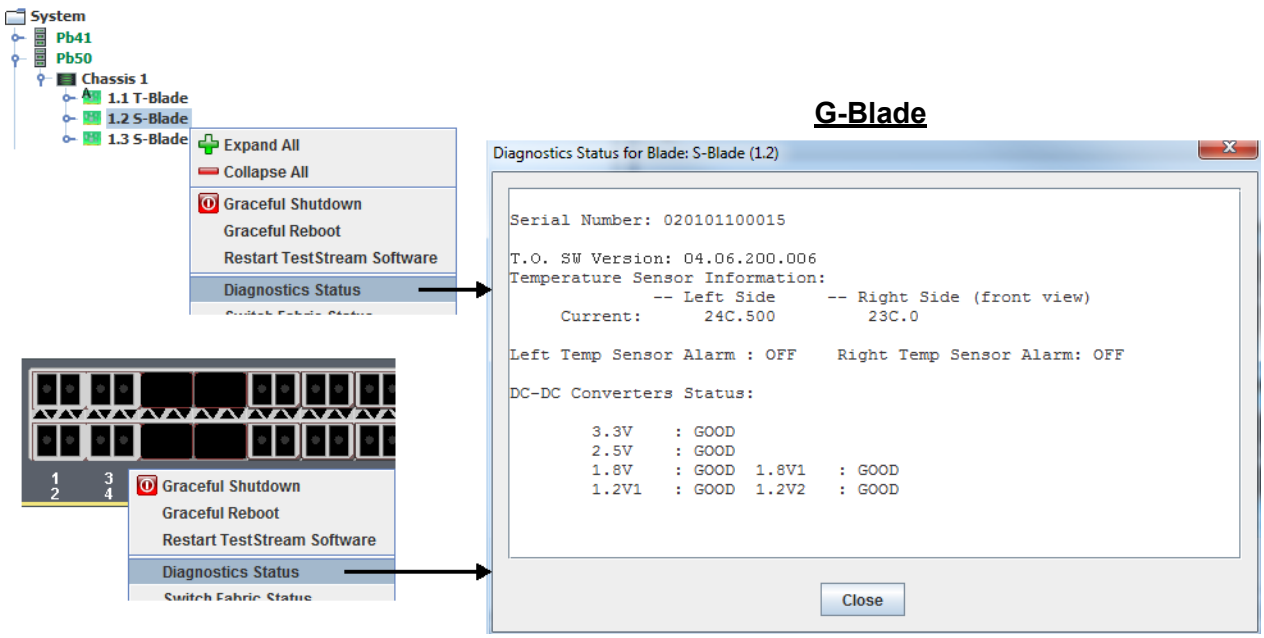
Blade

Click on the **System** tab. From the blade level, right-click on the blade name then select **Diagnostics Status** from the drop-down menu.
- or -
From the **Switch Graphic** view, right-click on the blade graphic then select **Diagnostics Status** from the drop-down menu.

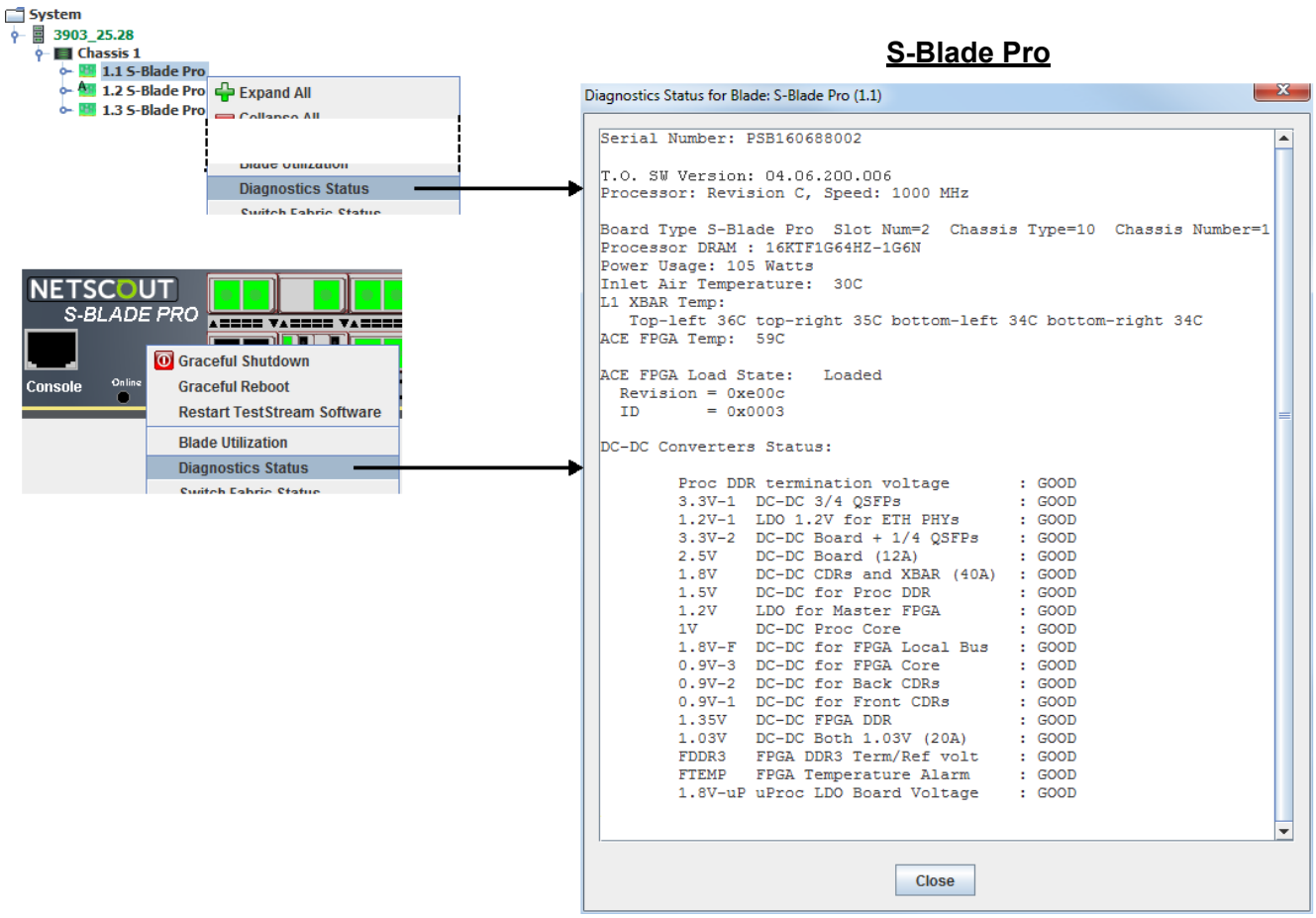
A screen displays the current status of the selected blade including temperature sensors, power converter status, filter resources currently available on the blade, and version of TestStream Management software installed on the blade.

> **Note:** Diagnostics Status for Blades is not supported on OS-16, OS-96, and OS-192 switches.

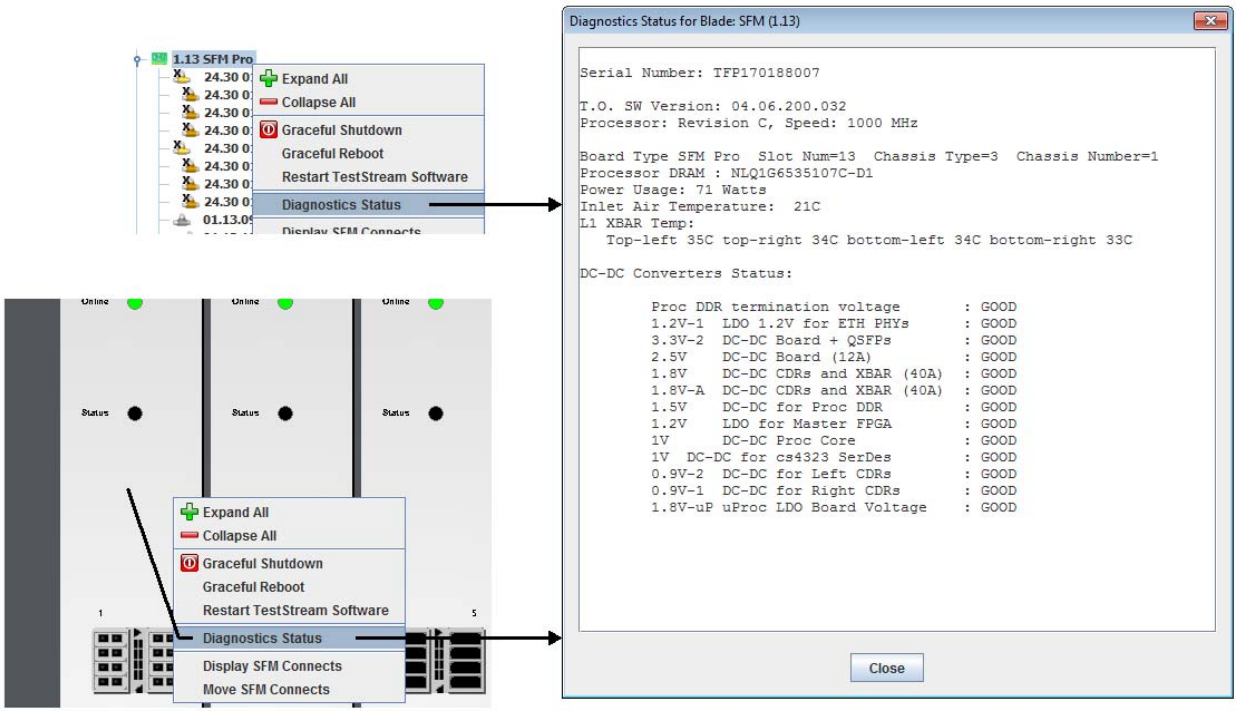




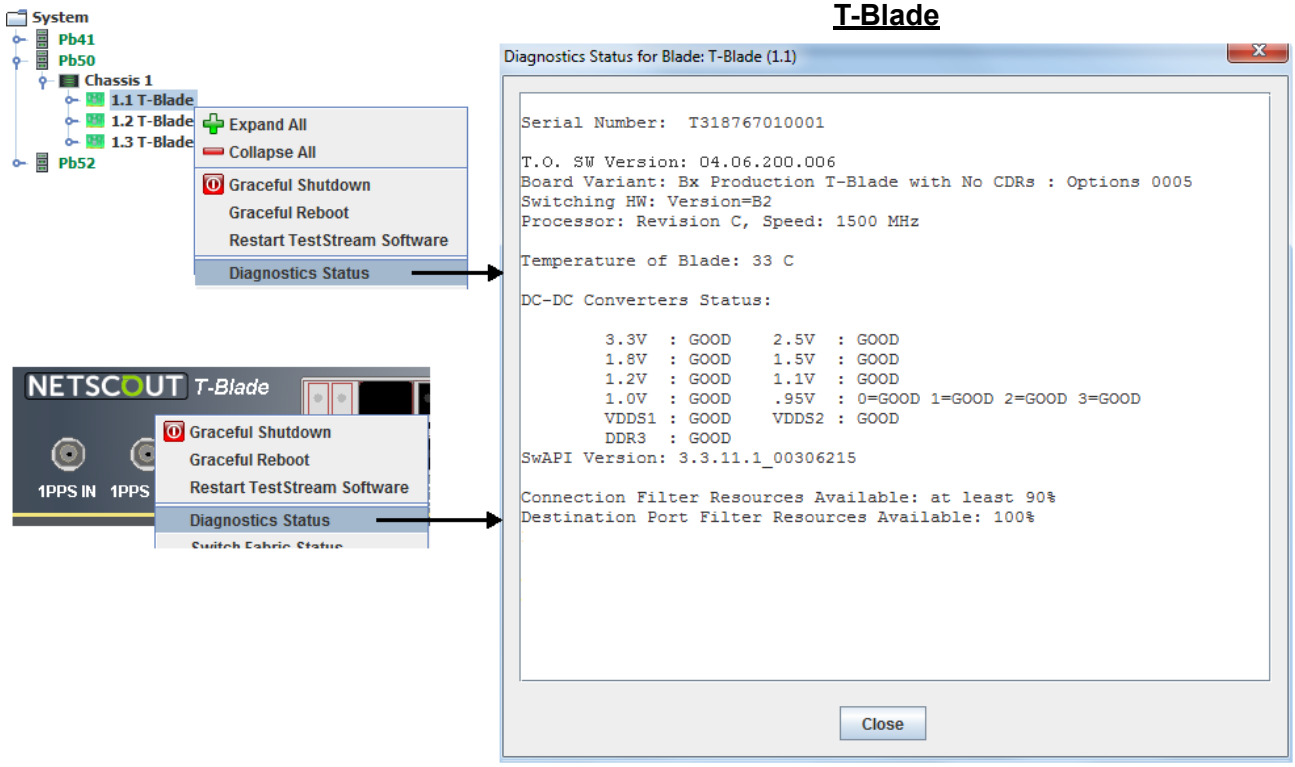
S-Blade Pro



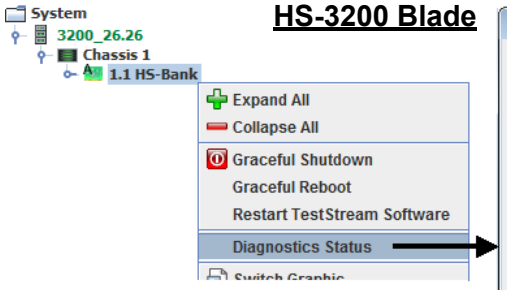
SFM Pro

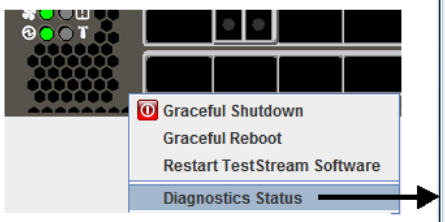


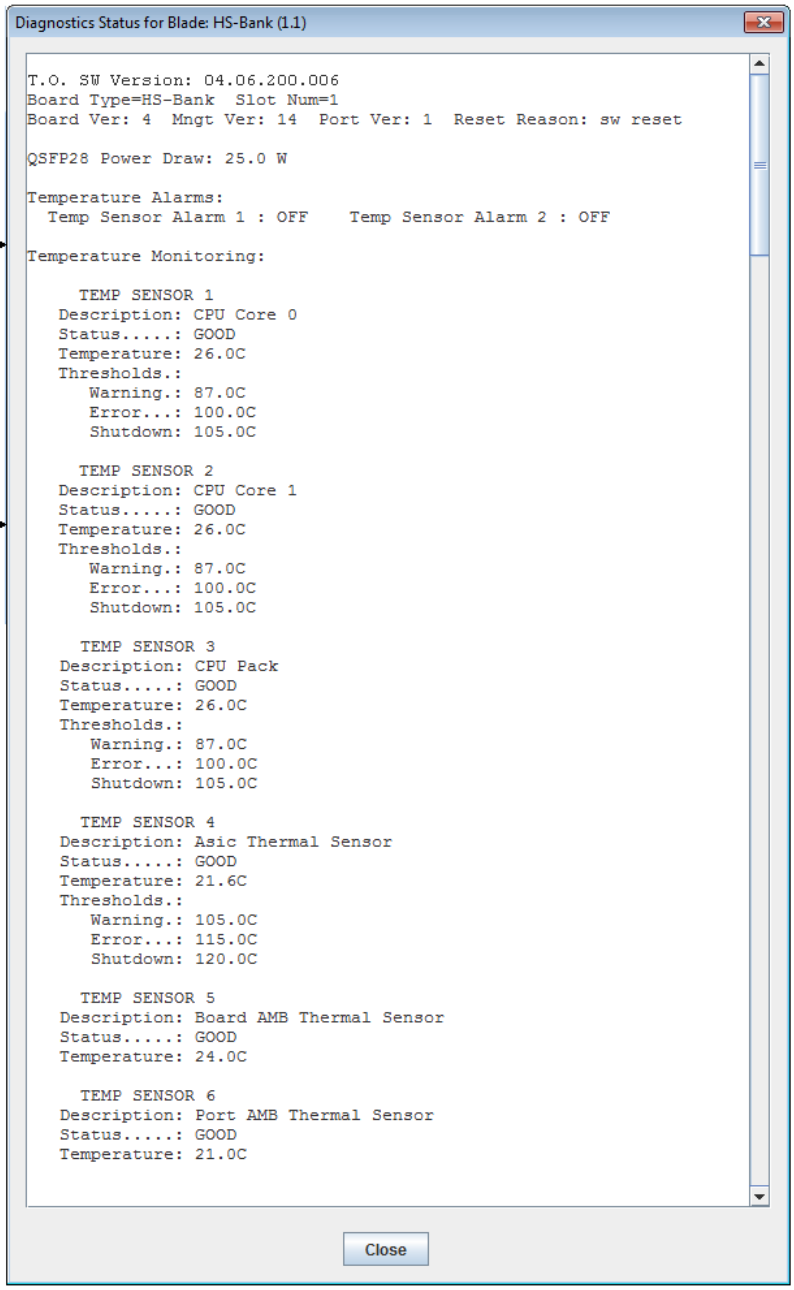
T-Blade

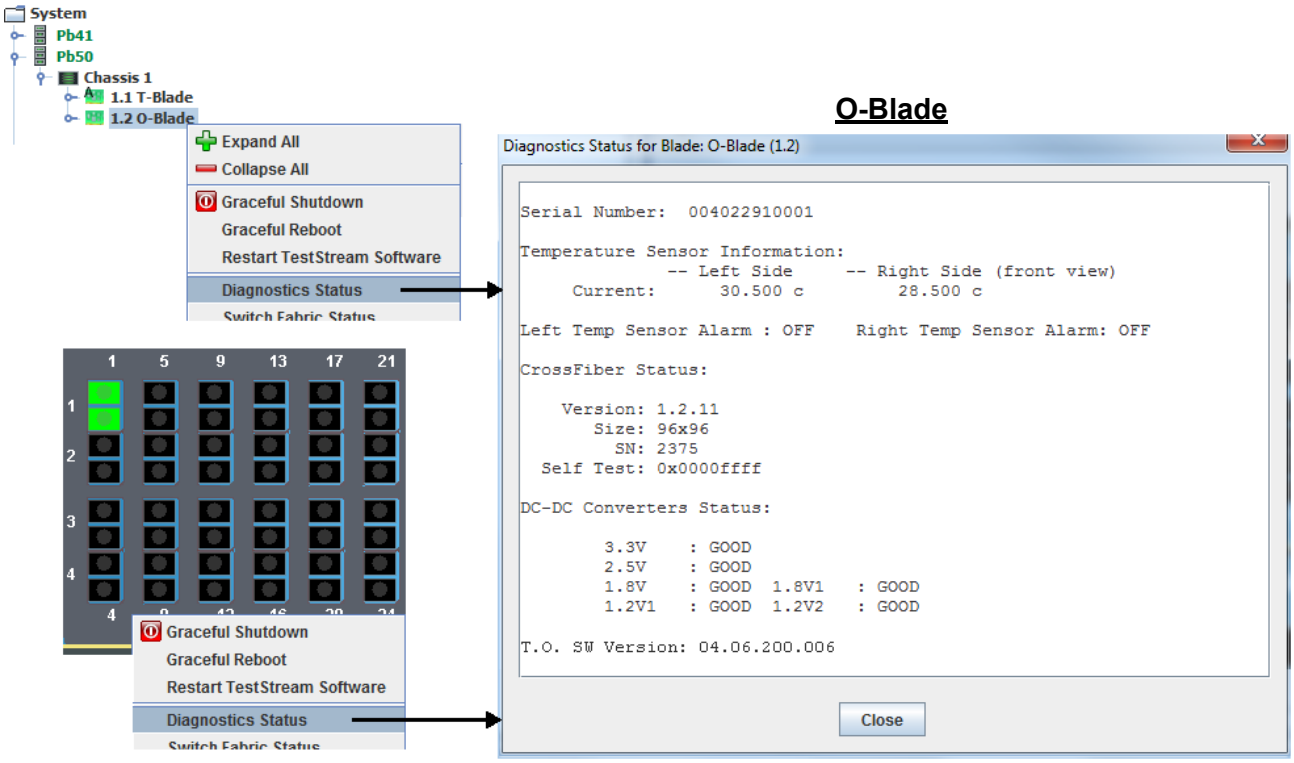

System
Pb41
Pb50
Chassis 1
1.1 T-Blade
1.2 T-Blade
1.3 T-Blade
Pb52
Expand All
Collapse All
Graceful Shutdown
Graceful Reboot
Restart TestStream Software
Diagnostics Status
NETSCOUT T-Blade
1PPS IN
1PPS
Graceful Shutdown
Graceful Reboot
Restart TestStream Software
Diagnostics Status
Diagnostics Status for Blade: T-Blade (1.1)
Serial Number: T318767010001
T.O. SW Version: 04.06.200.006
Board Variant: Bx Production T-Blade with No CDRs : Options 0005
Switching HW: Version=B2
Processor: Revision C, Speed: 1500 MHz
Temperature of Blade: 33 C
DC-DC Converters Status:
3.3V : GOOD 2.5V : GOOD
1.8V : GOOD 1.5V : GOOD
1.2V : GOOD 1.1V : GOOD
1.0V : GOOD .95V : 0=GOOD 1=GOOD 2=GOOD 3=GOOD
VDDS1 : GOOD VDDS2 : GOOD
DDR3 : GOOD
SwAPI Version: 3.3.11.1_00306215
Connection Filter Resources Available: at least 90%
Destination Port Filter Resources Available: 100%
Close

HS-3200 Blade








O-Blade
System
Pb41
Pb50
Chassis 1
1.1 T-Blade
1.2 O-Blade
Expand All
Collapse All
Graceful Shutdown
Graceful Reboot
Restart TestStream Software
Diagnostics Status
Switch Fabric Status
Graceful Shutdown
Graceful Reboot
Restart TestStream Software
Diagnostics Status
Switch Fabric Status
Diagnostics Status for Blade: O-Blade (1.2)
Serial Number: 004022910001
Temperature Sensor Information:
-- Left Side -- Right Side (front view)
Current: 30.500 c 28.500 c
Left Temp Sensor Alarm : OFF Right Temp Sensor Alarm: OFF
CrossFiber Status:
Version: 1.2.11
Size: 96x96
SN: 2375
Self Test: 0x0000ffff
DC-DC Converters Status:
3.3V : GOOD
2.5V : GOOD
1.8V : GOOD 1.8V1 : GOOD
1.2V1 : GOOD 1.2V2 : GOOD
T.O. SW Version: 04.06.200.006
Close

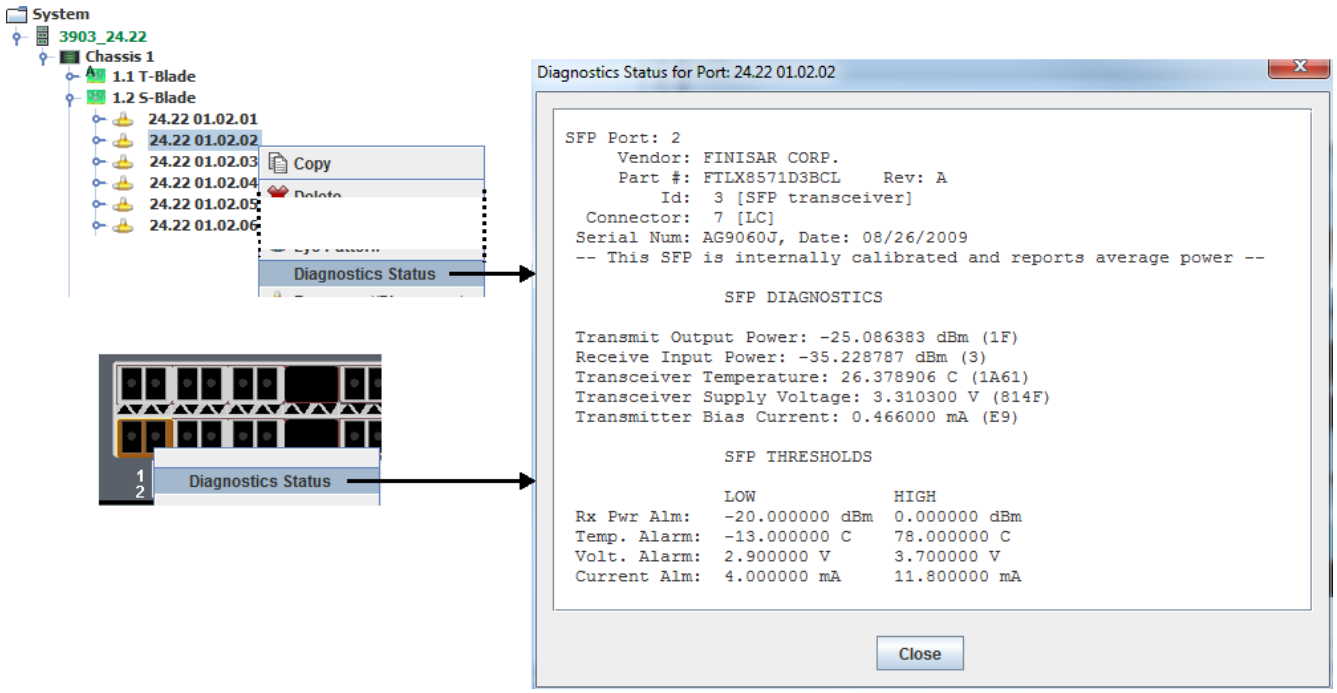
Port

Click on the **System** tab. From the port level, right-click on the port name then select **Diagnostics Status** from the drop-down menu.
- or -
From the **Switch Graphic** view, right-click on the selected port graphic then select **Diagnostics Status** from the drop-down menu

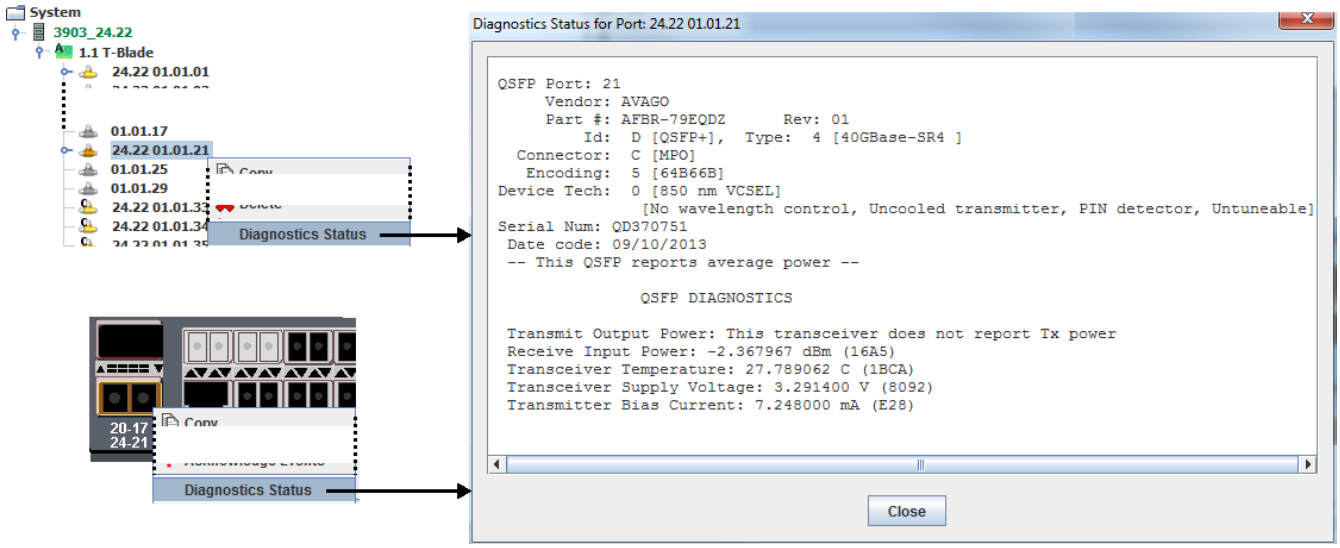
A screen displays the current status of the selected port including transceiver manufacturer specifications, transceiver average transmitter / receiver power levels, transceiver operating temperature, supply voltage, and operating current.

Note: Diagnostics Status for Ports is not supported on OS-16, OS-96, and OS-192 switches.

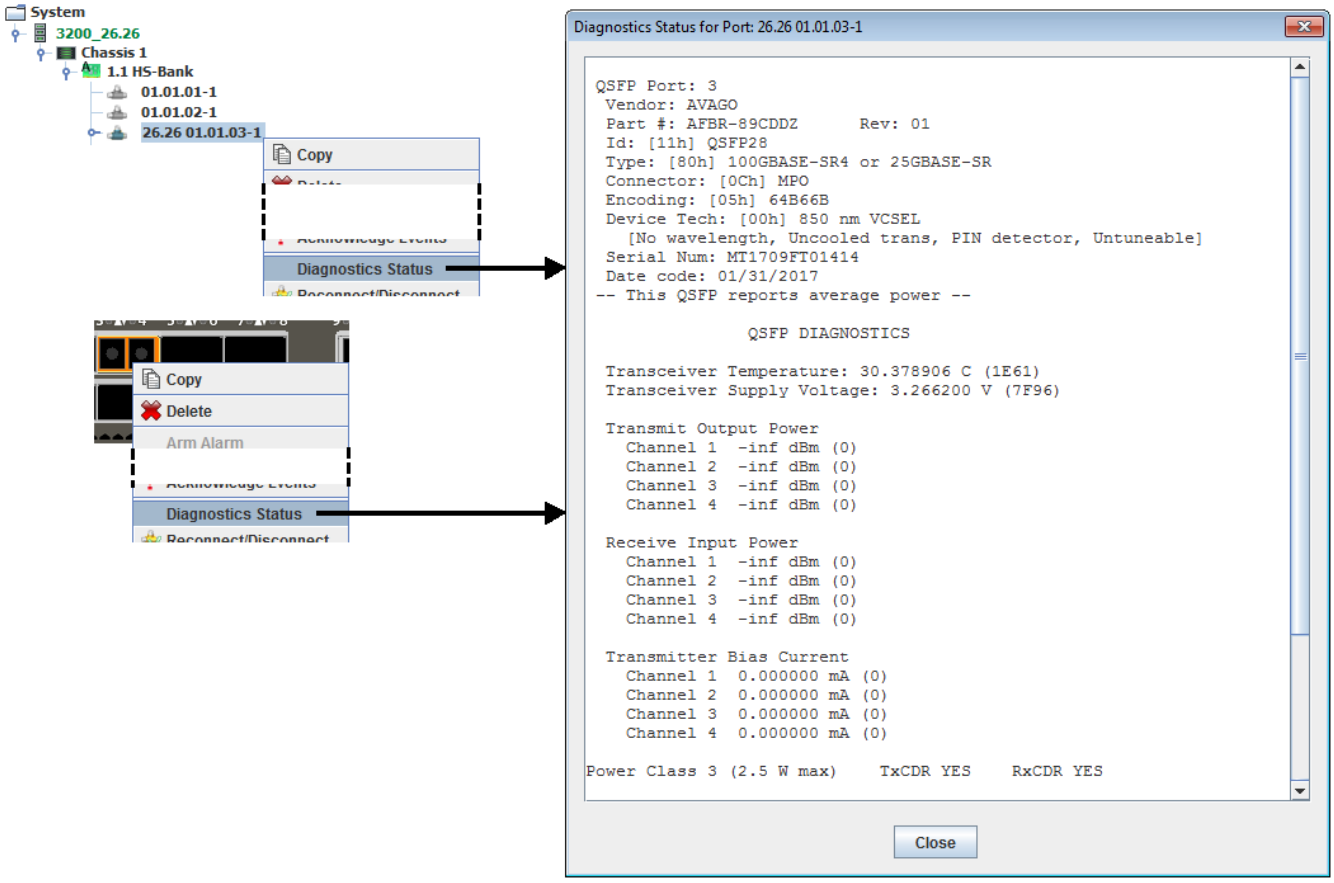
SFP Diagnostics Example



QSFP Diagnostics Example



HS-3200/HS-6400 Switch - QSFP Diagnostics Example



System Tests

The user can perform tests from the following levels:

- Switch Level - selected test is run on all ports of the selected switch.
- Chassis Level - selected test is run on all ports of the selected chassis.
- Blade Level - selected test is run on all ports of the selected blade.
- Port Level - selected test is run on all selected ports.

The following chart lists the tests, test levels, user access, and supported nGenius 3900 series switches for each test.

Table 7–1 TestStream Management Tests

Test	Switch	Chassis	Blade	Port	User	nGenius Supported System				
						3901 3901R	3903	3912	HS-3200	HS-6400
Current Port Path			X	X	All		X	X	X	X
Bad Paths	X	X	X	X	All	X	X	X	X	X
Data Path Test (Blade)			X		Diagnostic	X	X	X	X	X
Link Integrity Test			X		Diagnostic	X	X	X	X	X
Eye Pattern (Eye Diagram Analyzer)			X	X	All	Port Only	X	X		
Port Flapping				X	All	X	X		X	X

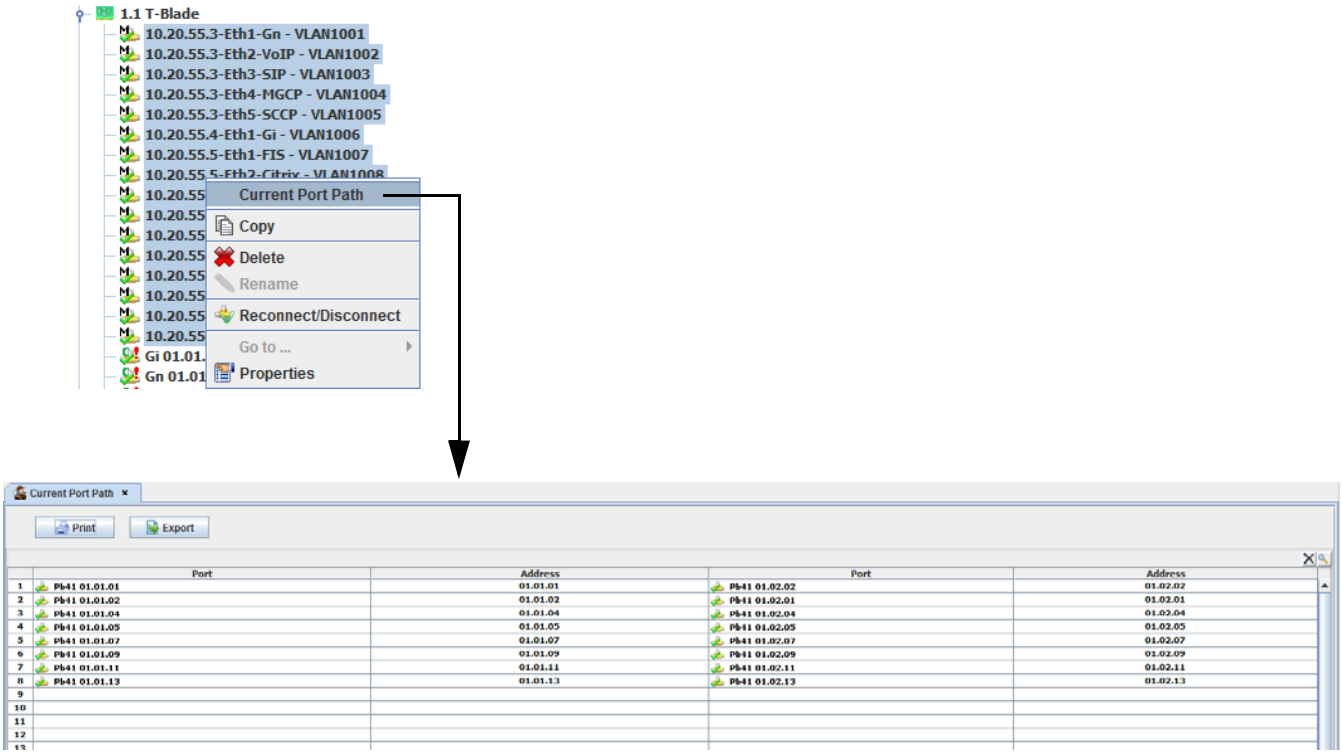
Current Port Path

Note: This function is not supported on nGenius 3901 / 3901R systems.

Displays selected active connected port paths in the system.

1 Right click on a connected port(s) then select Current Port Path. The Current Port Path window displays.

Port(s) Select



All of the connections going through the selected blade or ports are displayed:

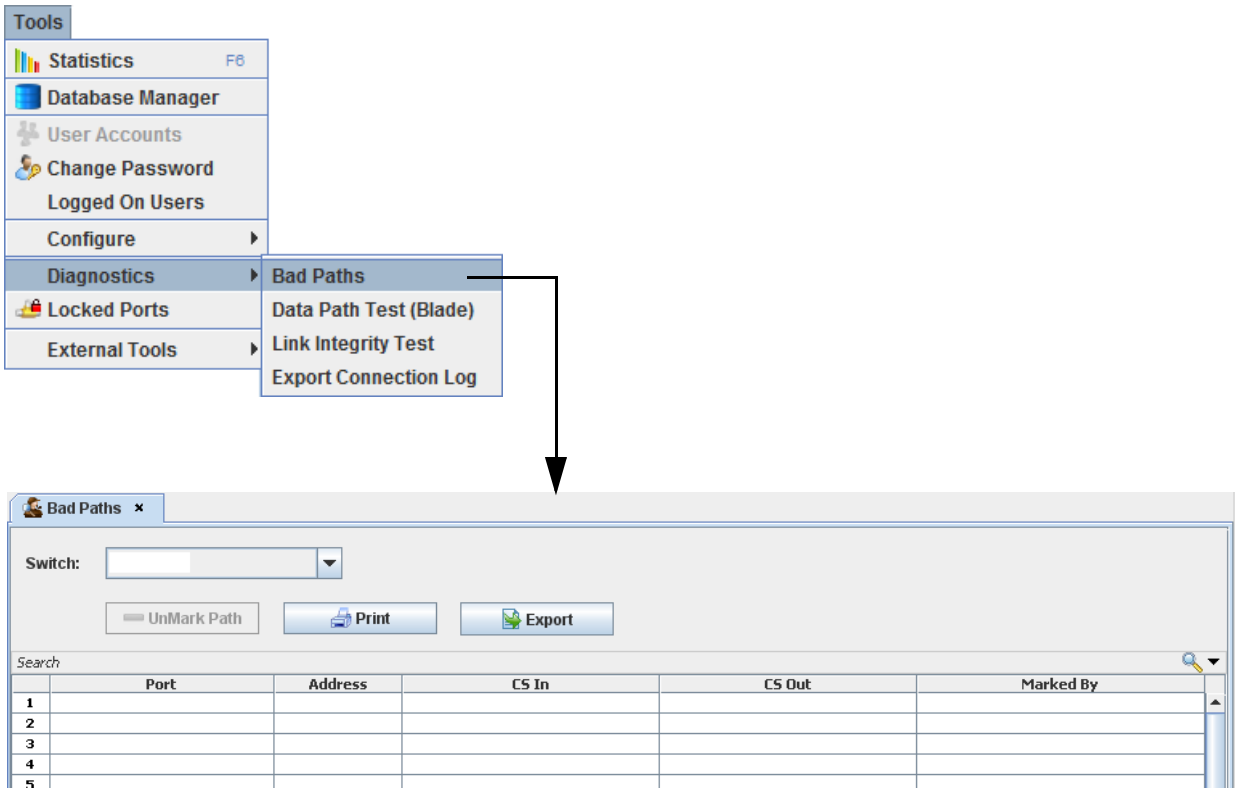
- Print - Prints current data from Current Port Path
- Export - Exports current data from Current Port Path to .csv file format
- Port - Starting Port Name
- Address - Starting Port Address
- Port - End Port Name
- Address - End Port Address

Bad Paths

The Bad Paths feature allows adding a non-operational path to a list of connection paths preventing the path(s) from being used when making a connection.

The Bad Paths diagnostic screen displays blade ports marked as inoperative; either outgoing / incoming / or in both directions.

1 Select **Tools > Diagnostics > Bad Paths**. The Bad Paths screen displays.



The display lists the ports that are marked as bad, identifying each path by port name, port address, and direction of port failure (i.e., outgoing / incoming / or in both directions).

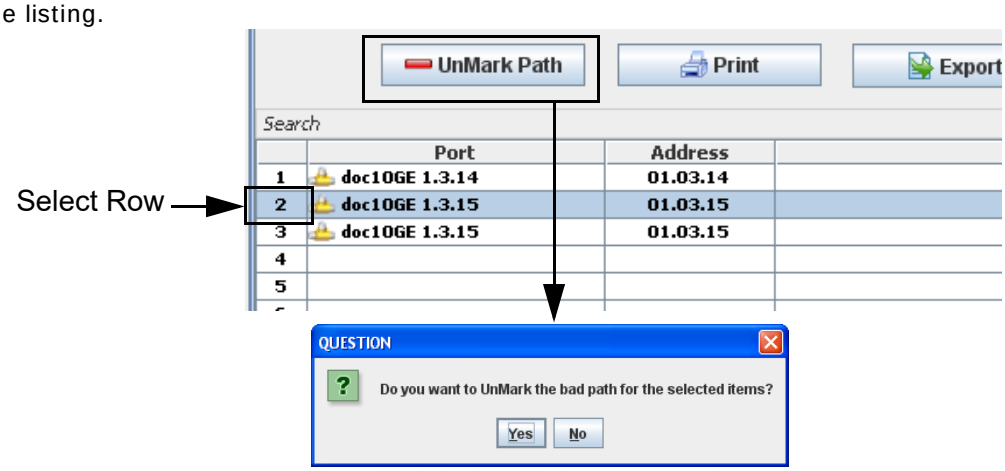
2 If required, the list can be sent to a printer (**Print**) and/or saved (**Export**) to a .CSV file format.

Unmark Bad Path

To unmark a path and return the path to service:

1 Select the row number of the port to unmark; the row highlights to reflect the selection. Multiple paths can be selected by using the Ctrl key and clicking on the required rows.

2 Click **UnMark Path**. Answer **Yes** to the verification prompt. The selected port is removed from the listing.



Data Path Test (Blade)

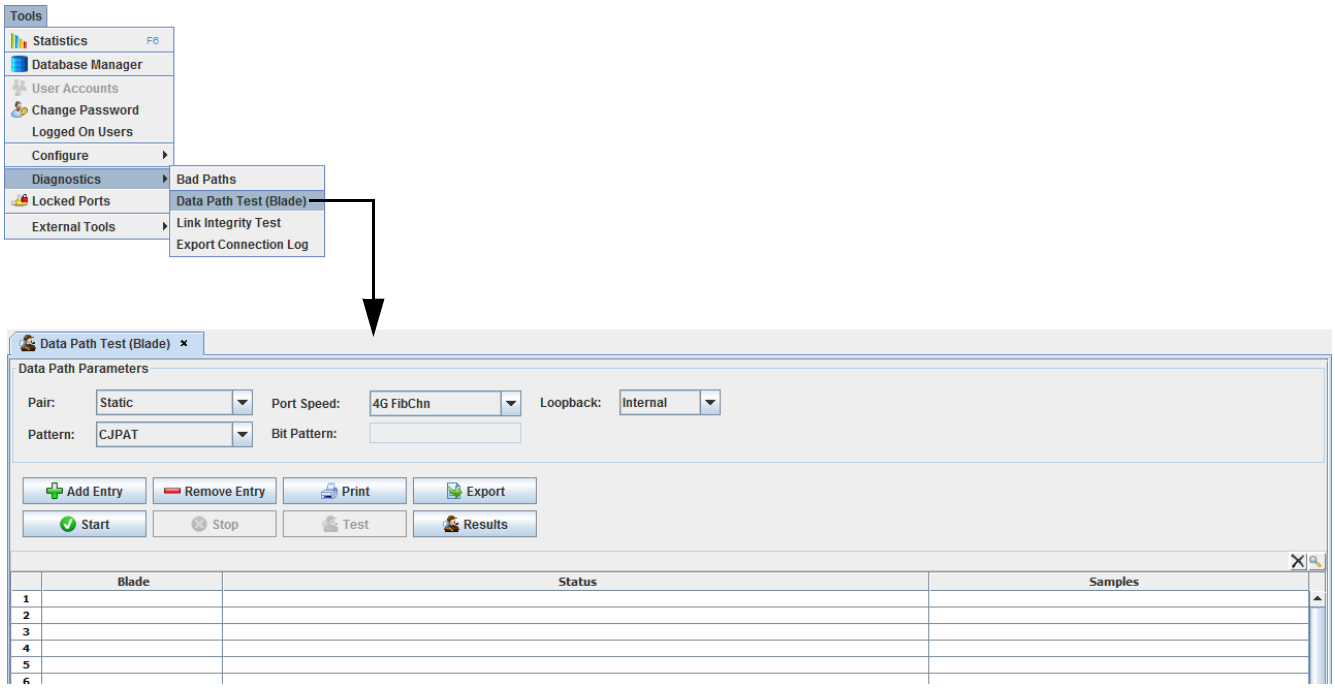
Note: This is a Diagnostic Level feature.

Tests all unconnected ports on selected blades in the same switch by generating programmed data on the selected blades.

Note: This test is disruptive to connected ports/paths under test.

Note: MULTIPLE PORT DOMAIN
If the ports in the blades selected for the Data Path test are a mix of different port domains, the user must select the port domain to test. Ports assigned to other domains are removed from the test.

1 Select **Tools > Diagnostics > Data Path Test (Blade)**. The Data Path Test (Blade) window displays.



2 Select the **System** tab. Drag over the blades to test and place in the Blade row.

3 Select the required test parameters:

- Pair: Static or Sliding.
- Loopback: Internal or External.
- Pattern:
  CJPAT - Continuous Jitter Tolerance Test Pattern
  CRPAT - Continuous Random Test Pattern
  CSPAT - Continuous Sequential Test Pattern
  PRBS7 - Pseudo-Random Bit Sequence (7)
  PRBS23 - Pseudo-Random Bit Sequence (23)
  PRBS31 - Pseudo-Random Bit Sequence (31)
  User Defined - 64 bit
- Port Speed: 1/2/4/8 GB FibChn and 1/10 GB Ethernet; Auto (the Data Generator speed is set according to the port configuration / SFP speed. Otherwise the speed defaults to the highest speed supported by the port domain).
- Bit Pattern: This field is active if User Defined 64-bit was selected - A user defined 64-bit (hex) pattern can be entered if required.

- Bi-Directional: Select if running test data in both directions.

4 Click **Start**.
The test displays the results of each loop and the total results after all loops are run.

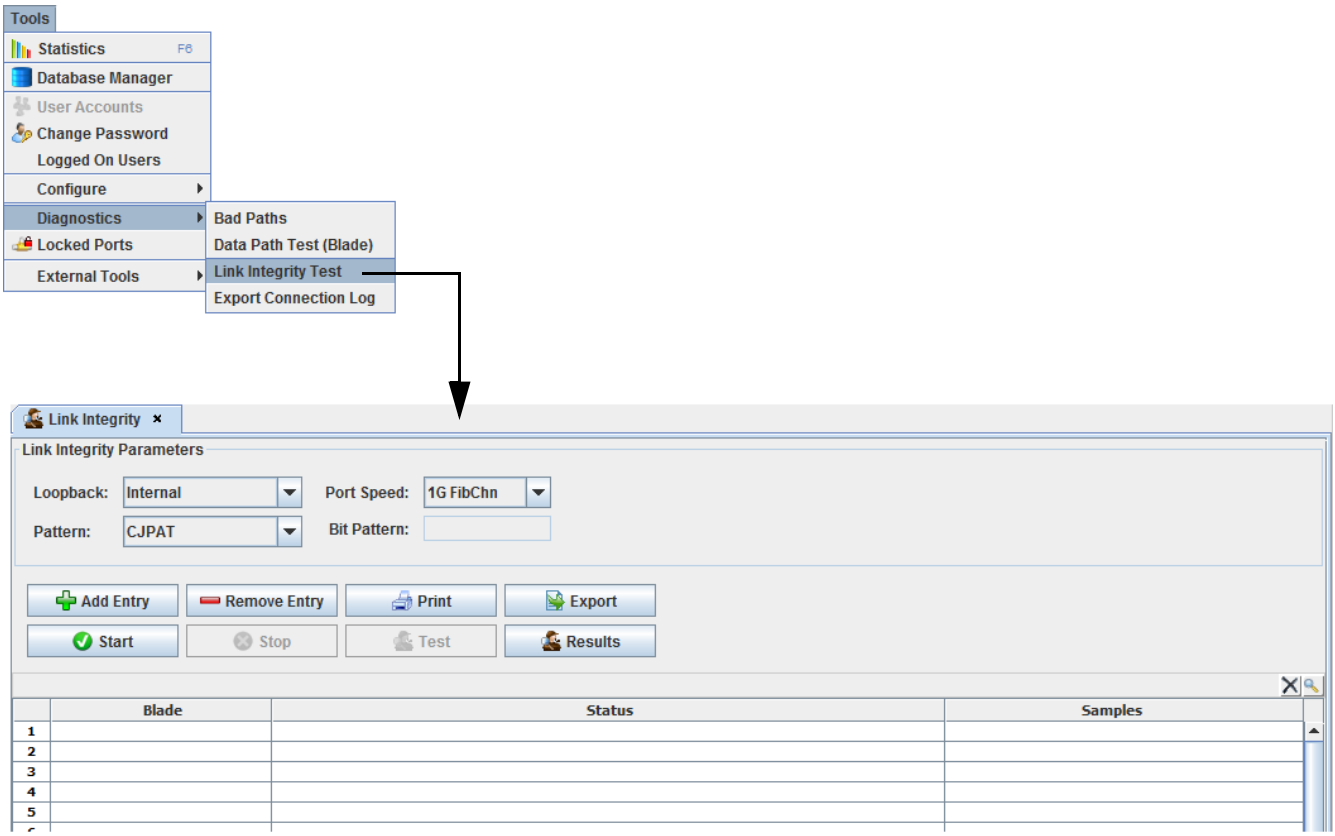
5 If required, the test results can be sent to a printer (**Print**) and/or saved (**Export**) to a .CSV file format.

Link Integrity Test

Note: This is a Diagnostic Level feature.

This test checks the data path traces of a selected blade.

1 Select **Tools > Diagnostics > Link Integrity Test**. The Link Integrity window displays.



2 Select the **System** tab. Drag over the blade to test and place in the Blade row.

3 Select the required test parameters:

- Loopback: Internal or External.
- Pattern:
  CJPAT - Continuous Jitter Tolerance Test Pattern
  CRPAT - Continuous Random Test Pattern
  CSPAT - Continuous Sequential Test Pattern
  PRBS7 - Pseudo-Random Bit Sequence (7)
  PRBS23 - Pseudo-Random Bit Sequence (23)
  PRBS31 - Pseudo-Random Bit Sequence (31)
  User Defined - 64 bit
- Port Speed: 1/2/4/8 GB FibChn and 1/10 GB Ethernet; Auto (the Data Generator speed is set according to the port configuration / SFP speed. Otherwise the speed defaults to the highest speed supported by the port domain).
- Bit Pattern: This field is active if User Defined 64-bit was selected - A user defined 64-bit (hex) pattern can be entered if required.

4 Click **Start**.
The test displays the results of each loop and the total results after all loops are run.

5 If required, the test results can be sent to a printer (**Print**) and/or saved (**Export**) to a .CSV file format.

Eye Pattern (Eye Diagram Analyzer)

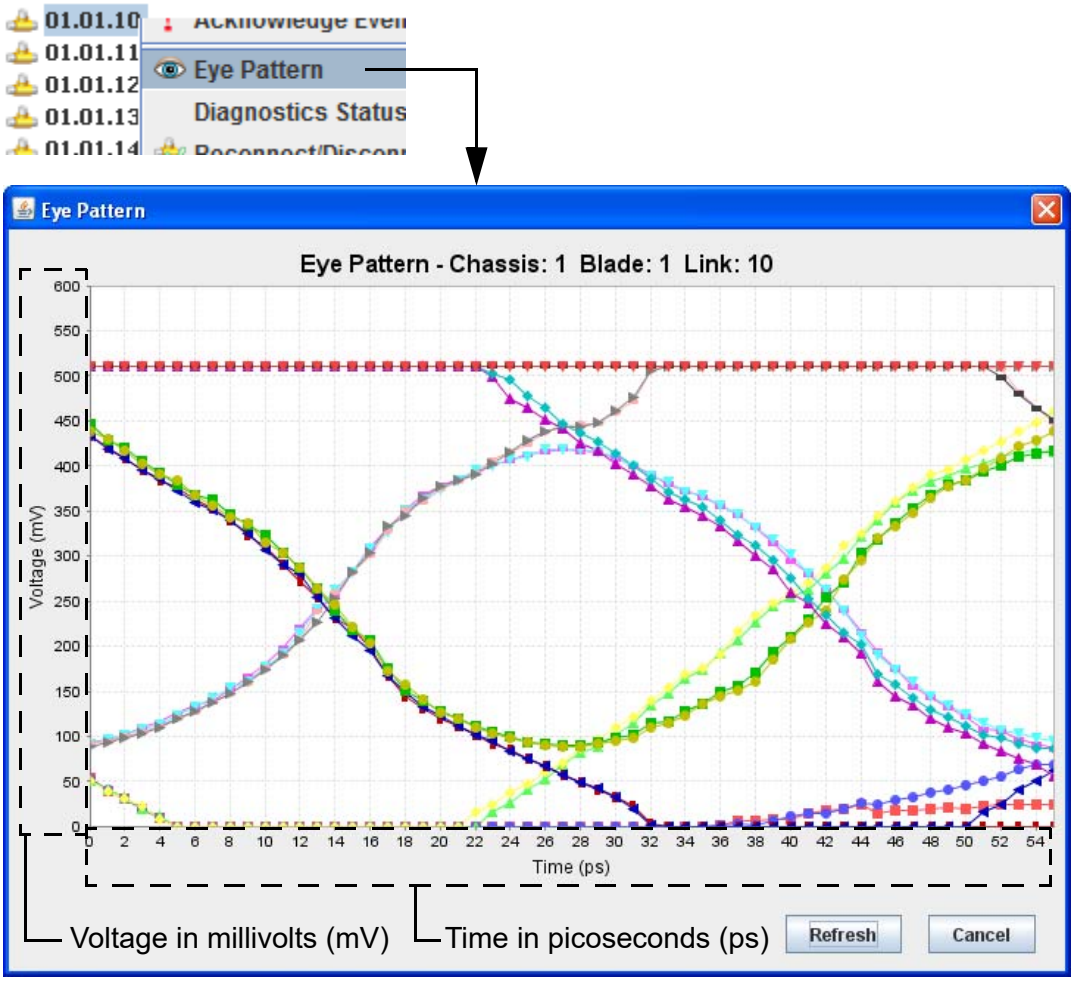
Note: Eye Pattern is supported on S-Blades only. This function is not supported on OS-16, OS-96, OS-192, or HS-3200 systems.

Eye Pattern provides a method of analyzing the quality of a data stream using a series of measurements within a given time period, with a displayed output similar to an oscilloscope screen. A data signal from a receiver is continuously sampled and applied to a vertical input
(voltage, in millivolts), with the data rate (time, in picoseconds) used to trigger a horizontal sweep. The resulting display produces a waveform display referred to as an eye diagram. The more open the eye is, the less signal distortion is on the data stream. Distortion appears as a closure of the eye pattern.

Eye Pattern is accessible from the blade and blade port levels. When selecting a blade, the user enters a back-link number (i.e., 1 - 96) reflecting the 96 bi-directional ports associated with the center stage switches.

Single Port Display

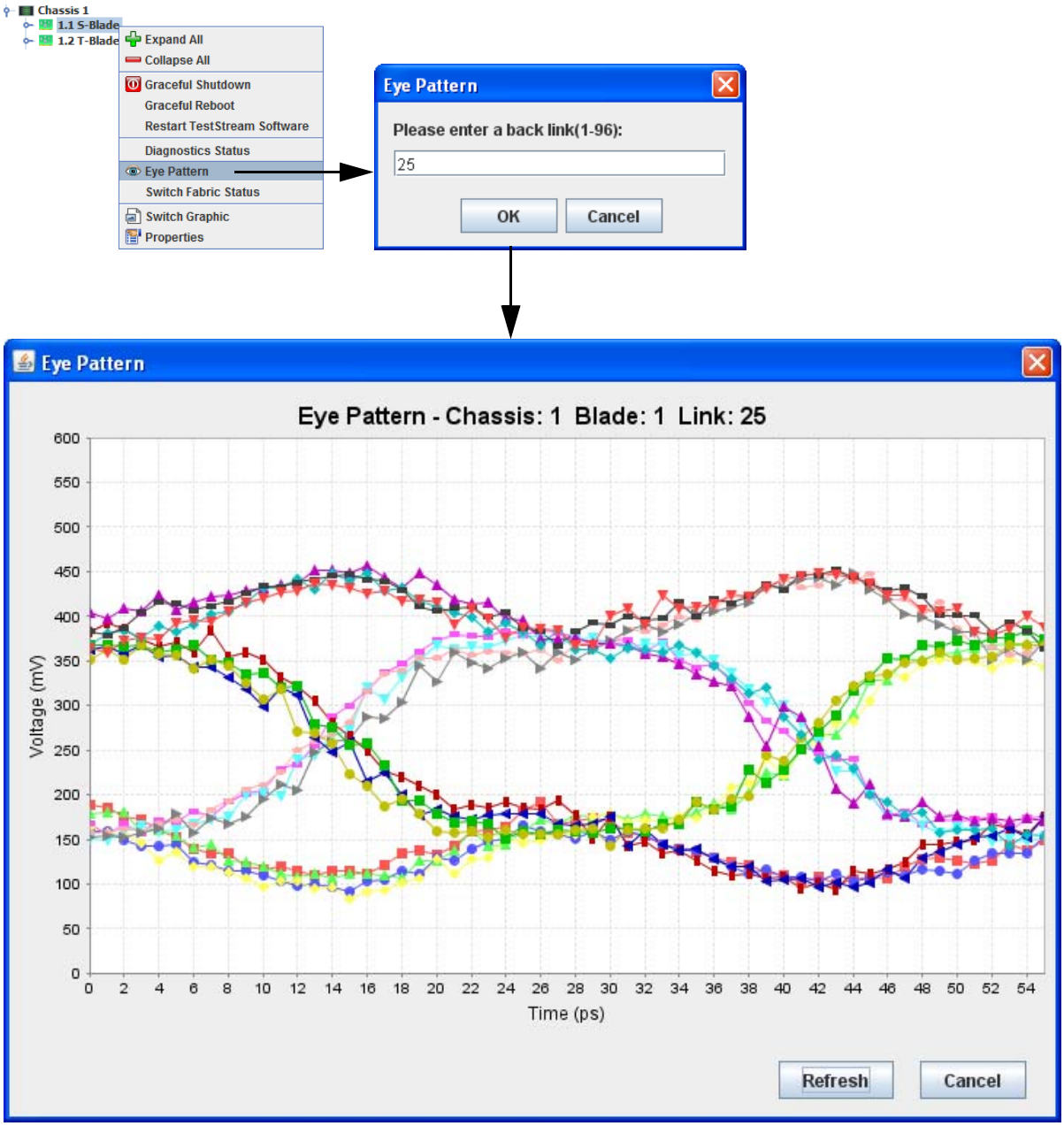
From the System level, select and right-click on a port. Select **Eye Pattern** from the port menu. The Eye Pattern screen displays.



Blade Display

Note: This function is not available on nGenius 3901 / 3901R, or HS-3200 switches.

From the System level, select and right-click on a blade. Select **Eye Pattern** from the port menu. Enter a blade back link number, then **OK**. The Eye Pattern screen displays.



Port Flapping

Port Flapping consists of turning off and then on the SFP/QSFP optical transmitters and receivers in accordance with configured flapping parameters; only duplex connected ports may be flapped. Single or multiple ports can be flapped as required. Port flapping is designed for use in the nGenius 3900 series switch S-Blade/S-Blade Pro/G-Blade where optical SFP/QSFPs are present. Refer to OS-96 / OS-192 Port Flapping Operation Notes on page 7-21.

Note: Port Flapping is accomplished via CLI commands only, the TestStream Management GUI is not supported (refer to Command Line Interface Commands on page A-1).

Port Flapping Operation Notes

- Port Flapping is supported via the CLI commands only
- Port Flapping should only be performed by a single user/session at a time
- Closing or Logging Off a session will stop all port flapping
- A maximum of 10 concurrent ports flapping is supported
- Flap ports on one nGenius 3900 series switch at a time
- S-Blades/S-Blade Pros/G-Blades with Duplex connected ports with fiber SFP/QSFPs are supported
- Simplex and Mirror port connections are not supported

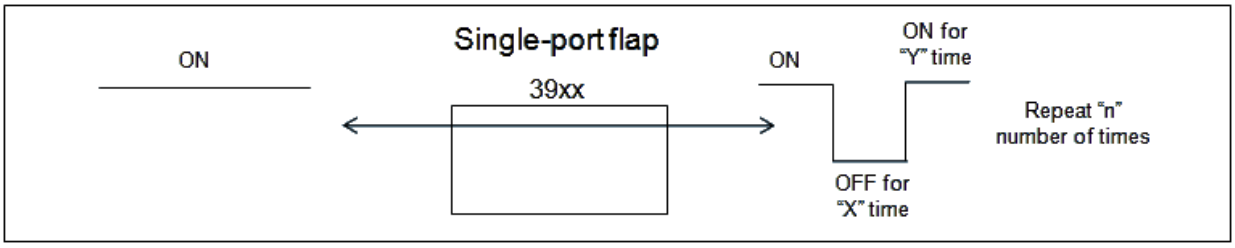
Note: Port Flapping Times
Port Flapping Off/On time parameters coupled with repeat counts can result in cycle times as brief as 270ms or as long as 45+years. It is not recommended that you set port function times that exceed 2 hours (refer to the **Flap Start** command in the CLI specification for parameters).

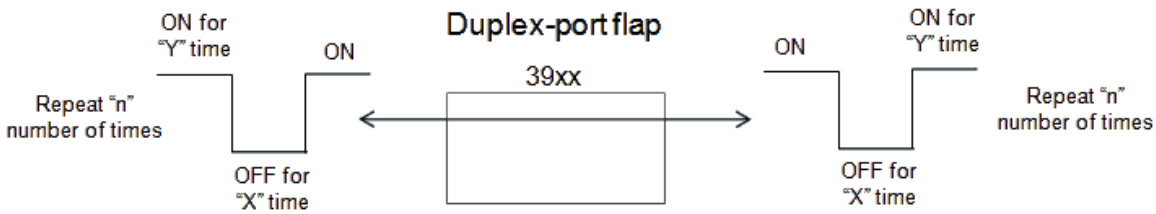
OS-96 / OS-192 Port Flapping Operation Notes

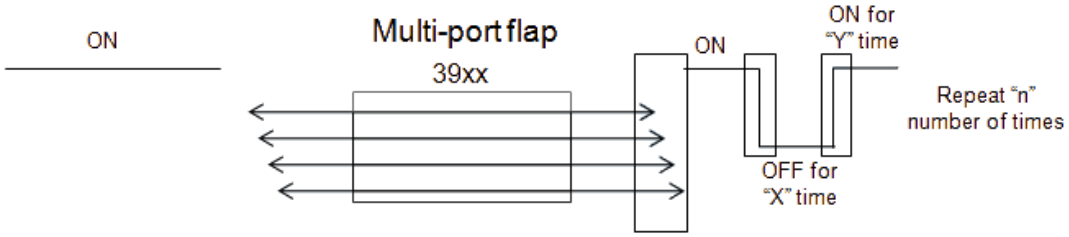
- Port Flapping should only be performed by a single user/session at a time
- Only 1 concurrent port flap is supported

Port Flapping Examples

The typical application for port flapping is in cable break simulation. See the examples below.






ON
Multi-port flap
39xx
ON
ON for
"Y" time
Repeat "n"
number of times
OFF for
"X" time

Changing SSH System Access Passwords

Important: This section describes changing the passwords used for SSH access to the nGenius 3900series switch or TestStream Management server. This does not change any user passwords for accessing the 3900 through the Client GUI or CLI.

Note: If changing either the ONPATH or Root passwords, please contact Customer Support (refer to Contacting NETSCOUT Customer Support on page 1-2).

ONPATH Username

1 Using a terminal program (e.g., putty) access the blade or server to start an ssh session (refer to Starting a CLI Session on page A-3); log on as **onpath** user:

login as: ***root*** <enter>

root@192.168.56.101's password:*old_password* <enter>

Linux HorizON 2.6.26-2-486 #1 Thu Nov 25 01:49:20 UTC 2010 i686

Last login: Fri Jul 26 14:22:07 2013 from 192.168.56.1

2 Change the user password by entering **passwd sudo passwd onpath** <enter>

a At the prompt, enter the new password **newpassword** <enter>

b Retype the new password for confirmation **newpassword** <enter>

Enter new UNIX password:*password_example1* <enter>

Retype new UNIX password:*password_example1* <enter>

passwd: password updated successfully

Root Username

1 Using a terminal program (e.g., putty) access the blade or server to start an ssh session; log on as **root** user:

login as: ***root*** <enter>

root@192.168.56.101's password:old_password <enter>

Linux HorizON 2.6.26-2-486 #1 Thu Nov 25 01:49:20 UTC 2010 i686

Last login: Fri Jul 26 14:34:12 2013 from 192.168.56.1

2 Change the user password by entering **passwd** <enter>

a At the prompt, enter the new password **newpassword** <enter>

b Retype the new password for confirmation **newpassword** <enter>

HorizON:~# passwd root <enter>

Enter new UNIX password:*password_example1* <enter>

Retype new UNIX password:*password_example1* <enter>

passwd: password updated successfully

Appendix A
Command Line Interface Commands

This appendix provides a comprehensive list of all Command Line Interface (CLI) commands, syntax, parameters, and expected responses used on the NETSCOUT TestStream Management software.

Important:
Prior to running any scripts you must first use the TestStream Management System GUI to define your nGenius 3900 series switch(es). Use the System > New Switch command to define a switch, and the Switch > Properties command to configure all switch properties. CLI commands can then be used to access all other capabilities of the TestStream Management software, with the following exceptions:
• Maintenance Utility Commands: Retrieve Connects, Verify Connects

Note:
Topology connections (ports to ports, groups to groups) created using CLI commands should only be modified using CLI commands and not through the TestStream Management System GUI.

Important:
Command Line Interface Character Limitation Notice:
The CLI command line prompt has a limitation of 1024 characters; do not enter more than 1024 characters in a single CLI prompt.

CLI Interface				
Name	**Interface**	**# Sessions**	**Command Set & Protocol**	**Alarms**
Telnet Link	TCP/IP LAN Berkeley Socket	127 maximum	Simple CLI, Telnet	Yes

The CLI Interface supports the following:

- Alarm Reporting
- Control (switching, activating connections etc.)
- Display (Switch Status, Port Statistics, etc.)
- Logical Configuration (Configure Ports, Groups, Rules, Filters, etc.)
- Maintenance Functions (Backup, Restore, etc.)

Command Language and Descriptions on page A-8, defines the CLI Commands. The CLI Interface supports most of the command functionality, with the following exceptions:

- Defining and Configuring Switches
- Port Historical Statistics
- Exporting Data
- Managing User Accounts
- Configuring Syslog Forwarding
- Configuring Client Time Zone
- Organize Favorites

- SNMP Traps
- Logon Message
- Switch Diagnostics
- External Tools
- Launch Tutorials/User's Guide
- Verify Connections
- Port Beacons
- Renaming Groups, Rules and Filters
- Starting Stats on all members of a Group or Topology
- Initial CLI Remote Access Configuration

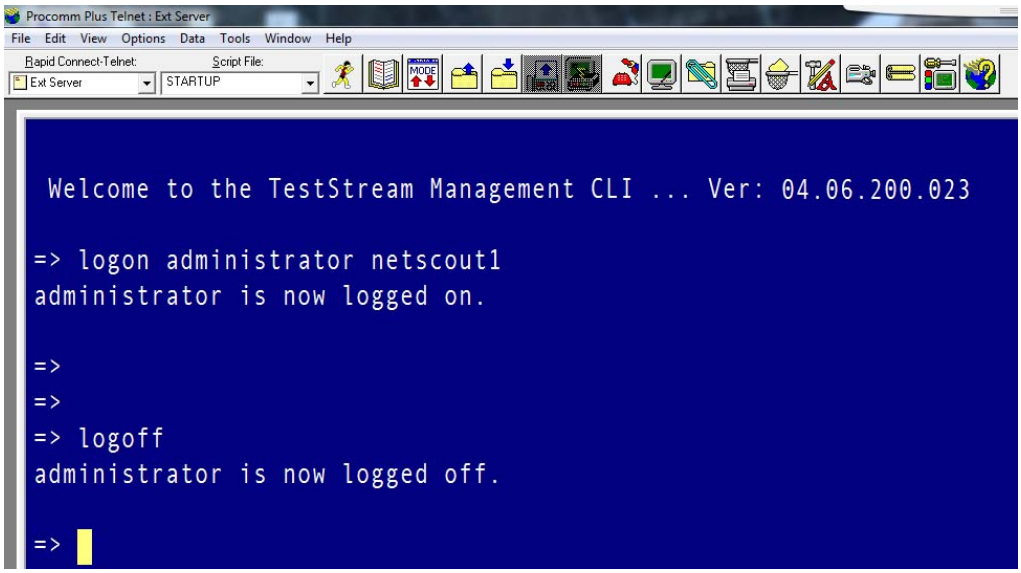
Starting a CLI Session

CLI Access - Telnet

1. From the TestStream GUI, configure your Telnet remote access settings: **Tools > Configure > Remote Access** (refer to Configure Remote Access on page 4-25).
2. Using a terminal emulator application (e.g., Procomm), start a Telnet CLI session using a configured Telnet port (refer to Configure Remote Access on page 4-25, CLI Access to the TestStream Management Server on page 2-13, and CLI Access using an nGenius 3900 Series Blade Console Port on page 2-13).
3. Type in an assigned TestStream Management user name and password followed by the Enter key.

Note: When the user logs in for the first time after being added or after a password reset, the logon command will prompt the user to enter a new password. The logon command will require the user to enter the default password first, then enter the new password and then to confirm the new password.

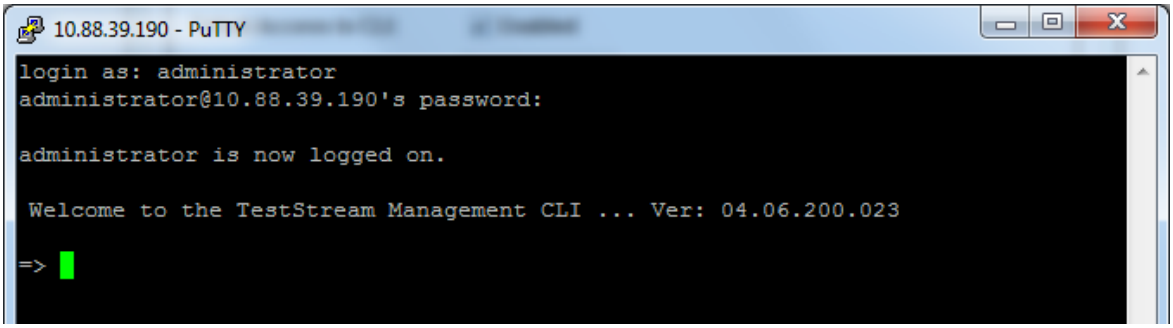
A successful login displays the following:



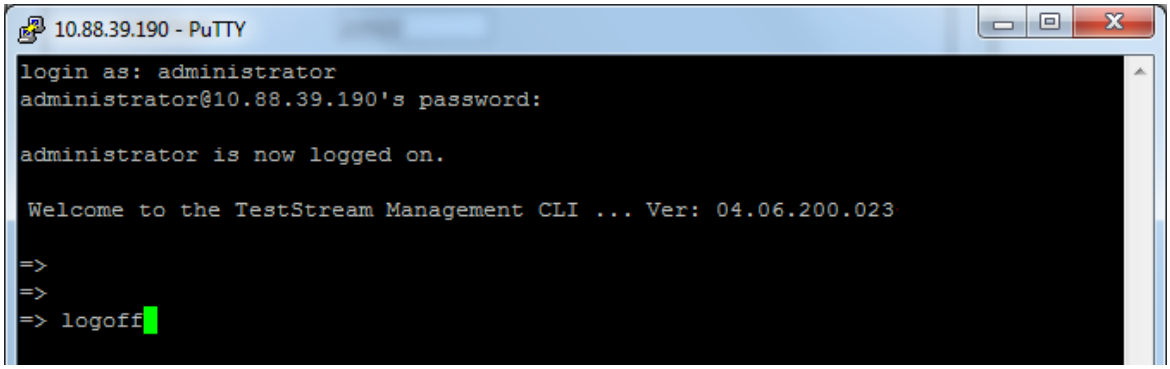
During this CLI session, the user is logged onto TestStream Management and can begin issuing CLI commands. Use the **logoff** command to end the CLI session and **exit** command to terminate the telnet session.

CLI Access - SSH

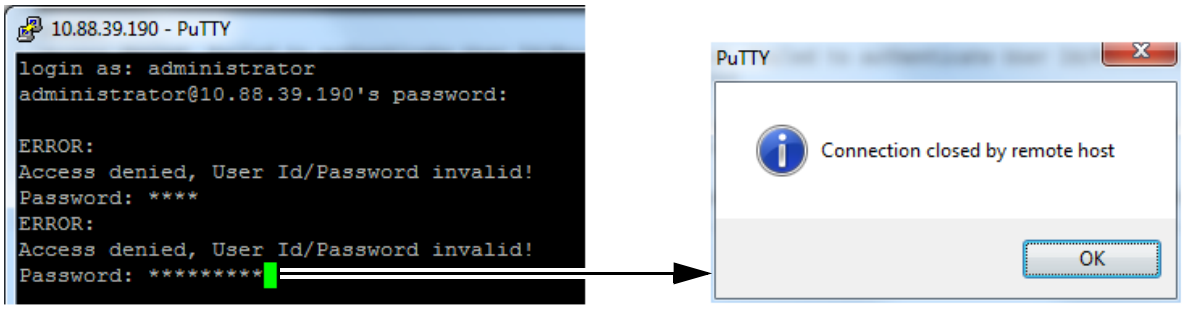
1. From the TestStream GUI, configure your SSH remote access settings: **Tools > Configure > Remote Access** (refer to Configure Remote Access on page 4-25).
2. Using a terminal emulator application (e.g., PuTTY), start an SSH CLI session using a configured SSH port (refer to Configure Remote Access on page 4-25, CLI Access to the TestStream Management Server on page 2-13, and CLI Access using an nGenius 3900 Series Blade Console Port on page 2-13).
3. Type in an assigned TestStream Management user name followed by the Enter key. Then type in the corresponding assigned password followed by the Enter key.
   A successful login displays the following:



During this CLI session the user is logged onto TestStream Management and can begin issuing CLI commands. Use the **logoff** command to end the CLI session.



During login, if the password is incorrectly entered, the user is allowed three consecutive attempts. After the third login failure, the session automatically ends.



Telnet Interface, Operating Modes, And States

The Telnet Link CLI interface supports concurrent control of up to 127 TCP/IP Telnet terminals across a TCP/IP network, requiring TCP/IP support. The Telnet interface is configured from TestStream Management (**Tools > Configure Remote Access**; refer to Configure Remote Access on page 4-25). The user can enable/disable the CLI port, configure the port used, and set an inactivity period to be used to terminate the session. The default CLI settings are:

- CLI Port: 53058
- CLI Enabled: Yes
- Terminate on Inactivity: Never

Command Language and Syntax Rules

In the Command Description section, the following syntax rules apply:

- Upper case words are literal keywords, i.e., they must be entered as shown. The keywords may be entered in lower case. When the keyword can be abbreviated, the most abbreviated form is shown in bold text.
- Example: **GRO**UP - acceptable entries are GRO, GROU and GROUP.
- Words in lower case italics represent variables. Example: ***port*** - enter mnemonic port name.
- Words enclosed in braces and separated by vertical bars are alternate selections, one word must be chosen.
- Example: {**TES**T|**MIR**ROR} - select either TEST or MIRROR.
- Words enclosed in square brackets are optional. Example: [**GRO**UP] - the word GROUP may be omitted.
- User defined names (mnemonics) are case sensitive, that is abc is not the same as ABC, and embedded spaces are allowed. A sequence of embedded spaces is treated as one space. Mnemonic names containing embedded spaces must be enclosed in quotes.
- Placing a space and "?" after a command will output the documentation on that command. If a partial command is entered, the output will be the documentation of any commands that fit the description.
- Example: **SHO GRO** ? – will show the help documentation for the show groups command.
- On the other hand **SHO** ? will show the help documentation for show groups, show ports, show switches, etc.
- Pressing escape while the telnet is printing a large amount of information (for example the help command) will pause. Hit escape again to resume.
- Port numbers are only valid on an embedded server unless the SELect SWItch command is used. Port numbers are written as cc.ss.pp
- Error messages come in 3 separate general forms: The first occurs when the CLI does not recognize your command: "** Unknown or invalid command". The second occurs very rarely when you enter too many arguments in and states "Too many positional arguments". The last is when the CLI recognizes your command but notices that there is an error in the command. These last group of errors always states "ERROR: " before displaying the specific reason behind the error. In certain commands the "ERROR: " is shown only partially capitalized as in "Error:"

Command Language, Keyword and Variable Definitions

The following are keywords unique to the command language interface:

- **FORCE**
  For commands that list this keyword, if FORCE is not specified, then the command may display a warning message, for example, before breaking connections, and then waiting for the operator to specify whether to continue or to abort the command. If FORCE is specified, then the command will continue without prompting the operator. When the command language interface is being

used by an external intelligence that cannot tolerate interactive prompts, for example Expect scripts, then these commands should specify FORCE. If not, then instead of displaying the warning, the command will be aborted with an error message.

- **SEARCH**
  This optional keyword may be specified on most of the DISPLAY commands; refer to Command Language and Descriptions on page A-8 for individual command descriptions. If the SEARCH option is specified, then only those response lines that contain the ***text*** specified after the SEARCH keyword are displayed, allowing the SEARCH option to filter out unwanted lines. For example, **DISPLAY AUDIT TRAIL SEARCH LOGON** would display just the LOGON transactions. The search comparison is case insensitive, it also treats multiple space characters as a single space.

Table A-1 Command Language Interface Mnemonic Variables

Mnemonic	Definition
cc	Chassis number: nGenius 3900 series switch 1-8
group	A 50 character mnemonic name defining a specific group, that is a collection of ports on the same switch.
interface	An 8 character port Interface type.
password	A 50 character (no embedded spaces) logon password. The password is case sensitive.
port	A 50 character mnemonic name defining a specific blade port (or port pair) on the switch. Note: A user can enter a 46 character base-name with the last 4 characters reserved for a sub-port suffix.
pp	PORT number: T-Blade 1 - 48, S-Blade 1 - 48, S-Blade 64 1 - 64, S-Blade Pro 1 - 96
ss	Blade number: nGenius 3900 series switch 1-12
switchname	A 50 character mnemonic name defining a specific switch.
dd	Subport number either 01 or 02.
userid	A 50 character (no embedded spaces) user logon ID. The ID is not case sensitive.

Table A-2 CLI Display Symbols & Abbreviations

Symbol	Definition
@	The Port/Group Alarm is Armed.
ALM	The Port/Group has an unacknowledged alarm.
ALT	The Port has an active Alert.
c	The Port is connected to an Interactive Test DCE.
CONNECTED	The Group is fully connected and has not been revised since the Connect Group.
name ##	The number (##) of Ports in the named Group.
## name	The Port/Group member (##) sequence number in a Group.
PORT	The Port is a member of a normal Port Connection.
PRTNUM	The Port physical address of the port. cc.ss.pp or subport cc.ss.pp.tt.

CLI commands (e.g., CONNECT), and keywords (e.g., FORCE) are not case sensitive.

Note: CLI Topology is defined as the default topology where connections will reside if the user does not specify a different topology with the **-t** (*--topology)* option in the Activate, Deactivate, Connect, and Disconnect commands.

CONTROL E:
Redisplays the last command on the command prompt line.

Up Arrow:
Redisplays the last 5 commands on the command prompt line.

CLI Usage Notes

The following describes how to use CLI commands when making blade connections and viewing blade port real time statistics.

Displaying Statistics on a Selected Switch Port - Quick Reference

Use the following commands (in this order) to display port statistics on a switch.

1 Select the switch:

sel swi switchname

Example:

select switch Sw1

Switch Sw1 has been selected

2 Begin real time statistics on the required port:

start stats prtn port_number

Example:

start stats prtn 1.1.1

Successful

3 Display the port statistics:

show stats prtn port_number

Example:

show stats prtn 1.1.1

Port Name :Sw1 Port1

Subport Name :Sw1 Port1.Rx

Port Address :1.1.1

Direction :Rx

Port Type :10G ETH

Switch Name :Sw1

Statistics Overview

Ports real time statistics can be viewed for connected or unconnected ports. Unconnected ports are powered up when statistics are enabled so that they can monitor the traffic. Statistics reporting must first be enabled for the ports of interest. One or more ports may be enabled at once. If a port name/number is specified then both receive and transmit statistics are enabled. If a subport name/number is specified then only one direction is enabled. If there are spaces in the port list then put quotes around the whole list. It is not necessary to put quotes around each individual name.

START STATS PORT port1
START STATS PORT port1,port2,port3
START STATS PORT “port 1, port 2, port 3”

It may take up to 5 seconds to start the statistics.

Once the statistics are started the counters will begin to accumulate and they can be viewed using the SHOW STATS command. Specify a single port or subport, create a port list, or use the wildcard symbol to see all the stats that are started:

SHOW STATS PORT port1
SHOW STATS PRTNUM 1.1.1.2
SHOW STATS PORT port1,port2,port3
SHOW STATS PORT *

Showing multiple ports in the same command insures they were read at relatively the same time.

Statistics can be reset to zero either individually, in groups, or all at once. Each user has a separate view of the statistics and resetting will not affect the other users.

RESET STATS PORT port1
RESET STATS PRTNUM 1.1.1.2
RESET STATS PORT port1,port2,port3
RESET STATS PORT *

Statistics collection can be stopped using the following command. This will not affect other users. When the last user stops statistics on a port and the port is not actively connected the port is powered down.

STOP STATS PORT port1
STOP STATS PRTNUM 1.1.1.2
STOP STATS PORT port1,port2,port3
STOP STATS PORT *

Topologies

A topology is a logical concept that allows multiple connections to be grouped together and acted upon as a unit, with all connections residing within a topology. Topologies can be created using a separate command:

ADD TOPOLOGY “My Topology”

However, it is not necessary to specifically add a topology using this command because the topology will be created automatically when using the -t option of a connect command. For example:

CONNECT -t “My Topology” GROUP srcGroup dstGroup

This command will create “My Topology” if it does not already exist, and place the connection there. All connections within a topology can be deactivated or activated as a group using the DEACTIVATE or ACTIVATE commands. For example:

DEACTIVATE TOPOLOGY “My Topology”

This will stop traffic flowing through all the connections on “My Topology” without tearing down the connection associations. The traffic can be restarted later with the command:

ACTIVATE TOPOLOGY “My Topology”

It is not necessary to specify topologies when connecting. You can ignore topologies altogether and let the connections reside in the default topology “CLI Topology”. This is where you will see them if viewing from the GUI.

Connections

The CLI commands support connecting ports and groups with an optional filter.

Simple Port-to-Port Connections

To connect two ports use the -s option for simplex, one-way connections or -d for duplex, two-way connections. Either the port name/number or the subport name/number can be used for simplex connections. For simplex connections the source port must always come first, followed by the destination port.

To connect two ports (or subports), by name or number, on the default topology in a one-way connection:
CONNECT -s PORT port1 port2
- or -
CONNECT -s PRTNUM 1.1.1.1 2.2.2.2

To connect two ports by name or number on the default topology in a two-way connection:
CONNECT -d PORT port1 port2
- or -
CONNECT -d PORT port1 PRTNUM 2.2.2

To connect in another topology:
CONNECT -d -t “My Topology” PORT port1 port2

Filtered Connections

Filters can be used to allow only certain Ethernet frames to be sent to the destination. Connections between Source Groups and Destination Groups and Ports can use a filter. You have the option of putting ports into Source Groups and Destination Groups so that they may be connected and disconnected together.

To create the groups:
ADD SOURCE GROUP srcGroup
ADD PORT srcPort TO srcGroup
ADD DESTINATION GROUP dstGroup
ADD PORT dstPort TO dstGroup

To create a filter:
ADD RULE “TCP IP Traffic” “permit ip.proto==TCP”
ADD FILTER TcpFilter
ADD RULE “TCP IP Traffic” TO TcpFilter

To connect use the -f option for the filter:
CONNECT -f TcpFilter GROUP srcGroup dstGroup
- or -
CONNECT -f TcpFilter PORT port1 PRTNUM 2.2.2

Aggregation Connections

Aggregating traffic from multiple sources can be achieved two ways:

1. By simply connecting multiple ports to the same destination(s). Use the -s option to specify simplex, one-way connections:
   CONNECT -s PORT span1 outputPort1
   CONNECT -s PORT span2 outputPort1
   CONNECT -s PORT span3 outputPort1
2. By putting multiple ports into a Source Group connecting to a Port or Destination Group. This also allows filtering.

   To create the groups:
   ADD SOURCE GROUP “AggregatedPorts”
   ADD PORT span1 TO “AggregatedPorts”
   ADD PORT span2 TO “AggregatedPorts”
   ADD PORT span3 TO “AggregatedPorts”

   ADD DESTINATION GROUP “OutputPortGroup”
   ADD PORT outputPort1 TO “OutputPortGroup”

   To connect, directly or through a filter, optionally specifying a topology:
   CONNECT GROUP “AggregatedPorts” “OutputPortGroup”
   - or -
   CONNECT -f TcpFilter GROUP “AggregatedPorts” “OutputPortGroup”
   - or -
   CONNECT -t “My Topology” -f TcpFilter GROUP “AggregatedPorts” PORT outputPort1

Multicast Connections

Sending the same traffic to multiple destinations can be achieved two ways:

1. By simply connecting a port to multiple destination ports (or subports). Use the -s option to specify simplex, one-way connections:
   CONNECT -s PORT span1 port2
   CONNECT -s PORT span1 port3

2. By putting multiple ports into a Destination Group and putting the source port(s) into a Source Group and connecting them. Or by connecting a source port or subport to a Destination Group.

   To create the groups:
   ADD DESTINATION GROUP “MulticastPorts”
   ADD PORT port1 TO “MulticastPorts”
   ADD PORT port2 TO “MulticastPorts”
   ADD PORT port3 TO “MulticastPorts”

   ADD SOURCE GROUP “InputPorts”
   ADD PORT span1 TO “InputPorts”

   To connect, directly or through a filter:
   CONNECT GROUP “InputPorts” “MulticastPorts”
   - or -
   CONNECT -f TcpFilter GROUP “InputPorts” “MulticastPorts”
   - or -
   CONNECT -f TcpFilter PORT span1 GROUP “MulticastPorts”

Load-Balanced Connections

Distributing a traffic stream across multiple ports can be achieved by creating a Destination Group, specifying the LOADBALANCE option, and putting all the destination ports into it. A Source Group or Source Port can then be connected. Filters also may be used. Two types of distribution are supported, equal-distribution and session-based. The type of distribution is configured as a switch property in the GUI; it cannot be configured via the CLI.

To create the Load Balancing Destination Group:
ADD DESTINATION GROUP “LoadBalancedPorts” LOADBALANCE
ADD PORT port1 TO “LoadBalancedPorts”
ADD PORT port2 TO “LoadBalancedPorts”
ADD PORT port3 TO “LoadBalancedPorts”

To connect, directly or through a filter, optionally specifying a topology:
CONNECT GROUP srcGroup LoadBalancedPorts
- or -
CONNECT -f TcpFilter GROUP srcGroup LoadBalancedPorts
- or -
CONNECT -t “My Topology” -f TcpFilter GROUP srcGroup LoadBalancedPorts
- or -
CONNECT -t “My Topology” -f TcpFilter PORT span1 GROUP LoadBalancedPorts

Combination Connections

Connection features can be combined in various ways. For example you can aggregate, loadbalance, and filter all in the same connection:
CONNECT -f TcpFilter GROUP “Aggregated Ports” “LoadBalancedPorts”

You can load balance to some ports and multicast to other ports using an aggregated stream of traffic, filtering one and not the other by using two commands:
CONNECT -f TcpFilter GROUP “AggregatedPorts” “LoadBalancedPorts”
CONNECT GROUP “AggregatedPorts” “MulticastPorts”

Disconnecting Connections

Disconnecting differs from deactivation in that the connection associations are deleted and removed from the topology when disconnecting. The traffic cannot then be restored with the ACTIVATE command.

To disconnect a single connection follow the same pattern as the connect command:
DISCONNECT -s PORT port1 port2
DISCONNECT -d -t “My Topology” PORT port1 port2
DISCONNECT GROUP “InputPorts” “MulticastPorts”
DISCONNECT -f TcpFilter PORT span1 GROUP “MulticastPorts”

To disconnect multiple connections use the wildcard symbol (*) in place of either the source or destination:
DISCONNECT -s PORT port1 *
DISCONNECT -d PORT * port2
DISCONNECT GROUP “InputPorts” *

For filtered connections you must always specify the filter when disconnecting:
DISCONNECT -f TcpFilter GROUP “AggregatedPorts” “OutputPort”
- or -
DISCONNECT -f TcpFilter GROUP “AggregatedPorts” *
- or -
DISCONNECT -f TcpFilter GROUP * “OutputPort”

If you wish to disconnect all connections on a topology it may be easier to deactivate and then delete the topology:
DEACTIVATE TOPOLOGY “My Topology”
DELETE TOPOLOGY “My Topology”

xSL Ports

You can configure an xSL port through the CLI with the “ADD TO switchname [TESt|MIRror|XSl|CLone] PORt”.

While CLI can be used to configure an xSL port, there are no CLI commands to associate or disassociate xSL ports from one another to create or remove xSLs.

CLI Command List

The following describes the syntax and description of each command. The CLI commands are separated into the following categories:

- S-Blade Pro Specific on page A-13
- T-Blade Specific on page A-15
- HS-3200/H6400 Specific on page A-28
- Standard Commands - TestStream Lab Manager and TestStream Controller on page A-31

S-Blade Pro Specific

- **ACT**ivate **SCAnner *name***
  Activates a port scanner.

  Examples:
  Activate scanner ScannerA
  act sca 'Scanner ABC'

- **ADD IMP**airment ***name*** {**DEL**ay|**LN**|**LP**} ***value***
  Add an impairment.
  DELay: Number of milliseconds to delay (range 0.1 - 1600). Must be to a 10th of a percent.
  LN: Drop 1 out of every N packets (2 - 4294967296).
  LP: Drop percentage of packets (range 0.0001 - 99.9999).

  Examples:
  add imp myimp delay 50
  add imp myimp LP .001

- **ADD TO SCAnner *scannername*** {**POR**t|**PRTN**um} ***portname*** [***position***]
  Add a port to a scanner. The position starts at 1 and if not specified the port will be added to the end of the scanner. If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Examples:
  Add to Scanner ScannerA port 'BLZ 1.2.4'
  ADD to scanner ScannerA prtn 1.2.4

- **DEA**ctivate **SCAnner *name***
  Deactivate a port scanner.

  Examples:
  deactivate sca scannerA
  dea sca 'SCANNER ABC'

- **DEL**ete {**POR**t|**PRTN**um} ***portname*** **FRO**m **SCAnner *scannername***
  Delete a port from a scanner by name. If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp. PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Examples:
  DELETE PORT 'Port A' from SCAnner ScannerA
  del por portA from sca "Scanner A"
  del prtn 1.1.17 from sca Scanner1

- **DEL**ete **IMP**airment ***name***
  Delete impairment by name.

  Example:
  del imp myimp

- **LOCK SCAnner *name* MM/DD/YYYY-HH:MM** [***comment***]
  Lock port scanner until date/time specified. If comment contains spaces, then it must be enclosed in single or double quotes.

  Example:
  LOCK SCANNER 'SCANNER ABC' 10/30/2011-5:30

- **REN**ame **SCAnner** ***scannername newscannername***
  Rename the specified port scanner.

  Example:
  ren sca 'SCANNER AB' 'SCANNER CD'

- **REV**ise **BLA**de ***bladeaddress*** **BRI**dge **LAN**e **UTI**lization ***value***.
  Revise Blade bridge lane allocation for utilization for S-Blade Pro. Value can be in the range of (0-8).
  Increasing the number of utilization lanes will reduce the number of shared resources available if Extended Fabric Mode is enabled.

  Example:
  rev bla 1.2 bri lan util 4

- **REV**ise **IMP**airment ***name*** {Disable|Enable} {**DEL**ay|**LN**|**LP**} ***value***
  Enable / disable Impairment properties.
  DELay: Number of milliseconds to delay (range 0.1 - 1600). Must be to a 10th of a percent.
  LN: Drop 1 out of every N packets (2 - 4294967296).
  LP: Drop percentage of packets (range .0001 - 99.9999).

  Examples:
  rev imp myimp delay 50
  rev imp myimp LP .001

- **REV**ise **SCAnner** ***scannername*** **ROV**ing **INT**erval ***seconds***
  Revise port scanner roving interval (30-300 secs).

  Example:
  rev sca ScannerA rov int 60

- **REV**ise **SWI**tch ***switchname*** **SBL**ade **PRO MOD**e {**NOR**mal|**UTI**lization}

  Revise a switch's S-Blade Pro Mode. S-Blade Pro Mode allows S-BLADE Pro blades to operate in Normal mode or Utilization mode. Normal Mode allows for all bridge ports to be available for connections, while Utilization Mode reserves half of the bridge ports for statistics collection.

  Examples:

  REVISE SWITCH MySwitch SBLade PRO MODe NOR

  rev swi MySwitch sbl pro mod util

- **REV**ise **SWI**tch ***switchname*** **SBL**ade **PRO EXT**ended **FAB**ric **MOD**e {**ENA**ble|**DIS**able}

  Revise switch to enable / disable the S-Blade Pro Extended Fabric Mode.

  S-Blade Pro Extended Fabric Mode uses shared resources to increase the number of connections between standard Layer-1 ports.

  In order to maximize Extended Fabric Mode, it is recommended that:

  1. Connections between Smart ports and Standard Layer-1 ports be kept to a minimum.
  2. Port Utilization metrics are not enabled on standard Layer-1 ports.

  Example:

  rev swi MySwitch sbl pro ext fab mod ena

- **SHO**w **BLA**de **UTI**lization ***bladeaddress***
  Show Blade utilization for S-Blade Pro

  Example:
  show bla util 1.2

- **SHO**w **SCAnner**s [**SEA**rch ***text***]
  Display a list of all defined Scanners and the number of members in each.
  To display a specific scanner use the syntax:
  show sca search ScannerA

  To display all scanners use the syntax:
  show sca

  Example:
  show sca

- **SHO**w **IMP**airments [**SEA**rch ***text***]
  Display a list of all defined impairments.

  Example:
  how imp search ImpairmentA

- **UNL**ock **SCAnner** ***name***
  Unlock a port scanner. Only the user that locked the port scanner or an Administrator can unlock a port scanner.

  Examples:
  unlock SCANNER 'SCANNER ABC'
  unlock sca ScannerA

T-Blade Specific

- **ACT**ivate [*options*] {**POR**t|**PRTN**um|**GRO**up|**GEN**erator|**DEVICEP**ort} ***source*** [**POR**t|**PRTN**um|**GRO**up|**DEVICEP**ort] ***destination***
  Activate the connection(s) between the source and destination. Activation causes the ports to power up and traffic to start flowing. If no topology is specified the default topology "CLI Topology" is used. Must use the -f 'filter name' option to activate filtered connections. Must use the -I 'impairment name' option to activate impaired connections. Wildcards (*) are accepted for source or destination name, but not both.

  options (case sensitive):
  -h [**--help**] Show options help
  -d [**--duplex**] A duplex port connection
  -F [**--force**] Force without showing warnings
  -f [**--filter**] arg Connection through filter, arg = filter name
  -I [**--impairment**] arg Connection through impairment, arg = impairment name
  -s [**--simplex**] A simplex port connection
  -t [**--topology**] arg Connections in this topology, arg = topology name

  Examples:
  activate group groupAsrc *
  activate group * groupBdest
  act --duplex -t MyTopology PORT "My Src Port ABC" "My Dest Port ABC"
  ACTIVATE -s PORT SPAN1 *
  ACTIVATE -s PORT * Analyzer1
  act -f ArpFilter GRO "Network Ports" Analyzer
  ACT -f VlanFilter GRO "Network Ports" PORT Tool1
  ACT -I DropXImp PORT "PORT A" PORT ToolPort

- **ADD DES**TINATION **GRO**UP ***name*** [**LOA**DBALANCE]
  Add a new destination group. Defaults to a multicast group where each port receives a copy of each frame. Specifying LOAdbalance creates a load balancing group where frames are distributed among the ports.

  Examples:
  ADD destination group DestA
  add des group 'Dst ABC' LOADBAL

- **ADD FIL**TER ***name***
  Adds a new filter.

  Examples:
  Add filter FilterA
  Add fil 'Filter ABC'

- **ADD PAC**ketdef ***packetdefname packetdef***
  Add a new packet definition.
  Valid fields are:
  packet.size
  eth.src
  eth.dst
  eth.type
  vlan.id
  vlan2.id
  ip.dst

ip.src
ipv6.dst
ipv6.src
ip.version
ipv6.version
ip.ttl
ipv6.hoplimit
ipv6.flowlabel
l4.proto
ipv6.nxt
ip.dscp
ipv6.traffic_class
l4.srcport
l4.dstport
raw.packet (false = 0, true = 1)
payload.type (increment=2, repeat=3, random=4, specific=5)
payload.data (no spaces allowed)

Examples:
Add pac 'EthType ARP' 'packet.size==69 eth.type==80F3'
Add pac 'Source MAC' 'eth.src==01:02:03:04:05:06'
Add pac 'VLAN 1' 'vlan.id==100'
Add pac 'TCP IP' 'ip.proto==6'
Add pac 'TCP IPV6' 'ipv6.nxt==6'
ADD pac 'IP Addr' 'ip.src==1.2.3.4 ip.dst==3.4.5.6'
ADD pac 'Raw Packet 1' 'raw.packet = 1 payload.data=ABBB011099EF223454EFEF'

- **ADD PAC**ketdef ***packetdefname*** TO ***streamname*** [*position*]
  Add a packetdef to a stream. Valid positions are from 1 to the first position after the last existing rule in the stream. If not specified, the packetdef will be added to the end of the stream.

  Examples:
  Add PACketdef packetDefA to atreamA
  Add PACketdef packetDefB to streamA 1
  Add PACketdef 'packetdef ABC' to 'stream ABC'

- **ADD RUL**E ***rulename rules***
  Adds a new rule. ***rules*** is the list of actions/conditions eg. “permit eth.type==ARP”.

  action condition:

  Where *action* is a single word, either **permit** or **deny**, and *condition* specifies one or more fields to match:
  fieldname==value [&& fieldname==value ...]

  Fieldnames are typically followed by “==” and a value. Exceptions are “all”, “ip”, and “ipv6”, which do not require the “==” and value.
  Either a double (==) or single (=) equal sign is accepted, and may be surrounded by spaces nor not.

  For specifying multiple fields within a single Ethernet frame use “&&”. The alternatives “&”, and “AND” are also accepted.

  Examples:
  permit ip.addr==192.168.1.3 && tcp.port==80 (permits only frames that match both the IP address and TCP port number).
  deny vlan.id=1234 AND ip (denies all IP packets that have VLAN ID 1234).

  Values specified for fields may include a mask by using the “/” symbol.

  Examples:
  permit eth.src == 11:22:33:00:00:00/FF:FF:FF:00:00:00 (matches only the first three bytes of a MAC address).
  deny ip.src == 192.168.0.0/255.255.0.0 (can also be written 192.168.0.0/16 in CIDR format).
  permit ipv6.dst == 1234::/32 (can also be written 1234::/FFFF::).
  permit tcp.srcport==2000/0xFFF8 (specifies port 2000-2007. Masks for numeric fields may be written as decimal or hexadecimal numbers).

Defining Filter Rules Using Ranges

For the following fields ranges, lists, and combinations of ranges and lists are allowed. Ranges use a dash “-“, lists are comma separated:

- vlan.id
- vlan.priority
- vlans.id
- vlan2.priority
- ip.addr, ip.src, ip.dst
- ip.ttl
- l4.port, l4.srcport, l4.dstport
- tcp.port, tcp.srcport, tcp.dstport
- udp.port, udp4.srcport, udp.dstport

Syntax: Accepts ranges and lists, in addition to masks.

- Range separated by a dash
  Examples:
  - vlan.id == 1-100
  - ip.src == 192.168.1.1-192.169.181.54
- Lists of numbers that need not be contiguous
  Examples:
  - tcp.srcport == 80, 8080
  - ip.dst == 192.168.1.1, 192.169.2.2, 10.88.37.150
- Mixture of ranges and lists
  Examples:
  - vlan.id == 1,3,5,200-1999
  - ip.src == 192.168.1.1-192.168.2.255, 10.88.35.36
- Single number with a mask
  Examples:
  - vlan.id == 256/0xFF
  - ip.src == 192.168.0.0/16
  - ip.src == 192.168.0.0/255.255.0.0
  - ipv6.src ==1234:5678::/32
  - ipv6.src == 1234:0000::/FFFF:0000:FFFF::

Valid fields:

Field Name	Description
all	Matches all frames. Does not use "==value".
eth.src	Source MAC address
eth.dst	Destination MAC address
eth.type	Ethernet Type
vlan.id	VLAN ID in first VLAN tag
vlan.priority	VLAN Priority in first VLAN tag
vlan2.id	VLAN ID in second VLAN tag
vlan2.priority	VLAN Priority in second VLAN tag

Field Name	Description
ip	IPv4 frame, does not use "==value". Designates all normal IP version 4 packets, and also those encapsulated in MPLS headers and VN-Tag headers (when VN-Tag detection is enabled for the switch).
ip.addr	Either source or destination IPv4 address
ip.src	Source IPv4 address
ip.dst	Destination IPv4 address
ipv6	IPv6 frame, does not use "==value". Designates all normal IP version 6 packets, and also those encapsulated in MPLS headers and VN-Tag headers (when VN-Tag detection is enabled for the switch).
ipv6.addr	Either source or destination IPv6 address
ipv6.src	Source IPv6 address
ipv6.dst	Destination IPv6 address
ip.ttl	IPV4 Time-To-Live
l4.proto	Layer 4 Protocol
ip.proto	IPV4 Layer 4 Protocol
ipv6.nxt	Layer 4 Protocol in the last IPV6 header
ip.tos.dscp	IPV4 DSCP value (6 bits)
ipv6.traffic_class.dscp	IPV6 DSCP value (6 bits)
ip.tos	IPV4 Type Of Service – 8 bits including 6-bit DSCP value
ipv6.traffic_class	IPV6 Traffic Class – 8 bits including 6-bit DSCP value
l4.port	Either Source or Destination TCP or UDP Layer 4 port
l4.srcport	TCP or UDP Layer 4 Source Port
l4.dstport	TCP or UDP Layer 4 Destination Port
tcp.port	Either Source or Destination TCP Layer 4 port
tcp.srcport	TCP Source Port
tcp.dstport	TCP Destination Port
udp.port	Either Source or Destination UDP Layer 4 port
udp.srcport	UDP Source Port
udp.dstport	UDP Destination Port
l4.data[n]	Layer 4 deep inspection, where n= the byte offset: TCP/UDP = 0-37 for IPv4, 0-11 for IPv6. Offset 0 starts at the first byte following the layer-4 TCP/UDP header Other Protocols = 0-39 for IPv4, 0-13 for IPv6. Offset 0 starts at the start of the layer-4 header. Note that only the first 112 bytes of the Ethernet frame can be inspected. Optional headers prior to layer-4 in the frame may push bytes beyond this limit.

Examples:
Add rul RuleA "permit all"
Add rul 'Deny ARP' 'deny eth.type==ARP'
Add rul 'Source MAC' 'permit eth.src==01:02:03:04:05:06'
Add rul 'VLANS' 'permit vlan.id==101-199,1000-2000'
Add rul 'TCP IP' 'permit ip.proto==TCP'

Add rul 'TCP IPV6' 'permit ipv6.nxt==TCP'
Add rul 'TCP IP' 'permit l4.proto==TCP'
ADD RULE 'IP Addr 1.2.x.x' 'permit ip.src==1.2.0.0/255.255.0.0'
ADD RULE 'IP Addr 1.2.x.x' 'permit ip.src==1.2.0.0/16'
ADD RULE 'IP Addr 1.2.x.x' 'permit ip.src==1.2.0.0-1.2.255.255'
ADD RULE 'TCP HTTP' 'permit tcp.port==80,8080'

Note: Refer to Creating Number Ranges in Rules Using Masks on page 3-218 and Filter Usage Examples - Using Filters to Load Balance Traffic on page 3-215.

- **ADD RUL**E ***rulename*** **TO** ***filtername*** [**position**]
  Add a rule to a filter. Valid positions are from 1 to the first position after last existing rule in the filter. If not specified the rule will be added to the end of the filter.

  Examples:
  Add rule ruleA to filterA
  Add rule ruleB to filterA 1
  Add rul ‘rule ABC’ to ‘filter ABC’

Note: Refer to Creating Number Ranges in Rules Using Masks on page 3-218 and Filter Usage Examples - Using Filters to Load Balance Traffic on page 3-215.

- **ADD STRE**am ***name***
  Add a new stream.

  Examples:
  Add stream StreamA
  Add stre 'Stream ABC'

- **ADD TO** switchname [**TE**st|**MIR**ror|**XS**1|**CL**one] **POR**t cc.bb.pp portname {**1GFib**|**2GFib**|**4GFib**|**8GFib**|**GIG-E**|**CU-GIG-E**|**OC-3/stm-1**|**OC-12/stm-4**|**OC-48/stm-16**|**OC-192/stm-64**|**OPTical**|**10GEth**|**25GEth**|**40GEth**|**50GEth**|**100GEth**|**100MFib**|**CU10000**|**CPRI9**|**CPRI8**|**CPRI7**|**CPRI6**|**CPRI5**|**CPRI4**|**CPRI3**|**CPRI2**|**CPRI1**} [**LOSON**|**LOSOFF**] [**1**|**2**|**5**|**10**|**30**] [**STA**ndard|**QSF**p4sfp]

  Examples:
  Add to BlzSwi PORT 1.2.4 "BLZ 1.2.4" 4GFib LOSON 5
  Add to myswitch POR 1.1.2 ’m 01.01.02’ 10GEth
  Add to Blz2 TES Port 1.1.1 BlzTap1 GIG-E
  Add to BlxSw XSL POR 1.3.1 ’xSL 1.3.1’ 10GEth
  Add to myswitch 4 POR 1.1.1 ’m 01.01.01’ 25GEth

- **CON**nect [*options*] {**POR**t|**PRTN**um|**GRO**up|**GEN**erator|**DEVICEP**ort} <*source*> [**POR**t|**PRTN**um|**GRO**up|**DEVICEP**ort] <*destination*>
  Connect ports or groups. Port-to-port connections must specify simplex (-s) or duplex (-d). Filters can optionally be specified with the -f 'filter name' option. Filters allow only a subset of the traffic, based on rules, to reach the destination. Connection Groups cannot use the -f 'filter name' option. Impairments can optionally be specified with the -I 'Impairment name' option. If no topology is specified (-t) the connection will be created as part of the default topology “CLI Topology”. If the specified topology does not already exist it will be created. If an inactive connection is specified then the ports will not be powered up and no traffic will flow until the connection is activated. Connections may be activated individually or an entire topology can be activated at once. Refer to the ACTivate (and DEActivate) commands. Using multiple topologies allows groups of connections to be activated, deactivated, and deleted together in one command. Surround names containing spaces with double quotes (“name”).

  options (case sensitive):
  -h [**--help**] Show options help
  -d [**--duplex**] Create a duplex port connection
  -f [**--filter**] arg Use a named filter, arg = filter name
  -I [**--impairment**] arg Use a named impairment, arg = impairment name
  -F [**--force**] Force a connection without showing warnings
  -i [**--inactive**] Create an inactive connection
  -s [**--simplex**] Create a simplex port connection
  -t [**--topology**] arg Put connection in this topology, arg = topology name

Examples:
CONN --simplex PORT port1 PORT port2
CONNECT -d PRTNUM 1.1.1 2.2.2
CONNECT -s PRTNUM 1.2.3.1 1.2.4.2
conn -s port SPAN1 port "Analyzer Tool Port"
CONNECT GROUP grp1 GROUP grp2
CONNECT GROUP SrcGrp DstGrp
CONN --inactive GROUP SrcGrp DstGrp
CONNECT -f "Deny ARP Filter" GROUP grp1 grp2
CONNECT -f VlanFilter GRO "Network Ports" PORT Tool1
CONNECT -I DelayImp PORT "Port A" PORT Tool1

- **CRE**ate **STA**tistics **REP**ort [**POR**t|**PRTN**um] (*port-list*) **FRO**m **MM/DD/YYYY-HH:MM TO MM/DD/YYYY-HH:MM** [***idleValue***] [**SHOW**|**EXP**ort] [***filename***]
  Create a statistics report for the list of ports specified. The port list is specified using the port name if the PORT option is used. If the PRTNUM option is used then each port is specified with its physical port address in the form cc.ss.pp. The port-list is specified within parenthesis as a comma separated list. If only a single port is specified, then the parenthesis are not necessary. Optional idle value defaults to 1 if not specified. SHOW option will display the report on the console, EXPORT will export the report in csv format to a file. SHOW is the defualt if nothing is specified. filename can be either a regular filespec format (d:/directory/filename) or a URL formatted specification(".csv" is automatically appended to the filename specified.)
  The Select Switch command must be issued before this command if using PRTNUM.

  Examples:
  CREATE STATS REP ('PHL 1.4.6','PHL 1.4.7','PHL 1.4.8','PHL 1.4.9') FROm 03/04/2017-12:00 TO 03/08/2017-12:00 EXPort c:\StatReport
  cre sta rep prtn (1.4.6,1.4.7,1.4.8,1.4.9) FROm 03/04/2017-12:00 TO 03/08/2017-12:00 4
  cre sta rep prtn 1.3.4 FROm 03/04/2017-12:00 TO 03/08/2017-12:00 2 EXPort ftp://admin:password@10.88.55.44/OnPATH/myreport

- **DEA**ctivate [*options*] {**POR**t|**PRTN**um|**GRO**up|**GEN**erator|**DEVICEP**ort} ***source*** [**POR**t|**PRTN**um|**GRO**up|**DEVICEP**ort] ***destination***
  Deactivate the connection(s) between the source and destination. Deactivating causes traffic to stop flowing and the ports to power down if they should not stay up for any other reason, such as being in another connection or collecting statistics. The connection remains in its topology and can be reactivated later either individually or by activating the entire topology. If no topology is specified the default topology "CLI Topology" is used. Must use the -f 'filter name' option to deactivate filtered connections. Must use the -I 'impairment name' option to deactivate impaired connections. Wildcards (*) are accepted for source or destination name, but not both.

  options (case sensitive):
  -F [**--force**] Force without showing warnings
  -h [**--help**] Show options help
  -d [**--duplex**] A duplex port connection
  -f [**--filter**] arg Connection through filter, arg = filter name
  -I [**--impairment**] arg Connection through impairment, arg = impairment name
  -s [**--simplex**] A simplex port connection
  -t [**--topology**] arg Connections in this topology, arg = topology name

  Examples:
  deactivate group groupAsrc *
  deactivate group * groupBdest
  deact --duplex -t MyTopology PORT "Src Port ABC" "Dest Port ABC"
  deact -s PORT SPAN1 *
  deact -s PORT * Analyzer1
  DEACTIVATE GROUP groupA *
  deact -f ArpFilter GRO "Network Ports" Analyzer
  DEACTIVATE -f VlanFilter GRO "Network Ports" PORT Tool1

- **DEL**ETE **FIL**TER ***name***
  Delete an existing filter.

  Examples:
  DEL filter FilterA
  delete fil ‘Filter ABC’

- **DEL**ete **GEN**erator ***name***
  Delete an existing generator.

  Examples:
  DEL generator GeneratorA
  delete gen 'GEN ABC'

- **DEL**ete **PAC**ket **DEF**inition ***name***
  Delete an existing Packet Definition.

  Examples:
  DEL PAC DEF PacketDefA
  delete pac def 'PD ABC

- **DEL**ete **PAC**ket **DEF**inition ***packetdefname*** **FRO**m ***streamname***
  Delete a Packet Definition from a Stream.

  Examples:
  del pac def 'Packet A' from StreamA
  delete pac def PD1 from 'Steam ABC'

- **DEL**ETE **RUL**E ***name***
  Delete an existing rule.

  Examples:
  DEL rule RuleA
  delete rul 'Rule ABC'

- **DEL**ETE **RUL**E ***rulename*** **FRO**m ***filtername***
  Delete a rule from a filter by name.

  Examples:
  DELETE RULE 'Permit VOIP' from FilterA
  del rul DropArps from "Test Filter"

- **DEL**ete **STR**eam ***name***
  Delete an existing Stream.

  Examples:
  DEL str StreamA
  delete stream 'Stream ABC'

- **DISC**onnect [***options***] {**POR**t|**PRTN**um|**GRO**up|**GEN**erator|**DEVICEP**ort} ***source*** [**POR**t|**PRTN**um|**GRO**up|**DEVICEP**ort] ***destination***
  Disconnect the connection(s) between the source and destination. Disconnecting causes traffic to stop flowing and the ports to power down if they should not stay up for any other reason, such as being in another connection or collecting statistics. The connection is also removed from the topology. If no topology is specified the default topology "CLI Topology" is used. Must use the -f 'filter name' option to disconnect filtered connections. Must use the -I 'impairment name' option to disconnect impaired connections. Wildcards (*) are accepted for source or destination name, but not both. To stop the traffic but keep the connections in the topology, use the Deactivate command instead. Surround names containing spaces with double quotes ("name").

  options (case sensitive):
  -F [**--force**] Force without showing warnings
  -h [**--help**] Show options help
  -d [**--duplex**] A duplex port connection
  -f [**--filter**] arg Connection through filter, arg = filter name
  -I [**--impairment**] arg Connection through impairment, arg = impairment name
  -s [**--simplex**] A simplex port connection
  -t [**--topology**] arg Connections in this topology, arg = topology name

  Examples:
  disconnect group groupA *
  discon --duplex -t MyTopology PORT "Src Port ABC" "Dest Port ABC"
  discon -s PORT "SPAN 1" *
  discon -s PORT * Analyzer1
  DISC GROUP groupA *
  discon -f ArpFilter GRO "Network Ports" Analyzer
  DISCONNECT -f VlanFilter GRO "Network Ports" PORT Tool1

- **EXP**ort **STA**tistics **REP**ort [**POR**t|**PRTN**um] (*port-list*) **FRO**m **MM/DD/YYYY-HH:MM TO MM/DD/YYYY-HH:MM *filename***
  Export a statistics report for the list of ports specified. The port list is specified using the port name if the PORT option is used. If the PRTNUM option is used then each port is specified with its physical port address in the form cc.ss.pp. The port-list is specified within parenthesis as a comma separated list. If only a single port is specified, then the parenthesis are not necessary.

  filename can be either a regular filespec format (d:/directory/filename) or a URL formatted specification(".csv" is automatically appended to the filename specified.)
  The Select Switch command must be issued before this command if using PRTNUM.

  Examples:
  EXPORT STATS REP ('PHL 1.4.6','PHL 1.4.7','PHL 1.4.8','PHL 1.4.9') FROm 03/04/2017-12:00 TO 03/08/2017-12:00 c:\StatReport

  exp sta rep prtn 1.3.4 FROm 03/04/2017-12:00 TO 03/08/2017-12:00 ftp://admin:password@10.88.55.44/OnPATH/myreport

- **RESE**t **STATS PCE** {**POR**t|**PRTN**um} [*|name[,name...]]
  Reset the real time statistics counters to zero on the specified PCE port. The PCE port must have been previously started.

  Examples:
  reset stats pce prtnum 1.1.PCE1
  reset stats pce port dedup1

- **RESE**t **STATS** {**POR**t|**PRTN**um} [*|name[,name...]]
  Reset the real time statistics counters to zero on the specified port(s) or subport(s). The port(s) or subport(s) must have been previously started. The wildcard (*) resets all stats that have been previously started.

  Examples:
  reset stats port SpanA
  RESET STATS prtnum "1.1.1, 1.1.2.1, 1.1.3.2"
  rese stats port SpanBTx,SpanBRx
  reset stats port *

- **REV**ise **BLA**de *bladeaddress* **PCE** {**ENA**ble|**DIS**able}
  Revise Blade will enable / disable the Packet Conditioning Engine.

  Example:
  rev bla 1.2 pce ena,

- **REV**ise **PCE** {**POR**t|**PRTN**um} *portname* **IMP**airment {**DIS**able|**ENA**ble} {**DEL**ay|**LN**|**LP**} [value]
  Revise PCE port properties to enable / disable Impairment on the PCE Port.
  Set 'Enable' to turn on an impairment

  DELay: Number of milliseconds to delay (range 1 - 300).

  LN: Drop 1 out of every N packets.

  LP: Drop percentage of packets (range .0001 - 100)
  PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Examples:
  rev pce port myport imp enable delay 50
  rev pce prtnum 01.01.PCE1 imp enable LP .001

- **REV**ise {**POR**t|**PRTN**um} *port* **AUTON**egotiate {**ENA**ble|**DIS**able}
  Revise port configuration for auto-negotiation settings. Set 'ENAble' to turn auto-negotiation on. Valid only for GIG-E ports. PRTNUM is only valid on an embedded server unless Select Switch command has been issued.

  Examples:
  rev prtn 1.2.4 autoneg enable
  rev prtn 1.2.4 auton dis

- **REV**ise {**POR**t|**PRTN**um} *port* **CONG**estion **ALA**rm {**ENA**bled|**DIS**abled}
  Revise a port's congestion alarm mode. PRTNUM is only valid on an embedded server unless Select Switch command has been issued.

  Examples:
  rev prtn 1.2.4 cong ala ena
  rev prtn 1.2.4 cong ala dis

- **REV**ise {**POR**t|**PRTN**um} *port* **DES**tination **FIL**ter {*filtername*|**NONE**}
  Revise the Destination Filter of the specified port. Destination filters can permit and deny Ethernet frames that would be transmitted from this port. There is an implicit 'permit all' if no filter is selected and for frames that do not match any rules of a selected filter. Selecting 'NONe' stops Destination Filtering on the port. If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp.
  PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Examples:
  rev por 'Tool 1' Destination Filter 'No HTTPS'
  revise prtnum 1.2.4 DES FIL 'Feed 1'
  Revise Port Network1 Destination Filter NONE

- **REV**ise {**POR**t|**PRTN**um} *port* **NANO**stamp {**ENA**ble|**DIS**able}
  Revise the destination port configuration for Nanostamping. Set to 'Enable' to add a Nanostamp. This appends a nanosecond-level free running counter value to all packets sent on this port. The value of the counter is captured when packets are received, and optionally added to packets when they are transmitted. Set to 'Disable' to stop adding Nanostamps. PRTNUM is only valid on an embedded server unless Select Switch command has been issued.

  Examples:
  revise port "Analyzer Tool" nanostamp enable
  rev prtn 1.2.4 nano dis

- **REV**ise {**POR**t|**PRTN**um} *port* {**RXT**hreshold|**TXT**hreshold} {**HI**gh|**LO**w} [**ARM**|**DISARM**][event] [reset] [event_duration] [reset_duration]
  Revise the port configuration threshold settings. Threshold settings enable event notifications when the traffic utilization goes above or below a certain percent for the specified amount of time. Receive (RxThreshold), transmit (TXThreshold), high and low thresholds are specified independently. ARM enables the threshold configuration and DISARM disables it. If neither ARM nor DISARM is specified then it remains unchanged. The 'event' value is the utilization percentage at which the event is triggered. The 'reset' value is the utilization percentage at which a previously triggered event is cleared, allowing another event to be triggered.

  For HIGH threshold settings:
  - The event value must be higher than the reset value.
  - The 'event_duration' is the number of seconds during which the utilization must exceed the event threshold in order for the event to trigger.
  - The 'reset_duration' is the number of seconds during which the utilization must drop below the reset threshold in order for the event to clear.

  For LOW threshold settings:
  - The event value must be lower than the reset value.
  - The 'event_duration' is the number of seconds during which the utilization must drop below the event threshold in order for the event to trigger.
  - The 'reset_duration' is the number of seconds during which the utilization must exceed the reset threshold in order for the event to clear. The numeric values: event, reset, event_duration, and reset_duration must be specified in that order, and cannot be skipped over. In other words you cannot set the durations without also first setting the event and reset values, but you can set the event and reset values without the durations. Duration values default to 1 second if never set.

Each triggered event and cleared event will appear in the port alarm log.
If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp
PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Examples:
REVISE PORT NetworkPort1 RxTHRESHOLD HIGH ARM 85 75 10 60
rev prtn 1.2.4 TxT lo 10 25 5 3
REV Port "Team A Input" RXThreshold LOW DISARM
REV Port AnalyzerTool TxThresh HIGH ARM 95

- **REV**ise {**POR**t|**PRTN**um} port **SLIC**ing {**ENA**ble|**DIS**able}
  Revise the destination port configuration for Packet Slicing. Set to 'Enable' to slice packets to 160 bytes. This slices all packets sent on this port to 160 bytes. Set to 'Disable' to stop slicing packets.
  PRTNUM is only valid on an embedded server unless Select Switch command has been issued.

  Examples:

  revise port "Analyzer Tool" slicing enable
  rev prtn 1.2.4 slic dis

- **REV**ise {**POR**t|**PRTN**um} *port* **VLA**ntag {**KEE**p|**ADD**|**REP**lace|**REM**ove} [**ID** *value*]
  Revise source port configuration for VLAN settings.
  Setting 'KEEp' on this, and setting 'UNTagkeep' on the destination port this port connects to, will leave the frame unchanged. Setting 'ADD' and 'ID value' on this port, and setting 'Allow Tag' on the destination port this port connects to, will add a new VLAN Tag. Setting 'REPlace' and 'ID value' on this port, and setting 'ALLowtag' on the destination port this port connects to, will replace the outer VLAN if the original packet already has a VLAN Tag or will add a new VLAN Tag if the original packet does not have a VLAN Tag. Setting 'REMove' on this port, and setting 'UNTagkeep' on the destination port this port connects to, will remove the outer VLAN Tag if the original packet has any.

  Examples:
  rev prtn 1.2.4 vlantag add id 104
  rev prtn 1.2.4 vlantag keep

- **REV**ise {**POR**t|**PRTN**um} *port* **VLA**ntag {**ALL**owtag|**UNT**agkeep} [**TPI**d *value*]
  Revise destination port configuration for VLAN settings.
  Set 'ALLowtag' and 'TPId value' on this port when connected source port set to 'ADD' or 'REPlace'.
  Set 'UNTagkeep' on this port when connected source port set to 'KEEp' or 'REMove'.

  Examples:
  rev prtn 1.2.4 vlantag allowtag tpid 0x8100
  rev prtn 1.2.4 vlantag untagkeep

- **REV**ise {**POR**t|**PRTN**um} *port* **VLA**ntag **ID** *value*
  Revise source port configuration for VLAN ID settings. If PORt is used specify the port name; if PRTNum is used specify the port number as cc.ss.pp.
  PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Example:
  rev prtn 1.2.4 vlantag id 104

- **REV**ise {**POR**t|**PRTN**um} *port* **VLA**ntag **TPI**d *value*
  Revise destination port configuration for VLAN TPID settings. If PORt is used specify the port name; if PRTNum is used specify the port number as cc.ss.pp.
  PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Example:
  rev prtn 1.2.4 vlantag tpid 0x8100

- **REV**ise {**POR**t|**PRTN**um} *port* **VNT**ag {**ALL**owtag|**UNT**ag}
  Revise destination port configuration for VN-Tag stripping settings.
  Set 'ALLowtag' to leave VN-Tag unchanged. 'ALLowtag' is valid only when the source port is on the same T-Blade. VN-Tags are automatically stripped when the frame is sent to another board.
  Set 'UNTag' to remove VN-Tag.
  PRTNUM is only valid on an embedded server unless Select Switch command has been issued.

  Examples:
  rev prtn 1.2.4 vntag allow
  REVISE PORT MyAnalyzer vntag untag

- **REV**ise **RUL**e *rulename rule*
  Replaces a rules action and conditions with a new action and conditions. If the rule is being used in an active connection the new rule is applied to the hardware immediately. See ADD RULE for rule syntax and available conditions

  Examples:
  Rev rul RuleA "permit all"
  REVISE RULE 'Deny IP Addresses' 'deny ip.addr==10.1.1.1 - 10.10.255.255'

- **REV**ise **SWI**tch ***switchname*** **VNT**ag **DET**ection {**ENA**bled|**DIS**abled}
  Revise a switch's VN-Tag Detection mode. VN-Tag Detection mode allows filtering and load balancing of the encapsulated IP packet of VN-Tagged frames, and optional removal of VN-Tags. In VN-Tag Detection Mode, if the source and destination ports are on different blades the VN-Tags will always be removed. If VN-Tag Detection Mode is not enabled, VN-Tagged frames will pass through the system with VN-Tags intact.

  Examples:
  REVISE SWITCH MySwitch VNTAG DETECTION ENABLED
  rev swi MySwitch vnt det dis

- **SHO**W **DEST**INATION **GRO**UPS [**SEA**RCH ***text***]
  Display a list of all defined Destination Groups and the number of members in each.

  Example:
  SHOW DEST GRO “load bal 1”

- **SHO**w **CON**nected **ISL**
  Display a list of all connected ISL ports.

  Example:
  SHOW CON ISL

- **SHO**W **FIL**TERS [**SEA**RCH ***text***]
  Display a list of all defined filters and the number of rules in each.

  Example:
  show filter FilterA

- **SHO**w **GEN**erators [**SEA**rch ***text***]
  Display a list of all defined Stream Generators and the topologies they are associated with.

  Examples:
  show gen search StreamGeneratorA
  show gen

- **SHO**W **INF**ORMATION {**GRO**UP|**POR**T|**PRTN**UM|**SWI**TCH|**FIL**TER|**IMP**airment} ***name***
  Display detailed information of the specified Connection/Source/Destination Group, port, switch, filter, or Impairment. If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp
  PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Examples:
  SHOW info port 'LAB 1.1.1'
  show info prtn 1.1.1

- **SHO**w [**GRO**up|**FIL**ter|**TOP**ology|**SCAnner**|**STR**eam|**GEN**erator] **MEM**bers ***name***
  Display a list of ports contained in a Connection Group, Source Group, Destination Group, or Port Scanner, rules in a filter, packet definitions in a stream, stream in a generator, or members of a topology.

  Examples:
  SHOW gro Mem GrpA
  sho fil Mem 'VOIP Filter'
  sho sca Mem ScannerA
  display topology Mem 'CLI Topology'
- **SHO**W {**POR**T|**PRTN**UM|**GRO**UP|**FIL**TER|**IM**Pairent|**DEVICEP**ort} ***name*** **TOP**OLOGIES
  Display the Topologies where the specified object is used.

  Examples:
  SHOW GROUP 'Source 2' TOP
  SHOW PRTNUM 01.01.01 TOP
  SHOW IMP myimp TOP
- **SHO**w **PAC**ket **DEF**inition [**SEA**rch ***text***]
  Display a list of all defined Packet Definitions.

  Examples:
  show pac def PacketDefA
  show pac
- **SHO**W **RUL**ES [**SEA**RCH ***text***]
  Display a list of all defined rules.

  Examples:
  Show Rules
  SHO RUL search VOIP
- **SHO**w **STR**eams [**SEA**rch ***text***]
  Display a list of all defined Streams and the number of members in each.

  Examples:
  show str search StreamA
  show str
- **SHO**w **STATS PCE** {**POR**t|**PRTN**um} *portname*
  Display the real time statistics counters on the specified PCE port. The PCE port must have been previously started.
  PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Example:
  show stats pce port dedup1
- **SHO**w **STATS** {**POR**t|**PRTN**um} [*|name[,name...]]
  Display the real time statistics counters on the specified port(s) or subport(s). The port(s) or subport(s) must have been previously started. The wildcard (*) shows all stats that have been previously started.
  PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Examples:
  show stats port SpanA
  SHOW STATS prtnum "1.1.1, 1.1.2.1, 1.1.3.2"
  sho stats port SpanBTx
  show stats port *
- **STA**rt **STATS PCE** {**POR**t|**PRTN**um} *portname*
  Start real time statistics collection on the specified PCE port.

  Example:
  STA STATS pce prtnum 01.01.PCE1
- **STA**rt **STATS** {**POR**t|**PRTN**um} name[,name...]
  Start real time statistics collection on the specified port(s) or subport(s).

  Examples:
  STA STATS prtnum "1.1.1, 1.1.2.1, 1.1.3.2"
  sta stats port SpanA
  start stats port SpanBRx

- **STO**p **STATS PCE** {**POR**t|**PRTN**um} *portname*
  Stop real time statistics collection on the specified PCE port. The PCE port must have been previously started.

  Example:
  sto stats pce port dedup1

- **STO**p **STATS** {**POR**t|**PRTN**um} [*|name[,name...]]
  Stop real time statistics collection on the specified port(s) or subport(s). The port(s) or subport(s) must have been previously started. The wildcard (*) stops collecting all stats that have been previously started.

  Examples:
  sto stats port SpanA
  STOP STATS prtnum "1.1.1, 1.1.2.1, 1.1.3.2"
  stop stats port SpanBTx
  stop stats port *

HS-3200/H6400 Specific

- **ENA**ble {**POR**t|**PRTN**um} port
  Enable the specified port.
  This command only applies to primary ports on HS-3200.
  If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp
  PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

  Examples:
  ENAble PORT 'BLZ 1.2.1-1'
  enable prtn 1.2.1

Usage: **ADD TO** switchname [lanes] [**TES**t|**MIR**ror|**XS**l|**CL**one] **POR**t cc.bb.pp portname
{1GFib|2GFib|4GFib|8GFib|16GFib|GIG-E|CU-GIG-E|OC-3/stm-1|OC-12/stm-4|
OC-48/stm-16|OC-192/stm-64|OPTical|10GEth|25GEth|40GEth|50GEth|100GEth|
100MFib|CU10000|CPRI9|CPRI8|CPRI7|CPRI6|CPRI5|CPRI4|CPRI3|CPRI2|CPRI1|
SAS3G/6G/12G|OTU1|OTU2|OTU2E|Generic} [LOSON|LOSOFF] [1|2|5|10|30]
[**STA**ndard|**QSF**p4sfp]

Add a new port to a switch.

[lanes] only applies to 10GEth and 25GEth on the primary port of an HS-3200 or HS-6400

If no type parameter is specified then a normal port is created.

CPRI Options are used for CPRI interfaces. The actual speeds are:

CPRI 9 (12,165.12 mbps)

CPRI 8 (10,137.6 mbps)

CPRI 7 (9,830.4 mbps)

CPRI 6 (6,144.0 mbps)

CPRI 5 (4,915.2 mbps)

CPRI 4 (3,072.0 mbps)

CPRI 3 (2,457.6 mbps)

CPRI 2 (1,228.8 mbps)

CPRI 1 (614.4 mbps)

[STANDARD|QSFP4SFP] only applies on the primary port of an S-Blade Pro

Ex: Add to BlzSwi PORT 1.2.4 'BLZ 1.2.4' 4GFib LOSON 5

Add to myswitch POR 1.1.2 'm 01.01.02' 10GEth

Add to Blz2 TES Port 1.1.1 BlzTap1 GIG-E

Add to BlxSw XSL POR 1.3.1 'xSL 1.3.1' 10GEth

Add to myswitch 4 POR 1.1.1 'm 01.01.01' 25GEth

Usage: **REV**ise {**POR**t|**PRTN**um} port
[lanes]
{1GFib|2GFib|4GFib|8GFib|16GFib|GIG-E|CU-GIG-E|OC-3/stm-1|OC-12/stm-4|
OC-48/stm-16|OC-192/stm-64|OPTical|10GEth|25GEth|40GEth|50GEth|100GEth|
100MFib|CU10000|CPRI9|CPRI8|CPRI7|CPRI6|CPRI5|CPRI4|CPRI3|CPRI2|CPRI1|
SAS3G/6G/12G|OTU1|OTU2|OTU2E|Generic} [LOSON|LOSOFF] [1|2|5|10|30]

Revise the interface of the specified port.

CPRI Options are used for CPRI interfaces. The actual speeds are:

CPRI 9 (12,165.12 mbps)

CPRI 8 (10,137.6 mbps)

CPRI 7 (9,830.4 mbps)

CPRI 6 (6,144.0 mbps)

CPRI 5 (4,915.2 mbps)

CPRI 4 (3,072.0 mbps)

CPRI 3 (2,457.6 mbps)

CPRI 2 (1,228.8 mbps)

CPRI 1 (614.4 mbps)

[lanes] only applies to 10GEth and 25GEth on the primary port of an HS-3200 or HS-6400

LOSON/LOSOFF must be,followed by the number of seconds. port must be

a port name if PORt is used, otherwise portname is cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev por 'Blz 1.2.4' 10GEth

rev prtn 1.2.4 10GEth LOSON 2

rev prtn 1.2.4 10GEth LOSOFF

rev prtn 1.1.1 4 25GEth

To configure a port for 25G ETH with an adapter, set the interface to '25Geth' and 'lanes' to '1'.

Usage: **ADD TO** switchname [lanes] [**TES**t|**MIR**ror|**XS**l|**CL**one] **POR**t cc.bb.pp portname {1GFib|2GFib|4GFib|8GFib|16GFib|GIG-E|CU-GIG-E|OC-3/stm-1|OC-12/stm-4| OC-48/stm-16|OC-192/stm-64|OPTical|10GEth|25GEth|40GEth|50GEth|100GEth| 100MFib|CU10000|CPRI9|CPRI8|CPRI7|CPRI6|CPRI5|CPRI4|CPRI3|CPRI2|CPRI1| SAS3G/6G/12G|OTU1|OTU2|OTU2E|Generic} [LOSON|LOSOFF] [1|2|5|10|30] [**STA**ndard|**QSF**p4sfp]

Add a new port to a switch.

[lanes] only applies to 10GEth and 25GEth on the primary port of an HS-3200 or HS-6400

If no type parameter is specified then a normal port is created.

CPRI Options are used for CPRI interfaces. The actual speeds are:

CPRI 9 (12,165.12 mbps)

CPRI 8 (10,137.6 mbps)

CPRI 7 (9,830.4 mbps)

CPRI 6 (6,144.0 mbps)

CPRI 5 (4,915.2 mbps)

CPRI 4 (3,072.0 mbps)

CPRI 3 (2,457.6 mbps)

CPRI 2 (1,228.8 mbps)

CPRI 1 (614.4 mbps)

[STANDARD|QSFP4SFP] only applies on the primary port of an S-Blade Pro

Ex: Add to BlzSwi PORT 1.2.4 'BLZ 1.2.4' 4GFib LOSON 5

Add to myswitch POR 1.1.2 'm 01.01.02' 10GEth

Add to Blz2 TES Port 1.1.1 BlzTap1 GIG-E

Add to BlxSw XSL POR 1.3.1 'xSL 1.3.1' 10GEth

Add to myswitch 4 POR 1.1.1 'm 01.01.01' 25GEth

For example:

ADD TO myswitch 1 POR 1.1.3 'my25Gport' 25GEth

To revise a port for 25G ETH with an adapter, set the interface to '25Geth' and 'lanes' to '1'

Usage: **REV**ise {**POR**t|**PRTN**um} port

[lanes]
{1GFib|2GFib|4GFib|8GFib|16GFib|GIG-E|CU-GIG-E|OC-3/stm-1|OC-12/stm-4|
OC-48/stm-16|OC-192/stm-64|OPTical|10GEth|25GEth|40GEth|50GEth|100GEth|
100MFib|CU10000|CPRI9|CPRI8|CPRI7|CPRI6|CPRI5|CPRI4|CPRI3|CPRI2|CPRI1|
SAS3G/6G/12G|OTU1|OTU2|OTU2E|Generic} [LOSON|LOSOFF] [1|2|5|10|30]

Revise the interface of the specified port.

CPRI Options are used for CPRI interfaces. The actual speeds are:

CPRI 9 (12,165.12 mbps)

CPRI 8 (10,137.6 mbps)

CPRI 7 (9,830.4 mbps)

CPRI 6 (6,144.0 mbps)

CPRI 5 (4,915.2 mbps)

CPRI 4 (3,072.0 mbps)

CPRI 3 (2,457.6 mbps)

CPRI 2 (1,228.8 mbps)

CPRI 1 (614.4 mbps)

[lanes] only applies to 10GEth and 25GEth on the primary port of an HS-3200 or HS-6400

LOSON/LOSOFF must be, followed by the number of seconds. The port must be a port name if **POR**t is used, otherwise portname is cc.ss.pp.

NOTE: **PRTNUM** is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev por 'Blz 1.2.4' 10GEth

rev prtn 1.2.4 10GEth LOSON 2

rev prtn 1.2.4 10GEth LOSOFF

rev prtn 1.1.1 4 25GEth

For example:

REV prtn 1.1.3 1 25GEth

Standard Commands - TestStream Lab Manager and TestStream Controller

=> help

Usage: **HELP** [PAGE number]

Display list of commands

The number of lines displayed per page can optionally be specified.

Press [Y|y] to view more results; any other key to exit.

Ex: help

help page 15

Usage: **EXIT**

Exit telnet session

Usage: **ACK**nowledge {**POR**t|**PRTN**um} **ALA**rms {**ALL|port**}

Acknowledge all port alarms on all switches, or all port alarms on the specified port. When the ACK PORT ALARMS ALL command is issued, then via a single command to each switch the server requests that the switch re-arm all port alarms that the switch had previously disabled due to reporting of that alarm to the server. If the switch reports successful completion of the re-arm command, then the UCS server moves all of that switch's port alarms from the port alarm current log to the port alarm history log. The latter command should be used after switching from the primary server to the backup server. It may also be used to determine the current alarm status of all connected ports.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: ACK POR ALA 'BLZ 1.2.4'

ack por ala all

Usage: **ACK**nowledge **SYS**tem **ALA**rms {**ALL|switch name**}

Acknowledge all system alarms or system alarms for a specific switch. This command can be issued for all switches via the ALL parameter or on a switch basis by specifying the switch name. Per port alarms, those system alarms that can be considered to have a bad/abnormal state, for example, power supply xx on CC yy is offline. Following acknowledgement of the alarm, if the bad/abnormal state persists, the alarm will be re-reported.

Ex: ACK SYS ALA ALL

ACK SYS ALA 'My3900'

Usage: **ACT**ivate **TOP**ology **name**

Activate all connections in a topology.

Ex: Activate topology TopologyA

act top 'TOPOLOGY ABC'

Usage: **ACT**ivate [options] {**POR**t|**PRTN**um|**GRO**up|**GEN**erator|**DEVICEP**ort} source [**POR**t|**PRTN**um|**GRO**up|**DEVICEP**ort] destination

Activate the connection(s) between the source and destination.

Activation causes the ports to power up and traffic to start flowing.

If no topology is specified the default topology "CLI Topology" is used, unless

device ports are specified, then the default topology "Device CLI Topology" is used.
Must use the -f 'filter name' option to activate filtered connections.
Must use the -I 'impairment name' option to activate impaired connections.
Wildcards (*) are accepted for source or destination name, but not both.
NOTE: Surround names containing spaces with double quotes ("name").
NOTE: DEVICEPort is only valid for TestStream Lab Manager.
options (case sensitive):

-h [**--help**] Show options help
-d [**--duplex**] A duplex port connection
-F [**--force**] Force without showing warnings
-f [**--filter**] arg Connection through filter, arg = filter name
-I [**--impairment**] arg Connection through impairment, arg = impairment name
-s [**--simplex**] A simplex port connection
-t [**--topology**] arg Connections in this topology, arg = topology name

Ex: activate group groupAsrc *
activate group * groupBdest
act --duplex -t MyTopology PORT "My Src Port ABC" "My Dest Port ABC"
ACTIVATE -s PORT SPAN1 *
ACTIVATE -s PORT * Analyzer1
act -f ArpFilter GRO "Network Ports" Analyzer
ACT -f VlanFilter GRO "Network Ports" PORT Tool1
ACT -I DropXImp PORT "PORT A" PORT ToolPort

Usage: **ADD DES**tination **GRO**up name [**LOA**dbalance]
Add a new destination group. Defaults to
a multicast group where each port receives a copy
of each frame. Specifying LOAdbalance creates a load balancing
group where frames are distributed among the ports.

Ex: ADD destination group DestA
add des group 'Dst ABC' LOADBAL

Usage: **ADD FIL**ter **name**
Add a new filter.

Ex: Add filter FilterA
Add fil 'Filter ABC'

Usage: **ADD GEN**erator **gname gspeed stream**
Add a new generator. Speed (0.0 - 40.0 Gbps in .5 Gbps increments)

Ex: Add gen GeneratorA 10.0 StreamA
Add gen 'Generator ABC' 18.5 'Stream ABC'

Usage: **ADD GRO**up **name**
Add a new Connection Group.

Ex: Add group GroupA
Add gro 'Group ABC'

Usage: **ADD IMP**airment **name** {**DEL**ay|**LN**|**LP**} **value**

Add an impairment.

DELay: Number of milliseconds to delay (range 0.1 - 1600). Must be to a 10th of a percent.

LN: Drop 1 out of every N packets (2 - 4294967296).

LP: Drop percentage of packets (range 0.0001 - 99.9999).

Ex: add imp myimp delay 50

add imp myimp LP .001

Usage: A**DD PAC**ketdef **packetdefname packetdef**

Add a new packet definition.

Ex: Add pac 'EthType ARP' 'packet.size==69 eth.type==80F3'

Add pac 'Source MAC' 'eth.src==01:02:03:04:05:06'

Add pac 'VLAN 1' 'vlan.id==100'

Add pac 'TCP IP' 'ip.proto==6'

Add pac 'TCP IPV6' 'ipv6.nxt==6'

ADD pac 'IP Addr' 'ip.src==1.2.3.4 ip.dst==3.4.5.6'

ADD pac 'Raw Packet 1' 'raw.packet = 1 payload.data=ABBB011099EF223454EFEF'

Valid fields are:

packet.size
eth.src
eth.dst
eth.type
vlan.id
vlan2.id
ip.dst
ip.src
ipv6.dst
ipv6.src
ip.version
ipv6.version
ip.ttl
ipv6.hoplimit
ipv6.flowlabel
l4.proto
ipv6.nxt
ip.dscp
ipv6.traffic_class
l4.srcport
l4.dstport
raw.packet (false = 0, true = 1)
payload.type (increment=2, repeat=3, random=4, specific=5)
payload.data (no spaces allowed)

Usage: **ADD PAC**ketdef **packetdefname TO streamname** [**position**]

Add a packetdef to a stream. Valid positions are from 1 to the first position after last existing rule in the stream. If not specified the packetdef will be

added to the end of the stream.

Ex: Add PACketdef packetDefA to atreamA

Add PACketdef packetDefB to streamA 1

Add PACketdef 'packetdef ABC' to 'stream ABC'

Usage: **ADD RUL**e **rulename rules**

Add a new rule.

Ex: Add rul RuleA "permit all"

Add rul 'Deny ARP' 'deny eth.type==ARP'

Add rul 'Source MAC' 'permit eth.src==01:02:03:04:05:06'

Add rul 'VLANS' 'permit vlan.id==101-199,1000-2000'

Add rul 'TCP IP' 'permit ip.proto==TCP'

Add rul 'TCP IPV6' 'permit ipv6.nxt==TCP'

Add rul 'TCP IP' 'permit l4.proto==TCP'

ADD RULE 'IP Addr 1.2.x.x' 'permit ip.src==1.2.0.0/255.255.0.0'

ADD RULE 'IP Addr 1.2.x.x' 'permit ip.src==1.2.0.0/16'

ADD RULE 'IP Addr 1.2.x.x' 'permit ip.src==1.2.0.0-1.2.255.255'

ADD RULE 'TCP HTTP' 'permit tcp.port==80,8080'

Valid fields are:

eth.src
eth.dst
eth.type
vlan.id
vlan.priority
vlan2.id
vlan2.priority
ip
ip.addr
ip.dst
ip.src
ipv6
ipv6.addr
ipv6.dst
ipv6.src
ip.ttl
l4.proto
ip.proto
ipv6.nxt
ip.tos.dscp
ipv6.traffic_class.dscp
ip.tos
ipv6.traffic_class
l4.port
tcp.port
udp.port
l4.srcport

tcp.srcport
udp.srcport
l4.dstport
tcp.dstport
udp.dstport
l4.data[n] where n is 0-39 for IPv4, 0-13 for IPv6

Usage: **ADD RUL**e **rulename TO filtername** [**position**]
Add a rule to a filter. Valid positions are from 1 to the first position after last existing rule in the filter. If not specified the rule will be added to the end of the filter.
Ex: Add rule ruleA to filterA
Add rule ruleB to filterA 1
Add rul 'rule ABC' to 'filter ABC'

Usage: **ADD SOU**rce **GRO**up **name**
Add a new Source Group.
Ex: Add source gro SourceA
add sou group 'Src ABC'

Usage: **ADD STRE**am **name**
Add a new stream.
Ex: Add stream StreamA
Add stre 'Stream ABC'

Usage: **ADD** [**POR**t|**PRTN**um] **portname TO groupname** [**position**]
Add a port to a Connection Group, Source Group, or Destination Group, or a subport to a Connection Group. If a subport is specified to be added to a Source or Destination Group its parent port will be added instead. Connections between Source and Destination Groups are one-way, traffic flows from Source to Destination. The position starts at 1 and if not specified the port/subport will be added to the end of the group. If the SUBPORT option is not used, portname must be a port name unless PRTNUM is used, otherwise portname is cc.ss.pp.
NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.
Ex: Add port 'BLZ 1.2.4' to GroupA
ADD prtn 1.2.4 to GroupA
add subport 'Blz 1.2.4.Tx' to ConnectionGroupA
Add subport prtn 1.2.4.2 to 'Connection Group ABC' 3

Usage: **ADD TOP**ology [**STA**ndard|**DEV**ice] **name**
Add a new topology. Default is standard
NOTE: DEVice is only valid for TestStream Lab Manager.
Ex: Add topology DEV TopologyA
Add top 'Topology ABC'

Usage: **ADD TO TOP**ology name {**POR**t|**PRTN**um|**GRO**up|**FIL**ter|**IMP**airment|**DEVICEP**ort|**DEV**ice} **name**

Add a member to a Topology.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

NOTE: DEVICEPort and DEVice are only valid for TestStream Lab Manager.

Ex: add to TOP 'Topology A' port 'SPAN A1'

add to topology "Team A Connections" dev NEWDEV

Usage: **ADD TO** switchname [**lanes**] [**TES**t|**MIR**ror|**XS**l|**CL**one] **POR**t **cc.bb.pp portname** {**1GFib**|**2GFib**|**4GFib**|**8GFib**|**16GFib**|**GIG-E**|**CU-GIG-E**|**OC-3/stm-1**|**OC-12/stm-4**|**OC-48/stm-16**|**OC-192/stm-64**|**OPT**ical|**10GEth**|**25GEth**|**40GEth**|**50GEth**|**100GEth**|**100MFib**|**CU10000**|**CPRI9**|**CPRI8**|**CPRI7**|**CPRI6**|**CPRI5**|**CPRI4**|**CPRI3**|**CPRI2**|**CPRI1**|**SAS3G/6G/12G**|**OTU1**|**OYU2**|**OTU2E**|**Generic**} [**LOSON**|**LOSOFF**] [**1**|**2**|**5**|**10**|**30**] [**STA**ndard|**QSF**p4sfp]

Add a new port to a switch.

[lanes] only applies to 10GEth and 25GEth on the primary port of an HS-3200 or HS-6400

If no type parameter is specified then a normal port is created.

CPRI Options are used for CPRI interfaces. The actual speeds are:

CPRI 9 (12,165.12 mbps)

CPRI 8 (10,137.6 mbps)

CPRI 7 (9,830.4 mbps)

CPRI 6 (6,144.0 mbps)

CPRI 5 (4,915.2 mbps)

CPRI 4 (3,072.0 mbps)

CPRI 3 (2,457.6 mbps)

CPRI 2 (1,228.8 mbps)

CPRI 1 (614.4 mbps)

[STANDARD|QSFP4SFP] only applies on the primary port of an S-Blade Pro

Ex: Add to BlzSwi PORT 1.2.4 'BLZ 1.2.4' 4GFib LOSON 5

Add to myswitch POR 1.1.2 'm 01.01.02' 10GEth

Add to Blz2 TES Port 1.1.1 BlzTap1 GIG-E

Add to BlxSw XSL POR 1.3.1 'xSL 1.3.1' 10GEth

Add to myswitch 4 POR 1.1.1 'm 01.01.01' 25GEth

Usage: **ARM** {**POR**t|**PRTN**um} **port**

Arm (enable) the port alarm for the specified port.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: ARM PORT 'BLZ 1.2.4'

arm prtn 1.2.4

Usage: **BACK**up [**CRE**ate|**-C**|**LIS**t|**-L**|**DE**lete|**-D**] filename [**DBLOG**] [description]

LIST/-L = List backup set

filename, [DBLOG] and [description] are ignored

DELete/-D = Delete a backup set
[DBLOG] and [description] are ignored
CREate/-C = Create a backup set, this is default and no need to specify
Back up the server database.
[DBLOG] is optional to include all the Debug Logs in the switch and server.
[description] will be embedded on the backup set
filename can be either a regular filespec format (d:/directory/filename)
or a URL formatted specification. URL is applicable to CREATE option
".zip" is automatically appended to the filename specified.

Ex: Backup mtxdb 'IBM 12/10/09 backup'
backup ftp://admin:password@10.88.55.44/OnPATH/mybackup mydescription

Usage: **CLE**an **CON**nect switchname [**DBO**nly]
Cleans (disconnects) the connections from the server database and the switch controller for the. specified switch. If the DBOnly option is used then the connections are only cleaned from the server database.

Ex: cle con switch1
clean conn myswitch dbo

Usage: **CONF**igure **AAA** {**RAD**ius|**TAC**acs} {**IP1**|**IP2**} ip port secret [timeout] [retry]
Configure RADUIS and/or TACACS where ip is the IP address of the RADIUS or TACACS server, port is the socket port, secret is the shared secret, and optionally timeout and retry values can be specified in seconds.

Ex: CONFIG AAA Radius IP1 10.88.37.177 1812 WinRadius 3 1

Usage: **CONF**igure **AAA AD** FQDN1 fqdn **REALM** realm [FQDN2 fqdn]
Configure Active Directory where FQDN is the full name of the Domain Controller and realm contains a user account location.

Ex: CONFIG AAA AD FQDN1 blue.white.green REALM white.green FQDN2 blue2.white.green

Usage: **CONF**igure **AAA AD KT USER** user **PASS**word password **ENC**ryption encyption_method
Configure Active Directory Keytab information for creating kerberos ticket and keytab where user is the existing user name of the Domain, password is the user's password and encryption contains the encryption method.

Ex: CONFIG AAA AD KT USER test PASSword XXXX ENCryption aes256-cts-hmac-sha1-96

Usage: **CONF**igure **AAA ORD**er {**RAD**ius|**TAC**acs|**LOC**al|**AD**} [**RAD**ius|**TAC**acs|**LOC**al|**AD**] [**RAD**ius|**TAC**acs|**LOC**al|AD] [**RAD**ius|**TAC**acs|**LOC**al|**AD**]
Configure the order in which authentication is done. Highest priority is first.

Ex: CONFIG AAA Order Radius Local

Usage: **CONF**igure **FIL**e filename [**SIM**ulate]
Configure (add, revise, delete) ports and port parameters. The configuration changes are defined by the contents of file filename. filename can be either a regular filespec format (d:/directory/filename.ext) or a URL formatted specification.
If the SIMULATE keyword is defined, then the input file is only checked for syntax

errors and the configuration is not changed. If the SIMULATE keyword is not specified, then if the syntax is correct the configuration changes will be made.

Ex: CONF File CFI/cfgMySwitch SIM

conf file ftp://user:password@192.168.0.2/Server/CFI/cfgSwiB

Usage: **CON**Figure **POR**t portnum [**lanes**] {**1000**|**CU1000**|**2000**|**2500**|**4000**|**8000**|**16000**|**10000**|**40000**|**OPT**ical|**100000**|**25000**|**50000**|**100MFib**|**CU10000**} {**ETH**ernet|**FIB**er|**SON**et} **name**

DEPRECATED. Use REVise {PORt|PRTNum} port ... instead.

Configure a port where portnum is the physical address cc.pp.ss and name is the portname.

[lanes] only applies to 10000 and 25000 on the primary port of an HS-3200 or HS-6400

Speed specified must be valid for the protocol type specified.

Ex: CONFIG port 1.1.1 1000 ETH 'NYC 1'

Ex: CONFIG port 1.1.1 4 25000 ETH 'NYC 1'

Usage: **CONF**igure **REM**ote **ACC**ess {**HTTP**|**HTTPS**|**SSH**|**CLI**|**RESTHTTP**|**RESTHTTPS**} {**ENA**ble|**DIS**able} port [**NEVER**|**TERM**inate] time

Configure remote access for HTTP, HTTPS, SSH, CLI, REST API over HTTP or REST API over HTTPS.

Each can be enabled or disabled and the port may be modified.

The port is ignored for the DISABLE option. Optionally, an idle time can be configured to terminate the client/ssh/cli/rest session due to inactivity.

Revising the idle time for HTTP or HTTPS may terminate all the GUI clients.

Revising SSH parameters may terminate all the SSH CLI sessions.

Revising CLI parameters may terminate all CLI sessions.

Revising RESTHTTP or RESTHTTPS parameters may terminate all REST API sessions.

'time' is ignored for the NEVER option.

Inactivity setting will be left alone if neither NEVER nor TERMinate specified.

Ex: CONFIG REM ACC HTTPS ENA 99

CONF REM ACC HTTP DIS

Usage: **CONF**igure **SNMP** {ENAble|DISable} {v3|v1_v2|all} [**GLO**bal]

Configure to enable or disable SNMP versions.

GLObal will apply globally in all switches. It works for external server only.

Ex: conf snmp ena all

conf snmp dis v1_v2

Usage: **CONF**igure **SNMP SYSC**ontact systemcontact [**SYSL**ocation systemlocation] [**GLO**bal]

Configure to set new system contact for SNMP.

Configure SNMP also allows user optionally to set new system location.

GLObal will apply globally in all switches. It works for external server only.

Ex: conf snmp sysc 'support@netscout.com'

conf snmp sysc 'support@netscout.com' sysl 'Marlton, NJ'

Usage: **CONF**igure **SNMP SYSL**ocation systemlocation [**SYSC**ontact systemcontact] [**GLO**bal]

Configure to set new system location for SNMP.

Configure SNMP also allows user optionally to set new system contact info.

GLObal will apply globally in all switches. It works for external server only.

Ex: conf snmp sysl 'Westford, MA'

conf snmp sysl 'Westford, MA' sysc 'support@netscout.com'

Usage: **CONF**igure **SNMP ROCO**mmunity readonlycommunityname

Configure read only community name string for SNMP.

GLObal will apply globally in all switches. It works for external server only.

Ex: conf snmp roco public

Usage: **CONF**igure **SNMP AUTH**entication {**NON**e|**MD5**|**SHA**} [**PRIV**acy {**NON**e|**DES**|**AES**}] [**GLO**bal]

Configure to set an authentication protocol for SNMP.

GLObal will apply globally in all switches. It works for external server only.

Ex: conf snmp auth md5

conf snmp auth sha priv des

Usage: **CONF**igure **SNMP PRIV**acy {**NON**e|**DES**|**AES**} [**AUTH**entication {**NON**e|**MD5**|**SHA**}] [**GLO**bal]

Configure to set a privacy protocol SNMP.

GLObal will apply globally in all switches. It works for external server only.

Ex: conf snmp priv des auth md5

Usage: **CONF**igure **SNMP PWAU**thentication newauthpassword verifyauthpassword [**GLO**bal]

Configure to modify the Authentication password for SNMP.

GLObal will apply globally in all switches. It works for external server only.

Ex: conf snmp pwau netscout2 netscout2

Usage: **CONF**igure **SNMP PWPR**ivacy newprivacypassword verifyprivacypassword [**GLO**bal]

Configure to modify privacy password for SNMP.

GLObal will apply globally in all switches. It works for external server only.

Ex: conf snmp pwpr netscout2 netscout2

Usage: **CON**nect [options] {**POR**t|**PRTN**um|**GRO**up|**GEN**erator|**DEVICEP**ort} <source> [**POR**t|**PRTN**um|**GRO**up|**DEVICEP**ort] <destination>

Connect ports or groups.

Port-to-port connections must specify simplex (-s) or duplex (-d).

Filters can optionally be specified with the -f 'filter name' option.

Filters allow only a subset of the traffic, based on rules, to

reach the destination. Connection Groups cannot use the -f 'filter name' option.

Impairments can optionally be specified with the -I 'Impairment name' option.

If no topology is specified (-t) the connection will be created as part of the

default topology "CLI Topology", unless device ports are specified, then the

default topology "Device CLI Topology" is used. If the specified topology does

not already exist it will be created.

If an inactive connection is specified then the ports will not be powered up and no traffic

will flow until the connection is activated. Connections may be activated individually

or an entire topology can be activated at once. Refer to the ACTivate (and DEActivate)

commands. Using multiple topologies allows groups of connections to be activated, deactivated,

and deleted together in one command.

NOTE: Surround names containing spaces with double quotes ("name").

NOTE: DEVICEPort is only valid for TestStream Lab Manager.

options (case sensitive):

-h [**--help**] Show options help

-d [**--duplex**] Create a duplex port connection

-f [**--filte**r] arg Use a named filter, arg = filter name

-I [**--impairment**] arg Use a named impairment, arg = impairment name

-F [**--force**] Force a connection without showing warnings

-i [**--inactive**] Create an inactive connection

-s [**--simplex**] Create a simplex port connection

-t [**--topology**] arg Put connection in this topology, arg = topology name

Ex: CONN --simplex PORT port1 PORT port2

CONNECT -d PRTNUM 1.1.1 2.2.2

CONNECT -s PRTNUM 1.2.3.1 1.2.4.2

conn -s port SPAN1 port "Analyzer Tool Port"

CONNECT GROUP grp1 GROUP grp2

CONNECT GROUP SrcGrp DstGrp

CONN --inactive GROUP SrcGrp DstGrp

CONNECT -f "Deny ARP Filter" GROUP grp1 grp2

CONNECT -f VlanFilter GRO "Network Ports" PORT Tool1

CONNECT -I DelayImp PORT "Port A" PORT Tool1

Usage: **CRE**ate **STA**tistics **REP**ort [**POR**t|**PRTN**um] (port-list) **FRO**m **MM/DD/YYYY-HH:MM TO MM/DD/YYYY-HH:MM** [idleValue] [**SHOW**|**EXP**ort] [filename]

Create a statistics report for the list of ports specified.

The port list is specified using the port name if the PORT option is used.

If the PRTNUM option is used then each port is specified with its physical port address in the form cc.ss.pp.

The port-list is specified within parenthesis as a comma separated list. If only a single port is specified, then the parenthesis are not necessary.

Optional idle value defaults to 1 if not specified.

SHOW option will display the report on the console, EXPORT will export the report in csv format to a file.

SHOW is the defualt if nothing is specified.

filename can be either a regular filespec format (d:/directory/filename)

or a URL formatted specification(".csv" is automatically appended to the filename specified.)

NOTE: The Select Switch command must be issued before this command if using PRTNUM.

Ex: CREATE STATS REP ('PHL 1.4.6','PHL 1.4.7','PHL 1.4.8','PHL 1.4.9') FROm 03/04/2017-12:00 TO 03/08/2017-12:00 EXPort c:\StatReport

cre sta rep prtn (1.4.6,1.4.7,1.4.8,1.4.9) FROm 03/04/2017-12:00 TO 03/08/2017-12:00 4

cre sta rep prtn 1.3.4 FROm 03/04/2017-12:00 TO 03/08/2017-12:00 2 EXPort ftp://admin:password@10.88.55.44/OnPATH/myreport

Usage: **DEA**ctivate **TOP**ology **name**

Deactivate all connections in a topology.

Ex: deactivate top TopologyA

dea top 'TOPOLOGY ABC'

Usage: **DEA**ctivate [options] {**POR**t|**PRTN**um|**GRO**up|**GEN**erator|**DEVICEP**ort} source [**POR**t|**PRTN**um|**GRO**up|**DEVICEP**ort] destination

Deactivate the connection(s) between the source and destination.

Deactivating causes traffic to stop flowing and the ports to power down if they should not stay up for any other reason, such as being in another connection or collecting statistics.

The connection remains in its topology and can be reactivated later either individually or by activating the entire topology. If no topology is specified the default topology "CLI Topology" is used, unless device ports are specified, then the default topology "Device CLI Topology" is used.

Must use the -f 'filter name' option to deactivate filtered connections.

Must use the -I 'impairment name' option to deactivate impaired connections.

Wildcards (*) are accepted for source or destination name, but not both.

NOTE: Surround names containing spaces with double quotes ("name").

NOTE: DEVICEPort is only valid for TestStream Lab Manager.

options (case sensitive):

-F [**--force**] Force without showing warnings

-h [**--help**] Show options help

-d [**--duplex**] A duplex port connection

-f [**--filter**] arg Connection through filter, arg = filter name

-I [**--impairment**] arg Connection through impairment, arg = impairment name

-s [**--simplex**] A simplex port connection

-t [**--topology**] arg Connections in this topology, arg = topology name

Ex: deactivate group groupAsrc *

deactivate group * groupBdest

deact --duplex -t MyTopology PORT "Src Port ABC" "Dest Port ABC"

deact -s PORT SPAN1 *

deact -s PORT * Analyzer1

DEACTIVATE GROUP groupA *

deact -f ArpFilter GRO "Network Ports" Analyzer

DEACTIVATE -f VlanFilter GRO "Network Ports" PORT Tool1

Usage: **DEL**ete **FIL**ter **name**

Delete an existing filter.

Ex: DEL filter FilterA

delete fil 'Filter ABC'

Usage: **DEL**ete G**EN**erator **name**

Delete an existing generator.

Ex: DEL generator GeneratorA

delete gen 'GEN ABC'

Usage: **DEL**ete **GRO**up **name**

Delete an existing Connection Group, Source Group, or Destination Group.

Ex: DEL group GroupA

delete gro 'Group ABC'

Usage: **DEL**ete **IMP**airment **name**

Delete impairment by name.

Ex: del imp myimp

Usage: **DEL**ete **PAC**ket **DEF**inition **name**

Delete an existing Packet Definition.

Ex: DEL PAC DEF PacketDefA

delete pac def 'PD ABC'

Usage: **DEL**ete **PAC**ket **DEF**inition **packetdefname FRO**m **streamname**

Delete a Packet Definition from a Stream.

Ex: del pac def 'Packet A' from StreamA

delete pac def PD1 from 'Steam ABC'

Usage: **DEL**ete {**POR**t|**PRTN**um} **port**

Delete a port from a switch.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: Del PORT 'BLZ 1.2.4'

del prtn 1.2.4

Usage: **DEL**ete [**SUBP**ort]{**POR**t|**PRTN**um} **portname FRO**m **groupname**

Delete a port or subport from a Connection Group, Source Group, or Destination Group.

If the SUBPORT option is not used, then portname must be a port name

unless the PRTNUM option is used, otherwise it is cc.ss.pp.

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: del port 'BLZ 1.2.4' from GroupA

del por 'BLZ 1.2.4' from GroupA

del subport 'BLX 1.2.4.Tx' from GroupA

del subport prtn 1.2.4.2 from GroupA

delete por Blz1.2.1 from 'Group ABC'

Usage: **DEL**ete {**POR**t|**PRTN**um|**GRO**up|**FIL**ter|**IMP**airment|**DEVICEP**ort|**DEV**ice} **name FRO**m **TOP**ology **name**

Delete a member from a Topology. If there are multiple copies,

for example multiple copies of a filter, then all are deleted.

Members may not be deleted if they are in an active connection.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

NOTE: DEVICEPort and DEVice are only valid for TestStream Lab Manager.

Ex: del port 'SPAN A1' from TOP 'Topology A'

del filter VOIP from topology "Team A Connections"

del GRO 'Analyzer Load Balance' from top TestTeam

del IMP 'Delay 50' from top TestTeam22

Usage: **DEL**ete **RUL**e **name**

Delete an existing rule.

Ex: DEL rule RuleA

delete rul 'Rule ABC'

Usage: **DEL**ete **RUL**e **rulename FRO**m **filtername**

Delete a rule from a filter by name.

Ex: DELETE RULE 'Permit VOIP' from FilterA

del rul DropArps from "Test Filter"

Usage: **DEL**ete **STR**eam **name**

Delete an existing Stream.

Ex: DEL str StreamA

delete stream 'Stream ABC'

Usage: **DEL**ete **TOP**ology name [**FORCE**]

Delete an existing topology.

Optional argument FORCE allows administrator privileges user to delete other user's private topology.

Ex: DEL TOPOLOGY TopologyA

delete top 'My Topology ABC'

Usage: **DIAGS**tat {**BLA**de|**CHA**ssis|**POR**t|**PRTN**um|**SWI**tch} **name**

Display diagnostic status for the specified blade, chassis port or switch.

Name must be a port name if PORt is used, otherwise name is cc.ss.pp.

NOTE: BLADE, CHASSIS and PRTNUM are only valid on an embedded server unless Select Switch command has been issued.

Ex: DIAGSTAT SWI switchA

SEL SWI myswitch

DIAGSTAT port 'LAB 1.1.1'

DIAGSTAT prtn 1.1.1

DIAGSTAT bla 1.2

DIAGSTAT cha 3

Usage: **DISA**rm {**POR**t|**PRTN**um} **port**

Disarm the port alarms for the specified port.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: DISarm PORT 'PHL 1.2.3'

disa prtn 1.2.4

Usage: **DISC**onnect * [switchname]

Disconnect all connections on a server or switch. If the switchname parameter is specified only the connections on that switch will be disconnected.

Ex: DISC *

DISC * MySwitch

Usage: **DISC**onnect [options] {**POR**t|**PRTN**um|**GRO**up|**GEN**erator|**DEVICEP**ort} source [**POR**t|**PRTN**um|**GRO**up|**DEVICEP**ort] destination

Disconnect the connection(s) between the source and destination.

Disconnecting causes traffic to stop flowing and the ports to power down if they should not stay up for any other reason, such as being in another connection or collecting statistics. The connection is also removed from the topology.

If no topology is specified the default topology "CLI Topology" is used, unless device ports are specified, then the default topology "Device CLI Topology" is used.

Must use the -f 'filter name' option to disconnect filtered connections.

Must use the -I 'impairment name' option to disconnect impaired connections.

Wildcards (*) are accepted for source or destination name, but not both.

To stop the traffic but keep the connections in the topology, use the Deactivate command instead.

NOTE: Surround names containing spaces with double quotes ("name").

NOTE: DEVICEPort is only valid for TestStream Lab Manager.

options (case sensitive):

-F [**--force**] Force without showing warnings

-h [**--help**] Show options help

-d [**--duplex**] A duplex port connection

-f [**--filter**] arg Connection through filter, arg = filter name

-I [**--impairment**] arg Connection through impairment, arg = impairment name

-s [**--simplex**] A simplex port connection

-t [**--topology**] arg Connections in this topology, arg = topology name

-i [**--ignore**] Return "Successful" if there is nothing to disconnect

Ex: disconnect group groupA *

discon --duplex -t MyTopology PORT "Src Port ABC" "Dest Port ABC"

discon -s PORT "SPAN 1" *

discon -s PORT * Analyzer1

DISC GROUP groupA *

discon -f ArpFilter GRO "Network Ports" Analyzer

DISCONNECT -f VlanFilter GRO "Network Ports" PORT Tool1

Usage: **ENA**ble {**POR**t|**PRTN**um} **port**

Enable the specified port.

This command only applies to primary ports on HS-3200 or HS-6400.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: ENAble PORT 'BLZ 1.2.1-1'

enable prtn 1.2.1

Usage: **EXP**ort **STA**tistics **REP**ort [**POR**t|**PRTN**um] (port-list) **FRO**m **MM/DD/YYYY-HH:MM TO MM/DD/YYYY-HH:MM filename**

Export a statistics report for the list of ports specified.

The port list is specified using the port name if the PORT option is used.

If the PRTNUM option is used then each port is specified with its physical port address in the form cc.ss.pp.

The port-list is specified within parenthesis as a comma separated list. If only a single port is specified, then the parenthesis are not necessary.

filename can be either a regular filespec format (d:/directory/filename)

or a URL formatted specification(".csv" is automatically appended to the filename specified.)

NOTE: The Select Switch command must be issued before this command if using PRTNUM.

Ex: EXPORT STATS REP ('PHL 1.4.6','PHL 1.4.7','PHL 1.4.8','PHL 1.4.9') FROm 03/04/2017-12:00 TO 03/08/2017-12:00 c:\StatReport

exp sta rep prtn 1.3.4 FROm 03/04/2017-12:00 TO 03/08/2017-12:00 ftp://admin:password@10.88.55.44/OnPATH/myreport

Usage: **FLA**p **STA**rt {**GRO**up|**POR**t|**PRTN**um|**DEVICEP**ort} name flap-off-time flap-on-time flap-repeat-count

Start port flapping on port or group. flap-on-time is a value from 250-720,000 msec, flap-off-time is a value from 20-720,000 msec and flap-repeat-count is a value from 1-1,000,000.

name must be a port name or group name unless PRTNUM is used.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

NOTE: DEVICEPort is only valid for TestStream Lab Manager.

Ex: Flap start PRTN 1.1.2 250 250 300

fla sta gro GrpA 500 250 1000

flap sta port 'PS 01.01.01' 250 250 400

flap sta devicep 'Device1-01' 350 500 500

Usage: **FLA**p **STO**p {**GRO**up|**POR**t|**PRTN**um|**DEVICEP**ort} **name**

Stop port flapping on port or device port. port must be a port name if PORt is used, otherwise it is cc.ss.pp.

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

NOTE: DEVICEPort is only valid for TestStream Lab Manager.

Ex: flap sto por 'PS 01.01.01'

flap sto prtn 1.1.1

flap sto gro GrpA

flap sto devicep 'Device1-01'

Usage: **LIC**ense **INS**tall filename

Install license.

Ex: LIC INS ftp://admin:password@10.88.55.44/msrv1C6F65424F6E.mlf

Usage: **LOCK** [**SIM**plex] {**POR**t|**PRTN**um} name MM/DD/YYYY-HH:MM [comment]

Lock duplex or simplex port until date/time specified. If comment contains spaces, then it must be enclosed

in single or double quotes. name must be a duplex or simplex port name if PORt is used, otherwise it is cc.ss.pp or cc.ss.pp.dd.

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: LOCK PORT 'PL 1.1.2' 10/30/2011-5:30
LOCK PRTN 1.1.2 10/30/2011-5:30
LOCK sim PORT 'PL 1.1.2.Tx' 10/30/2011-5:30
LOCK sim PRTN 1.1.2.1 10/30/2011-5:30

Usage: **LOGOFF**

Logoff from the server. The telnet connection remains intact.
The operator my only issue the LOGON command.

Ex: LOGOFF

Usage: **LOG**on **userid password**

After the Telnet interface comes online, logon is required before execution of any other commands is permitted. The userid and password may not contain any embedded spaces.

Ex: LOGon admin password

Usage: **MOV**e **SFM CON**nections name

Moves the connections on the specified SFM.
This command is only available for 3912 switches.
Name is cc.ii where 'cc' is the chassis number and 'ii' is the SFM ID (1-8) corresponding to the slot number (13-20).
Name is only valid on an embedded server unless Select Switch command has been issued.

Ex: MOVe SFM CONnections 1.2

Usage: **PASSWORD**

Change user password.

Ex: password

Usage: **REC**oncile {**POR**t|**PRTN**um|**SWI**tch} name

Reconnnect/Disconnect single port or all ports on a switch. The PORT or PRTNUM option will reconnect a connected port and disconnect a disconnected port. Reconciling ports on a switch will allow the user to ensure that the switch contains all the connections that the server has. This is useful after a database restore.

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rec SWI NYSE
reconcile port "SW1 01.01.15"
recon prtn 1.1.2

Usage: **REN**ame {**POR**t|**PRTN**um} **port newportname**

Rename the specified port. **newportname** is always a port name.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: ren por 'Blz 1.2.4' 'Blz 2GFC 1.2.4'

Usage: **RESE**t **PAS**sword userid

Reset a users's password.

Ex: rese pas tester

Usage: **RESE**t **STATS PCE** {**POR**t|**PRTN**um} [*|name[,name...]]

Reset the real time statistics counters to zero on the specified PCE port.

The PCE port must have been previously started.

Ex: reset stats pce prtnum 1.1.PCE1

reset stats pce port dedup1

Usage: **RESE**t **STATS** {**POR**t|**PRTN**um} [*|name[,name...]]

Reset the real time statistics counters to zero on the specified port(s) or subport(s).

The port(s) or subport(s) must have been previously started.

The wildcard (*) resets all stats that have been previously started.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: reset stats port SpanA

RESET STATS prtnum "1.1.1, 1.1.2.1, 1.1.3.2"

rese stats port SpanBTx,SpanBRx

reset stats port *

Usage: **REST**ore **BACk**up **specification**

Restore backup database from the location specification. Specification can be either a backup located on the server or a remote file. Do not specify the extension.

*** WARNING ****

The Server will be restarted and Telnet session will terminate once the database is restored

Ex: rest bac 3901bkup

rest bac ftp://admin:password@10.88.55.44/OnPATH/mybackup

Usage: **RET**rieve **INV**entory **switchname** [FILE **filename**]

Retrieve the board inventory, serialization and version information from the switch. If the FILE option is used then the inventory is saved to the specified file/URL.

Ex: RET INV Blaze

RET INV Blaze FILE 3901Inv

ret inv 3901 FILE ftp://admin:password@10.88.55.44/OnPATH/Invent.log

Usage: **REV**ise **BLA**de bladeaddress **PCE** {**ENA**ble|**DIS**able}

Revise Blade will enable / disable the Packet Conditioning Engine

Ex: rev bla 1.2 pce ena

Usage: **REV**ise **BLA**de bladeaddress **BRI**dge **LAN**e **UTI**lization value

Revise Blade bridge lane allocation for utilization for S-Blade Pro

Value can be in the range of (0-8)

Note - Increasing the number of utilization lanes will reduce the number of shared resources available if Extended Fabric Mode is enabled.

Ex: rev bla 1.2 bri lan util 4

Usage: **REV**ise **IMP**airment name {**DIS**able|**ENA**ble} {**DEL**ay|L**N**|**LP**} value

Enable / disable Impairment properties.

DELay: Number of milliseconds to delay (range 0.1 - 1600). Must be to a 10th of a percent.

LN: Drop 1 out of every N packets (2 - 4294967296).

LP: Drop percentage of packets (range .0001 - 99.9999).

Ex: rev imp myimp delay 50

rev imp myimp LP .001

Usage: **REV**ise **PCE** {**POR**t|**PRTN**um} portname **IMP**airment {**DIS**able|**ENA**ble} {**DEL**ay|**LN**|**LP**} [value]

Revise PCE port properties to enable / disable Impairment on the PCE Port.

Set 'Enable' to turn on an impairment

DELay: Number of milliseconds to delay (range 1 - 300).

LN: Drop 1 out of every N packets.

LP: Drop percentage of packets (range .0001 - 100)

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev pce port myport imp enable delay 50

rev pce prtnum 01.01.PCE1 imp enable LP .001

Usage: **REV**ise {**POR**t|**PRTN**um} port [**lanes**]

{**1GFib**|**2GFib**|**4GFib**|**8GFib**|**16GFib**|**GIG-E**|**CU-GIG-E**|**OC-3/stm-1**|**OC-12/stm-4**|**OC-48/stm-16**|**OC-192/stm-64**|**OPT**ical|**10GEth**|**25GEth**|**40GEth**|**50GEth**|**100GEth**|**100MFib**|**CU10000**|**CPRI9**|**CPRI8**|**CPRI7**|**CPRI6**|**CPRI5**|**CPRI4**|**CPRI3**|**CPRI2**|**CPRI1**|**SAS3G/6G/12G**|**OTU1**|**OTU2**|**OTU2E**|**Generic**} [**LOSON**|**LOSOFF**] [**1**|**2**|**5**|**10**|**30**]

Revise the interface of the specified port.

CPRI Options are used for CPRI interfaces. The actual speeds are:

CPRI 9 (12,165.12 mbps)

CPRI 8 (10,137.6 mbps)

CPRI 7 (9,830.4 mbps)

CPRI 6 (6,144.0 mbps)

CPRI 5 (4,915.2 mbps)

CPRI 4 (3,072.0 mbps)

CPRI 3 (2,457.6 mbps)

CPRI 2 (1,228.8 mbps)

CPRI 1 (614.4 mbps)

[lanes] only applies to 10GEth and 25GEth on the primary port of an HS-3200 or HS-6400

LOSON/LOSOFF must be,followed by the number of seconds. port must be a port name if PORt is used, otherwise portname is cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev por 'Blz 1.2.4' 10GEth
rev prtn 1.2.4 10GEth LOSON 2
rev prtn 1.2.4 10GEth LOSOFF
rev prtn 1.1.1 4 25GEth

Usage: **REV**ise {**POR**t|**PRTN**um} port **AUTON**egotiate {**ENA**ble|**DIS**able}
Revise port configuration for auto-negotiation settings.
Set 'ENAble' to turn auto-negotiation on. Valid only for GIG-E ports.
NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp
NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.
Ex: rev prtn 1.2.4 autoneg enable
rev prtn 1.2.4 auton dis

Usage: **REV**ise {**POR**t|**PRTN**um} port **CONG**estion **ALA**rm {**ENA**bled|**DIS**abled}
Revise a port's congestion alarm mode.
NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp
NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.
Ex: rev prtn 1.2.4 cong ala ena
rev prtn 1.2.4 cong ala dis

Usage: **REV**ise {**POR**t|**PRTN**um} port **DES**tination **FIL**ter {**filtername**|**NONE**}
Revise the Destination Filter of the specified port.
Destination filters can permit and deny Ethernet frames that would
be transmitted from this port. There is an implicit 'permit all' if no
filter is selected and for frames that do not match any rules of a selected filter.
Selecting 'NONe' stops Destination Filtering on the port.
NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp
NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.
Ex: rev por 'Tool 1' Destination Filter 'No HTTPS'
revise prtnum 1.2.4 DES FIL 'Feed 1'
Revise Port Network1 Destination Filter NONE

Usage: **REV**ise {**POR**t|**PRTN**um} port **EXT**ernal **TRA**nsmit {**ENA**bled|**DIS**abled}
Revise a Clone port's External Transmit setting.
This command is valid only for Clone ports.
Enabling External Transmit causes traffic that is internally looped
through the Clone port to also be transmitted externally from this port.
NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp
NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.
Ex: rev por 'Clone 1' EXTERNAL TRANSMIT ENABLED
revise prtnum 1.2.4 ext tra dis

Usage: **REV**ise {**POR**t|**PRTN**um} port **FOR**ce **LIN**k **UP** {**ENA**bled|**DIS**abled}

Revise a Test port's Force Link Up setting.
This command is valid only for Test ports.
Enabling Force Link Up causes the port to come up and stay up even when
there is no signal being received from the attached device. This also
prevents any Link Down events from being reported when the attached device goes down.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev por 'Tool 1' FORCE LINK UP ENABLE
revise prtnum 1.2.4 for lin up dis

Usage: **REV**ise {**POR**t|**PRTN**um} port **HIS**torical **STATS** {**ALW**ays|**NEV**er|**CON**nected}
Revise the port's Historical Statistics configuration.
When ALWAYS is specified the port will be powered up (unless the port's
POWER configuration is set to OFF) and statistics will be collected and stored.
When NEVER is selected no historical statistics will be collected even if the
port is in a connection or collecting Real Time statistics.
When CONNECTED is selected historical statistics are collected only when the
port is in an active connection.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev por 'Tool 1' historical stats never
revise prtnum 1.2.4 HIS STATS ALW
Revise Port Network1 Historical Stats CONNECTED

Usage: **REV**ise {**POR**t|**PRTN**um} port **NANO**stamp {**ENA**ble|**DIS**able}
Revise the destination port configuration for Nanostamping.
Set to 'Enable' to add a Nanostamp.
This appends a nanosecond-level free running counter value to all packets
sent on this port. Note that the value of the counter is captured when
packets are received, and optionally added to packets when they are transmitted.
Set to 'Disable' to stop adding Nanostamps.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: revise port "Analyzer Tool" nanostamp enable
rev prtn 1.2.4 nano dis

Usage: **REV**ise {**POR**t|**PRTN**um} port **POW**er {**ON**|**OFF**|**ASN**eeded}
Revise the port's power configuration.
When ON is selected the port will be powered up always.
When OFF is selected the port will be powered down even when in an active connection.
When ASNeeded is selected the port will be powered up if it is in an active
connection, if it is collecting Real Time or Historical statistics,
or when the port is an xSL port. Otherwise the port is powered off.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev por 'Tool 1' POWER ON

revise prtnum 1.2.4 power off

Revise Port Network1 POW AsNeeded

Usage: **REV**ise {**POR**t|**PRTN**um} port **SLIC**ing {**ENA**ble|**DIS**able}

Revise the destination port configuration for Packet Slicing.

Set to 'Enable' to slice packets to 160 bytes.

This slices all packets sent on this port to 160 bytes.

Set to 'Disable' to stop slicing packets.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: revise port "Analyzer Tool" slicing enable

rev prtn 1.2.4 slic dis

Usage: **REV**ise {**POR**t|**PRTN**um} port {**RXT**hreshold|**TXT**hreshold} {**HI**gh|**LO**w} [**ARM**|**DISARM**] [event] [reset] [event_duration] [reset_duration]

Revise the port configuration threshold settings. Threshold settings enable event notifications when the traffic utilization

goes above or below a certain percent for the specified amount of time.

Receive (RxThreshold), transmit (TXThreshold), high and low thresholds are specified independently.

ARM enables the threshold configuration and DISARM disables it.

If neither ARM nor DISARM is specified then it remains unchanged.

The 'event' value is the utilization percentage at which the event is triggered.

The 'reset' value is the utilization percentage at which a previously triggered event is cleared,

allowing another event to be triggered.

For HIGH threshold settings:

- The event value must be higher than the reset value.
- The 'event_duration' is the number of seconds during which the utilization must exceed the event threshold in order for the event to trigger.
- The 'reset_duration' is the number of seconds during which the utilization must drop below the reset threshold in order for the event to clear.

For LOW threshold settings:

- The event value must be lower than the reset value.
- The 'event_duration' is the number of seconds during which the utilization must drop below the event threshold in order for the event to trigger.
- The 'reset_duration' is the number of seconds during which the utilization must exceed the reset threshold in order for the event to clear.

The numeric values: event, reset, event_duration, and reset_duration must be specified in that order,

and cannot be skipped over. In other words you cannot set the durations without also first setting the

event and reset values, but you can set the event and reset values without the durations.

Duration values default to 1 second if never set.

Each triggered event and cleared event will appear in the port alarm log.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: REVISE PORT NetworkPort1 RxTHRESHOLD HIGH ARM 85 75 10 60

rev prtn 1.2.4 TxT lo 10 25 5 3

REV Port "Team A Input" RXThreshold LOW DISARM

REV Port AnalyzerTool TxThresh HIGH ARM 95

Usage: **REV**ise {**POR**t|**PRTN**um} port **SUF**fix suffix1 suffix2

Revise port configuration for subport suffix settings.

suffix1 is suffix used on subport 1, suffix2 for subport 2.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev prtn 1.2.4 suffix Rx Tx

rev prtn 1.2.4 suf In Out

Usage: **REV**ise {**POR**t|**PRTN**um} port **TYPE** {**NOR**mal|**TES**t|**XSL**|**MIR**ror|**CLO**ne}

Revise port configuration for type.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev prtn 1.2.4 type clone

Usage: **REV**ise {**POR**t|**PRTN**um} port **VLA**ntag {**KEE**p|**ADD**|**REP**lace|**REM**ove} [**ID** value]

Revise source port configuration for VLAN settings.

Setting 'KEEp' on this, and setting 'UNTagkeep' on the destination port this port connects to, will leave the frame unchanged.

Setting 'ADD' and 'ID value' on this port, and setting 'Allow Tag' on the destination port this port connects to, will add a new VLAN Tag.

Setting 'REPlace' and 'ID value' on this port, and setting 'ALLowtag' on the destination port this port connects to will replace the outer VLAN if the original packet already has a VLAN Tag or will add a new VLAN Tag if the original packet does not have a VLAN Tag.

Setting 'REMove' on this port, and setting 'UNTagkeep' on the destination port this port connects to, will remove the outer VLAN Tag if the original packet has any.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev prtn 1.2.4 vlantag add id 104

rev prtn 1.2.4 vlantag keep

Usage: **REV**ise {**POR**t|**PRTN**um} port **VLA**ntag {**ALL**owtag|**UNT**agkeep} [**TPI**d value]

Revise destination port configuration for VLAN settings.

Set 'ALLowtag' and 'TPId value' on this port when connected source port set to 'ADD' or 'REPlace'.

Set 'UNTagkeep' on this port when connected source port set to 'KEEp' or 'REMove'.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev prtn 1.2.4 vlantag allowtag tpid 0x8100

rev prtn 1.2.4 vlantag untagkeep

Usage: **REV**ise {**POR**t|**PRTN**um} port **VLA**ntag **ID** value

Revise source port configuration for VLAN ID settings.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev prtn 1.2.4 vlantag id 104

Usage: **REV**ise {**POR**t|**PRTN**um} port **VLA**ntag **TPI**d value

Revise destination port configuration for VLAN TPID settings.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev prtn 1.2.4 vlantag tpid 0x8100

Usage: **REV**ise {**POR**t|**PRTN**um} port **VNT**ag {**ALL**owtag|UNTag}

Revise destination port configuration for VN-Tag stripping settings.

Set 'ALLowtag' to leave VN-Tag unchanged. 'ALLowtag' is valid only when the source port is on the same blade. VN-Tags are automatically stripped when the frame is sent to another board.

Set 'UNTag' to remove VN-Tag.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: rev prtn 1.2.4 vntag allow

REVISE PORT MyAnalyzer vntag untag

Usage: **REV**ise **RUL**e rulename rule

Replaces a rule?s action and conditions with a new action and conditions.

If the rule is being used in an active connection the new rule is applied to the hardware immediately.

See ADD RULE for rule syntax and available conditions

Ex: Rev rul RuleA "permit all"

REVISE RULE 'Deny IP Addresses' 'deny ip.addr==10.1.1.1 - 10.10.255.255'

Usage: **REV**ise **SWI**tch switchname **AUTODIS**crepancy {**ENA**ble|**DIS**able}

Revise switch to enable / disable the Auto Discrepancy.

Enabling Auto Discrepancy Detection on a 3900 switch will enable the system to automatically reconfigure blades when boards are removed or installed and reconfigure port interface types when installed SFPs are changed.

Ex: rev swi 1.2 MySwitch autodis ena

Usage: **REV**ise **SWI**tch switchname **BAC**kplane **CONG**estion **ALA**rm {**ENA**bled|**DIS**abled}

Revise the switch backplane congestion alarm setting. Congestion alarms are possible only when the backplane is in Aggregation Mode.

Congestion alarm events appear in the system alarm log. Only one outstanding congestion alarm will be reported between any two blades for each direction. When the outstanding alarm is acknowledged the system is then rearmed to report the next congestion event.

Ex: REVISE SWITCH Production1 BACKPLANE CONGESTION ALARM ENABLE

rev swi "Team A Switch" back cong ala dis

Usage: **REV**ise **SWI**tch switchname **BAC**kplane **MOD**e {**GUA**ranteed|**EXT**ended|**AGG**regation} [**SES**sion-based|**EQU**al-distribution]

Revise the switch backplane bandwidth mode. Valid only for PFS 3903 switches.

The backplane mode determines how traffic will cross the backplane ports from one blade to another.

GUARANTEED mode guarantees that no traffic will be dropped due to backplane oversubscription.

Total bandwidth in guaranteed mode is 120 Gb between each pair of blades in each direction.

EXTENDED mode also guarantees that no traffic will be dropped due to oversubscription and allows more

than 120Gb of bandwidth by switching resources away from front ports on an as-needed basis.

When front port resources are switch to the backplane the front port is no longer available for use.

AGGREGATION mode allows backplane oversubscription. The backplane is treated as one large 110 Gb

pipe bewtween two blades, allowing many connections to share the bandwidth. Traffic can be distributed in

Aggregation mode in either a SESSION-BASED (default) or EQUAL-DISTRIBUTION fashion. Session-based guarantees

that packets from the same session, in either direction, will be transmitted on the same port, thus keeping

the packets in order. This, however, could result in unequal utilization of backplane ports and congestion.

EQUAL_DISTRIBUTION distributes packets across the backplane more or less equally, minimizing the chance of congestion.

However, packets may get out of order with Equal-distribution.

WARNING: Changing the backplane will cause traffic to be disrupted.

Ex: REVISE SWITCH Switch1 BACKPLANE MODE GUARANTEED

rev swi Switch3 bac mod agg equal

Revise switch "Team A Switch" backplane mode extended

REV SWI TestLabSwitch BACK MODE Aggregation Session-based

Usage: **REV**ise **SWI**tch switchname **BAC**kplane **TXT**hreshold **HI**gh [**ENA**bled|**DIS**abled] [event_percent] [reset_percent]

Revise the switch configuration backplane threshold settings. The Threshold setting enables event notifications when the traffic utilization goes above or below the specified percent.

This setting is valid only when the backplane is set to Aggregation mode.

If the backplane loadbalancing type is set to Session-based then an event will be triggered if at least

one of the aggregated ports sending traffic from one blade to another goes above the threshold.

If set to Equal-distribution then an event will be triggered if the average of all ports is above

the threshold. The reset event is triggered when the traffic then goes below the reset percentage.

Once a threshold event is reported it will not be reported again until utilization drops below the reset percent.

Each triggered event and cleared event will appear in the system alarm log.

Ex: REVISE SWITCH Production1 BACKPLANE TxTHRESHOLD HIGH ENA 85 75

rev swi Switch3 bac TxT hi disable

REV SWI TestLabSwitch back TxThresh HIGH ENABLE 95

Usage: **REV**ise **SWI**tch switchname **CFP**strip {**ENA**bled|**DIS**abled}

Revise a switch's Cisco FabricPath (CFP) Stripping mode (parsing/stripping CFP headers)

CFP Stripping mode allows filtering and load balancing of the encapsulated packet in CFP frames.

When CFP Stripping is enabled, CFP headers will be detected (and parsed) on ingress and stripped on egress.

When CFP Stripping is disabled, CFP frames will pass through the system with CFP headers intact.

Ex: REVISE SWITCH MySwitch CFPSTRIP ENABLED

rev swi MySwitch cfp dis

Usage: **REV**ise **SWI**tch switchname **CONS**ole {**ENA**bled|**DIS**abled} [password]

Revise a switch's local console configuration. If the local console is enabled,

then the password must be specified.

Ex: REVISE SWITCH MySwitch CONS ena mypassword

rev swi MySwitch CONS dis

Usage: **REV**ise **SWI**tch switchname **LOA**dbalancing {**SES**ion-based|**EQU**al-distribution}

Revise a switch's loadbalancing group distribution type.

Session-based ensures that frames from the same session will be transmitted

from the same destination port in the load balancing group.

Sessions are defined as follows:

IP frames: Source and Destination IP addresses and Protocol

Non-IP frames: Source and Destination MAC addresses and EtherType

The Equal-distribution setting will cause the frames to be randomly distributed

among the ports in the load balancing group

Ex: REVISE SWITCH MySwitch LOAD SESS

rev swi "My Switch" loadbalancing equal-distribution

Usage: **REV**ise **SWI**tch switchname **LOA**dbalance {**FAILO**ver|**FAILB**ack} {**MAN**ual|**AUTO**matic **DEL**ayed seconds}

Revise a switch's loadbalancing group failover or failback mode and delay timer

in seconds. In Automatic mode valid numbers are between 0 and 86400 seconds (24 hours).

These timers determine how long the system will wait after a link down event to move

traffic from the down port(s) to other up port(s) in the load balancing group; or

how long the system will wait after a link up event to move traffic from

failed-over port(s) back to the original port(s) in the load balancing group.

In Manual mode traffic is not moved.

Ex: REVISE SWITCH MySwitch LOAD FAILO AUTO DEL 5

rev swi MySwitch loadbalance failover automatic delay 60

REVISE SWITCH MySwitch LOAD FAILO MANUAL

REVISE SWITCH MySwitch LOAD FAILB AUTO DEL 30

rev swi MySwitch loadbalance failback automatic delay 600

Revise Switch MySwitch Loadbalance FAILBACK Manual

Usage: **REV**ise **SWI**tch switchname **SBL**ade P**RO MOD**e {**NOR**mal|**UTI**lization}

Revise a switch's S-Blade Pro Mode. S-Blade Pro Mode allows S-BLADE Pro blades to operate in Normal mode or Utilization mode.

Normal Mode allows for all bridge ports to be available for connections, while Utilization Mode reserves half of the bridage ports for statistics collection

Ex: REVISE SWITCH MySwitch SBLade PRO MODe NOR

rev swi MySwitch sbl pro mod util

Usage: **REV**ise **SWI**tch switchname **SBL**ade **PRO EXT**ended **FAB**ric **MOD**e {**ENA**ble|**DIS**able}

Revise switch to enable / disable the S-Blade Pro Extended Fabric Mode (only valid for 3903).

S-Blade Pro Extended Fabric Mode uses shared resources to increase the number of connections between

standard Layer-1 ports. In order to maximize Extended Fabric Mode, it is recommended that:

1. Connections between Smart ports and Standard Layer-1 ports be kept to a minimum.
2. Port Utilization metrics are not enabled on standard Layer-1 ports.

Ex: rev swi MySwitch sbl pro ext fab mod ena

Usage: **REV**ise **SWI**tch switchname **VNT**ag **DET**ection {**ENA**bled|**DIS**abled}

Revise a switch's VN-Tag Detection mode. VN-Tag Detection mode allows filtering

and load balancing of the encapsulated IP packet of VN-Tagged frames, and optional removal of VN-Tags.

In VN-Tag Detection Mode, if the source and destination ports are on different blades the VN-Tags will always be removed. If VN-Tag Detection Mode is not enabled, VN-Tagged frames will pass through the system with VN-Tags intact.

Ex: REVISE SWITCH MySwitch VNTAG DETECTION ENABLED

rev swi MySwitch vnt det dis

Usage: **REV**ise **SWI**tch **IP** [options]

Revise a switch's IP configuration. Only IP version 4 is supported.

The switch must be previously selected using the SELect SWItch command unless using an embedded server.

At least one option must be specified, and all options may be specified in the same command.

Options can be specified in the short form (-I) or long form (--ip1) and are equivalent.

The upper case options (-I, -N, -G, -S) signify the primary settings, the lower case options signify the secondary settings

WARNING: The switch will reboot and all connections will be interrupted!

options (case sensitive):

-h [**--help**] Show options help

-I [**--ip1**] arg Switch Primary IP address

-N [**--net1**] arg Switch Primary netmask

-G [**--gate1**] arg Switch Primary gateway

-i [**--ip2**] arg Switch Secondary IP address

-n [**--net2**] arg Switch Secondary netmask

-g [**--gate2**] arg Switch Secondary gateway
-S [**--srv1**] arg Server 1 IP address
-s [**--srv2**] arg Server 2 IP address

Ex: rev swi ip -I 10.20.37.4 -N 255.255.252.0 -G 10.20.36.1
revise switch IP --srv1 0.0.0.0 --srv2 0.0.0.0
rev swi IP --ip2 10.20.37.5 -net2 255.255.252.0 -g 10.20.36.1

Usage: **RUN filename**[.EVT]

Run (execute) event file filename.EVT. The event file must contain a list of valid CLI commands, excluding RUN. Comands that support the FORCE option will be process as if FORCE was specified. **filename** can be either a regular file specification format (/directory/filename.ext) or a URL formatted specification (ftp://username:password@host:port/path). The response for each of the ASCII commands is returned to event response file **filename.RSP** in the same directory or to the same ftp server using the original username and password as the EVT file. The user must have both write and delete privilege. A RUN command completed message is issued upon completion of execution of the last command in the RUN command file.

Ex: RUN connLab.evt
run ftp://user:password@192.168.0.2/Server/connTest
ftp requires read/write/delete privileges

Usage: **SEL**ect **SWI**tch **switchname**

Select a switch that switch-specific commands will use as default on an external server, for example Add port. This command must be issued to use the PRTNUM option on a command on an external server. It is not required and will be ignored on an embedded server.

Ex: sel swi My3903
sel swi Blaze

Usage: **SHO**w **AAA**

Displays the current AAA configuration on the server.

Ex: sho aaa

Usage: **SHO**w [**POR**t|**SYS**tem] **ALA**rms [**CUR**rent|**HIS**tory] [**SEA**rch:]

Display a list of port or system alarms, either current(unacknowledged) or historical(acknowledged).

Ex: SHOw POR ALA CUR

Usage: **SHO**w **AUD**it [**TRA**il] [**CSV filename**] [**SEA**rch text]

Display the audit trail. The log contains the history of user actions that change the state of something. If the CSV option is used, then a comma separated value file is created containing the audit trail fields. The "SEArch text" option searches only the audit trail text (4th) column.

Ex: show aud tra
show aud

Usage: **SHO**w **BLA**de **UTI**lization **bladeaddress**

Show Blade utilization for S-Blade Pro

Ex: show bla util 1.2

Usage: **SHO**w **CON**nected **GRO**ups [**SEA**rch text]

Display a list of all connected groups.

Ex: SHOW CON GRO

SHOW CON GRO SEA 'BLZ 1.1.2'

Usage: **SHO**w **CON**nected **ISL**

Display a list of all connected ISL ports.

Ex: SHOW CON ISL

Usage: SHOw **CON**nected **POR**ts [**SEA**rch **text**]

Display a list of all connected ports. Only port connections established by CONNECT PORT|GROUP are displayed.

Ex: SHOW CON POR

SHOW CON POR SEA 'BLZ 1.1.2'

Usage: **SHO**w **CON**nected **TES**ts [**SEA**rch **text**]

Display a list of all connected test/tap ports.

Ex: SHOW CON TES

SHOW CON TEST SEA 'BLZ 1.1.2'

Usage: **SHO**w {**CON**nection|**RAWCON**} [**DET**ails] {**SWI**tch|**POR**t|**PRTN**um|**GRO**up|*} [**param**] [**PAGE**] [**number**]

Display a summary or details for connected ports and/or groups on a particular switch or on a server.

The number of connections per display page can optionally be specified.

RAWCON is used with scripting

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: sho conn *

show conn SWI MySwitch

show conn details POR PortA

show conn * PAGE 20

Usage: **SHO**w **DEST**ination **GRO**ups [SEArch **text**]

Display a list of all defined Destination Groups and the number of members in each.

Ex: SHOW DEST GRO "load bal 1"

Usage: **SHO**w **FIL**ters [**SEA**rch **text**]

Display a list of all defined filters and the number of rules in each.

Ex: show filter search FilterA

Usage: **SHO**w **GEN**erators [**SEA**rch **text**]

Display a list of all defined Stream Generators and the topologies they are associated with.

Ex: show gen search StreamGeneratorA

show gen

Usage: **SHO**w **GRO**ups [**SEA**rch **text**]

Display a list of all defined Connection Groups and the number of members in each.

Ex: show gro GrpA

Usage: **SHO**w [**GRO**up|**FIL**ter|**TOP**ology|**SCA**nner|**STR**eam|**GEN**erator] **MEM**bers **name**

Display a list of ports contained in a Connection Group, Source Group, Destination Group, or Port Scanner,

rules in a filter, packet definitions in a stream, stream in a generator, or members of a topology.

NOTE: SCAnner only valid for TestStream Lab Manager.

Ex: SHOW gro Mem GrpA

sho fil Mem 'VOIP Filter'

sho sca Mem ScannerA

show topology Mem 'CLI Topology'

Usage: **SHO**w [**GRO**up|FILter|**TOP**ology|**SCA**nner|**STR**eam|**GEN**erator] **MEM**bers **name**

Display a list of ports contained in a Connection Group, Source Group, Destination Group, or Port Scanner,

rules in a filter, packet definitions in a stream, stream in a generator, or members of a topology.

NOTE: SCAnner only valid for TestStream Lab Manager.

Ex: SHOW gro Mem GrpA

sho fil Mem 'VOIP Filter'

sho sca Mem ScannerA

show topology Mem 'CLI Topology'

Usage: **SHO**w **IMP**airments [**SEA**rch **text]**

Display a list of all defined impairments.

Ex: show imp search ImpairmentA

Usage: **SHO**w **INF**ormation {**GRO**up|**POR**t|**PRTN**um|**SWI**tch|**FIL**ter|**IMP**airment} name

Display detailed information of the specified Connection/Source/Destination Group, port, switch, filter, or Impairment.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: SHOW info port 'LAB 1.1.1'

show info prtn 1.1.1

Usage: **SHO**w **LIC**ense

Displays installed license feature.

Ex: sho lic

Usage: **SHO**w **LOC**ked **POR**ts [**SWI**tch] [name]

Show locked ports. Displays a list of all locked ports or if switch is specified then all locked ports on the specified switch.

Ex: show lock port

show lock port LabSwitch

sho loc por swi LabSwitch

Usage: **SHO**w **PAC**ket **DEF**inition [**SEA**rch **text**]

Display a list of all defined Packet Definitions

Ex: show pac def PacketDefA

show pac

Usage: **SHO**w **PATH** {**POR**t|**PRTN**um} port

Show connection path for the specified port.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: SHO PATH PRTN 1.1.1

SHO PATH POR PortA

Usage: **SHO**w **POR**ts [**SEA**rch **text**]

Display a list of defined ports

Ex: SHOW Ports

Usage: **SHO**w **POR**ts **WIT**h [options]

Display a list of defined ports with a matching configuration.

Port names can use the wildcard symbols asterisk (*) and question mark (?).

* will match any number of characters.

? will match any single character.

For example:

--name Tool* (will match any name starting with 'Tool')

--name Network? (will match any name starting with 'Network'
and followed by a single character,
such as Network1, Network2, NetworkA, etc.)

NOTE: Surround names containing spaces with double quotes ("name").

options (case sensitive):

-h [**--help**] Show options help

--dstfilter arg Destination Filter name

--name arg Port name

--verbose Verbose output

Ex: SHOW Ports with --dstfilter "Drop HTTPS Filter"

SHO POR WIT --dstfilter "Only VOIP Filter"

SHOW PORTS WITH --name Tool*

sho por wit --name Network?

SHOw PORts WITH --name Tool* --dstfilter "Drop HTTPS" --verbose

Usage: **SHO**w {**POR**t|**PRTN**um|**GRO**up|**FIL**ter|**IMP**airent|**DEVICEP**ort} name **TOP**ologies

Display the Topologies where the specified object is used.

NOTE: DEVICEPort is only valid for TestStream Lab Manager.

Ex: SHOW GROUP 'Source 2' TOP

SHOW PRTNUM 01.01.01 TOP

SHOW IMP myimp TOP

Usage: **SHO**w {PORt|**PRTN**um} [**INFO**|**RAWINFO**] {*|portname} [**SWI**tch] [switchname] [**PAGE**] [number]

Displays port configuration, connection and SFP diagnostic status for specified port

or for all ports on a switch or for all ports on a server.

RAWINFO is used with scripting.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: show port info 'PL 01.01.01'

show port info *

sho port *

show port info * SWI MySwitch

show prtn info 1.1.2

show prtn 1.1.3

Usage: **SHO**w **REM**ote **ACC**ess

Displays the current remote access configuration on the server.

Ex: sho rem acc

Usage: **SHO**w **RUL**es [**SEA**rch **text**]

Display a list of all defined rules.

Ex: Show Rules

SHO RUL search VOIP

Usage: **SHO**w **SERV**ers [**DET**ails]

Show the online and standby server IP addresses and their status.

Ex: SHOW SERVERS

sho serv det

Usage: **SHO**w SFM **CON**nections name

Displays a list of connections on the specified SFM.

This command is only available for 3912 switches.

Name is cc.ii where 'cc' is the chassis number and 'ii' is the SFM ID (1-8)

corresponding to the slot number (13-20).

Name is only valid on an embedded server unless Select Switch command has been issued.

Ex: SHOw SFM CONnections 1.2

Usage: **SHO**w **SNMP**

Display current SNMP conf.

Ex: show snmp

Usage: **SHO**w **SOU**rce **GRO**ups [**SEA**rch **text**]

Display a list of all defined Source Groups and the number of members in each.

Ex: show sou gro SG1

Usage: **SHO**w **STATS PCE** {**POR**t|**PRTN**um} portname

Display the real time statistics counters on the specified PCE port.

The PCE port must have been previously started.

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: show stats pce port dedup1

Usage: **SHO**w **STATS** {**POR**t|**PRTN**um} [*|name[,name...]]

Display the real time statistics counters on the specified port(s) or subport(s).

The port(s) or subport(s) must have been previously started.

The wildcard (*) shows all stats that have been previously started.

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: show stats port SpanA

SHOW STATS prtnum "1.1.1, 1.1.2.1, 1.1.3.2"

sho stats port SpanBTx

show stats port *

Usage: **SHO**w **STAT**us

Display current alarm counts and code version.

Ex: SHOW STAT

Usage: **SHO**w **STR**eams [**SEA**rch **text]**

Display a list of all defined Streams and the number of members in each.

Ex: show str search StreamA

show str

Usage: **SHO**w **SWI**tch **FAB**ric **STAT**us switchname [bladeaddress]

Retrieves the number of currently available 1G, 10G and 40G connections between blades on the specified switch. If the optional **bladeaddress** is specified then only the connections on that blade are shown. Blade addresses are specified as chassis and slot cc.ss.

In the response numeric values show the number of connections still available, blanks indicate 0 connections available. Dashes mean N/A.

Ex: Show swi fab stat Switch1

SHOW SWITCH FABRIC STATUS Switch1 1.2

Usage: **SHO**w **SWI**tch **IP**

Show the switch's IP configuration.

The switch must be previously selected using the SELect SWItch command unless using an embedded server.

Ex: SHO SWI IP

show switch ip

Usage: **SHO**w **SWI**tches

Show a list of names for all defined switches

Ex: SHOW SWI

Usage: **SHO**w **SWI**tch {*|switch_name}

Show a list of the defined switches and each switch's model, IP address, discovery selection, link propagation,

and current status.

Ex: SHOW SWI *

sho swi myswitch

Usage: **SHO**w **TES**t [**POR**ts] [**SEA**rch **text**]

Display a list of the defined tap/test ports.

Ex: Show Tes

Usage: **SHO**w **TOP**ologies [**SEA**rch **text**] [**ALL**]

Display a list of public and user's private topologies and the number of members in each.

Administrator privileges only: ALL lists private topologies for all users.

Ex: SHOW TOP

SHOW TOPOLOGIES SEARCH 'Security Team Topology'

Usage: **SHO**w **USER** [**STAT**ic|**LOCK**ed]

Show all active users if the optional parameter is not used.

If the STATIC parameter is used then command shows a list of all defined users.

If the LOCKED parameter is used then command shows a list of all defined users

and whether the accounts are locked or not.

Usage: **SHUT**down {**SWI**tch|**BLA**de|**SFM**} [**REBO**ot|**REST**art] name [**FORCE**]

Shutdown the specified switch or blade.

For SWITCH, 'name' must be a switch name.

For BLAde, 'name' is cc.ss where 'cc' is the chassis number and 'ss' is the slot number.

For SFM, 'name' is cc.ii where 'cc' is the chassis number and 'ii' is the SFM ID (1-8)

corresponding to the slot number (13-20).

NOTE: REBOot and RESTart options are only available for BLAde or SFM.

BLAde and SFM are only valid on an embedded server unless Select Switch command has been issued.

SFM is only valid for 3912 switches.

Ex: SHUTdown SWI switchA

SEL SWI myswitch

SHUTdown BLAde REBOot 1.2

SHUTdown BLAde RESTart 1.3

SHUTdown SFM RESTart 1.5

Usage: **STA**rt **STATS PCE** {**POR**t|**PRTN**um} portname

Start real time statistics collection on the specified PCE port.

Ex: STA STATS pce prtnum 01.01.PCE1

Usage: **STA**rt **STATS** {**POR**t|**PRTN**um} name[,name...]

Start real time statistics collection on the specified port(s) or subport(s).

Ex: STA STATS prtnum "1.1.1, 1.1.2.1, 1.1.3.2"

sta stats port SpanA

start stats port SpanBRx

Usage: **STO**p **STATS PCE** {**POR**t|**PRTN**um} portname

Stop real time statistics collection on the specified PCE port.

The PCE port must have been previously started.

Ex: sto stats pce port dedup1

Usage: **STO**p **STATS** {**POR**t|**PRTN**um} [*|name[,name...]]

Stop real time statistics collection on the specified port(s) or subport(s).

The port(s) or subport(s) must have been previously started.

The wildcard (*) stops collecting all stats that have been previously started.

Ex: sto stats port SpanA

STOP STATS prtnum "1.1.1, 1.1.2.1, 1.1.3.2"

stop stats port SpanBTx

stop stats port *

Usage: **TERM**inate [**SESS**ion] id

Terminate session

id = session id from SHOW USER

Ex: TERM SESSION 3

Usage: **UNL**ock [**SIM**plex] {**POR**t|**PRTN**um} name

Unlock a duplex or simplex port. Only the user that locked the port or an Administrator can unlock a port.

name must be a duplex or simplex port name if PORt is used, otherwise it is cc.ss.pp or cc.ss.pp.dd.

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: unlock PORT 'PL 1.1.2'

unlock PRNT 1.1.2

unlock SIM PRTN 1.1.2.1

unl sim port 'PL 1.1.2.Tx'

Usage: **UNS**elect **SWI**tch

Unselect a switch which applies SNMP Agent conf globally in all switches on an external server

Ex: uns swi

Standard Commands - TestStream Lab Manager Only

=> help

Usage: **ACT**ivate **SCA**nner **name**

Activates a port scanner.

Ex: Activate scanner ScannerA

act sca 'Scanner ABC'

Usage: **ADD DEV**ice devicename [**numports**]

Add a new Device.

Specify number ports the device will have (1-256). The default is zero.

Ex: Add DEVice DeviceA 6

Add dev 'Device ABC'

Usage: **ADD DEV**ice **POR**ts devicename numports

Add Device Ports to a device.

Ex: Add DEVice PORts DeviceA 6

Add dev por 'Device ABC' 12

Usage: **ADD RES**ervation topologyname MM/DD/YYYY-HH:MM MM/DD/YYYY-HH:MM [**ACT**]

Add a reservation to a topology. Specify start date/time(UTC) followed by end date/time(UTC)

Optionally specify if reservation should activate topology upon start

Ex: ADD RES 'TOPOLOGY ABC' 10/30/2011-5:30 10/30/2011-6:30 ACT

Usage: **ADD TO SCA**nner scannername {**POR**t|**PRTN**um} portname [**position**]

Add a port to a scanner. The position starts at 1 and if not

specified the port will be added to the end of the scanner.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: Add to Scanner ScannerA port 'BLZ 1.2.4'

ADD to scanner ScannerA prtn 1.2.4

Usage: **CONF**igure **DEV**ice **POR**t name {**1GFib**|**2GFib**|**4GFib**|**8GFib**|**16GFib**|**GIG-E**|**CU-GIG-E**|**OC-3/stm-1**|**OC-12/stm-4**|**OC-48/stm-16**|**OC-192/stm-64**|**OPT**ical|**10GEth**|**25GEth**|**40GEth**|**50GEth**|**100GEth**|**100MFib**|**CU10000**|**CPRI9**|**CPR18**|**CPR17**|**CPRI16**|**CPRI5**|**CPRI4**|**CPRI3**|**CPRI12**|**CPRI1**|**SAS3G/6G/12G**|**OTU1**|**OTU2**|**OTU2E**|**Generic**}

Configure a device ports interface.

Ex: CONFIG DEV POR DevicePort-1 10GEth

Usage: **CONF**igure **DEV**ice **TOP**ologies **RES**ervation **REQ**uired {**ENA**bled|**DIS**abled}

Enable will require Device Topologies to be reserved before they can be activated.

Disable wiil allow Device Topologies to be activated without needing a reservation.

Ex: CONFIG DEV TOP RES REQ ENA

Usage: **CONF**igure **REM**ote **SER**ver 'server name' 'ip address' {**TEL**net|**SSH**} PortNumber 'username' 'password' {**GLO**bal|**PRI**vate}

Configure a Remote Server.

'server name' is the name of the new Remote Server

'ip address' is the IPV4 address of the new Remote Server.

PortNumber is the TCP port number to use for 'TELnet' or 'SSH'.

'username' is the User Name to login to the Remote Server.

'password' is the password of the Remote Server.

GLOBAL : Accessible to all users.

PRIVATE : Only accessible to creator.

Ex: CONFIG REMOTE SERVER 'MyRemoteServer' '192.168.0.1' TELNET 22 'admin' 'mypassword' GLOBAL

Usage: **CON**Figure **REP** 'profile name' 'remote server' 'execution command' 'description'

Configure a Remote Execution Profile (REP).

'profile name' is the name of the new Remote Execution Profile

'remote server' is the name of a defined Remote Server.

'execution command' is the command to execute on the Remote Server.

'description' is an optional description of the new REP.

Ex: CONFIG REP 'MyREP' 'MyRemoteServer' '/home/myname/MyScript.py' 'This is my new REP'

Usage: **CONF**igure **RRE NAME** profilename *OFFSET* offset

Configure a Reservation Remote Execution (RRE) profile.

'profilename' is the name of the new RRE profile

'offset' is the deactivation execution offset (minutes).

Ex: CONFIG RRE NAME 'MyRRE' OFFSET 60

Usage: **DEA**ctivate **SCA**nner name

Deactivate a port scanner.

Ex: deactivate sca ScannerA

dea sca 'SCANNER ABC'

Usage: **DEL**ete **DEV**ice name

Delete an existing device.

Ex: DEL DEVice DeviceA

delete dev 'Device ABC'

Usage: **DEL**ete **DEV**ice **POR**t name

Delete an existing device port.

Ex: DEL DEVice port DevicePortA

delete dev por 'Device Port ABC'

Usage: **DEL**ete **RRE NAME** profilename

Delete a Reservation Remote Execution (RRE) profile.

'profilename' is the name of the RRE profile to delete

Ex: DEL RRE NAME 'MyRRE'

Usage: **DEL**ete {**POR**t|**PRTN**um} portname **FRO**m **SCA**nner scannername

Delete a port from a scanner by name.

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: DELETE PORT 'Port A' from SCAnner ScannerA

del por portA from sca "Scanner A"

del prtn 1.1.17 from sca Scanner1

Usage: **DEL**ete **REM**ote **SER**ver 'server name'

Delete a Remote Server.

'remote server name' is the name of the Remote Server to delete

Ex: DELETE REM SER 'MySrv'

Usage: **DEL**ete **REP** 'profile name'

Delete a Remote Execution Profile (REP).

'profile name' is the name of the Remote Execution Profile to delete

Ex: DELETE REP 'MyREP'

Usage: **DEL**ete **RES**ervation topologyname MM/DD/YYYY-HH:MM

Delete a reservation. Specify topology name and start date/time(UTC)

Ex: DEL RES 'TOPOLOGY ABC' 10/30/2011-5:30

Usage: **EXP**ort **RES**ervation **REP**ort **FRO**m MM/DD/YYYY-HH:MM TO MM/DD/YYYY-HH:MM filename

Export a reservation report to a csv file.

Filename can be either a regular filespec format (d:/directory/filename)

or a URL formatted specification(".csv" is automatically appended to the filename specified.)

Ex: EXPORT RES REP FROm 03/04/2017-12:00 TO 03/08/2017-12:00 c:\ResReport

exp res rep FROm 03/04/2017-12:00 TO 03/08/2017-12:00 ftp://admin:password@10.88.55.44/OnPATH/myreport

Usage: **FIND RES**ervation topologyname duration {M|H|D} [MM/DD/YYYY MM/DD/YYYY] [hh:mm hh:mm] [day day]

Find an available time when the topology can be reserved (all resources available) within specified parameters

duration {M|H|D} - length of time of the reservation. It can be specified in {M}inutes, {H}ours or {D}ays

A {D}ay is as long as a workday if [hh:mm hh:mm] is specified, else it is 24 hours

Optionally specify search parameters

[MM/DD/YYYY MM/DD/YYYY] - Optional. Calendar Window - Specifies start and end dates to look for an available window

If not specified, the search starts now till a reservation time is found.

[hh:mm hh:mm] - Optional. Workday - Specifies start and end of a work day in 24 hour notation (UTC)

If not specified, the default is a work day that starts at 00:00 and ends at 23:59

[day day] - Optional. Work week - Specifies start and end of the work week. 'day' is one of: SUN, MON, TUE, WED, THR, FRI, SAT

If not specified, the default is a work week of SUN to SAT.

If a single day is requested, it must be specified as 'day day', for example: 'mon mon' or 'wed wed'

There can be no skipped optional parameters. The following are all valid

Ex: FINd RES 'TOPOLOGY ABC' 2 D 10/30/2021 11/07/2021 08:00 05:00 MON FRI

Ex: FINd RES 'TOPOLOGY ABC' 1 H 08/14/2021 08/14/2021 12:00 16:00

Ex: FINd RES 'TOPOLOGY ABC' 30 M 04/02/2021 04/08/2021

Ex: FINd RES 'TOPOLOGY ABC' 1 D

Usage: **LOCK SCA**nner name MM/DD/YYYY-HH:MM [**comment]**

Lock port scanner until date/time specified. If comment contains spaces, then it must be enclosed in single or double quotes.

Ex: LOCK SCANNER 'SCANNER ABC' 10/30/2011-5:30

Usage: **MAP** [**SUBP**ort] [**POR**t|**PRTN**um] portname **TO** deviceportname

Map a port or subport to a Device Port

NOTE: If PORt is used specify the port name, if PRTNum is used specify the port number as cc.ss.pp

NOTE: PRTNUM is only valid on an embedded server unless the Select Switch command has been issued.

Ex: Map port 'BLZ 1.2.4' to DevicePortA

map prtn 1.2.4 to DevicePortA

map subport 'Blz 1.2.4.Tx' to DevicePortA

MAP subport prtn 1.2.4.2 to 'DevicePort ABC'

Usage: REMove DEVice PORt name

Remove an existing device port from a device.

Ex: REM DEVice port DevicePortA

remove dev por 'Device Port ABC'

Usage: **REN**ame **DEV**ice devicename newdevicename

Rename the specified device.

Ex: ren dev 'DEVICE AB' 'DEVICE CD'

Usage: **REN**ame **DEV**ice **POR**t deviceportname newdeviceportname

Rename the specified device port.

Ex: ren dev 'DEVICE PORT AB' 'DEVICE PORT CD'

Usage: **REN**ame **SCA**nner scannername newscannername

Rename the specified port scanner.

Ex: ren sca 'SCANNER AB' 'SCANNER CD'

Usage: **REV**ise **REM**ote **SER**ver 'current server name' 'new server name' 'ip address' {**TEL**net|**SSH**} PortNumber 'username' 'password' {**GLO**bal|**PRI**vate}

Revise a Remote Server.

'current server name' is the name of the existing Remote Server

'new server name' is the new name for this Remote Server

'ip address' is the new IPV4 address of the Remote Server.

PortNumber is the new TCP port number to use for 'TELnet' or 'SSH'.

'username' is the new User Name to login to the Remote Server.

'password' is the new password of the Remote Server.

GLOBAL : Accessible to all users.

PRIVATE : Only accessible to creator.

Ex: REVISE REMOTE SERVER 'MyRemoteServer' 'NewRemSrvName' '192.168.0.1' TELNET 22 'admin' 'mypassword' GLOBAL

Usage: **REV**ise **REP** 'profile name' 'new profile name' 'remote server' 'execution command' 'description'

Revise a Remote Execution Profile (REP).

'profile name' is the name of the existing Remote Execution Profile

'new profile name' is the new name of the REP.

'remote server' is the name of a defined Remote Server.

'execution command' is the command to execute on the Remote Server.

'description' is an optional description of the REP.

Ex: REVISE REP 'MyREP' 'MyNewREP' 'MyRemoteServerNew' '/home/myname/MyScript.py' 'This is my new REP'

Usage: **REV**ise **RES**ervation topologyname MM/DD/YYYY-HH:MM [ACT] [remoteexecutionname]

Revise a reservation to a topology specified by the start date/time(UTC).

Optionally specify if reservation should activate topology upon start and

Whether to use remote execution.

Ex: REV RES 'TOPOLOGY ABC' 10/30/2011-5:30 10/30/2011-6:30 ACT ?test10-automation?

Usage: **REV**ise **RES**ervation **TIM**e topologyname MM/DD/YYYY-HH:MM to MM/DD/YYYY-HH:MM MM/DD/YYYY-HH:MM

Revise a reservation time to a topology specified by the start date/time(UTC)

to a new start date/time(UTC) followed by a new end date/time(UTC).

The new start date/time or end date/time may be the same as the original.

To extend an active reservation, the new start date/time must match the original start date/time.

If the requested time change can be made, the command returns success and the reservation will use the new date/time.

If the requested time change can?t be made, the command returns failure, a list of resources that were

not available and the reservation time is kept unchanged.

Ex: REV RES TIM 'TOPOLOGY ABC' 10/30/2011-5:30 to 10/30/2011-5:30 11/05/2011-6:30

Usage: **REV**ise **RRE NAME** profilename {**RREN**ame|**STA**rt|**POS**t|**PRE**|**END**} newname {**OFF**set|**TIM**eout} value **PARMS** commandparms

Revise a Reservation Remote Execution (RRE) profile.

'profilename' is the name of the RRE profile to revise

'newname' is the new name of the RRE profile or a change to one of the 4 Remote Execution (RE) profiles

RREName Change the RRE Name and deactivation execution offset.

STArt Change the Reservation Start profile name, command arguments and timeout.

POSt Change the Post-Activation RE profile name, command arguments and timeout.

PRE Change the Pre-Deactivation RE profile name, command arguments and timeout.

END Change the Reservation End RE profile name, command arguments and timeout.

'value' is the new RRE deactivation execution offset, or the new timeout for the specified RE profile.

'comandparms' is the new string to append when calling the specified RE profile (not used for RREName).

Ex: REV RRE NAME 'MyRRE' RREName 'NewRRE' OFFSET 10

REVISE RRE NAME 'MyRREprofile' POST 'MyPostProfile' TIMEOUT 60 PARMS '+X -D +h'

Usage: **REV**ise **SCA**nner scannername **ROV**ing **INT**erval seconds

Revise port scanner roving interval (30-300 secs).

Ex: rev sca ScannerA rov int 60

Usage: **SHO**w **DEV**ices [**SEA**rch **text**]

Display a list of all defined Devices and the number of members in each.

Ex: show dev search DeviceA

show dev

Usage: **SHO**w **DEV**ice **POR**ts [**SEA**rch **text**]

Display a list of defined device ports

Ex: SHOW DEV PORts

Usage: **SHO**w **DEV**ice **TOP**ologies **RES**ervation **REQ**uired

Displays the current device topologies setting on the server.

Ex: sho dev top res req

Usage: **SHO**w **REP** [**SEA**rch string]

Display a list of all defined remote execution profiles.

Ex: Show REP

SHO REP search 'MyRemoteExecProfile'

Usage: **SHO**w **REP MAT**ch repname

Display only the remote execution profile named 'repname'.

Ex: Show REP MAT 'MyRemoteExecProfile'

Usage: **SHO**w **REM**ote **SER**ver [**SEA**rch string]

Display a list of all defined remote servers.

Ex: SHOw REM SER

show remote server search 'MyRemoteServer'

Usage: **SHO**w **REM**ote **SER**ver **MAT**ch rsname

Display only the remote server named 'rsname'.

Ex: show remote server match 'MyRemoteServer'

Usage: **SHO**w **RES**ervation [**SEA**rch topology] [MM/DD/YYYY-HH:MM] [MM/DD/YYYY-HH:MM]

Display a list of all scheduled reservations.

Ex: Show RES

SHO RES search TopologyA

SHO RES search TopologyA 04/03/2021-10:00

SHO RES search TopologyA 04/03/2021-10:00 05/03/2021-10:00

Usage: **SHO**w **RRE** [**SEA**rch string]

Display a list of all defined reservation remote executions.

Ex: Show RRE

SHO RRE search 'MyRemoteScript'

Usage: **SHO**w **RRE MAT**ch rrename

Display only the reservation remote execution named 'rrename'.

Ex: SHO RRE match 'MyRemoteScript'

Usage: **SHO**w **SCA**nners [**SEA**rch **text**]

Display a list of all defined Scanners and the number of members in each.

Ex: show sca search ScannerA

show sca

Usage: **UNL**ock **SCA**nner name

Unlock a port scanner. Only the user that locked the port scanner or an Administrator can unlock a port scanner.

Ex: unlock SCANNER 'SCANNER ABC'

unlock sca ScannerA

Usage: **UNM**ap **DEV**ice **POR**t name

Unmap an existing device port.

Ex: UNM DEVice PORt DevicePortA

unmap dev por 'Device Port ABC'

Appendix B
Restoring the TestStream Management Server

The external Teststream Management Server is delivered with the Teststream Management software pre-installed on the following hardened operating systems:

- CentOS-7.8 Linux for Dell R720, R730, R740, and R320 platforms

The Teststream Management Server ships to new customers with the software and license fully installed. New customers do not need to install either the software or the license.

Your Teststream Management package contains the following media to be used only in the event that reinstalling the software and/or operating system is required:

- Teststream Management Server Restore DVD (dependent on platform):
  - CentOS-6.6 Linux for Dell R720, R730, R740, and R320 platforms - includes Teststream Management

Set aside the Restore DVD for possible future use. If you need to reinstall the Teststream Management software and/or operating system, contact NETSCOUT Customer Support (refer to Contacting NETSCOUT Customer Support on page 1-2) prior to performing a system restore on your Teststream Management Server.

Before You Begin

Restoring the Teststream Management Server is a two-step process:

- Re-image the system drive(s) with operating system software.
- Reinstall the Teststream Management Server application.

Be sure to use the correct Restore DVD for your server.

Before attempting to restore the server, record the following system information:

IP Address:	
Netmask:	
Default Gateway:	
Hostname:	
Domain name:	
Name Server(s):	

Teststream Management Database Backup

The restore process will completely reformat the hard drive. If possible, from Teststream Management, perform a backup of the connectivity database to an external storage location - not to the Teststream Management Server hard drive (refer to Backup on page 4-21 or the BACKup CLI command on page A-36).

Restore the Linux OS

1. Place the Restore DVD in the DVD drive tray.
2. Reboot the system:

   # reboot
3. Make sure the system boots from the DVD. Use the F2 Setup Menu or the F11 Boot Menu to change or select the boot order.
4. When the Operating System installation is complete, reboot the system (when prompted).
5. When the DVD tray opens, remove the DVD.

Installing the Teststream Management Application

1. Log in using the default login information:

   Login**: root**

   Password**: r00tme**
2. Set the system and hwclock:

   date mmddhhmmyyyy

   hwclock --systohc
3. Type the following:

   cd /opt/install

   To install Teststream Manager, type: **./tsinstall.plx**
4. After TestStream installs, you will be forced to change the Server passwords on the next login.

Setting Network Configuration

1. Type the following:

   cd /opt/install

   ./TO_ServerConfig.plx
2. Enter a valid IP address.
3. Enter a valid netmask.
4. Enter a valid gateway.
5. Enter a simple hostname.
6. Enter a domain name.
7. Enter the IP address of a nameserver.
8. Enter another nameserver? (y/n)
9. Continue (y/n)
10. Configuring TestStream Server Please Wait...
11. Do you want to reboot now? (y/n)
12. If you did not choose the 'reboot now' option, then you must manually reboot for the changes to take effect.

    Reboot system; **# reboot**

Teststream Management Database Restore

From Teststream Management, restore the Teststream Management database with the backup file previously created (refer to Restore on page 4-21 or the RESTORE Backup CLI command on page A-47).

Note: NTP Server information should be set from the Teststream Management GUI.

Appendix C
TestStream Restful API

NetScout TestStream Rest API

TestStream 5.3.0 Rest API users must start a session before issuing any request with the exception for these two requests:

GET /api/teststream/v1/session/commands

POST /api/teststream/v1/session/commands/login

For the other requests the user must provide a Bearer Authorization header with the token returned in the 'login' request.

In order to avoid errors, please avoid using the following special characters in the name of objects: '/', '?', '#'.

The content type used in requests and responses is JSON.

Note: Rest API is not supported when the TestStream Management Server runs in an S-Blade (embedded server).

Sessions

Supported commands

The following URL is used to obtain a list of supported commands for session handling.

GET /api/teststream/v1/session/commands

No authorization header is required. When successful, it returns a status of **200** and a JSON structure with the supported commands.

Example:

```
GET /api/teststream/v1/session/commands
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 20:00:15 GMT
Server: Apache
Content-Length: 341
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
   "login": {
        "parameters": {},
        "purpose": "open a session using basic authorization (username and password). If successful,
it returns token to use in subsequent request using the bearer authentication"
```

```
    },
    "logout": {
        "parameters": {},
        "purpose": "close a session. Session is identified in token delivered in the bearer
authentication header"
    }
}
```

Logging In

Log in requests must provide a Basic Authorization header. If the authorization succeeds, a status of **200** is returned and the response body returns a token to be used in subsequent request as part of the Bearer Authentication header.

POST /api/teststream/v1/session/commands/login

> **Note:** When the user logs in for the first time after being added or after a password reset, the login command for sessions will fail, returning an error message that will prompt the user to use the CLI or GUI to update the password.

Example:

```
POST /api/teststream/v1/session/commands/login
Authorization: Basic YWRtaW5pc3RyYXRvcjpuZXRzY291dDE=
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 20:17:55 GMT
Server: Apache
Content-Length: 202
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJkMmFkYmY4Ny05OWY3LTQ5OWEtYWU4My1h
MWY4YzJjZDc0M2QiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.loo0ojlxtyZx5CfL2hwIviOre3VoS0DjX
VCkK4v_e-8"
}
```

Logging Out

Log out requests terminate the session. If successful, it returns a status of **200** and the token will not be valid anymore.

POST /api/teststream/v1/session/commands/logout

Example:

```
POST /api/teststream/v1/session/commands/logout
```

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJkMmFkYmY4Ny05OWY3LTQ5OWEtYWU4My1hM
WY4YzJjZDc0M2QiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.loo0ojlxtyZx5CfL2hwIviOre3VoS0DjXV
CkK4v_e-8
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 21:13:06 GMT
Server: Apache
Content-Length: 31
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "User logged out!"
}
```

Get Session Parameters

The following URL is used to obtain the session's parameters. If successful, a status of 200 is returned.

GET /api/teststream/v1/session

Example:

```
GET /api/teststream/v1/session HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI3NTQ0NTNiMS1lNGJjLTRjNGItYjBhYi1hN
zg4NjhkYTYzNTUiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.eZgluFTEDhMpjgBJGRWWitrDhJxmZSntMu
bVHf2OIVM
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Postman-Token: 89a2efb1-a73b-4614-86fb-dbc2c4fe6f51
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Fri, 25 Mar 2022 14:18:22 GMT
Server: Apache
Content-Length: 19
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: application/json

{"timezone":"UTC"}
```

Update Session Parameters

The URL below is used to update the session's parameters. The request body must include a JSON object with members as specified in the table below. If the request is successful a status of **200** is returned. If any of the requested parameters are invalid, a status of **400** is returned.

Table C-1 Groups by Group Type

Member Name	Optional	Type	Default Value	Description
timezone	No	string		Time zone to use for the current session. Updating the time zone will affect future commands that use dates and time of day. Supported values follow the IANA time zone database version 2022.a.

PUT /api/teststream/v1/session

Example:

```
PUT /api/teststream/v1/session HTTP/1.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI3NTQ0NTNiMS1lNGJjLTRjNGItYjBhYi1hN
zg4NjhkYTYzNTUiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.eZgluFTEDhMpjgBJGRWWitrDhJxmZSntMu
bVHf2OIVM
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Postman-Token: 8b0819f9-1d4c-409d-8170-2a426ae60e9e
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 41

{
"timezone" : "America/New_York"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Fri, 25 Mar 2022 15:49:21 GMT
Server: Apache
Content-Length: 61
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Successful. Timezone set to 'America/New_York'"}

PUT /api/teststream/v1/session HTTP/1.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI3NTQ0NTNiMS1lNGJjLTRjNGItYjBhYi1hN
zg4NjhkYTYzNTUiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.eZgluFTEDhMpjgBJGRWWitrDhJxmZSntMu
bVHf2OIVM
User-Agent: PostmanRuntime/7.29.0
Accept: */*
```

```
Postman-Token: 56c27e2a-2c68-45a8-8b0e-ada6350b306a
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 42

{
"timezone" : "America/Palo_Alto"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400 BAD REQUEST
Date: Fri, 25 Mar 2022 15:50:35 GMT
Server: Apache
Content-Length: 130
Connection: close
Content-Type: application/json

{"message":" Failed to set session parameters!. Error type [API Failure!], error string
[Unknown timezone 'America/Palo_Alto']"}
```

Groups

List of Defined Groups by Group Type

The URL below is used to obtain a collection of groups of the specified type. It supports a query parameter as shown in the table below. If the request is successful, a list of groups matching the request criteria is returned with a status of **200**. If the requested query parameter is invalid, a status of **400** is returned.

Table C-2 Groups by Group Type

Optional Query Parameter	Values	Default Value (if not present)
type	["source", "destination", "connection"]	"connection"

GET /api/teststream/v1/groups

Examples:

```
GET /api/teststream/v1/groups?type=foo
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400
status: 400
Date: Wed, 29 May 2019 21:20:02 GMT
Server: Apache
```

```
Content-Length: 33
Connection: close
Content-Type: application/json
{
    "message": "Invalid group type"
}

GET /api/teststream/v1/groups?type=source
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 21:21:18 GMT
Server: Apache
Content-Length: 53
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "group type": "source",
    "groups": [],
    "groups count": 0
}

GET /api/teststream/v1/groups?type=connection
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 21:22:37 GMT
Server: Apache
Content-Length: 100
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "group type": "connection",
```

```
    "groups": [
        {
            "group name": "ConnGrp1",
            "members count": 0
        }
    ],
    "groups count": 1
}
```


```
GET /api/teststream/v1/groups?type=source
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 21:50:23 GMT
Server: Apache
Content-Length: 95
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
```

```
{
    "group type": "source",
    "groups": [
        {
            "group name": "SrcGrp1",
            "members count": 6
        }
    ],
    "groups count": 1
```


List of Group Members

The following URL is used to obtain the group members of the specified group (replace <group_name> with the desired group name). If the group does not exist, a status of **400** is returned. Otherwise, it returns a status of **200** and the list of members of the group.

GET /api/teststream/v1/groups/<group_name>

Examples:

```
GET /api/teststream/v1/groups/SrcGrp1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
```

```
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 21:50:28 GMT
Server: Apache
Content-Length: 119
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: application/json
{
    "group name": "SrcGrp1",
    "members count": 6,
    "names": [
        "01.03.01",
        "01.03.02",
        "01.03.03",
        "01.03.04",
        "01.03.05",
        "01.03.06"
    ]
}

GET /api/teststream/v1/groups/erererer
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjY2ZhYzg1YS03M2QzLTQ3ZTUtYTAwOS00Z
DZkNDM3ZjU4MzUiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.f118RoLFNx9-1VgyePZOTamaYf4_5hvGZ7
3S4Lab97M
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400
status: 400
Date: Thu, 30 May 2019 21:45:41 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 107
Connection: close
Content-Type: application/json
{
    "message": "  Failed to get group!!. Error type [API Failure!], error string [ERROR:
Group not found!  ]"
}
```

Topologies

List of Defined Topologies

The following URL is used to obtain a list of defined topologies. The request supports an optional query parameter as described in the table below. If successful, it returns a status of **200** and the list of defined topologies.

Table C-3 Defined Topologies

Optional Query Parameter	Values	Default Value (if not present)
search	string type	empty string

GET /api/teststream/v1/topologies

Examples:

```
GET /api/teststream/v1/topologies
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 22:04:31 GMT
Server: Apache
Content-Length: 132
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "topologies": [
        {
            "members count": 2,
            "topology name": "devTopo1"
        },
        {
            "members count": 6,
            "topology name": "stdTopo1"
        }
    ],
    "topologies count": 2
}

GET /api/teststream/v1/topologies?search=dev
```

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 22:20:33 GMT
Server: Apache
Content-Length: 105
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "search text": "dev",
    "topologies": [
        {
            "members count": 2,
            "topology name": "devTopo1"
        }
    ],
    "topologies count": 1
}
```

Creating a Topology

The following URL is used to create a topology. The request body must include a JSON object with members as specified in the table below. If successful, a status of **201** is returned. Otherwise, a status of **400** is returned.

Table C-4 Creating a Topology

Member Name	Optional	Value	Default Value
topology name	No	string	
topology type	No	[“standard”, “device”]	

POST /api/teststream/v1/topologies

Examples:

```
POST /api/teststream/v1/topologies
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
content-length: 68
Connection: keep-alive
{
   "topology name" : "restopo1",
   "topology type" : "standard"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 201
status: 201
Date: Wed, 29 May 2019 22:09:14 GMT
Server: Apache
Content-Length: 53
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. Topology restopo1 added.  "
}

POST /api/teststream/v1/topologies
Content-Type: application/json
```

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
content-length: 27
Connection: keep-alive
{
   "topology name" : "restopo1"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400
status: 400
Date: Wed, 29 May 2019 22:10:40 GMT
Server: Apache
Content-Length: 56
Connection: close
Content-Type: application/json
{
    "message": "Missing \"topology type\" in request body"
}

POST /api/teststream/v1/topologies
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
content-length: 67
Connection: keep-alive
{
   "topology name" : "restopo1",
   "topology type": "standard"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400
status: 400
Date: Wed, 29 May 2019 22:16:01 GMT
Server: Apache
```

```
Content-Length: 139
Connection: close
Content-Type: application/json
{
   "message": "  Failed to add topology [restopo1]!. Error type [API Failure!], error string
[ERROR: restopo1 - Topology already exists!  ]"
}
```

List of Topology Members

The following URL is used to obtain the members of the specified topology (replace <topology_name> with the desired topology name). If the topology does not exist, a status of **400** is returned. Otherwise, it returns a status of **200** and the list of members of the topology. Members are listed per member type. When devices are members of the topology, the selected device ports within those devices are listed in the “device ports from devices” member.

GET /api/teststream/v1/topologies/<topology_name>

Examples:

```
GET /api/teststream/v1/topologies/devTopo1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 22:22:26 GMT
Server: Apache
Content-Length: 500
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: application/json
{
    "connection groups": {
        "count": 0,
        "names": []
    },
    "destination groups": {
        "count": 0,
        "names": []
    },
    "device ports": {
        "count": 0,
        "names": []
    },
    "device ports from devices": {
        "count": 4,
```

```
        "names": [
            "Device1-01",
            "Device1-02",
            "Device2-01",
            "Device2-02"
        ]
    },
    "devices": {
        "count": 2,
        "names": [
            "Device1",
            "Device2"
        ]
    },
    "filters": {
        "count": 0,
        "names": []
    },
    "impairments": {
        "count": 0,
        "names": []
    },
    "members count": 2,
    "ports": {
        "count": 0,
        "names": []
    },
    "source groups": {
        "count": 0,
        "names": []
    },
    "subports": {
        "count": 0,
        "names": []
    },
    "topology name": "devTopo1"
}
```


Deleting a Topology

The following URL is used to delete the specified topology (replace <topology_name> with the desired topology name). If the topology does not exist or it can't be deleted, a status of **400** is returned. Otherwise, a status of **200** is returned.

DELETE /api/teststream/v1/topologies/<topology_name>

Examples:

```
DELETE /api/teststream/v1/topologies/restopo1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
```

```
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Wed, 29 May 2019 22:24:18 GMT
Server: Apache
Content-Length: 55
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. Topology restopo1 deleted.  "
}

DELETE /api/teststream/v1/topologies/restopo1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyNTdjOWU1MS04MTM4LTRkMGUtYjlhNy1kO
WY1YmM1MTA1YjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.VJYxH7m3qJnh6MeOEJoTPELCTapsV9e8en
x6j5HtSXc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 10.88.38.136:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400
status: 400
Date: Wed, 29 May 2019 22:25:22 GMT
Server: Apache
Content-Length: 115
Connection: close
Content-Type: application/json
{
   "message": "  Failed to delete topology!. Error type [API Failure!], error string [ERROR:
Topology not found!  ]"
}
```

List of Commands Supported for a Topology

The following URL is used to obtain a list of supported commands for topology handling for the specified topology (replace <topology_name> with the desired topology name). If successful, a status of **200** is returned. For each listed command, the parameters required in the request body are shown.

GET /api/teststream/v1/topologies/<topology_name>/commands

Example:

```
GET /api/teststream/v1/topologies/devtopo1/commands HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIzYjJiMWQ4Zi0yYmI4LTQ5YTgtOWRmMi1mZ
TY1YWM1ODJhMDEiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.RgL9afmzyvrXVkNcv6LKlHDhndVhKkq_cG
b_uOLdgEY
User-Agent: PostmanRuntime/7.28.4
Accept: */*
Postman-Token: 611170d0-eb77-445a-88c8-c0aa5f739c36
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 10 Oct 2021 17:05:40 GMT
Server: Apache
Content-Length: 6186
Keep-Alive: timeout=15, max=98
Connection: Keep-Alive
Content-Type: application/json
{
    "activate": {
        "parameters": {},
        "purpose": "activate all the associations on the topology"
    },
    "activate-connection": {
        "parameters": {
            "connection type": "'duplex' or 'simplex'.",
            "destination name": "name of the destination",
            "destination type": "'port', or 'group', or 'device port' (Lab Manager only)",
           "filter name": "name of a filer to use between source and destination. Optional.",
            "force": "boolean. If 'true', forces an activation without showing warnings.
Optional. Defaults to 'false'.",
           "impairment name": "name of an impairment to use between source and destination.
Optional.",
            "source name": "name of the source",
           "source type": "'port', or 'group', or 'generator', or 'device port' (Lab Manager
only)"
        },
        "purpose": "activate a connection between source and destination"
```

```
    },
    "add-reservation": {
        "parameters": {
            "activate": "boolean. If 'true', forces an activation of the topology when
reservation begins. Optional. Defaults to 'false'.",
            "end date": "calendar end date and time to schedule the reservation
(MM/DD/YYYY-HH:MM).",
           "remote exec": "name of a remote execution app. Optional. Defaults to no remote
execution.",
            "start date": "calendar start date and time to schedule the reservation
(MM/DD/YYYY-HH:MM)."
        },
        "purpose": "schedule a reservation time window for a device topology."
    },
    "connect": {
        "parameters": {
            "activate": "boolean. If 'true', association is created without activation.
Optional. Defaults to 'true'.",
            "connection type": "'duplex' or 'simplex'.",
            "destination name": "name of the destination",
            "destination type": "'port', or 'group', or 'device port' (Lab Manager only)",
          "filter name": "name of a filter to use between source and destination. Optional.",
            "force": "boolean. If 'true', forces a connection without showing warnings.
Optional. Defaults to 'true'.",
           "impairment name": "name of an impairment to use between source and destination.
Optional.",
            "source name": "name of the source",
          "source type": "'port', or 'group', or 'generator', or 'device port' (Lab Manager
only)"
        },
       "purpose": "make an association between source and destination and activate it (unless
opting not to)"
    },
    "deactivate": {
        "parameters": {},
        "purpose": "deactivate all the associations on the topology"
    },
    "deactivate-connection": {
        "parameters": {
            "connection type": "'duplex' or 'simplex'.",
            "destination name": "name of the destination",
            "destination type": "'port', or 'group', or 'device port' (Lab Manager only)",
          "filter name": "name of a filer to use between source and destination. Optional.",
            "force": "boolean. If 'true', forces a deactivation without showing warnings.
Optional. Defaults to 'false'.",
           "impairment name": "name of an impairment to use between source and destination.
Optional.",
            "source name": "name of the source",
```

"source type": "'port', or 'group', or 'generator', or 'device port' (Lab Manager only)"
},
"purpose": "deactivate a connection between source and destination"
},
"delete-member": {
"parameters": {
"member name": "name of the member",
"member type": "'port', or 'group', or 'filter', or 'impairment', or 'device port' (Lab Manager only)"
},
"purpose": "delete a member from the topology. It must not be in an active connection."
},
"delete-reservation": {
"parameters": {
"start date": "calendar start date and time (MM/DD/YYYY-HH:MM) of the scheduled reservation to delete."
},
"purpose": "delete a reservation for a device topology."
},
"disconnect": {
"parameters": {
"connection type": "'duplex' or 'simplex'.",
"destination name": "name of the destination",
"destination type": "'port', or 'group', or 'device port' (Lab Manager only)",
"filter name": "name of a filer to use between source and destination. Optional.",
"force": "boolean. If 'true', forces a disconnect without showing warnings. Optional. Defaults to 'true'.",
"impairment name": "name of an impairment to use between source and destination. Optional.",
"source name": "name of the source",
"source type": "'port', or 'group', or 'generator', or 'device port' (Lab Manager only)"
},
"purpose": "deactivate and remove the association between source and destination"
},
"find-reservation": {
"parameters": {
"duration": "amount of time the reservation is for.",
"duration type": "units for 'duration': 'minutes', or 'hours', or 'days'.",
"end date": "calendar date to end looking for reservation (MM/DD/YYYY). Optional.",
"end work day": "time (UTC) for end of each work day in which to schedule reservation, in hours and minutes (HH:MM). Optional. Defaults to '23:59'.",
"end work week": "end of week boundary to search for reservation time. One of 'sun','mon',tue','wed','thr','fri','sat'. Optional. Defaults to 'sat'.",
"start date": "calendar date to start looking for reservation (MM/DD/YYYY). Optional. Defaults to today.",
"start work day": "time (UTC) for start of each work day in which to schedule reservation, in hours and minutes (HH:MM). Optional. Defaults to '00:00'.",

```
            "start work week": "start of week boundary to search for reservation time.  One
of 'sun','mon',tue','wed','thr','fri','sat'. Optional. Defaults to 'sun'."
        },
      "purpose": "find a reservation time window for a device topology when all its resources
are available."
    },
    "get-reservations": {
        "parameters": {
            "end date": "calendar end date and time to schedule the reservation
(MM/DD/YYYY-HH:MM). Optional.",
            "start date": "calendar start date and time to filter the reservation
(MM/DD/YYYY-HH:MM). Optional."
        },
        "purpose": "get reservations for a specific device topology."
    },
    "revise-reservation": {
        "parameters": {
            "activate": "boolean. If 'true', forces an activation of the topology when
reservation begins. Optional. Defaults to 'false'.",
            "remote exec": "name of a remote execution app. Optional. Defaults to no remote
execution.",
           "start date": "calendar start date and time (MM/DD/YYYY-HH:MM) of the reservation
to revise."
        },
        "purpose": "revise the 'activate' or 'remote exec' parameters of a reservation for
a device topology."
    },
    "revise-reservation-time": {
        "parameters": {
            "new end date": "new calendar end date and time (MM/DD/YYYY-HH:MM) of the
reservation.",
            "new start date": "new calendar start date and time (MM/DD/YYYY-HH:MM) of the
reservation.",
           "start date": "calendar start date and time (MM/DD/YYYY-HH:MM) of the reservation
to revise."
        },
        "purpose": "revise a reservation time for a device topology specified by the start
and end date/time(UTC)."
    }
}
```


Activating a Topology

The following URL is used to activate the specified topology (replace <topology_name> with the desired topology name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

POST /api/teststream/v1/topologies/<topology_name>/commands/activate

Example:

```
POST /api/teststream/v1/topologies/restopo1/commands/activate
```

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI3ZTZlZTRiNS1hNDMyLTQ4OGItYWRmZC0yN
TdjZjI2NTVkYjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.FRKRPOJcMWC1wJ0yRlSvkC9WJw1evagIXz
XsXJAmIIY
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Thu, 30 May 2019 21:31:20 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 48
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. restopo1 activated.  "
}
```

Deactivating a Topology

The following URL is used to deactivate the specified topology (replace <topology_name> with the desired topology name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

POST /api/teststream/v1/topologies/<topology_name>/commands/deactivate

Examples:

```
POST /api/teststream/v1/topologies/restopo1/commands/deactivate
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI3ZTZlZTRiNS1hNDMyLTQ4OGItYWRmZC0yN
TdjZjI2NTVkYjciLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.FRKRPOJcMWC1wJ0yRlSvkC9WJw1evagIXz
XsXJAmIIY
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Thu, 30 May 2019 21:31:23 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 50
Keep-Alive: timeout=5, max=89
Connection: Keep-Alive
Content-Type: application/json
{
```

```
    "message": "Successful. restopo1 deactivated.  "
}
```

```
POST /api/teststream/v1/topologies/restopo10/commands/deactivate
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJlYTU4MGQ4Yi04ZGNkLTQ4NjgtYjI1Mi0zZ
mFlYjViOTRlMDIiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.F7kDg5b5IqnnW3KqVfu5s3z9nXI-AtBsSJ
lWcb8mqH8
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400
status: 400
Date: Thu, 30 May 2019 22:18:44 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 119
Connection: close
Content-Type: application/json
{
    "message": "  Failed to deactivate topology!. Error type [API Failure!], error string
[ERROR: Topology not found!  ]"
}
```

Creating a Connection in a Topology

Create a connection in the specified topology and optionally activate the connection (replace <topology_name> with the desired topology name). If successful, a status of **201** is returned. Otherwise a status of **400** is returned.The request body:

Table C-5 Creating a Connection in a Topology

Member Name	Optional	Value	Default Value
connection type	No	[“duplex”, “simplex”]	
activate	Yes	true, false]	true
source type	No	[“port”, “group”, “generator”, “device port”]	
source name	No	string type	
destination type	No	[“port”, “group”, “device port”]	
destination name	No	string type	
force	Yes	[true, false]	false
filter name	Yes	string type	“”
impairment name	Yes	string type	“”

```
POST   /api/teststream/v1/topologies/<topology_name>/commands/connect
```

Example:

```
POST /api/teststream/v1/topologies/restopo1/commands/connect
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJmZjE1YjU2Ni0zZDBmLTQyMGYtYTI0NS0yY
mI0ZjVhMzkxMjgiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9._Kx2PlaT4DWsmrZwfx6Xi2VD3TCqjs4MLl
fq3pSBB80
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 188
Connection: keep-alive
{
   "connection type" : "duplex",
   "activate" : false,
   "source type" : "port",
   "source name" : "01.01.31-1",
   "destination type" : "port",
   "destination name" : "01.01.27-1"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 201
status: 201
Date: Wed, 29 May 2019 22:54:50 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 28
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful.  "
}
```

Disconnecting a Connection

Remove a connection in the specified topology (replace <topology_name> with the desired topology name). If successful, a status of **200** is returned. Otherwise a status of **400** is returned. The request body:

Note: If there are extra members, in addition to the ones listed below, they will be ignored.

Table C-6 Disconnecting a Connection

Member Name	Optional	Value	Default Value
connection type	No	[“duplex”, “simplex”]	
source type	No	[“port”, “group”, “generator”, “device port”]	
source name	No	string type	

Table C-6 Disconnecting a Connection

Member Name	Optional	Value	Default Value
destination type	No	[“port”, “group”, “device port”]	
destination name	No	string type	
force	Yes	[true, false]	false
filter name	Yes	string type	“”
impairment name	Yes	string type	“”

POST /api/teststream/v1/topologies/<topology_name>/commands/disconnect

Example:

```
POST /api/teststream/v1/topologies/restopo1/commands/disconnect
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIxOTI1ZDYzYi1mZDE5LTQ0OTctOWQxMS0xN
GNhMDYxN2YyOTQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.WUVLqdmNWCBdYYP-9MgzY4f7cT0ASmqo-c
nbd70iF2M
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 188
Connection: keep-alive
{
   "connection type" : "duplex",
   "activate" : false,
   "source type" : "port",
   "source name" : "01.01.31-1",
   "destination type" : "port",
   "destination name" : "01.01.27-1"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Thu, 30 May 2019 22:45:53 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 53
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. 01.01.31-1 disconnected.  "
}
```

Activating a Connection

Activate an existing connection in the specified topology (replace <topology_name> with the desired topology name). If successful, a status of **200** is returned. Otherwise a status of **400** is returned.The request body:

Note: If there are extra members, in addition to the ones listed below, they will be ignored.

Table C-7 Activating a Connection

Member Name	Optional	Value	Default Value
connection type	No	[“duplex”, “simplex”]	
source type	No	[“port”, “group”, “generator”, “device port”]	
source name	No	string type	
destination type	No	[“port”, “group”, “device port”]	
destination name	No	string type	
force	Yes	[true, false]	false
filter name	Yes	string type	“”
impairment name	Yes	string type	“”

POST /api/teststream/v1/topologies/<topology_name>/commands/activate-connection

Example:

```
POST /api/teststream/v1/topologies/restopo1/commands/activate-connection
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJmOTE2ZDk1Zi00YjI1LTQ2NjUtYjdkYS03Y
2MzOTYwNmU4MjQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.0uuoDyyHRl2Rq6rdeFa-0juATAKR1QoLPx
7F9N5341U
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 188
Connection: keep-alive
{
   "connection type" : "duplex",
   "source type" : "port",
   "source name" : "01.01.31-1",
   "destination type" : "port",
   "destination name" : "01.01.27-1"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Thu, 30 May 2019 22:50:49 GMT
Server: Apache/2.4.25 (Debian)
```

```
Content-Length: 64
Keep-Alive: timeout=5, max=92
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. 01.01.31-1 to 01.01.27-1 activated.  "
}
```

Deactivating a Connection

Deactivate an existing connection in the specified topology (replace <topology_name> with the desired topology name). If successful, a status of **200** is returned. Otherwise a status of **400** is returned. The request body:

Note: If there are extra members, in addition to the ones listed below, they will be ignored).

Table C-8 Deactivating a Connection

Member Name	Optional	Value	Default Value
connection type	No	[“duplex”, “simplex”]	
source type	No	[“port”, “group”, “generator”, “device port”]	
source name	No	string type	
destination type	No	[“port”, “group”, “device port”]	
destination name	No	string type	
force	Yes	[true, false]	false
filter name	Yes	string type	“”
impairment name	Yes	string type	“”

POST /api/teststream/v1/topologies/<topology_name>/commands/deactivate-connection

Example:

```
POST /api/teststream/v1/topologies/restopo1/commands/deactivate-connection
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJmOTE2ZDk1Zi00YjI1LTQ2NjUtYjdkYS03Y
2MzOTYwNmU4MjQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.0uuoDyyHRl2Rq6rdeFa-0juATAKR1QoLPx
7F9N5341U
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 188
Connection: keep-alive
{
   "connection type" : "duplex",
   "activate" : false,
   "source type" : "port",
```

```
   "source name" : "01.01.31-1",
   "destination type" : "port",
   "destination name" : "01.01.27-1"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Thu, 30 May 2019 22:50:53 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 66
Keep-Alive: timeout=5, max=91
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. 01.01.31-1 to 01.01.27-1 deactivated.  "
}
```

Deleting a Member

Delete a member on the specified topology (replace <topology_name> with the desired topology name). If successful, a status of **200** is returned. Otherwise a status of **400** is returned. The request body:

Table C-9 Deleting a Member

Member Name	Optional	Value	Default Value
member type	No	[“port”, “group”, “filter”, “impairment”, “device port”]	
member name	No	string	

POST /api/teststream/v1/topologies/<topology_name>/commands/delete-member

Examples:

```
POST /api/teststream/v1/topologies/restopo1/commands/delete-member
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJmOTE2ZDk1Zi00YjI1LTQ2NjUtYjdkYS03Y
2MzOTYwNmU4MjQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.0uuoDyyHRl2Rq6rdeFa-0juATAKR1QoLPx
7F9N5341U
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 61
Connection: keep-alive
{
   "member type" : "port",
   "member name" : "fooooooooo"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400
status: 400
Date: Thu, 30 May 2019 22:51:06 GMT
```

```
Server: Apache/2.4.25 (Debian)
Content-Length: 125
Connection: close
Content-Type: application/json
{
    "message": "  Failed to remove [foooooooo]!.. Error type [API Failure!], error string
[ERROR: Port foooooooo not found!  ]"
}
```

```
POST /api/teststream/v1/topologies/restopo1/commands/delete-member
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJmOTE2ZDk1Zi00YjI1LTQ2NjUtYjdkYS03Y
2MzOTYwNmU4MjQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.0uuoDyyHRl2Rq6rdeFa-0juATAKR1QoLPx
7F9N5341U
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 34
Connection: keep-alive
{
   "member name" : "foooooooo"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400
status: 400
Date: Thu, 30 May 2019 22:51:06 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 54
Connection: close
Content-Type: application/json
{
    "message": "Missing \"member type\" in request body"
}
```

```
POST /api/teststream/v1/topologies/restopo1/commands/delete-member
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJmOTE2ZDk1Zi00YjI1LTQ2NjUtYjdkYS03Y
2MzOTYwNmU4MjQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.0uuoDyyHRl2Rq6rdeFa-0juATAKR1QoLPx
7F9N5341U
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 62
Connection: keep-alive
{
   "member type" : "port",
   "member name" : "01.01.31-1"
}
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Thu, 30 May 2019 22:51:06 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 28
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful.  "
}
```

Add Reservation

The following URL is used to schedule a reservation time window for the specified device topology (replace <topology_name> with the desired device topology name). If successful, a status of **201** is returned. Otherwise, a status of **400** is returned.

POST /api/teststream/v1/topologies/<topology_name>/commands/add-reservation

The request body:

Table C-10 Adding a Reservation

Member Name	Optional	Type	Default Value	Description
start date	No	string		Calendar start date and time to schedule the reservation (MM/DD/YYYY-HH:MM)
end date	No	string		Calendar end date and time to schedule the reservation (MM/DD/YYYY-HH:MM)
activate	Yes	boolean	false	If 'true', forces an activation of the topology when reservation begins.
remote exec	Yes	string	""	Name of a reservation remote execution.

Examples:

```
POST /api/teststream/v1/topologies/top1/commands/add-reservation HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJlYWE5NWQ2MS02YjQwLTQxMjItODdjMi1kNjE5ZTQ2
YTJlYjAiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.9O2-oS78arT-BrDGAYLAcMpl8m2ri3pipqHDYuNqTZc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: 5429e51c-c633-4826-945a-da170ad047dd
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 126

{
"activate": true,
"end date": "09/18/2021-18:00",
"start date": "09/18/2021-17:00",
"remote exec": ""
```

```
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 201 CREATED
Date: Mon, 21 Jun 2021 15:17:37 GMT
Server: Apache
Content-Length: 48
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Topology successfully reserved. "}


POST /api/teststream/v1/topologies/top1/commands/add-reservation HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJlYWE5NWQ2MS02YjQwLTQxMjItODdjMi1kNjE5ZTQ2
YTJlYjAiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.9O2-oS78arT-BrDGAYLAcMpl8m2ri3pipqHDYuNqTZc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: d7a64b88-138d-40c2-8a68-f1b0c0683964
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 126

{
"activate": true,
"end date": "09/18/2021-18:00",
"start date": "09/18/2021-17:00",
"remote exec": ""
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400 BAD REQUEST
Date: Mon, 21 Jun 2021 15:45:52 GMT
Server: Apache
Content-Length: 213
Connection: close
Content-Type: application/json

{
  "message":" Failed to add topology reservation!. Error type [API Failure!], error string [ERROR:
device1-001: is not available at this time! device1-002: is not available at this time! Reservation
Rejected ]"
}
```

Delete Reservation

The following URL is used to delete a reservation for the specified device topology (replace <topology_name> with the desired device topology name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

DELETE /api/teststream/v1/topologies/<topology_name>/commands/delete-reservation

For historical reasons, POST is also supported. The request body:

Table C-11 Deleting a Reservation

Member Name	Optional	Type	Default Value	Description
start date	No	string		Calendar start date and time of the scheduled reservation to delete (MM/DD/YYYY-HH:MM)

Example:

```
DELETE /api/teststream/v1/topologies/top1/commands/delete-reservation HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJlYWE5NWQ2MS02YjQwLTQxMjItODdjMi1kNjE5ZTQ2
YTJlYjAiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.9O2-oS78arT-BrDGAYLAcMpl8m2ri3pipqHDYuNqTZc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: 9b7824f0-4185-4864-8cbe-8a99f390ba4c
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 42

{
"start date": "09/18/2021-17:00"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Mon, 21 Jun 2021 15:25:11 GMT
Server: Apache
Content-Length: 47
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Topology reservation successfully deleted. "}
```

Find Reservation

The following URL is used to find a reservation time window when all the resources are available for the specified device topology (replace <topology_name> with the desired device topology name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

GET /api/teststream/v1/topologies/<topology_name>/commands/find-reservation

The request body:

Table C-12 Finding a Reservation

Member Name	Optional	Type	Default Value	Description
duration	No	integer		Amount of time the reservation is for.

Table C-12 Finding a Reservation

Member Name	Optional	Type	Default Value	Description
duration type	No	[minutes, hours, days]		Units of the 'duration' parameters.
start date	Yes	string	today's date	Calendar date to start looking for a reservation. (MM/DD/YYYY)
end date	Yes	string		Calendar date to end looking for a reservation. (MM/DD/YYYY)
start work day	Yes	string	"00:00"	Time (UTC) for start of each work day in which to schedule reservation, in hours and minutes (HH:MM)
end work day	Yes	string	"23:59"	Time (UTC) for end of each work day in which to schedule reservation, in hours and minutes (HH:MM)
start work week	Yes	[sun, mon, tue, wed, thr, fri, sat]	"sun"	Start of week boundary to search for reservation.
end work week	Yes		"sat"	End of week boundary to search for reservation.

Example:

```
GET /api/teststream/v1/topologies/top1/commands/find-reservation HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJlYWE5NWQ2MS02YjQwLTQxMjItODdjMi1kNjE5ZTQ2
YTJlYjAiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.9O2-oS78arT-BrDGAYLAcMpl8m2ri3pipqHDYuNqTZc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: 8a7d68f6-bcc0-4251-9b46-8a963004bb52
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 241

{
"duration": 30,
"duration type": "hours",
"end date": "10/10/2021",
"start date": "09/10/2021",
"end work day end": "23:59",
"start work day start": "00:00",
"end work week end": "fri",
"start work week start": "mon"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Mon, 21 Jun 2021 16:02:15 GMT
Server: Apache
Content-Length: 87
```

```
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{
   "end date":"09/11/2021-06:00",
   "start date":"09/10/2021-00:00",
   "topology name":"top1"
}
```

Revise Reservation

The following URL is used to revise a reservation 'activate' or ' remote exec' parameters for the specified device topology (replace <topology_name> with the desired device topology name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

POST /api/teststream/v1/topologies/<topology_name>/commands/revise-reservation

The request body:

Table C-13 Revising a Reservation

Member Name	Optional	Type	Default Value	Description
start date	No	string		Calendar start date and time (MM/DD/YYYY-HH:MM) of the reservation to revise.
activate	Yes	boolean	false	If 'true', forces an activation of the topology when reservation begins.
remote exec	Yes	string	""	Name of a reservation remote execution.

Example:

```
POST /api/teststream/v1/topologies/top1/commands/revise-reservation HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJlYWE5NWQ2MS02YjQwLTQxMjItODdjMi1kNjE5ZTQ2
YTJlYjAiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.9O2-oS78arT-BrDGAYLAcMpl8m2ri3pipqHDYuNqTZc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: f32ce297-0399-4870-afc5-1faf3c854765
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 89

{
   "activate": true,
   "start date": "09/18/2021-15:00",
   "remote exec": ""
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Mon, 21 Jun 2021 16:13:02 GMT
Server: Apache
```

```
Content-Length: 48
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Topology successfully reserved. "}
```

Revise Reservation Time

The following URL is used to revise a reservation time for the specified device topology (replace <topology_name> with the desired device topology name). The original reservation is identified by uts start and end date/time (UC). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

POST /api/teststream/v1/topologies/<topology_name>/commands/revise-reservation-time

The request body:

Table C-14 Revising a Reservation Time

Member Name	Optional	Type	Default Value	Description
start date	No	string		Calendar start date and time (MM/DD/YYYY-HH:MM) of the reservation to revise.
end date	No	string		New calendar start date and time (MM/DD/YYYY-HH:MM) of the reservation.
new end date	No	string		New calendar end date and time (MM/DD/YYYY-HH:MM) of the reservation.

Example:

```
POST /api/teststream/v1/topologies/top1/commands/revise-reservation-time HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJlYWE5NWQ2MS02YjQwLTQxMjItODdjMi1kNjE5ZTQ2
YTJlYjAiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.9O2-oS78arT-BrDGAYLAcMpl8m2ri3pipqHDYuNqTZc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: 14d1b4d5-c999-419e-a18d-d96ab3181b87
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 163126

{
"start date": "09/18/2021-17:00",
"new end date": "09/18/2021-16:00",
"new start date": "09/18/2021-15:00"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Mon, 21 Jun 2021 16:36:37 GMT
Server: Apache
Content-Length: 48
Keep-Alive: timeout=15, max=100
```

```
Connection: Keep-Alive
Content-Type: application/json

{"message":"Topology successfully reserved. "}
```

Get Reservations

The following URL is used to get existing reservations for the specified device topology (replace <topology_name> with the desired device topology name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

GET /api/teststream/v1/topologies/<topology_name>/commands/get-reservations

The request body:

Table C-15 Getting a Reservation Time

Member Name	Optional	Type	Default Value	Description
start date	Yes	string	now	Calendar start date and time to filter the reservation (MM/DD/YYYY-HH:MM).
end date	Yes	string	end of time	Calendar end date and time to schedule the reservation (MM/DD/YYYY-HH:MM).

Examples:

```
GET /api/teststream/v1/topologies/top1/commands/get-reservations HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJlYWE5NWQ2MS02YjQwLTQxMjItODdjMi1kNjE5ZTQ2
YTJlYjAiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.9O2-oS78arT-BrDGAYLAcMpl8m2ri3pipqHDYuNqTZc
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: b4a50052-8d28-4f94-bd16-a3b3425fc2ca
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Mon, 21 Jun 2021 16:41:10 GMT
Server: Apache
Content-Length: 240
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{
    "reservations": [
        {
            "activate": "No",
            "end date time": "09/18/2021-18:00",
            "remote exec": "RRE1 Profile123",
            "start date time": "09/18/2021-17:00",
            "topology name": "top1",
            "user": "administrator"
        }
    ],
```

```
    "reservations count": 1
}

GET /api/teststream/v1/topologies/top1/commands/get-reservations HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJlYWE5NWQ2MS02YjQwLTQxMjItODdjMi1kNjE5ZTQ2
YTJlYjAiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.9O2-oS78arT-BrDGAYLAcMpl8m2ri3pipqHDYuNqTZc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: e40602fa-c28e-4269-b2bb-d057e2fc5c1e
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 79

{
"end date": "10/18/2022-18:00",
"start date": "10/18/2021-17:00"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Mon, 21 Jun 2021 16:54:54 GMT
Server: Apache
Content-Length: 64
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: application/json

{
    "reservations": [],
    "reservations count": 0
}
```

Getting the session time zone

The following URL is used to obtain session information. If successful, a status of 200 is returned.

GET /api/teststream/v1/session

Example:

```
GET /api/teststream/v1/session HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI3NTQ0NTNiMS1lNGJjLTRjNGItYjBhYi1hNzg4Njhk
YTYzNTUiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.eZgluFTEDhMpjgBJGRWWitrDhJxmZSntMubVHf2OIVM
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Postman-Token: 89a2efb1-a73b-4614-86fb-dbc2c4fe6f51
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Fri, 25 Mar 2022 14:18:22 GMT
```

```
Server: Apache
Content-Length: 19
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: application/json

{"timezone":"UTC"}
```

Setting the session time zone

The URL below is used to update the parameters of a session. If the request is successful a status of 200 is returned. If any of the requested parameters are invalid, a status of 400 is returned.

Table C-16 Adding a Remote Server

Member Name	Optional	Type	Default Value	Description
timezone	No	string		Time zone to use for the current session. Updating the time zone will affect future commands that use dates or time of day. Supported values follow the IANA time zone database version 2022.a.

PUT /api/teststream/v1/session

Example:

```
PUT /api/teststream/v1/session HTTP/1.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI3NTQ0NTNiMS1lNGJjLTRjNGItYjBhYi1hNzg4Njhk
YTYzNTUiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.eZgluFTEDhMpjgBJGRWWitrDhJxmZSntMubVHf2OIVM
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Postman-Token: 8b0819f9-1d4c-409d-8170-2a426ae60e9e
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 41

{
"timezone" : "America/New_York"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Fri, 25 Mar 2022 15:49:21 GMT
Server: Apache
Content-Length: 61
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Successful. Timezone set to 'America/New_York'"}

PUT /api/teststream/v1/session HTTP/1.1
Content-Type: application/json
```

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI3NTQ0NTNiMS1lNGJjLTRjNGItYjBhYi1hNzg4Njhk
YTYzNTUiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.eZgluFTEDhMpjgBJGRWWitrDhJxmZSntMubVHf2OIVM
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Postman-Token: 56c27e2a-2c68-45a8-8b0e-ada6350b306a
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 42

{
"timezone" : "America/Palo_Alto"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400 BAD REQUEST
Date: Fri, 25 Mar 2022 15:50:35 GMT
Server: Apache
Content-Length: 130
Connection: close
Content-Type: application/json

{"message":" Failed to set session parameters!. Error type [API Failure!], error string [Unknown
timezone 'America/Palo_Alto']"}
```

Remote Execution Manager

Remote Servers

Remote servers can be added, modified, deleted, or listed.

Adding a Remote Server

The following URL is used to add a remote server. If successful, a status of **201** is returned. Otherwise, a status of **400** is returned.

POST /api/teststream/v1/remote-execution-manager/remote-servers

The request body:

Table C-17 Adding a Remote Server

Member Name	Optional	Type	Default Value	Description
name	No	string		Name of the remote server to create (max. 50 characters).
ip address	No	string		IPv4 address of the remote server.
access type	No	['telnet', 'ssh']		Use 'telnet' or 'ssh' when accessing the remote server.
port number	No	integer		Port number to use for the selected access type.
username	No	string		Username of the user account to use to access the remote server (max. 50 characters)

Table C-17 Adding a Remote Server

Member Name	Optional	Type	Default Value	Description
password	No	string		Password of the user account to use to access the remote server (max. 96 characters)
visible to all	No	boolean		If 'true', remote server is visible to all users. If 'false', it is only visible to the TestStream user that created it.

Example:

```
POST /api/teststream/v1/remote-execution-manager/remote-servers HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJhNmVmOWU4NS04YzYyLTQ1NjItOTdmNi02NjcxNTZk
OWZkY2MiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.jfVHMGGnwJAMv6XOeVa_ZixkqRuYMfUbCwKOnZYmzYs
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.1
Accept: */*
Postman-Token: 1e875e8e-80b5-462b-a5ce-b0856ca5a8d6
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 220

{
"name" : "AutomationServer",
"ip address" : "10.88.39.206",
"access type" : "telnet",
"port number" : 23,
"username" : "johndoe",
"password" : "jdsecret",
"visible to all" : true
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 201 CREATED
Date: Sun, 11 Jul 2021 16:28:42 GMT
Server: Apache
Content-Length: 56
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Remote Server added successfully.\r\n\r\n"}
```

Get a list of Remote Servers

The following URL is used to get a list of configured remote servers. If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

GET /api/teststream/v1/remote-execution-manager/remote-servers

The request supports an optional query parameter as described in the table below:

Table C-18 Getting a List of Remote Servers

Member Name	Type	Default Value (if not present)	Description
search	string	Empty string	Search string used to match remote server names (case sensitive).

Examples:

```
GET /api/teststream/v1/remote-execution-manager/remote-servers HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: 3829dcac-a0a8-4b98-b1b4-9a22af1e383a
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Tue, 22 Jun 2021 08:36:45 GMT
Server: Apache
Content-Length: 391400
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "remote server count": 2,
    "remote servers": [
        {
            "access type": "ssh",
            "created by": "administrator",
            "ip address": "10.88.39.200",
            "name": "LabAutomationServer",
            "port number": 22020,
            "username": "onpath",
            "visible to all": true
        },
        {
            "access type": "telnet",
            "created by": "administrator",
            "ip address": "10.88.39.206",
            "name": "AutomationServer",
            "port number": 23,
            "username": "johndoe",
            "visible to all": true
        }
    ],
    "search text": ""
}
```

```
GET /api/teststream/v1/remote-execution-manager/remote-servers?search=%27Lab%27 HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJhNmVmOWU4NS04YzYyLTQ1NjItOTdmNi02NjcxNTZk
OWZkY2MiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.jfVHMGGnwJAMv6XOeVa_ZixkqRuYMfUbCwKOnZYmzYs
User-Agent: PostmanRuntime/7.28.1
Accept: */*
Postman-Token: 59712de4-a03b-437f-8492-c92dad9fa6af
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 11 Jul 2021 16:32:01 GMT
Server: Apache
Content-Length: 235
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "remote server count": 1,
    "remote servers": [
        {
            "access type": "ssh",
            "created by": "administrator",
            "ip address": "10.88.39.200",
            "name": "LabAutomationServer",
            "port number": 22020,
            "username": "onpath",
            "visible to all": true
        }
    ],
    "search text": "Lab"
```

Revise a Remote Server

The following URL is used to revise the configuration of a remote server (replace <remote_server_name> with the desired remote server name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

PUT /api/teststream/v1/remote-execution-manager/remote-servers/<remote_server_name>

The request body:

Table C-19 Revising a Remote Server

Member Name	Optional	Type	Default Value	Description
name	Yes	string	<remote_server_name>	Name of the remote server to create (max. 0 characters).
ip address	No	string		IPv4 address of the remote server.
access type	No	['telnet', 'ssh']		Use 'telnet' or 'ssh' when accessing the remote server.
port number	No	integer		Port number to use for the selected access type.

Table C-19 Revising a Remote Server

Member Name	Optional	Type	Default Value	Description
username	No	string		Username of the user account to use to access the remote server (max. 50 characters)
password	No	string		Password of the user account to use to access the remote server (max. 96 characters)
visible to all	No	boolean		If 'true', remote server is visible to all users. If 'false', it is only visible to the TestStream user that created it.

Example:

```
PUT /api/teststream/v1/remote-execution-manager/remote-servers/AutomationServer HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJhNmVmOWU4NS04YzYyLTQ1NjItOTdmNi02NjcxNTZk
OWZkY2MiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.jfVHMGGnwJAMv6XOeVa_ZixkqRuYMfUbCwKOnZYmzYs
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.1
Accept: */*
Postman-Token: 13a34553-7da3-47f3-8d69-de89628ff7bc
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 175

{
"ip address": "10.88.39.205",
"access type": "ssh",
"port number": 22,
"username": "rootdoe",
"password": "r00tdoe",
"visible to all": false
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 11 Jul 2021 16:34:46 GMT
Server: Apache
Content-Length: 62
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"\r\nRemote Server revised successfully.\r\n\r\n"}
```

Delete a Remote Server

The following URL is used to delete a remote server (replace <remote_server_name> with the desired remote server name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

DELETE /api/teststream/v1/remote-execution-manager/remote-servers/<remote_server_name>

Example:

```
DELETE /api/teststream/v1/remote-execution-manager/remote-servers/AutomationServer HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: f51aa104-fe80-46ad-b108-ccb15c37db99
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Tue, 22 Jun 2021 10:14:15 GMT
Server: Apache
Content-Length: 58
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Remote Server deleted successfully.\r\n\r\n"}
```

Remote Execution Profiles

Adding a Remote Execution Profile

The following URL is used to add a remote execution profile. If successful, a status of **201** is returned. Otherwise, a status of **400** is returned.

POST /api/teststream/v1/remote-execution-manager/remote-execution-profiles

The request body:

Table C-20 Adding a Remote Execution Profile

Member Name	Optional	Type	Default Value	Description
name	No	string		Name of the remote execution profile to create (max. 50 characters).
rep remote server	No	string		Name of the remote server to be used to execute the command.
rep execution command	Yes	string	empty string	Command to execute in the remote server (max. 512 characters).
rep description	Yes	string	empty string	Description of the remote execution profile (max. 250 characters).

Examples:

```
POST /api/teststream/v1/remote-execution-manager/remote-execution-profiles HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
```

```
Accept: */*
Postman-Token: c1b56b0c-5d8e-44f4-a2c2-71f8a10201fd
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 290

{
   "name" : "Reset Cisco Router",
   "rep remote server" : "LabAutomationServer",
   "rep execution command" : "/usr/local/bin/reset-cisco-router.py",
   "rep description" : "Will reset the Cisco Router. IP address added as argument in reservation
remote execution profile"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 201 CREATED
Date: Tue, 22 Jun 2021 12:23:44 GMT
Server: Apache
Content-Length: 67
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Remote Execution Profile added successfully.\r\n\r\n"}

POST /api/teststream/v1/remote-execution-manager/remote-execution-profiles HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: 4a9670d5-1bde-407e-9850-abc6e0c6a70b
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 341

{
   "name" : "Configure Cisco Router",
   "rep remote server" : "MyNewFancyRemoteServer",
   "rep execution command" : "/usr/local/bin/configure-cisco-router.py",
   "rep description" : "Will configure the Cisco Router. IP address and configuration profile name
are added as argument in reservation remote execution profile"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400 BAD REQUEST
Date: Tue, 22 Jun 2021 12:27:02 GMT
Server: Apache
Content-Length: 114
Connection: close
Content-Type: application/json
```

{"message":" Failed to Add REP!. Error type [Command error], error string [ERROR!! Remote Server not found!]"}

Get a list of Remote Execution Profiles

The following URL is used to get a list of configured remote execution profiles. If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

GET /api/teststream/v1/remote-execution-manager/remote-execution-profiles

The request supports an optional query parameter as described on the table below:

Table C-21 Getting a List of Remote Execution Profiles

Member Name	Type	Default Value	Description
search	string	empty string	Search string used to match remote execution profile names (case sensitive).

Examples:

```
GET /api/teststream/v1/remote-execution-manager/remote-execution-profiles HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: 2e1e1d7d-b23e-4b49-8896-d692d2f80778
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Tue, 22 Jun 2021 12:35:15 GMT
Server: Apache
Content-Length: 611
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json
{
    "rep count": 2,
    "rep profiles": [
        {
            "rep description": "Will reset the Cisco Router. IP address added as argument in
reservation remote execution profile",
            "rep execution command": "/usr/local/bin/reset-cisco-router.py",
            "name": "Reset Cisco Router",
            "rep remote server": "LabAutomationServer"
        },
        {
          "rep description": "Will configure the Cisco Router. IP address and configuration profile
name are added as argument in reservation remote execution profile",
            "rep execution command": "/usr/local/bin/configure-cisco-router.py",
            "name": "Configure Cisco Router",
            "rep remote server": "LabAutomationServer"
        }
```

```
    ],
    "search text": ""
}

GET /api/teststream/v1/remote-execution-manager/remote-execution-profiles?search=%22Reset%22
HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: b511cc58-2e27-4991-85dc-872516a923f7
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Tue, 22 Jun 2021 12:37:47 GMT
Server: Apache
Content-Length: 312
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: application/json
{
    "rep count": 1,
    "rep profiles": [
        {
            "rep description": "Will reset the Cisco Router. IP address added as argument in
reservation remote execution profile",
            "rep execution command": "/usr/local/bin/reset-cisco-router.py",
            "name": "Reset Cisco Router",
            "rep remote server": "LabAutomationServer"
        }
    ],
    "search text": "Reset"
}
```

Revise a Remote Execution Profile

The following URL is used to revise a remote execution profile (replace <remote_execution_profile_name> with the desired remote execution profile name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

PUT /api/teststream/v1/remote-execution-manager/remote-execution-profiles/<remote_execution_profile_name>

The request body:

Table C-22 Revising a Remote Execution Profile

Member Name	Optional	Type	Default Value	Description
name	No	string	<remote_execution_profile_name>	Name of the remote execution profile (max. 50 characters).

Table C-22 Revising a Remote Execution Profile

Member Name	Optional	Type	Default Value	Description
rep remote server	No	string		Name of the remote server to be used to execute the command.
rep execution command	Yes	string	empty string	Command to execute in the remote server (max. 512 characters).
rep description	Yes	string	empty string	Description of the remote execution profile (max. 250 characters).

Example:

```
PUT /api/teststream/v1/remote-execution-manager/remote-execution-profiles/Reset%20Cisco%20Router
HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: 69f5e16b-e45f-4616-a61c-8c52c03da187
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 299

{
   "name" : "Factory Reset Cisco Router",
   "rep remote server" : "LabAutomationServer",
   "rep execution command" : "/usr/local/bin/reset-cisco-router.py",
   "rep description" : "Will reset the Cisco Router. IP address added as argument in reservation
remote execution profile"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Tue, 22 Jun 2021 12:49:24 GMT
Server: Apache
Content-Length: 69
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Remote Execution Profile revised successfully.\r\n\r\n"}
```

Delete a Remote Execution Profile

The following URL is used to delete a remote execution profile (replace <remote_execution_profile_name> with the desired remote execution profile name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

DELETE /api/teststream/v1/remote-execution-manager/remote-execution-profiles/<remote_execution_profile_name>

Example:

```
DELETE
/api/teststream/v1/remote-execution-manager/remote-execution-profiles/Configure%20Cisco%20Router
HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: e2c4c7db-5ddc-46b1-8b53-0d4931f68511
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Tue, 22 Jun 2021 12:51:44 GMT
Server: Apache
Content-Length: 69
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Remote Execution Profile deleted successfully.\r\n\r\n"}
```

Reservation Remote Execution Profiles

Reservation remote execution profile is used in reservations to automate the execution of commands at four different stages of the reservation:

- Pre activation
- Post activation
- Pre deactivation
- Reservation end

Adding a Reservation Remote Execution Profile

The following URL is used to add a reservation remote execution profile. If successful, a status of **201** is returned. Otherwise, a status of **400** is returned.

POST /api/teststream/v1/remote-execution-manager/reservation-remote-executions

The request body:

Table C-23 Adding a Reservation Remote Execution Profile

Member Name	Optional	Type	Default Value	Description
name	No	string		Name of the new reservation remote execution profile to create (max. 50 characters).
pre deactivation execution offset	Yes	integer	0	How many minutes before the reservation end to run the pre deactivation command.
reservation start	Yes	stage dict (see below)	{"enable": false}	Configuration for the reservation start stage of a reservation.
post activation	Yes	stage dict (see below)	{"enable": false}	Configuration for the post activation stage of a reservation.
pre deactivation	Yes	stage dict (see below)	{"enable": false}	Configuration for the pre deactivation stage of a reservation.

Table C-23 Adding a Reservation Remote Execution Profile

Member Name	Optional	Type	Default Value	Description
reservation end	Yes	stage dict (see below)	{"enable": false}	Configuration for the reservation end stage of a reservation.

The stage dictionary:

Table C-24 Stage Dictionary for Adding a Reservation Remote Execution Profile

Member Name	Optional	Type	Default Value	Description
enable	Yes	boolean	false	If 'true', the stage is enabled. If 'false', the stage is disabled.
rep name	If 'enable' is set to 'true', it must be provided. If 'enable' is set to 'false', it is ignored.	string		The name of the remote execution profile to execute at this stage.
command parms	If 'enable' is set to 'true', it is optional. If 'enable' is set to 'false', it is ignored.	string	empty string	Additional parameters (arguments) to pass to the remote execution command (max. 512 characters). It allows for local customization of a remote execution profile command.
timeout	If 'enable' is set to 'true', it is optional. If 'enable' is set to 'false', it is ignored.	integer	0	Timeout in minutes for the execution of the command.

Example:

```
POST /api/teststream/v1/remote-execution-manager/reservation-remote-executions HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJhNmVmOWU4NS04YzYyLTQ1NjItOTdmNi02NjcxNTZk
OWZkY2MiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.jfVHMGGnwJAMv6XOeVa_ZixkqRuYMfUbCwKOnZYmzYs
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.1
Accept: */*
Postman-Token: cceea191-5810-4a60-b435-878c130737b4
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 760

{
    "name": "RRE2 Profile99",
    "pre deactivation execution offset": 37,
    "reservation start": {
        "enable": true,
        "rep name": "PreActivation",
        "command parms": "+Hello +Profile99",
        "timeout": 13
    },
    "post activation": {
        "enable": true,
        "rep name": "PostActivation",
        "command parms": "+Hangon +Profile99",
        "timeout": 14
```

```
    },
    "pre deactivation": {
        "enable": true,
        "rep name": "PreDeactivation",
        "command parms": "+Collect +Profile99",
        "timeout": 15
    },
    "reservation end": {
        "enable": true,
        "rep name": "ReservationEnd",
        "command parms": "+Cleanup +Profile99",
        "timeout": 16
    }
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 201 CREATED
Date: Sun, 11 Jul 2021 16:37:34 GMT
Server: Apache
Content-Length: 62
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"Reservation Remote Execution added successfully"}
```

Get a list of Reservation Remote Execution Profiles

The following URL is used to get a list of configured reservation remote execution profiles. If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

GET /api/teststream/v1/remote-execution-manager/reservation-remote-executions

The request supports an optional query parameter as described on the table below:

Table C-25 Getting a List of Reservation Remote Execution Profiles

Member Name	Type	Default Value	Description
search	string	empty string	Search string used to match remote execution profile names (case sensitive).

Examples:

```
GET /api/teststream/v1/remote-execution-manager/reservation-remote-executions HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJhNmVmOWU4NS04YzYyLTQ1NjItOTdmNi02NjcxNTZk
OWZkY2MiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.jfVHMGGnwJAMv6XOeVa_ZixkqRuYMfUbCwKOnZYmzYs
User-Agent: PostmanRuntime/7.28.1
Accept: */*
Postman-Token: 4c9c783c-b5ab-44ad-909b-c46db5ec5e2f
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 11 Jul 2021 16:39:35 GMT
```

```
Server: Apache
Content-Length: 1076
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{
    "rre count": 2,
    "rre profiles": [
        {
            "name": "RRE1 Profile123",
            "post activation": {
                "command parms": "+Hangon2 +Profile123",
                "enable": true,
                "rep name": "PostActivation",
                "timeout": 16
            },
            "pre deactivation": {
                "command parms": "+Collect2 +Profile123",
                "enable": true,
                "rep name": "PreDeactivation",
                "timeout": 17
            },
            "pre deactivation execution offset": 10,
            "reservation end": {
                "command parms": "+Cleanup2 +Profile123",
                "enable": true,
                "rep name": "ReservationEnd",
                "timeout": 18
            },
            "reservation start": {
                "command parms": "+Hello2 +Profile123",
                "enable": true,
                "rep name": "PreActivation",
                "timeout": 15
            }
        },
        {
            "name": "RRE2 Profile99",
            "post activation": {
                "command parms": "+Hangon +Profile99",
                "enable": true,
                "rep name": "PostActivation",
                "timeout": 14
            },
            "pre deactivation": {
                "command parms": "+Collect +Profile99",
                "enable": true,
                "rep name": "PreDeactivation",
                "timeout": 15
            },
            "pre deactivation execution offset": 37,
            "reservation end": {
```

```
                "command parms": "+Cleanup +Profile99",
                "enable": true,
                "rep name": "ReservationEnd",
                "timeout": 16
            },
            "reservation start": {
                "command parms": "+Hello +Profile99",
                "enable": true,
                "rep name": "PreActivation",
                "timeout": 13
            }
        }
    ]
}
```


```
GET /api/teststream/v1/remote-execution-manager/reservation-remote-executions?search=Profile123
HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: 6ac383a5-9fe3-454a-aed3-e421f70340f8
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 11 Jul 2021 16:41:35 GMT
Server: Apache
Content-Length: 586
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/jso
```


```
{
    "rre count": 1,
    "rre profiles": [
        {
            "name": "RRE1 Profile123",
            "post activation": {
                "command parms": "+Hangon2 +Profile123",
                "enable": true,
                "rep name": "PostActivation",
                "timeout": 16
            },
            "pre deactivation": {
                "command parms": "+Collect2 +Profile123",
                "enable": true,
                "rep name": "PreDeactivation",
                "timeout": 17
            },
            "pre deactivation execution offset": 10,
```

```
            "reservation end": {
                "command parms": "+Cleanup2 +Profile123",
                "enable": true,
                "rep name": "ReservationEnd",
                "timeout": 18
            },
            "reservation start": {
                "command parms": "+Hello2 +Profile123",
                "enable": true,
                "rep name": "PreActivation",
                "timeout": 15
            }
        }
    ],
    "search text": "Profile123"
}
```

Revise a Reservation Remote Execution Profile

The following URL is used to revise a reservation remote execution profile (replace <reservation_remote_execution_name> with the desired reservation remote execution profile name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

PUT /api/teststream/v1/remote-execution-manager/reservation-remote-executions/<reservation_remote_execution_name>

The request body:

Table C-26 Revising a Reservation Remote Execution Profile

Member Name	Optional	Type	Default Value	Description
name	Yes	string		Name of the new reservation remote execution profile to (max. 50 characters).
pre deactivation execution offset	Yes	integer	0	How many minutes before the reservation end to run the pre deactivation command.
reservation start	Yes	stage dict (see below)	{"enable": false}	Configuration for the reservation start stage of a reservation.
post activation	Yes	stage dict (see below)	{"enable": false}	Configuration for the post activation stage of a reservation.
pre deactivation	Yes	stage dict (see below)	{"enable": false}	Configuration for the pre deactivation stage of a reservation.
reservation end	Yes	stage dict (see below)	{"enable": false}	Configuration for the reservation end stage of a reservation.

The stage dictionary:

Table C-27 Stage Dictionary for Revising a Reservation Remote Execution Profile

Member Name	Optional	Type	Default Value	Description
enable	Yes	boolean	false	If 'true', the stage is enabled. If 'false', the stage is disabled.

Table C-27 Stage Dictionary for Revising a Reservation Remote Execution Profile

Member Name	Optional	Type	Default Value	Description
rep name	If 'enable' is set to 'true', it must be provided. If 'enable' is set to 'false', it is ignored.	string		The name of the remote execution profile to execute at this stage.
command parms	If 'enable' is set to 'true', it is optional. If 'enable' is set to 'false', it is ignored.	string	empty string	Additional parameters (arguments) to pass to the remote execution command (max. 512 characters). It allows for local customization of a remote execution profile command.
timeout	If 'enable' is set to 'true', it is optional. If 'enable' is set to 'false', it is ignored.	integer	0	Timeout in minutes for the execution of the command.

Example:

```
PUT /api/teststream/v1/remote-execution-manager/reservation-remote-executions/RRE2%20Profile99
HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJhNmVmOWU4NS04YzYyLTQ1NjItOTdmNi02NjcxNTZk
OWZkY2MiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.jfVHMGGnwJAMv6XOeVa_ZixkqRuYMfUbCwKOnZYmzYs
Content-Type: application/json
User-Agent: PostmanRuntime/7.28.1
Accept: */*
Postman-Token: f8e1eb29-02d1-4c9b-a6f0-d8fc5e462813
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 579

{
    "name": "RRE2 Profile99",
    "pre deactivation execution offset": 22,
    "reservation start": {
        "enable": true,
        "rep name": "PreActivation",
        "command parms": "+Hello2 +Profile99",
        "timeout": 23
    },
    "post activation": {
        "enable": true,
        "rep name": "PostActivation",
        "timeout": 24
    },
    "pre deactivation": {
        "enable": true,
        "rep name": "PreDeactivation",
        "command parms": "+Collect2 +Profile99"
    },
    "reservation end": {
        "timeout": "55"
    }
```

```
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 11 Jul 2021 16:43:40 GMT
Server: Apache
Content-Length: 77
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message":"\r\nReservation Remote Execution revised successfully.\r\n\r\n"}
```

Delete a Reservation Remote Execution Profile

The following URL is used to delete a reservation remote execution profile (replace <reservation_remote_execution_name> with the desired reservation remote execution profile name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

DELETE /api/teststream/v1/remote-execution-manager/reservation-remote-executions/<reservation_remote_execution_name>

Example:

```
DELETE /api/teststream/v1/remote-execution-manager/reservation-remote-executions/RRE2%20Profile99
HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI4NTQ4NDQ3MC1mY2VlLTQ4ZWUtYWQwMi0xYzdiMGM4
ZDg5OGQiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM2LjE5NCJ9.Mo0b3XcyRNoVENKleCVkmUz8XgesbgeglQUdvbxlzjc
User-Agent: PostmanRuntime/7.28.0
Accept: */*
Postman-Token: cd393165-a59f-4ed3-9011-1016a4d97959
Host: 10.88.38.133:8080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Tue, 22 Jun 2021 14:46:45 GMT
Server: Apache
Content-Length: 73
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/json

{"message": "Reservation Remote Execution deleted successfully.\r\n\r\n"}
```

Devices

List of Defined Devices

The following URL is used to obtain a list of defined devices. The request supports an optional query parameter as described in the table below. If successful, it returns a status of **200** and the list of defined devices. Otherwise it returns a status of **400**.

Table C-28 Defined Devices

Optional Query Parameter	Values	Default Value (if not present)
search	string type	empty string

GET /api/teststream/v1/devices

Example:

```
GET /api/teststream/v1/devices
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIxMDFhZjI0ZC1mYzA0LTQ5MjYtYWExZi0xN
GE0ZDQ2ODhkZGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.u2SzLk5wT9RGyoScpgiUb88XgE5S8R6iiK
whSyxX2vE
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 17:48:00 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 128
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/json
{
    "devices": [{
        "device name": "Device1",
        "number of ports": "9"
    }, {
        "device name": "Device2",
        "number of ports": "5"
    }],
    "devices count": 2
}
```

```
GET /api/teststream/v1/devices?search=rest
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIxMDFhZjI0ZC1mYzA0LTQ5MjYtYWExZi0xN
GE0ZDQ2ODhkZGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.u2SzLk5wT9RGyoScpgiUb88XgE5S8R6iiK
whSyxX2vE
```

```
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 17:48:03 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 54
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: application/json
{
    "devices": [],
    "devices count": 0,
    "search text": "rest"
}
```

Creating a New Device

The following URL is used to create a device. The request body must include a JSON object with members as specified in the table below. If successful, a status of **201** is returned. Otherwise, a status of **400** is returned.

Table C-29 Creating a New Device

Member Name	Optional	Value	Default Value
device name	No	string	
number of ports	No	integer	

POST /api/teststream/v1/devices

Example:

```
POST /api/teststream/v1/devices
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIxMDFhZjI0ZC1mYzA0LTQ5MjYtYWExZi0xN
GE0ZDQ2ODhkZGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.u2SzLk5wT9RGyoScpgiUb88XgE5S8R6iiK
whSyxX2vE
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 59
Connection: keep-alive
{
   "device name" : "RestDev1",
   "number of ports" : 5
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 201
status: 201
Date: Fri, 31 May 2019 17:48:01 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 44
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. RestDev1 added.  "
}
```

List of Device Ports for a Specified Device

The following URL is used to obtain the device ports of the specified device (replace <device_name> with the desired device name). If successful, it returns a status of **200** is returned and the list of device ports of the device. Otherwise, a status of **400** is returned.

GET /api/teststream/v1/devices/<device_name>

Example:

```
GET /api/teststream/v1/devices/RestDev1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIxMDFhZjI0ZC1mYzA0LTQ5MjYtYWExZi0xN
GE0ZDQ2ODhkZGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.u2SzLk5wT9RGyoScpgiUb88XgE5S8R6iiK
whSyxX2vE
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 17:48:04 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 432
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: application/json
{
    "device ports": [{
        "device port name": "RestDev1-01",
        "interface": "Undefined Interface",
        "map": ""
    }, {
        "device port name": "RestDev1-02",
        "interface": "Undefined Interface",
        "map": ""
    }, {
        "device port name": "RestDev1-03",
        "interface": "Undefined Interface",
        "map": ""
    }, {
        "device port name": "RestDev1-04",
        "interface": "Undefined Interface",
        "map": ""
    }, {
        "device port name": "RestDev1-05",
        "interface": "Undefined Interface",
        "map": ""
    }],
    "device ports count": 5
}
```

Deleting a device

The following URL is used to delete the specified device (replace <device_name> with the desired device name). If the device does not exist or it can't be deleted, a status of **400** is returned. Otherwise, a status of **200** is returned.

DELETE /api/teststream/v1/devices/<device_name>

Examples:

```
DELETE /api/teststream/v1/devices/RestDev1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIxMDFhZjI0ZC1mYzA0LTQ5MjYtYWExZi0xN
GE0ZDQ2ODhkZGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.u2SzLk5wT9RGyoScpgiUb88XgE5S8R6iiK
whSyxX2vE
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400
status: 400
Date: Fri, 31 May 2019 17:48:32 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 111
Connection: close
Content-Type: application/json
{
    "message": "  Failed to delete device!. Error type [API Failure!], error string [ERROR:
Device not found!  ]"
}

DELETE /api/teststream/v1/devices/RestDev2
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIxMDFhZjI0ZC1mYzA0LTQ5MjYtYWExZi0xN
GE0ZDQ2ODhkZGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.u2SzLk5wT9RGyoScpgiUb88XgE5S8R6iiK
whSyxX2vE
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 17:48:32 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 53
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
```

```
{
    "message": "Successful. Device RestDev2 deleted.  "
}
```

List of Commands Supported for a Device

The following URL is used to obtain a list of supported commands for device handling for the specified device (replace <device_name> with the desired device name). If successful, a status of **200** is returned. For each listed command, the parameters required in the request body are shown.

GET /api/teststream/v1/devices/<device_name>/commands

Example:

```
GET /api/teststream/v1/devices/RestDev1/commands
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIwODU2YzE5Mi03MzU4LTQ4YzktOGFiYS0zM
mE1NDRjZjM0OTgiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.rBaqcZ1opBv7_rxGdO4XVNgpB4qJam99Yv
162voOtHc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 18:10:31 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 265
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Content-Type: application/json
{
    "add-ports": {
        "parameters": {
            "number of ports": "number of device ports to add to the device."
        },
        "purpose": "increase the number of device ports of the device"
    },
    "rename": {
        "parameters": {
            "device name": "new name for the device."
        },
        "purpose": "change the name of a device"
    }
}
```

Renaming a Device

The following URL is used to rename a specified device (replace <device_name> with the desired device name). The request body must include a JSON object with members as specified in the table below. If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

Table C-30 Renaming a Device

Member Name	Optional	Value	Default Value
device name	No	string	

POST /api/teststream/v1/devices/<device_name>/commands/rename

Example:

```
POST /api/teststream/v1/devices/RestDev1/commands/rename
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIwODU2YzE5Mi03MzU4LTQ4YzktOGFiYS0zM
mE1NDRjZjM0OTgiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.rBaqcZ1opBv7_rxGdO4XVNgpB4qJam99Yv
162voOtHc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 31
Connection: keep-alive
{
"device name" : "RestDev2"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 18:10:31 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 45
Keep-Alive: timeout=5, max=92
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Device successfully renamed.  "
}
```

Adding Device Ports to a Device

The following URL is used to add ports to a specified device (replace <device_name> with the desired device name). The request body must include a JSON object with members as specified in the table below. If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

Table C-31 Adding Device Ports to a Device

Member Name	Optional	Value	Default Value
number of ports	No	integer	

POST /api/teststream/v1/devices/<device_name>/commands/add-ports

Example:

```
POST /api/teststream/v1/devices/RestDev2/commands/add-ports
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIwODU2YzE5Mi03MzU4LTQ4YzktOGFiYS0zM
mE1NDRjZjM0OTgiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.rBaqcZ1opBv7_rxGdO4XVNgpB4qJam99Yv
162voOtHc
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 26
Connection: keep-alive
{
     "number of ports" : 5
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 18:10:32 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 62
Keep-Alive: timeout=5, max=91
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. 5 device ports added to RestDev2.  "
}
```

Device ports

Device Port Information

The following URL is used to get information and configuration for the specified device port (replace <device_port_name> with the desired device port name). If successful, a status of **200** is returned. Otherwise a status of **400** is returned.

GET /api/teststream/v1/device-ports/<device_port_name>

Example:

```
GET /api/teststream/v1/device-ports/RestDev1-01
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYjY0MDBhMC05Y2Q3LTRlYzMtYTA1OS1jZ
DY1MDVmNzAzYzkiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.GId0g3ha9Om-y6dg2HdVXaP4hZn7T4L7r-
kNpTSr2MY
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 19:15:04 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 145
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: application/json
{
    "device ports": [{
        "device name": "RestDev1",
        "device port name": "RestDev1-01",
        "interface": "Undefined Interface",
        "map": ""
    }],
    "device ports count": 1
}
```

Deleting a Device Port

The following URL is used to delete the specified device port (replace <device_port_name> with the desired device port name). If successful, a status of **200** is returned. Otherwise a status of **400** is returned.

DELETE /api/teststream/v1/device-ports/<device_port_name>

Example:

```
DELETE /api/teststream/v1/device-ports/RestDev1-05
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyOWVhZDE5OS1kOGVmLTQ4M2QtOTNlNC1jN
mZiZmQ1ZjRkNTMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.uQ44aNi14cSyRw1CngfENQigta2Qwrd8iw
axEAWjEVs
```

```
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 18:24:20 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 61
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. Device Port RestDev1-05 deleted.  "
}
```

List of Commands Supported for a Device Port

The following URL is used to obtain a list of supported commands for device port handling for the specified device port (replace <device_port_name> with the desired device port name). If successful, a status of **200** is returned. For each listed command, the parameters required in the request body are shown.

GET /api/teststream/v1/device-ports/<device_port_name>/commands

Example:

```
GET /api/teststream/v1/device-ports/RestDev1-01/commands
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYjY0MDBhMC05Y2Q3LTRlYzMtYTA1OS1jZ
DY1MDVmNzAzYzkiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.GId0g3ha9Om-y6dg2HdVXaP4hZn7T4L7r-
kNpTSr2MY
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 19:15:28 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 667
Keep-Alive: timeout=5, max=92
Connection: Keep-Alive
Content-Type: application/json
{
    "configure": {
        "parameters": {
```

```
            "interface": "One of the following -
1GFib|2GFib|4GFib|8GFib|GIG-E|CU-GIG-E|OC-3/stm-1|OC-12/stm-4|OC-48/stm-16|OC-192/stm-64|O
PTical|10GEth|25GEth|40GEth|50GEth|100GEth|100MFib|CU10000|CPRI9|CPRI8|CPRI7|CPRI6|CPRI5|C
PRI4|CPRI3|CPRI2|CPRI1|UNDEFINED."
        },
        "purpose": "configure parameters of the device port. Currently, the only parameter
supported is the interface."
    },
    "map": {
        "parameters": {
            "port name": "name of the port to map to the device port."
        },
        "purpose": "map a port to a device port"
    },
    "rename": {
        "parameters": {
            "device port name": "new name for the device port."
        },
        "purpose": "change the name of a device port"
    },
    "unmap": {
        "parameters": {},
        "purpose": "unmap a port from a device port"
    }
}
```


Renaming a Device Port

The following URL is used to rename the specified device port (replace <device_port_name> with the desired device port name). The request body must include a JSON object with members as specified in the table below. If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

Table C-32 Renaming a Device Port

Member Name	Optional	Value	Default Value
device port name	No	string	

POST /api/teststream/v1/device-ports/<device_port_name>/commands/rename

Example:


```
POST /api/teststream/v1/device-ports/RestDev1-01/commands/rename
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyOWVhZDE5OS1kOGVmLTQ4M2QtOTNlNC1jN
mZiZmQ1ZjRkNTMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.uQ44aNi14cSyRw1CngfENQigta2Qwrd8iw
axEAWjEVs
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 44
```

```
Connection: keep-alive
{
"device port name" : "RestDev1-Port-01"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 18:24:44 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 50
Keep-Alive: timeout=5, max=91
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Device Port successfully renamed.  "
}
```

Configuring a Device Port

The following URL is used to configure the specified device port (replace <device_port_name> with the desired device port name). The request body must include a JSON object with members as specified in the table below. If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

Table C-33 Configuring a Device Port

Member Name	Optional	Value	Default Value
interface	No	string (see list below)	

Supported interfaces:

UNDEFINED, 1GFib, 2GFib, 4GFib, 8GFib, 16GFib, GIG-E, CU-GIG-E, OC-3/stm-1, OC-12/stm-4, OC-48/stm-16, OC-192/stm-64, OPTical, 10GEth, 25GEth, 40GEth, 50GEth, 100GEth, 100MFib, CU10000, CPRI9, CPRI8, CPRI7, CPRI6, CPRI5, CPRI4, CPRI3, CPRI2, CPRI1

Note: The ‘UNDEFINED” interface is used to ‘unconfigure’ the interface.

POST /api/teststream/v1/device-ports/<device_port_name>/commands/configure

Examples:

```
POST /api/teststream/v1/device-ports/RestDev1-Port-01/commands/configure
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyOWVhZDE5OS1kOGVmLTQ4M2QtOTNlNC1jN
mZiZmQ1ZjRkNTMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.uQ44aNi14cSyRw1CngfENQigta2Qwrd8iw
axEAWjEVs
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 27
Connection: keep-alive
{
"interface" : "10GEth"
```

```
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 18:24:56 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 69
Keep-Alive: timeout=5, max=89
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. Device Port RestDev1-Port-01 configured.  "
}


POST /api/teststream/v1/device-ports/RestDev1-Port-01/commands/configure
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiIyOWVhZDE5OS1kOGVmLTQ4M2QtOTNlNC1jN
mZiZmQ1ZjRkNTMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.uQ44aNi14cSyRw1CngfENQigta2Qwrd8iw
axEAWjEVs
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 30
Connection: keep-alive
{
"interface" : "UNDEFINED"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 18:25:09 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 69
Keep-Alive: timeout=5, max=87
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. Device Port RestDev1-Port-01 configured.  "
}
```

Mapping a Device Port

The following URL is used to map a port to the specified device port (replace <device_port_name> with the desired device port name). The request body must include a JSON object with members as specified in the table below. If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

Table C-34 Mapping a Device Port

Member Name	Optional	Value	Default Value
port name	No	string	

POST /api/teststream/v1/device-ports/<device_port_name>/commands/map

Example:

```
POST /api/teststream/v1/device-ports/RestDev1-02/commands/map
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYjY0MDBhMC05Y2Q3LTRlYzMtYTA1OS1jZ
DY1MDVmNzAzYzkiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.GId0g3ha9Om-y6dg2HdVXaP4hZn7T4L7r-
kNpTSr2MY
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length: 31
Connection: keep-alive
{
"port name" : "01.01.10-1"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 19:16:17 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 74
Keep-Alive: timeout=5, max=83
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. 01.01.10-1 mapped to device port RestDev1-02.  "
}
```

Unmapping a Device Port

The following URL is used to unmap the specified device port (replace <device_port_name> with the desired device port name). If successful, a status of **200** is returned. Otherwise, a status of **400** is returned.

POST /api/teststream/v1/device-ports/<device_port_name>/commands/unmap

Example:

```
POST /api/teststream/v1/device-ports/RestDev1-02/commands/unmap
```

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiI0YjBmOWIxNy05NjcwLTRlM2EtOWY2ZC0xM
TI1NDUzNjY4YjAiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.KZXn0pdKLZEbdKjUkWFixVQxNG0cK8AN7Q
075rj6SvY
User-Agent: PostmanRuntime/7.13.0
Accept: */*
Cache-Control: no-cache
Host: 172.23.26.23:8080
accept-encoding: gzip, deflate
content-length:
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200
status: 200
Date: Fri, 31 May 2019 19:27:23 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 62
Keep-Alive: timeout=5, max=81
Connection: Keep-Alive
Content-Type: application/json
{
    "message": "Successful. Device Port RestDev1-02 unmapped.  "
}
```

Ports

List of Defined Ports

The following URL is used to obtain a list of defined ports. The request supports an optional query parameter as described in the table below. If successful, it returns a status of 200 and the list of defined ports.

Table C-35 List of Defined Ports

Optional Query Parameter	Values	Default Value (if not present)
search	string type	Empty string

GET /api/teststream/v1/ports

Examples:

```
GET /api/teststream/v1/ports HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYWJhMjc5Ny0xYTZkLTQ3N2MtOTRlYi0xN
jE5MmI3NWJiNGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.JVXZZv84LnOQTfzpmsVSUbe2tG8ssbZnn9
2w375AqTQ
User-Agent: PostmanRuntime/7.20.1
Accept: */*
Cache-Control: no-cache
Host: 172.23.29.75:8080
Accept-Encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
```

```
Date: Sun, 06 Oct 2019 08:12:51 GMT
Server: Apache
Content-Length: 133
Connection: close
Content-Type: application/json
{
"ports count":9,
"ports names":[
"01.01.21",
"01.01.22",
"01.01.23",
"01.01.24",
"01.02.05",
"01.02.06",
"01.03.01",
"01.03.23",
"01.03.47"]
}
GET /api/teststream/v1/ports?search=%2203%22 HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYWJhMjc5Ny0xYTZkLTQ3N2MtOTRlYi0xN
jE5MmI3NWJiNGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.JVXZZv84LnOQTfzpmsVSUbe2tG8ssbZnn9
2w375AqTQ
User-Agent: PostmanRuntime/7.20.1
Accept: */*
Cache-Control: no-cache
Host: 172.23.29.75:8080
Accept-Encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 06 Oct 2019 08:16:13 GMT
Server: Apache
Content-Length: 67
Connection: close
Content-Type: application/json
{
"ports count":3,
"ports names":[
"01.03.01",
"01.03.23",
"01.03.47"]
}
```

Port information

The following URL is used to obtain the information about the specified port (replace <port_name> with the desired port name). If the port does not exist, a status of 400 is returned. Otherwise, it returns a status of
200 and the information about the port.

```
GET    /api/teststream/v1/ports/<port_name>
```

Examples:

```
GET /api/teststream/v1/ports/01.01.21 HTTP/1.1
```

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYWJhMjc5Ny0xYTZkLTQ3N2MtOTRlYi0xN
jE5MmI3NWJiNGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.JVXZZv84LnOQTfzpmsVSUbe2tG8ssbZnn9
2w375AqTQ
User-Agent: PostmanRuntime/7.20.1
Accept: */*
Cache-Control: no-cache
Host: 172.23.29.75:8080
Accept-Encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 06 Oct 2019 08:18:20 GMT
Server: Apache
Content-Length: 376
Connection: close
Content-Type: application/json
{
    "Rx conn state": "Connected",
    "SFP diag alarm": "Enabled",
    "Tx conn state": "Disconnected",
    "alarmed state": "Not Alarmed",
    "armed": "Enabled",
    "auto arm": "Disabled",
    "interface": "10GEth",
    "link State": "Powered Off",
    "link propagation": "Default",
    "lock state": "Unlocked",
    "module state": "Present",
    "port name": "01.01.21",
    "port number": [
        1,
        1,
        21
    ],
    "port type": "Normal",
    "switch name": "sw-29.75"
}

GET /api/teststream/v1/ports/ioioio HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYWJhMjc5Ny0xYTZkLTQ3N2MtOTRlYi0xN
jE5MmI3NWJiNGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.JVXZZv84LnOQTfzpmsVSUbe2tG8ssbZnn9
2w375AqTQ
User-Agent: PostmanRuntime/7.20.1
Accept: */*
Cache-Control: no-cache
Host: 172.23.29.75:8080
Accept-Encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400 BAD REQUEST
Date: Sun, 06 Oct 2019 08:20:29 GMT
Server: Apache
```

```
Content-Length: 107
Connection: close
Content-Type: application/json
{
    "message": "  Failed to get port!. Error type [API Failure!], error string [ERROR: Por
t not found! ]"
}
```

Deleting a Port

The following URL is used to delete the specified port (replace <port_name> with the desired port name). If the port does not exist or it can't be deleted, a status of 400 is returned. Otherwise, a status of 200 is returned.

DELETE /api/teststream/v1/ports/<port_name>

Example:

```
DELETE /api/teststream/v1/ports/01.01.01 HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYWJhMjc5Ny0xYTZkLTQ3N2MtOTRlYi0xN
jE5MmI3NWJiNGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.JVXZZv84LnOQTfzpmsVSUbe2tG8ssbZnn9
2w375AqTQ
User-Agent: PostmanRuntime/7.20.1
Accept: */*
Cache-Control: no-cache
Host: 172.23.29.75:8080
Accept-Encoding: gzip, deflate
Content-Length: 0
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 06 Oct 2019 08:22:58 GMT
Server: Apache
Content-Length: 34
Connection: close
Content-Type: application/json
{
    "message":"01.01.01 deleted. "
}
```

List of Commands Supported for a Port

The following URL is used to obtain a list of supported commands for a port (replace <port_name> with the desired port name). If successful, a status of 200 is returned. For each listed command, the parameters required in the request body are shown.

GET /api/teststream/v1/ports/<port_name>/commands

Example:

```
GET /api/teststream/v1/ports/01.01.02/commands HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYWJhMjc5Ny0xYTZkLTQ3N2MtOTRlYi0xN
jE5MmI3NWJiNGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.JVXZZv84LnOQTfzpmsVSUbe2tG8ssbZnn9
2w375AqTQ
User-Agent: PostmanRuntime/7.20.1
Accept: */*
```

```
Cache-Control: no-cache
Host: 172.23.29.75:8080
Accept-Encoding: gzip, deflate
Connection: keep-alive
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 06 Oct 2019 08:24:23 GMT
Server: Apache
Content-Length: 376
Connection: close
Content-Type: application/json
{
    "revise": {
        "parameters": {
            "interface": "One of the following - 1GFib|2GFib|4GFib|8GFib|16GFib|GIG-E|CU-G
IG-E|
OC-3/stm-1|OC-12/stm-4|OC-48/stm-16|OC-192/stm-64|OPTical|10GEth|25GEth|
40GEth|50GEth|100GEth|100MFib|CU10000|CPRI9|CPRI8|CPRI7|CPRI6|CPRI5|CPRI4|
CPRI3|CPRI2|CPRI1"
        },
        "purpose": "revise parameters of the port. Currently, the only parameter supported
 is the
interface."
    }
}
```

Revise a port

The following URL is used to revise the configuration of the specified port (replace <port_name> with the desired port name). The request body must include a JSON object with members as specified in the table below. If successful, a status of 200 is returned. Otherwise, a status of 400 is returned.

Table C-36 Mapping a Device Port

Member Name	Optional	Value	Default Value
interface	No	string (see list below)	

Supported interfaces:

UNDEFINED, 1GFib, 2GFib, 4GFib, 8GFib, 16GFib, GIG-E, CU-GIG-E, OC-3/stm-1, OC-12/stm-4, OC-48/stm-16, OC-192/stm-64, OPTical, 10GEth, 25GEth, 40GEth, 50GEth, 100GEth, 100MFib, CU10000, CPRI9, CPRI8, CPRI7, CPRI6, CPRI5, CPRI4, CPRI3, CPRI2, CPRI1

POST /api/teststream/v1/ports/<port_name>/commands/revise

Examples:

```
POST /api/teststream/v1/ports/01.01.02/commands/revise HTTP/1.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYWJhMjc5Ny0xYTZkLTQ3N2MtOTRlYi0xN
jE5MmI3NWJiNGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.JVXZZv84LnOQTfzpmsVSUbe2tG8ssbZnn9
2w375AqTQ
User-Agent: PostmanRuntime/7.20.1
Accept: */*
Cache-Control: no-cache
Host: 172.23.29.75:8080
```

```
Accept-Encoding: gzip, deflate
Content-Length: 29
Connection: keep-alive
{
   "interface" : "20GEth"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 400 BAD REQUEST
Date: Sun, 06 Oct 2019 08:26:36 GMT
Server: Apache
Content-Length: 110
Connection: close
Content-Type: application/json
{
    "message": "  Failed to revise port!. Error type [API Failure!], error string [ERROR:
Invalid interface!  ]"
}

POST /api/teststream/v1/ports/01.01.02/commands/revise HTTP/1.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdWJsaWNfaWQiOiJjYWJhMjc5Ny0xYTZkLTQ3N2MtOTRlYi0xN
jE5MmI3NWJiNGMiLCJyZW1vdGVfYWRkciI6IjEwLjg4LjM4LjEyMCJ9.JVXZZv84LnOQTfzpmsVSUbe2tG8ssbZnn9
2w375AqTQ
User-Agent: PostmanRuntime/7.20.1
Accept: */*
Cache-Control: no-cache
Host: 172.23.29.75:8080
Accept-Encoding: gzip, deflate
Content-Length: 28
Connection: keep-alive
{
   "interface" : "GIG-E"
}
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
HTTP/1.1 200 OK
Date: Sun, 06 Oct 2019 08:28:11 GMT
Server: Apache
Content-Length: 46
Connection: close
Content-Type: application/json
{
    "message": "Successful. 01.01.02 revised.  "
}
```

NETSCOUT SYSTEMS, INC.
310 Littleton Road
Westford, MA 01886-4105

Tel. 978 614-4000
888-999-5946
Fax 978-614-4004
E-mail info@netscout.com
Web www.netscout.com

733-1696 Rev. A