

Extreme SLX-OS Management Configuration Guide, 17r.2.00

Supporting the Extreme SLX 9850 and 9540 Devices

© 2017, Extreme Networks, Inc. All Rights Reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see www.extremenetworks.com/company/legal/trademarks. Specifications and product availability are subject to change without notice.

© 2017, Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, and MyBrocade are registered trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands, product names, or service names mentioned of Brocade Communications Systems, Inc. are listed at www.brocade.com/en/legal/brocade-Legal-intellectual-property/brocade-legal-trademarks.html. Other marks may belong to third parties.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Contents

Preface	7
Document conventions.....	7
Notes, cautions, and warnings.....	7
Text formatting conventions.....	7
Command syntax conventions.....	8
Extreme resources.....	8
Document feedback.....	8
Contacting Extreme Technical Support.....	9
About This Document	11
Supported hardware and software.....	11
Interface module capabilities.....	11
What's new in this document	11
Configuration Fundamentals	13
Configuration files.....	13
Default configuration files.....	13
Startup configuration files.....	13
Running configuration files.....	14
Displaying configurations.....	14
Saving configuration changes.....	14
Backing up configurations.....	15
Configuration restoration.....	16
Managing flash files.....	16
Rebooting the device.....	18
Session connection.....	18
Telnet.....	18
SSH.....	20
Configuring the terminal session parameters.....	24
Configuring a login banner.....	24
Ethernet management interfaces.....	25
Configuring a static Ethernet address.....	25
Displaying a management interface.....	26
Configuring IPv6 address on SLX platform.....	26
Configuring management IP addresses.....	29
Port management.....	30
SLX 9850 36x100G LC ports.....	30
Configuring breakout mode.....	32
10G/1G auto negotiation and auto detection mode.....	34
Configuring port speed and negotiation.....	35
Port flap dampening.....	35
Port transition hold timer.....	36
Link fault signaling.....	37
Interface Ethernet ports.....	39
Displaying device interfaces.....	39
Displaying slots and module status information.....	39
Slots and modules.....	40

Displaying slots and module status information.....	41
Disabling latch detection.....	42
Chassis and host names.....	43
Customizing chassis and host names.....	43
Changing the chassis IP address.....	44
System clock.....	45
Setting the clock.....	45
Management VRFs.....	45
VRF reachability.....	46
Zero Touch Provisioning.....	47
Routing for Zero Touch Provisioning.....	48
Using zero touch provisioning.....	48
ZTP configuration.....	49
Example of Zero Touch Provisioning in a two node topology	53
MAC address aging.....	55
TCAM application-resource monitoring.....	55
TCAM library-resource monitoring.....	56
Hardware profiles.....	56
TCAM profiles.....	56
TCAM sharing.....	57
Counter profiles.....	59
Hardware profile show commands	60
Management Module High Availability.....	61
Management module HA overview.....	61
Traffic forwarding features support for HA.....	63
SLX-OS and Linux Shell Interoperability.....	65
Overview	65
Limitations	65
Executing Linux shell commands from SLX-OS.....	66
Executing scripts from SLX-OS.....	66
Downloading a script to the SLX-OS device.....	66
Creating scripts in the Linux shell.....	67
Running scripts from the SLX-OS CLI.....	67
Accessing the Linux shell from SLX-OS.....	67
Executing SLX-OS commands from the Linux shell.....	68
Escalating Linux permissions to root.....	69
Saving and appending show command output to a file.....	69
Logs of Linux shell activities.....	70
Linux shell user entry and exit logs.....	70
Linux shell command execution logs.....	70
Configuring remote logging of Linux shell activities.....	71
Guest OS for TPVM.....	73
VM access management.....	73
Brocade SLX 9850 VM access management.....	73
Brocade SLX 9540 VM access management.....	79
Insight interface and TPVM.....	79
Insight interface.....	79
Inbound ACL-based mirroring.....	82
Insight interface port-channel.....	84

Insight interface LC recovery.....	85
Insight interface traffic management and QoS.....	85
Configuring QoS egress scheduling.....	87
Troubleshooting port-mirroring.....	89
TPVM.....	93
Supported third-party applications, packages, and hardware.....	93
TPVM installation and management.....	95
Third Party Virtual Machine (TPVM) service port support.....	104
Docker containers.....	105
Linux containers.....	107
Utilities installation and management.....	107
Assigning a static IP address on the TPVM Linux OS.....	109
Network Time Protocol (NTP).....	111
Network Time Protocol overview.....	111
Date and time settings.....	111
Time zone settings.....	111
Network Time Protocol Server Overview.....	111
Network Time Protocol Client Overview.....	112
Network Time Protocol Associations.....	112
Network Time Protocol Authentication.....	113
Configuring NTP.....	113
Authenticating an NTP server.....	115
Displaying the active NTP server.....	116
NTP server status when an NTP server is not configured.....	116
NTP server status when an NTP server is configured.....	116
SNMP.....	117
SNMP overview.....	117
Basic SNMP operation.....	117
SNMP community strings.....	118
SNMP groups.....	119
SNMP users.....	119
SNMP views.....	119
SNMP server hosts.....	119
Multiple SNMP server context to VRF mapping.....	119
Configuring SNMPv2.....	120
Configuring SNMPv3.....	121
Configuring an SNMP server context to a VRF.....	122
Offline SNMP ifIndex generation tool.....	123
Generating ifIndexes for various interfaces.....	124
Configuration examples for generating ifIndexes offline.....	124
LLDP.....	127
LLDP overview.....	127
Layer 2 topology mapping.....	127
LLDP configuration guidelines and restrictions.....	129
Configuring and managing LLDP.....	129
Understanding the default LLDP.....	129
Disabling LLDP globally.....	129
Configuring LLDP global parameters.....	130
Configuring LLDP profiles.....	131

Configuring an LLDP profile to an interface.....	132
Displaying LLDP information.....	133
Clearing LLDP-related information.....	134
Password Recovery.....	137
Recovering the admin password from the root account.....	137
VM root password recovery for Brocade SLX 9850.....	137
Recovering the VM root login account.....	138
Recovering the VM root password.....	139
Python Event-Management and Scripting.....	141
Python under Brocade operating systems	141
Python overview	141
Working interactively in the Python shell	141
Python scripts	143
Guidelines for writing Python scripts	143
Testing Python-script statements	143
Copying Python files to the device.....	144
Running Python scripts from the command line.....	145
Python scripts and run-logs	145
Python event-management	148
Configuring an event-handler profile	148
Activating an event-handler	149
Configuring event-handler options	150
Troubleshooting event-management.....	151
Aborting an event-handler action.....	151
Event-management show commands	151

Preface

- Document conventions..... 7
- Extreme resources..... 8
- Document feedback..... 8
- Contacting Extreme Technical Support..... 9

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Extreme technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.



CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names. Identifies keywords and operands. Identifies the names of GUI elements.
<i>italic text</i>	Identifies text to enter in the GUI. Identifies emphasis. Identifies variables.
Courier font	Identifies document titles. Identifies CLI output.

Format	Description
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, <code>--show WWN</code> .
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <code>member[member...]</code> .
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Extreme resources

Visit the Extreme website to locate related documentation for your product and additional Extreme resources.

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at www.extremenetworks.com. Product documentation for all supported releases is available to registered users at www.extremenetworks.com/support/documentation.

Document feedback

Quality is our first concern at Extreme, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com.

- Provide feedback to the Extreme Networks Information Development team about this document using our short [online feedback form](#)
- Email us directly at internalinfodev@extremenetworks.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Contacting Extreme Technical Support

As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.

If you require assistance, contact Extreme Networks using one of the following methods:

- [GTAC \(Global Technical Assistance Center\)](#) for immediate support
 - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact.
 - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) - Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) - A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) - Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

About This Document

- Supported hardware and software.....11
- What's new in this document11

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for SLX-OS Release 17r.2.00, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release:

- Brocade SLX 9850-4 router
- Brocade SLX 9850-8 router
- Brocade SLX 9540 switch

To obtain information about other Brocade OS versions, refer to the documentation specific to that version.

Interface module capabilities

The following table lists the supported capabilities for the following Brocade SLX 9850 interface modules:

- BR-SLX9850-10Gx72S-M
- BR-SLX9850-100Gx36CQ-M
- BR-SLX9850-10Gx72S-D
- BR-SLX9850-100Gx36CQ-D

TABLE 1 Brocade SLX 9850 interface modules capabilities

Capability	Modular interface module
MPLS	Yes
Packet Buffer memory per interface module	12GB (BR-SLX9850-10Gx72S-M) 36GB (BR-SLX9850-100Gx36CQ-M) 8GB (BR-SLX9850-10Gx72S-D) 24GB (BR-SLX9850-100Gx36CQ-D)

What's new in this document

The following table includes descriptions of new information added to this guide for the SLX OS 17r.2.00 software release.

NOTE

On October 30, 2017, Extreme Networks, Inc. acquired the SLX-OS product line from Brocade Communications Systems, Inc. This transitional release includes references to both companies.

TABLE 2 Summary of enhancements in SLX OS release 17r.2.00

Feature	Description	Described in
Guest VM storage	Updated the guest VM storage to 256GB.	Refer to Supported third-party applications, packages, and hardware topic.
TCAM sharing	Under supported TCAM profiles, you can enable sharing of TCAM resources for each security ACL or PBR ACL applied to multiple ports.	Refer to TCAM sharing topic.
Network Time Protocol Server Overview	An Network Time Protocol (NTP) server provides the correct network time on your device. NTP can be used to synchronize the time on devices across a network.	Refer to Network time protocol topic.
Network Time Protocol Client Overview	The NTP client maintains the server and peer state information as association.	Refer to Network time protocol topic.
Network Time Protocol Associations	Network Time Protocol work in one or more association modes.	Refer to Network time protocol topic.

For complete information, refer to the *SLX-OS 17r.2.00 Release Notes*.

Configuration Fundamentals

• Configuration files.....	13
• Session connection.....	18
• Ethernet management interfaces.....	25
• Configuring IPv6 address on SLX platform.....	26
• Configuring management IP addresses.....	29
• Port management.....	30
• Interface Ethernet ports.....	39
• Slots and modules.....	40
• Chassis and host names.....	43
• System clock.....	45
• Management VRFs.....	45
• Zero Touch Provisioning.....	47
• MAC address aging.....	55
• TCAM application-resource monitoring.....	55
• Hardware profiles.....	56

Configuration files

Brocade devices support three types of configuration files, default, startup, and running configuration files.

The startup configuration resides in the `/var/config/vcs/scripts` directory. Though the default configuration files are physically present in this directory, they are linked to the directory from their actual location.

When you boot up a device for the first time, the running configuration is identical to the startup configuration. As you configure the device, the changes are written to the running configuration. To save the changes, you must save the currently effective configuration (the running configuration) as the startup configuration. When the device reboots, the configuration changes become effective.

Default configuration files

Default configuration files are part of the firmware package for the device and are automatically applied to the startup configuration under the following conditions:

- When the device boots up for the first time and no customized configuration is available.
- When you restore the default configuration.

You cannot remove, rename, or change the default configuration. The default configuration file names are as follows:

- `defaultconfig.standalone`
- `defaultconfig.cluster`

Startup configuration files

The startup configuration is persistent. It is applied when the system reboots.

- When the device boots up for the first time, it uses the default configuration as the startup configuration, depending on the mode.
- When you make configuration changes to the running configuration and save the changes to the startup configuration with the **copy** command, the running configuration becomes the startup configuration.

The startup configuration file name is startup-config.

Running configuration files

The configuration currently effective on the device is referred to as the running configuration. Any configuration change you make while the device is online is made to the running configuration.

- The running configuration is nonpersistent.
- To save configuration changes, you must copy the running configuration to the startup configuration. If you are not sure about the changes, you can copy the changes to a file, and apply the changes later.

The running configuration file name is running-config.

Displaying configurations

The following examples illustrate how to display the default, startup, and running configurations, respectively.

Displaying the default configuration

To display the default configuration, enter the **show file** command with the default configuration filenames in privileged EXEC mode.

```
device# show file defaultconfig.standalone
device# show file defaultconfig.cluster
```

Displaying the startup configuration

To display the contents of the startup configuration, enter the **show startup-config** command in privileged EXEC mode.

```
device# show startup-config
```

Displaying the running configuration

To display the contents of the running configuration, enter the **show running-config** command in the privileged EXEC mode.

```
device# show running-config
```

Saving configuration changes

Configuration changes are nonpersistent and are lost on reboot unless you save them permanently. You have two options for saving configuration changes:

- Copy the running configuration to the startup configuration. The changes become effective upon reboot.
- Copy the running configuration to a file, and apply it at some later date.

NOTE

Always make a backup copy of your running configuration before you upgrade or downgrade the firmware.

Saving the running configuration

To save the configuration changes you made, copy the running configuration to the startup configuration. The next time the device reboots, it uses the startup configuration and the changes you made earlier become effective.

Enter the **copy running-config startup-config** command in privileged EXEC mode.

```
device# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [Y/N]: y
```

Saving the running configuration to a file

If you want to save the changes you made to the configuration, but you do not want the changes to take effect when the device reboots, you can save the running configuration to a file. You can apply the changes at some later time.

Enter the **copy running-config** command in privileged EXEC mode. Specify the file name as the file URL.

```
device# copy running-config flash://myconfig
```

Verify the transaction by listing the directory contents.

```
device# dir
total 32
drwxr-xr-x 2 251 1011 4096 Jun 5 07:08 .
drwxr-xr-x 3 251 1011 4096 Mar 11 00:00 ..
-rw-r--r-- 1 root sys 410 Jun 3 00:56 defaultconfig.standalone
-rw-r--r-- 1 root sys 695 Jun 3 00:56 defaultconfig.cluster
-rw-r--r-- 1 root root 183118 Jun 7 12:19 myconfig
-rw-r--r-- 1 root root 185650 Jun 5 09:38 startup-config
```

Applying previously saved configuration changes

When you are ready to apply the configuration changes you previously saved to a file, copy the file (*myconfig* in the example) to the startup configuration. The changes take effect after the device reboots.

Enter the **copy** command in privileged EXEC mode. Specify the file name as the file URL followed by the **startup-config** keyword.

```
device# copy flash://myconfig startup-config
This operation will modify your startup configuration. Do you want to continue? [Y/N]: y
```

Backing up configurations

Always keep a backup copy of your configuration files, so you can restore the configuration in the event the configuration is lost or you make unintentional changes.

The following recommendations apply:

- Upload the configuration backup copies to an external host or to an attached Brocade-branded USB device.

NOTE

USB access is always to the locally active management module (MM).

- Avoid copying configuration files from one device to another. Instead restore the device configuration files from the backup copy.

Copying a configuration file to an external host

You can copy the startup-config or running-config file to a remote server through FTP, SCP, TFTP, or SFTP.

In the following example, the startup configuration is copied to a file on a remote server by means of FTP.

```
device# copy startup-config ftp://admin:*****@10.34.98.133//archive/startup-config_device24-08_20101010
```

Backing up the startup configuration to a USB device

When you make a backup copy of a configuration file on an attached USB device, the destination file is the file URL on the USB device. You do not need to specify the target directory. The file is automatically recognized as a configuration file and stored in the default configuration directory.

1. Enable the USB device.

```
device# usb on
USB storage enabled
```

2. Enter the **copy startup-config** command with the destination file name.

```
device# copy startup-config usb://startup-config_slx-08_20160510
```

Configuration restoration

Restoring a configuration involves overwriting a given configuration file on the device by downloading an archived backup copy from an external host or from an attached USB device.

All interfaces remain online. The following parameters are unaffected:

- Interface management IP address
- Software feature licenses installed on the device
- Virtual IP address

NOTE

USB access is always to the locally active management module (MM).

Restoring the default configuration

This restoration procedure resets the configuration to the factory defaults. The default configuration files are always present on the device and can be restored with the **copy** command.

To restore the default configuration, perform the following procedure in privileged EXEC mode.

1. Enter the **copy default-config startup-config** command to overwrite the running configuration with the default configuration.

```
device# copy default-config startup-config
```

2. Confirm that you want to make the change by entering Y when prompted.

```
This operation will modify your startup configuration. Do you want to continue? [Y/N]: y
```

3. Reboot the device.

```
device# reload system
```

Managing flash files

The Brocade device provides a set of tools for removing, renaming, and displaying files you create in the device flash memory. You can use the display commands with any file, including the system configuration files. The **rename** and **delete** commands only apply to copies of configuration files you create in the flash memory. You cannot rename or delete any of the system configuration files.

Listing the contents of the flash memory

To list the contents of the flash memory, enter the **dir** command in privileged EXEC mode.

```
device# dir
total 572
drwxr-xr-x 2 251 1011 4096 Jun 5 07:08 .
drwxr-xr-x 3 251 1011 4096 Mar 11 00:00 ..
-rw-r--r-- 1 root sys 410 Jun 3 00:56 defaultconfig.standalone
-rw-r--r-- 1 root sys 695 Jun 3 00:56 defaultconfig.cluster
-rw-r--r-- 1 root root 185650 Jun 5 09:38 startup-config
```

Deleting a file from the flash memory

To delete a file from the flash memory, enter the **delete** command with the file name in privileged EXEC mode.

```
device# delete myconfig
```

NOTE

You cannot delete a system configuration file in flash memory.

Renaming a flash memory file

To rename a file in the flash memory, enter the **rename** command with the source and destination file names in privileged EXEC mode.

```
device# rename myconfig myconfig_20101010
```

NOTE

You cannot rename a system configuration file in flash memory.

Viewing the contents of a file in the flash memory

To investigate the contents of a file in the flash memory, enter the **show file** command with the file name in privileged EXEC mode.

```
device# show file defaultconfig.cluster
vlan dot1q tag native
!
cee-map default
remap fabric-priority priority 0
remap lossless-priority priority 0
priority-group-table 15.0 pfc off
priority-group-table 1 weight 40 pfc on
priority-group-table 2 weight 60 pfc off
priority-table 2 2 2 1 2 2 2 15.0
!
!
port-profile default
vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
!
protocol lldp
!
!
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging auditlog class SECURITY
!
end
```

NOTE

To display the contents of the running configuration, use the **show running-config** command. To display the contents of the startup configuration, use the **show startup-config** command.

Rebooting the device

You can reboot the management module or the chassis.

**CAUTION**

All reboot operations are disruptive, and the commands prompt for confirmation before executing. When you reboot a device, all traffic to and from it stops. All ports on that device remain inactive until the device comes back online.

NOTE

During the boot process system initialization, configuration data (default or user-defined) are applied to the device through configuration replay.

- The **fastboot** commands only reboots the management module on which the command is executed. Any unsaved configurations are lost. If you log in to the device IP address and enter this command, only the active management module reboots and POST is bypassed.

```
device# fastboot
```

- The **reload system** command performs a cold reboot that powers off and restarts the entire chassis. All session connections must be restarted. If the power-on self-test (POST) is enabled, POST is executed when the system comes back up.

```
device# reload system
```

Session connection

You can connect to your device through a console session on the serial port, or through a Telnet or Secure Shell (SSH) connection to the management port or the inband port belonging to either the mgmt-vrf or default-vrf Virtual Routing and Forwarding (VRF). You can use any account login present in the local device database or on a configured authentication, authorization, and accounting (AAA) server for authentication. For initial setup procedures, use the pre-configured administrative account that is part of the default device configuration.

The device must be physically connected to the network. If the device network interface is not configured or the device has been disconnected from the network, use a console session on the serial port.

Refer to the appropriate hardware guide for information on connecting through the serial port and establishing an Ethernet connection for a console session.

Telnet

Telnet allows access to management functions on a remote networking device. Unlike SSH, Telnet does not provide a secure, encrypted connection to the device.

Telnet support is available in privileged EXEC mode on all Brocade platforms. The device supports a maximum of 32 CLI sessions. Both IPv4 and IPv6 addresses are supported.

The Telnet service is enabled by default on the device. When the Telnet server is disabled, remote access to the device is restricted. Existing inbound Telnet connections are terminated and access to the device by additional inbound connections is not allowed until the

Telnet server is re-enabled. If you have admin privileges, you can disable and re-enable inbound Telnet connections from global configuration mode.

NOTE

Outgoing Telnet connections from the device to any remote device are not affected by disabling or enabling the Telnet server in the device.

NOTE

When using Telnet, the root ID is blocked and you cannot login as root.

The following features are not supported with Telnet:

- Displaying Telnet sessions
- Terminating hung Telnet sessions

NOTE

Telnet/SSH from standby to outside is not allowed.

Connecting to a Brocade device with Telnet

You can use the Telnet service to connect to the Brocade device.

A Telnet session allows you to access a device remotely using port 23. However, it is not secure. If you need a secure connection, use SSH.

1. Establish a Telnet session to the Brocade device from a remote device.

```
client# telnet 10.17.37.157
```

The example establishes a Telnet session to the device with the IP address of 10.17.37.157.

If the device is active and the Telnet service is enabled on it, a display similar to the following appears.

```
Trying 10.17.37.157...
Connected to 10.17.37.157.
Escape character is '^]'.
```

2. Once you have established the Telnet connection, you can log in normally.

```
device login: admin
Password:
SECURITY WARNING: The default password for at least
one default account (root, admin and user) have not been changed.

Welcome to the Brocade SLX-OS Software
admin connected from 10.252.24.5 using telnet on device
device#
```

NOTE

The default admin login name is admin. The default user name is user. The default password for both admin and user accounts is password.

Brocade recommends that you change the default account password when you log in for the first time. For more information on changing the default password, refer to the *Brocade SLX-OS Security Configuration Guide*.

Connecting to a remote device with Telnet

You can connect to a remote server from the device using a Telnet connection.

A Telnet session is not secure. If you need a secure connection, use SSH.

To connect to a remote server with Telnet, perform the following steps:

1. Establish a Telnet session connection to the remote device.

```
device# telnet 10.20.51.68 vrf mgmt-vrf
```

The example establishes a Telnet session to a device with the IP address of 10.20.51.68.

You can override the default port by using the **port-number** *port* option. However, the device must be listening on this port for the connection to succeed.

If the device is active and the Telnet service is enabled on it, a display similar to the following appears.

```
/fabos/cliexec/vrfcmd 0 /usr/bin/telnet 10.20.51.68 23
Trying 10.20.51.68...
Connected to 10.20.51.68.
Escape character is '^]'.
...
device login:
```

2. Once you have established the Telnet connection, you can log in normally.

Shutting down and re-enabling the Telnet service

The Telnet service is enabled by default. Shutting down the Telnet service forcibly disconnects all Telnet sessions running on a device.

To shut down and then re-enable the Telnet service, perform the following steps.

1. In privileged EXEC mode, enter global configuration mode.

```
device# configure terminal
```

2. To shut down the Telnet service on the device, enter **telnet server shutdown**.

```
device(config)# telnet server shutdown
```

All Telnet sessions including any currently active sessions are immediately terminated, and cannot be re-established until the service is re-enabled.

3. To re-enable the Telnet service on the device, enter **no telnet server shutdown**.

```
device(config)# no telnet server shutdown
```

SSH

Secure Shell (SSH) allows secure access to management functions on a remote networking device. Unlike Telnet, which offers no security, SSH provides a secure, encrypted connection to the device.

SSH support is available in privileged EXEC mode on all Brocade platforms. The device supports a maximum of 32 CLI sessions. Both IPv4 and IPv6 addresses are supported.

The SSH service is enabled by default on the device. When the SSH server is disabled, remote access to the device is restricted. Existing inbound SSH connections are terminated and access to the device by additional inbound connections are not allowed until the SSH

server is re-enabled. If you have admin privileges, you can disable and re-enable inbound SSH connections from global configuration mode.

NOTE

Outgoing SSH connections from the device to any remote device are not affected by disabling or enabling the SSH server in the device.

NOTE

When using SSH, the root ID is blocked and you cannot login as root.

NOTE

Telnet/SSH from standby to outside is not allowed.

Feature support for SSH

SSHv2 is the supported version of SSH, but not all features typically available with SSHv2 are supported on the Brocade devices.

The following encryption algorithms are supported:

- **3des-cbc** Triple-DES (default)
- **aes256-cbc** : AES in Cipher Block Chaining (CBC) mode with 256-bit key
- **aes192-cbc** : AES in CBC mode with 192-bit key
- **aes128-cbc** : AES in CBC mode with 128-bit key
- **aes256-gcm** : AES in Galios/Counter Mode (GCM) mode with 256-bit key
- **aes192-gcm** : AES in GCM mode with 192-bit key
- **aes128-gcm** : AES in GCM mode with 128-bit key
- **aes256-ctr** : AES in Counter Mode (CTR) mode with 256-bit key
- **aes192-ctr** : AES in CTR mode with 192-bit key
- **aes128-ctr** : AES in CTR mode with 128-bit key

The following Hash-based Message Authentication Code (HMAC) message authentication algorithms are supported:

- **hmac-md5** : MD5 encryption algorithm with 128-bit key (default).
- **hmac-sha1** : SHA1 encryption algorithm with 160-bit key.
- **hmac-sha2-256** : SHA2 encryption algorithm with 256-bit key.
- **hmac-sha2-512** : SHA2 encryption algorithm with 512-bit key.

The following host keys are supported:

- ssh-dsa
- ssh-rsa
- ECDSA

The following key exchange algorithms are supported:

- diffie-hellman-group-exchange-sha256
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1

SSH user authentication is performed with passwords stored on the device or on an external authentication, authorization, and accounting (AAA) server.

The following features are not supported with SSH:

- Displaying SSH sessions
- Deleting stale SSH keys

Connecting to a Brocade device with SSH

You can use SSH to connect to the Brocade device.

An SSH session allows you to access a device remotely using port 22.

1. Establish an SSH session connection to the Brocade device.

```
client# ssh admin@10.17.37.157
```

The example establishes an SSH session to the device with the IP address of 10.17.37.157.

2. Enter yes if prompted.

```
The authenticity of host '10.17.37.157 (10.17.37.157)' can't be established.
RSA key fingerprint is 9f:83:62:cd:55:6c:b9:e8:1d:79:ab:b4:04:f4:f6:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.17.37.157' (RSA) to the list of known hosts.
admin@10.17.37.157's password:
```

```
SECURITY WARNING: The default password for at least
one default account (root, admin and user) have not been changed.
```

```
Welcome to the Brocade SLX-OS Software
admin connected from 10.70.4.113 using ssh on device
device#
```

NOTE

The default admin login name is admin. The default user name is user. The default password for both admin and user accounts is password.

Brocade recommends that you change the default account password when you log in for the first time. For more information on changing the default password, refer to the *Brocade SLX-OS Security Configuration Guide*.

Connecting to a remote server with SSH

You can connect to a remote server from the device using the SSH (Secure Socket Handling) protocol to permit a secure (encrypted) connection.

To connect to a remote server with SSH, perform the following steps:

1. Establish an SSH connection with the login name and IP address for the remote server.

```
device# ssh 10.20.51.68 -l admin vrf mgmt-vrf
```

You can use the **-m** and **-c** options to override the default encryption and hash algorithms

2. Enter **yes** if prompted.

```
The authenticity of host '10.20.51.68 (10.20.51.68)' can't be established.
RSA key fingerprint is ea:32:38:f7:76:b7:7d:23:dd:a7:25:99:e7:50:87:d0.
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '10.20.51.68' (RSA) to the list of known hosts.
admin@10.20.51.68's password: *****
```

```
SECURITY WARNING: The default password for at least
one default account (root, admin and user) have not been changed.
Welcome to the Brocade SLX-OS Software
admin connected from 10.20.51.66 using ssh on C60_68F
```

Managing SSH public keys

You can import SSH public keys to establish an authenticated login for a device. You can also delete the key from the device to prevent it from being used for an authenticated login.

To manage the SSH keys, perform the following steps:

1. In privileged EXEC mode, import an SSH public key to the device.

```
device# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/bmeenaks/.ssh
file id_rsa.pub login fvt
```

This example imports the SSH public key for the admin user from the remote 10.70.4.106 host using the directory and file information to the key.

2. Enter the password for the user.

```
Password: *****
```

When the SSH key is imported, the following message appears.

```
device# 2016/01/14-10:28:58, [SEC-3050], 75,, INFO, SLX9850-4, Event: sshutil, Status: success,
Info: Imported SSH public key from 10.70.4.106 for user 'admin'.
```

3. Delete an SSH public key from the device prevents it from being used.

```
device# no certutil sshkey user admin
```

This example deletes the SSH key for the admin user.

Shutting down and re-enabling the SSH service

The SSH service is enabled by default. Shutting down the SSH service forcibly disconnects all SSH sessions running on a device.

To shut down and then re-enable the SSH service, perform the following steps.

1. In privileged EXEC mode, enter global configuration mode.

```
device# configure terminal
```

2. Shut down the SSH service on the device.

```
device(config)# ssh server shutdown
```

All SSH sessions are immediately terminated, and cannot be re-established until the service is re-enabled.

3. To re-enable the SSH service on the device, enter **no ssh server shutdown**.

```
device(config)# no ssh server shutdown
```

Configuring the terminal session parameters

You can set the terminal parameters for the current session. You can also set password attributes for the length of the session and login attempts.

To set the parameters, perform the following steps:

1. In privileged EXEC mode, set the display length.

```
device# terminal length 30
```

This example sets the lines to be displayed on the terminal session at 30 lines.

2. Set the timeout length.

```
device# terminal timeout 60
```

This example sets the timeout of 60 minutes for the terminal session.

3. Access global configuration mode.

```
device# configure terminal
```

4. Configure the maximum login attempts to establish a session.

```
device(config)# password-attributes max-retry 4
```

This example sets the maximum login attempts of four to establish a session.

5. Set the maximum number of minutes after which the user account is unlocked.

```
device(config)# password-attributes admin-lockout max-lockout-duration 5
```

This example specifies that the user account be unlocked after 5 minutes.

The following configuration is the example of the previous steps.

```
device# terminal length 30
device# terminal timeout 60
device# configure terminal
device(config)# password-attributes max-retry 4
device(config)# password-attributes admin-lockout max-lockout-duration 5
```

Configuring a login banner

The Brocade device can be configured to display a greeting message on user terminals as a banner when they enter the Privileged EXEC CLI level or access the device through Telnet.

Complete the following steps to set and display a banner.

1. In privileged EXEC mode, access global configuration mode.

```
device# configure terminal
Entering configuration mode terminal
```


2. Configure the login banner.

```
device(config)# banner login "Please do not disturb the setup on this device"
```

This example configure a text message on a single line by enclosing the text in double quotation marks (" ").

The banner can be up to 2048 characters long. To create a multi-line banner, enter the **banner login** command followed by the **Esc-m** keys. Enter **Ctrl-D** to terminate the input.

You can use the **no banner login** command to remove the banner.

3. Verify the configured banner.

```
device(config)# do show running-config banner
```

The configured banner is displayed.

```
banner login "Please do not disturb the setup on this device"
```

The following example is the configuration of the previous steps.

```
device# configure terminal
Entering configuration mode terminal
device(config)# banner login "Please do not disturb the setup on this device"
```

Ethernet management interfaces

The Ethernet network interface provides management access, including direct access to the device CLI. You must configure at least one IP address using a serial connection to the CLI before you can manage the system with other management interfaces. You can either configure static IP addresses, or you can use a Dynamic Host Configuration Protocol (DHCP) client to acquire IP addresses automatically. For IPv6 addresses, both static IPv6 and stateless IPv6 autoconfiguration are supported.

ATTENTION

Setting static IPv4 addresses and using DHCP are mutually exclusive. If DHCP is enabled, remove the DHCP client before you configure a static IPv4 address. However, this does not apply to IPv6 addresses.

Configuring a static Ethernet address

You can configure IPv4 and IPv6 static Ethernet network interface addresses in environments where the DHCP service is not available.

Before you configure a static address, connect to the device through the serial console.

To configure static Ethernet network interface addresses, perform the following steps:

1. In privileged EXEC mode, enter global configuration mode.

```
device# configure terminal
```

2. Access the interface management mode for the management interface.

```
device(config)# interface Management 1
```

This interface uses the default mgmt-vrf VRF.

3. Disable DHCP.

```
device(config-Management-1)# no ip address dhcp
```

- Configure the IP address for the management interface.

```
device(config-Management-1)# ip address 10.24.85.81/20
```

- If you are going to use an IPv6 address, configure the address.

```
device(config-Management-1)# ipv6 address 2001:DB8::69bc:832:e61f:13ff:fe67:4b94/32
```

- Verify the configuration.

```
device(config-Management-1)# do show running-config interface Management 1
interface Management 1
  no ip address dhcp
  ip address 10.24.85.81/20
  ipv6 address 2001:DB8::69bc:832:e61f:13ff:fe67:4b94/32
!
```

The following example is the configuration of the previous steps.

```
device# configure terminal
device(config)# interface Management 1
device(config-Management-1)# no ip address dhcp
device(config-Management-1)# ip address 10.24.85.81/20
device(config-Management-1)# ipv6 address 2001:DB8::69bc:832:e61f:13ff:fe67:4b94/32
```

Displaying a management interface

You can display the information about a management interface on the device. If an IP address has not been assigned to the network interface, you must connect to the CLI using a console session on the serial port. Otherwise, connect to the device through Telnet or SSH.

```
device# show interface Management 1
interface Management 1
  line-speed actual "1000baseT, Duplex: Full"
  line-speed configured Auto
  oper-status up
  ip address "static 10.20.161.66/20"
  ipv6 ipv6-address [ "static 2620:100:0:f814:10:20:161:66/64 preferred" ]
```

Configuring IPv6 address on SLX platform

Following are the basic prerequisites for configuring IPv6 address on SLX platform:

- SLX chassis with management modules.
- PC with reachability to the serial port of the active management module.
- IPv6 network assignment with a netmask and router address from the network administrators. This will generally be a /64 network.

NOTE

If you are provided an IPv6 prefix with a /65 to /128 netmask, assign the addresses according to your network administrator's direction, and do NOT follow this procedure.

NOTE

SLX platforms without redundant management modules only need to configure the M 1 interface.

To configure IPv6 addresses, perform the following steps:

1. Enter the show system command to know the STACK MAC and the BURNED IN MAC for each MM present in the system.

```
device# show system
Stack MAC           : 60:9c:9f:60:88:00

  -- UNIT 0 --
Unit Name           : 9850-8
Switch Status       :
Hardware Rev        :
Up Time             : up 21:00
Current Time        : 23:08:49 GMT
SLX-OS Version      : 17r.1.00
Jumbo Capable       : yes
Burned In MAC       : MM1 [60:9c:9f:46:e2:06]MM2 [60:9c:9f:47:10:7a]
Management IP       : 10.25.101.4
Management Port Status : UP
```

The MAC addresses are used to create the IPv6 SLAAC address for the following mapping:

- MM1 MAC - IPv6 address for interface M 1
- MM2 MAC - IPv6 address for interface M 2
- Stack MAC - IPv6 address for chassis virtual-ipv6

2. Convert each MAC address to a modified EUI-64 format, and then into the final IPv6 address for the interfaces by performing the following steps:

- a) Remove any punctuation from the MAC.

```
609c9f46e206
```

- b) Insert **fffe** after the first 6 characters.

```
609c9ffffe46e206
```

- c) Using a calculator application in HEX Mode on a PC, do a Bitwise OR operation of the modified MAC with 0200000000000000.

```
629c9ffffe46e206
```

- d) Convert the result to IPv6 format by inserting colons after every 4 characters from the right hand side.

```
629c:9fff:fe46:e206
```

- e) Prepare the IPv6 network information for use. This example uses a sample network of 2001:DB8::/32 provided by the Admin.

- Normalize the address to a fully expanded format.

```
2001:0DB8:0000:0000:0000:0000:0000:0000/32
```

- Remove the cidr notation.

```
2001:0DB8:0000:0000:0000:0000:0000:0000
```

- Remove the host portion of the address based on a /64 netmask.

```
2001:0DB8:0000:0000:
```

- Contract the remaining portion of the address of any leading zeros.

```
2001:DB8::
```

- f) Combine the IPv6 network prefix from step 2e and the result of step 2d to make the IPv6 address.

```
2001:DB8::629c:9fff:fe46:e206/32
```

- g) Repeat steps 2a to 2f for each MAC address.

3. Apply the addresses to the appropriate interfaces and configure the default route using the router address provided by the network administrator.

For more information, refer to [Configuring management IP addresses](#) on page 29.

Configuring management IP addresses

Management address configuration provides basic connectivity (such as SSH/telnet) to the device so that the device can be managed from various networks.

To configure management IPv4 and IPv6 addresses, perform the following steps:

1. In privileged EXEC mode, enter global configuration mode.

```
device# configure terminal
```

2. Configure IPv4 address and/or IPv6 address for the chassis.
 - Assign chassis virtual IPv4 address.

```
device(config)# chassis virtual-ip 10.25.101.4/22
```

- Assign chassis virtual IPv6 address.

```
device(config)# chassis virtual-ipv6 2001:DB8::629c:9ff:fe60:8800/32
```

Note that the chassis virtual-ipv6 address cannot be a link local address.

3. Access the interface management mode for the management interface.

```
device(config)# interface management 1
```

4. Assign the interface to the management VRF.

```
device(config-Management-1)# vrf forwarding mgmt-vrf
```

5. Disable DHCP.

```
device(config-Management-1)# no ip address dhcp
```

6. Assign IPv4 address and/or IPv6 address for the management interface MM1.
 - Assign IPv4 address.

```
device(config-Management-1)# ip address 10.25.101.29/22
```

- Assign IPv6 address.

```
device(config-Management-1)# ipv6 address 2001:DB8::629c:9fff:fe46:e206/32
device(config-Management-1)# exit
```

Note that, the IPv6 address cannot be a link local address.

Repeat steps 3 to 6 to assign different IPv4 and IPv6 addresses to MM2.

7. Configure the management VRF routes.

- IPv4 address.

```
device(config)# vrf mgmt-vrf
device(config-vrf-mgmt-vrf)# address-family ipv4 unicast
device(vrf-mgmt-vrf-ipv4-unicast)# ip route 0.0.0.0/0 10.25.100.1
```

- IPv6 address.

```
device(config)# vrf mgmt-vrf
device(config-vrf-mgmt-vrf)# address-family ipv6 unicast
device(vrf-mgmt-vrf-ipv6-unicast)# ipv6 route ::/0 2001:DB8::
```

Note that 6 unique addresses have to be used, and routes configured. The chassis virtual ip address (IPv4 and IPv6) are used for normal connectivity of the SLX (IE SSH/telnet) and is serviced/owned by the active MP. This means that the chassis-virtual IP is the primary address of the SLX management interfaces, not M 1 and M 2.

Port management

The Brocade device allows the port management of the Brocade SLX 9850 36x100G line card (LC), Brocade SLX 9850 72X10G line card, and features for interface Ethernet ports.

- Brocade SLX 9850 36x100G line card (LC) port management includes following:
 - 40G break-out to configure any 40G port in 36x100G LC as four 10G ports
 - 40G or 100G dual-speed port groups
- Brocade SLX 9540 port management includes the following:
 - Supports 54 ports in total. Ports 1 - 48 support 10G, 1G and 100 Mbps speed (default is 10G).
 - Ports 49-54 support 40G, 100G; and also support 4x10G and 4x25G breakout configurations. Default is 100G.
 - Forward Error Correction (FEC) is supported only in 100G mode.
- Interface Ethernet port management features discussed this section include the following:
 - Port transition hold timer
 - Port flap dampening
 - Link fault signaling

SLX 9850 36x100G LC ports

The SLX 9850 36x100G line card (LC) has six port groups with 10 ports each for a total of 60 ports. By default, each port group has six ports that are configured for 100G. The remaining ports are inactive.

On a port group, you can configure dual speed and breakout mode support.

- Dual speed support allows you to configure the ports in a port group as 40G, supporting QSFP+ optics. With this configuration, all ports in the group become active.
- Breakout mode support allows you to break out each 40G port into four 10G ports.

The following example displays the slot information for all slots in the chassis. The SLX 9850 36x100G line cards are in slots L1, L3, and L4.

```
device# show slots
Slot  Type      Description          ID      Status
-----
M1    MM v5      Management Module   179    ENABLED
M2
S1
VACANT
VACANT
```

S2	SFM4 v4	Switch Fabric Module	183	ENABLED
S3				VACANT
S4	SFM4 v4	Switch Fabric Module	183	ENABLED
S5	SFM4 v4	Switch Fabric Module	183	ENABLED
S6				VACANT
L1	LC36x100G v3	36-port 100GE card	181	ENABLED
L2	LC72X10G v5	72-port 10GE card	180	ENABLED
L3	LC36x100G v3	36-port 100GE card	181	ENABLED
L4	LC36x100G v3	36-port 100GE card	181	ENABLED

Limitations and considerations

- This LC can support 10G, 40G and 100G port speeds.
- Ports 1-6, 8-13, 15-20, 41-46, 48-53, and 55-60 can be configured as 100G ports.
- Ports 7, 14, 21-40, 47, 54 are 40G ports only.
- Both dual speed and breakout mode changes require the reload of the line card.

Configuring dual-speed ports

By default, six ports of a 36X100G port group are configured as 100G and the remaining four are inactive. You can configure the ports in a port group as 40G and activate all 10 ports.

Before performing the following procedure, you can display the port groups and their ports by using the **show hardware port-group** command.

```
device# show hardware port-group
Port-Group          Port
=====
3/1                 3/1 ,2 ,3 ,4 ,5 ,6 ,7 ,26 ,27 ,28
3/2                 3/8 ,9 ,10 ,11 ,12 ,13 ,29 ,30 ,31 ,32
3/3                 3/15 ,16 ,17 ,18 ,19 ,20 ,14 ,33 ,34 ,35
3/4                 3/41 ,42 ,43 ,44 ,45 ,46 ,21 ,22 ,23 ,24
3/5                 3/48 ,49 ,50 ,51 ,52 ,53 ,25 ,36 ,47 ,54
3/6                 3/55 ,56 ,57 ,58 ,59 ,60 ,37 ,38 ,39 ,40
```

* Only the first six ports in each group are 100g capable ports

Perform the following steps to configure the ports in a port group:

1. From privileged EXEC mode, power off the line card.

```
device# power-off linecard 3
```

Before changing the port speed, you must power off the LC.

NOTE

The interface and its current configuration will still exist in the configuration, displayed by the **show running-config** command, but operational commands do not display interfaces on this line card.

2. Access global configuration mode.

```
device# configure terminal
```

3. Access hardware configuration mode.

```
device(config)# hardware
```

4. Access the port group mode for the port group that you want to configure.

```
device(config-hardware)# port-group 3/1
```

- Configure the speed of the ports in the group to 40G.

```
device(config-port-group-3/1)# mode 40g
%Warning: port-group mode is a disruptive command.
Please power-cycle the line-card for the changes to take place
```

To reset the port speed to 100G, use the **mode 100g** command.

- Access privileged EXEC mode.

```
device(config-port-group-3/1)# Ctrl-z
```

NOTE

You can configure more than one port group on a LC before restoring its power.

- Restore power to the line card.

```
device# power-on linecard 3
```

- Verify the configuration.

```
device# show running-config hardware port-group
hardware
port-group 3/1
mode 40g
!
```

The following example shows the steps of the previous configuration.

```
device# power-off linecard 3
device# configure terminal
device(config)# hardware
device(config-hardware)# port-group 3/1
device(config-port-group-3/1)# mode 40g
%Warning: port-group mode is a disruptive command.
Please power-cycle the line-card for the changes to take place
device(config-port-group-3/1)# Ctrl-z
device# power-on linecard 3
```

SLX 9540 100G ports

The SLX 9540 has six 100G ports (ports 49-54) and by default, each port is in 100G mode.

User can configure 40G mode using the **speed 40000** command in interface configuration mode. Each 100G port also supports 4x25G and 4x10G breakout configurations, whereas SLX 9850 supports only 4x10G breakout. Breakout configuration is same as SLX 9850.

Configuring breakout mode

You can configure any 40G port on the 36X100G LC as four 10G ports and SLX 9540 supports 4x25 and 4x10G breakout configurations.

Before performing the following procedure, you can view the ports in the chassis and their status, use the **show interface brief** command:

Interface	IP-Address	Vrf	Status	Protocol
Port-channel 1	unassigned		administratively down	down
Port-channel 2	unassigned		administratively down	down
Ethernet 3/1	unassigned	default-vrf	up	up


```

...
Ethernet 3/72          unassigned default-vrf    up          down
Ethernet 3/125         unassigned default-vrf    up          down
Ethernet 3/126         unassigned default-vrf    up          down

```

Perform the following steps:

1. In privileged EXEC mode, power off the appropriate line card.

```
device# power-off linecard 4
```

NOTE

The interface and its current configuration will still exist in the configuration, displayed by the **show running-config** command, but operational commands will not display interfaces on this line card.

2. Access global configuration mode.

```
device# configure terminal
```

3. Access hardware configuration mode.

```
device(config)# hardware
```

4. Access the connector configuration mode for the port you wish to break out.

```
device(config-hardware)# connector 4/2
```

5. Configure the port into four 10G ports.

```
device(config-connector-4/2)# breakout mode 4x10g
%Warning: Sfp Breakout is a disruptive command.
Please save the running-config to startup-config and use reload command on the device or power-cycle
linecard on Chassis system for the changes to take effect.
```

6. Access privileged EXEC mode.

```
device(config-connector-4/2)# Ctrl-z
```

7. Restore power to the line card.

```
device# power-on linecard 4
```

NOTE

The SFP interfaces come up under the new mode with default configurations. Unaffected interfaces retain the configurations they had before the line card was powered off.

8. Verify the configuration.

```
device# show running-config hardware connector
hardware
connector 4/2
    breakout mode 4x10g
!
```

The following example shows the steps to configure breakout mode on 40G/100G port.

```
device# power-off linecard 4
device# configure terminal
device(config)# hardware
device(config-hardware)# connector 4/2
device(config-connector-4/2)# breakout mode 4x10g
%Warning: Sfp Breakout is a disruptive command.
Please save the running-config to startup-config and use reload command on the device or power-cycle
linecard on Chassis system for the changes to take effect.
device(config-port-group-4/2)# Ctrl-z
device# power-on linecard 4
```

10G/1G auto negotiation and auto detection mode

The Brocade SLX 9850 72X10G line card and SLX 9540 support 10G/1G auto negotiation and auto detection mode.

- Auto negotiation is supported on ports 1 to 24 on the front plate. However, ports 25 to 72 support 1G mode without auto negotiation.
- Auto detection occurs when the interface speed is configured based on the detected optic type.
- Only full duplex is supported in the CL37 auto-negotiation.

You can manually configure the port speed. In manual mode, the inserted optic must match the configured speed. Otherwise, the link will not come up. You can configure 1G mode with or without auto negotiation. The following speed matrix shows different combinations of modes on SLX 9850 and SLX 9540.

TABLE 3 Port speed matrix

	Ports 1 to 24 on SLX 9850 72x10G and Ports 1 to 48 on SLX 9540	Ports 25 to 72 on SLX 9850 72x10G
speed auto (default)	Auto-detection: <ul style="list-style-type: none"> • If 1G SFP optic is detected: Port is configured as 1G with 1000Base-X AN enabled. • If 1G SFP copper is detected: Port is configured as SGMII with 1000Base-T AN enabled; 1G, 100Mbps Full-Duplex advertised. • If 10G SFP is detected: port is configured as 10G 	Port is configured as 10G
speed 1000	Force to 1G mode, AN disabled	Force to 1G mode, AN disabled
speed 1000-auto	Force to 1G mode, AN enabled <ul style="list-style-type: none"> • If 1G SFP optic is detected: Port is configured as 1G with 1000Base-X AN enabled. • If 1G SFP copper is detected: Port is configured as SGMII with 1000Base-T AN enabled; 1G, 100Mbps Full-Duplex advertised. 	Configuration rejected
speed 10000	Force to 10G mode	Force to 10G mode
Speed 100	<ul style="list-style-type: none"> • If 1G SFP optic is detected: No configuration change; link stays down • If 1G SFP copper is detected: Port is configured as SGMII (AN enabled) but 1000Base-T AN disabled. 	Not supported
no speed	Equivalent to speed auto	Equivalent to speed auto

Configuring port speed and negotiation

You can configure the speed and negotiation for Brocade SLX 9850 72X10G line card ports.

In manual 1G or 10G mode, the inserted optic must match the configured speed.

Perform the following steps to change the port speed.

1. From privileged EXEC mode, access global configuration mode.

```
device# configure terminal
```

2. Access the interface configuration mode for the port that you want to configure.

```
device(config)# interface Ethernet 2/1
```

3. Change the port speed of interface, if required.

```
device(config-if-eth-2/1# speed 1000-auto
```

In this example, the port speed of interface 2/1 is changed from the default of 10G/1G auto detection mode to 1G with auto negotiation.

4. Activate the interface, if required.

```
device(config-if-eth-2/1)# no shutdown
```

5. Verify the configuration.

```
device(config-if-eth-2/1)# do show running-config interface ethernet 1/8
interface Ethernet 2/1
....
speed 1000-auto
no shutdown
!
```

The following example shows the steps in the previous configuration.

```
device# configure terminal
device(config)# interface Ethernet 2/1
device(config-if-eth-2/1)# speed 1000-auto
device(config-if-eth-2/1)# no shutdown
```

Port flap dampening

Port flap dampening allows you to configure a wait period before a port, whose link goes down then up, becomes enabled.

If the port link state toggles, from down to up or from up to down, for a specified number of times within a specified period, the interface is physically disabled for the specified wait period. Once the wait period expires, the port's link state is re-enabled. However, if the wait period is set to zero (0) seconds, or you want to re-enable the port before the wait period expires, the port must be manually re-enabled.

Configuring port flap dampening

By default, port flap dampening is disabled on the device. You can configure the threshold of link flapping to shut down the port and the time interval in which it remains shut down. This feature is available for all front ports on the device and is configured on the interface level.

Perform the following steps to configure port flap dampening:

1. From privileged EXEC mode, access global configuration mode.

```
device# configure terminal
```

2. Access the interface configuration mode for the port that you want to configure.

```
device(config)# interface Ethernet 1/4
```

3. Configure port flap dampening.

```
device(conf-if-eth-1/4)# link-error-disable 10 3 10
```

In this example, the values for the parameters are as follows:

- The toggle threshold is set to 10 times. The threshold is the number of times that the port's link state goes from up to down and down to up before the wait period is activated.
- The sampling time is set to 3 seconds. This time period is the amount of time during which the specified toggle threshold can occur before the wait period is activated.
- The wait time is set to 10 seconds. This period of time is the amount of time the port remains disabled (down) before it becomes enabled. Entering 0 indicates that the port will stay down until an administrative override occurs.

The following example shows the steps in the previous configuration.

```
device# configure terminal
device(config)# interface Ethernet 1/4
device(conf-if-eth-1/4)# link-error-disable 10 3 10
```

Port transition hold timer

The port transition hold timer delays the sending of port up or down events to Layer 2 protocols and prevents port link flapping from affecting upper layer protocols or applications. After the delay expires, the event is sent to the upper layer.

While link down events are reported immediately in the Syslog, their effect on higher level protocols such as OSPF is delayed according to how the hold timer is configured. When configured, the timer affects the physical link events. However, the resulting logical link events are also delayed.

NOTE

All LAG member ports must have the same delayed-link-event configuration.

NOTE

The delayed-link-event configuration is applicable only on a physical interface. It is not valid on a VLAN, VE, LAG, or loopback interfaces.

NOTE

The port transition hold timer does not take effect when the interface is administratively shut down.

Configuring the port transition hold timer

By default, the sending of an up or down port event is not delayed. You can configure a delay for either or both events.

Perform the following steps to configure the port transition hold timer:

1. From privileged EXEC mode, access global configuration mode.

```
device# configure terminal
```

2. Access the interface configuration mode for the port that you want to configure.

```
device(config)# interface Ethernet 4/2
```

3. Configure the port transition hold timer.

```
device(conf-if-eth-4/2)# delay-link-event 2 down
```

The polling iteration is 50 ms. In this example, 50 ms is multiplied by 2 and the sending of port down event is delayed by 100 ms. If the port is detected to be in the up state within the 100 ms, the delayed down event is cancelled.

You can specify a multiplier value from 1 to 200 for delay times from 50 ms to 10 seconds and a port event of **up**, **down**, or **both**.

4. Verify the configuration.

```
device(conf-if-eth-4/2)# do show running-config internet ethernet 4/2
interface Ethernet 4/2
...
delay-link-event 2 down
no shutdown
!
```

The following example shows the steps in the previous configuration.

```
device# configure terminal
device(config)# interface Ethernet 4/2
device(conf-if-eth-4/2)# delay-link-event 2 down
```

Link fault signaling

The Brocade SLX 9850 supports Link Fault Signaling (LFS) detection for interface types of 10G, 40G, 100G, and 40G breakout ports. It detects local and remote faults.

NOTE

LFS is not supported in 1G mode.

When the device detects a local fault, it returns a remote fault to the link partner. When the device detects a remote fault, it returns an idle state.

A port's physical link detection is independent of LFS detection. When either of these link fault signals is detected, the following behaviors occur:

- The link is declared as DOWN and the MM should display Protocol Down on the SLX-OS CLI.
- The physical link is not brought down in both of the previous cases. The peer side based on its implementation might display that the link is UP when the Brocade device displays that the link is DOWN due to a fault detection.
- The transmit (TX) packets, if any, are dropped at the MAC layer. The receive (RX) packets, if any, are dropped in the software.
- The detected signal is reported as a RASTRACE message on the line card. The same information is reported on the MM as a RASLOG. The same behavior occurs when the signal is cleared.

You can enable or disable LFS globally and on the interface level for both RX and TX directions:

- If the LFS is enabled for RX, the normal local and remote fault detection and processing described previously occur. If it is disabled for RX, local and remote fault detection are ignored.
- If the LFS is enabled for TX and a local fault occurs, a remote fault (pause frame) is generated to the remote side. If it is disabled for TX, the remote fault is not generated.

Configuring link fault signaling

By default, both TX and RX LFS are enabled. You can disable either RX or TX LFS globally or on the interface level.

Perform the following steps to configure LFS globally or on an interface.

1. From privileged EXEC mode, access global configuration mode.

```
device# configure terminal
```

2. Globally change the LFS, if required.

```
device(config)# link-fault-signaling rx off tx on
```

In this example, the global LFS is disabled for the link fault RX and enabled for link fault TX.

3. Access the interface configuration mode for the port that you want to configure.

```
device(config)# interface Ethernet 2/1
```

4. Shut down the interface.

```
device(conf-if-eth-2/1)# shutdown
```

The interface must be in the shutdown state before you disable or enable TX LFS.

5. Change the LFS for the interface.

```
device(conf-if-eth-2/1)# link-fault-signaling rx on tx off
```

In this example, the LFS for the interface is enabled for the link fault RX and disabled for the link fault TX. This configuration on the interface overrides the global configuration.

6. Enable the interface.

```
device(conf-if-eth-2/1)# no shutdown
```

7. Verify the configuration for the interface.

```
device(conf-if-eth-2/1)# do show running-config interface ethernet 2/1
interface Ethernet 2/1
...
 link-fault-signaling rx on tx off
 no shutdown
!
```

The following example shows the steps in the previous configuration.

```
device# configure terminal
device(config)# link-fault-signaling rx off tx on
device(config)# interface Ethernet 2/1
device(conf-if-eth-2/1)# shutdown
device(conf-if-eth-2/1)# link-fault-signaling rx on tx off
device(conf-if-eth-2/1)# no shutdown
```

Interface Ethernet ports

All Brocade device ports are pre-configured with default values that allow the device to be fully operational at initial startup without any additional configuration. In some configuration scenarios, changes to the port parameters may be necessary to adjust to attached devices or other network requirements.

Displaying device interfaces

The device supports Ethernet, loopback, management, and virtual Ethernet interfaces (VEs).

Enter the **show running-config interface** command to display the interfaces and their status.

The following example displays the Ethernet interfaces on the device. They are identified by the slot number, and port number, separated by forward slashes (/). For example, the notation 1/8 indicates port 8 located in slot 1 on a chassis.

```
device# show running-config interface ethernet
interface Ethernet 1/1
  no shutdown
!
interface Ethernet 1/2
  channel-group 101 mode active type standard
  lacp timeout long
  no shutdown
!
interface Ethernet 1/3
  channel-group 101 mode active type standard
  lacp timeout short
  no shutdown
!
interface Ethernet 1/4
  shutdown
!
interface Ethernet 1/5
  shutdown
!
interface Ethernet 1/6
  shutdown
!
interface Ethernet 1/8
  channel-group 143 mode active type standard
  lacp timeout short
  no shutdown
!
interface Ethernet 1/9
  shutdown
!
```

Displaying slots and module status information

You can display information for all slots in the chassis. You can also display latch detection configuration information for a specific module (line card).

- The following example shows the slot information for a Brocade SLX 9850-4 router.

```
device# show slots
Slot  Type      Description      ID      Status
-----
M1    MM v1        Management Module  179    ENABLED
M2    MM v3        Management Module  179    ENABLED
S1    SFM8 v6     Switch Fabric Module  187    UNLATCHED
S2    SFM8 v6     Switch Fabric Module  187    ENABLED
S3    SFM8 v6     Switch Fabric Module  187    ENABLED
S4    SFM8 v6     Switch Fabric Module  187    ENABLED
```

S5					VACANT
S6					VACANT
L1					VACANT
L2					VACANT
L3					VACANT
L4					VACANT
L5	LC72X10G v8	72-port 10GE card		180	UNLATCHED
L6					VACANT
L7					VACANT
L8	LC36x100G v3	36-port 100GE card		181	ENABLED

NOTE

The slot status indicates whether a slot is empty or contains an unlatched module:

- VACANT—The slot is empty.
- UNLATCHED—A module is inserted in the slot but it is not secured to the chassis with its captive screws. When the screws are installed, the module comes up automatically and its status changes.

- The following example shows latch detection configuration information for line card 1.

```
device# show latch-detection linecard 1
```

```

+-----+-----+-----+-----+-----+-----+-----+-----+
| slot | Module Type | Ver | Latch(L) | Latch(R) | Config In-Use | New Config | Enforce |
+-----+-----+-----+-----+-----+-----+-----+-----+
| LC1 | 36X100G | 4 | OPEN | CLOSED | ENABLE | DISABLE | YES |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

NOTE

The active latch detection configuration (Config In-Use) is stored on the line card at device startup or when the line card is reset. When the latch detection configuration is modified on the system using the **latch-detection** command, this is shown as the New Config (it is only detected and applied to the line card after the system is rebooted). The Enforce status indicates if latch detection is being enforced. When latch detection is enabled on a line card that supports latch detection, the Enforce status displays as YES.

Slots and modules

Modules (line cards) must be properly installed on the chassis to ensure that they are enabled when the system boots.

The line cards listed in the following table are installed on the chassis using two latch screws and latch detection is supported on these modules. Latch detection ensures that only line cards that are properly secured to the chassis using latch screws, are enabled when the system boots. When an unlatched line card is detected a Syslog message is displayed; for example:

```
2021/02/26-09:26:59, [PLAT-1013], 630, M2 | Active, INFO, SLX9850-8, Linecard:1 Version:4; Latch Screw Left:OPEN Right:INSTALLED
```

Latch detection can be disabled; for example, when you need to use a line card with a damaged latch screw or where the latch screw cannot be installed, you can disable latch detection using the **latch-detection** command. When latch detection is disabled, the line card may be enabled irrespective of the latch screw status.

TABLE 4 Modules (line cards) that support latch detection

Module	Type ID	Version
72 X 10G	180	6 and above
36 X 100G	181	4 and above

NOTE

Latch detection is always disabled on older line cards that do not support latch detection.

Displaying slots and module status information

You can display information for all slots in the chassis. You can also display latch detection configuration information for a specific module (line card).

- The following example shows the slot information for a Brocade SLX 9850-4 router.

```
device# show slots
Slot  Type          Description          ID      Status
-----
M1    MM v1             Management Module   179     ENABLED
M2    MM v3             Management Module   179     ENABLED
S1    SFM8 v6           Switch Fabric Module 187     UNLATCHED
S2    SFM8 v6           Switch Fabric Module 187     ENABLED
S3    SFM8 v6           Switch Fabric Module 187     ENABLED
S4    SFM8 v6           Switch Fabric Module 187     ENABLED
S5                                VACANT
S6                                VACANT
L1                                VACANT
L2                                VACANT
L3                                VACANT
L4                                VACANT
L5    LC72X10G v8       72-port 10GE card   180     UNLATCHED
L6                                VACANT
L7                                VACANT
L8    LC36x100G v3      36-port 100GE card  181     ENABLED
```

NOTE

The slot status indicates whether a slot is empty or contains an unlatched module:

- VACANT—The slot is empty.
- UNLATCHED—A module is inserted in the slot but it is not secured to the chassis with its captive screws. When the screws are installed, the module comes up automatically and its status changes.

- The following example shows latch detection configuration information for line card 1.

```
device# show latch-detection linecard 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| slot  | Module Type | Ver | Latch(L) | Latch(R) | Config In-Use | New Config | Enforce |
+-----+-----+-----+-----+-----+-----+-----+-----+
| LC1   | 36X100G     | 4   | OPEN     | CLOSED   | ENABLE        | DISABLE    | YES     |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

NOTE

The active latch detection configuration (Config In-Use) is stored on the line card at device startup or when the line card is reset. When the latch detection configuration is modified on the system using the **latch-detection** command, this is shown as the New Config (it is only detected and applied to the line card after the system is rebooted). The Enforce status indicates if latch detection is being enforced. When latch detection is enabled on a line card that supports latch detection, the Enforce status displays as YES.

Disabling latch detection

To use a line card with a damaged latch screw, you can disable latch detection.

Perform the following steps to identify a line card that is not properly installed and to disable latch detection on the line card.

1. In privileged EXEC mode, display slot information for the device.

```
device# show slots
```

Slot	Type	Description	ID	Status
M1	MM v1	Management Module	179	ENABLED
M2	MM v3	Management Module	179	ENABLED
S1	SFM8 v6	Switch Fabric Module	187	UNLATCHED
S2	SFM8 v6	Switch Fabric Module	187	ENABLED
S3	SFM8 v6	Switch Fabric Module	187	ENABLED
S4	SFM8 v6	Switch Fabric Module	187	ENABLED
S5				VACANT
S6				VACANT
L1	LC72X10G v8	72-port 10GE card	180	UNLATCHED
L2				VACANT
L3				VACANT
L4				VACANT
L5				VACANT
L6				VACANT
L7				VACANT
L8	LC36x100G v3	36-port 100GE card	181	LOADING

In this example, the status of L1 (UNLATCHED) indicates that a module is inserted but not properly secured to the chassis by its latch screws.

2. Display latch detection configuration information for line card 1.

```
device# show latch-detection linecard 1
```

slot	Module Type	Ver	Latch(L)	Latch(R)	Config In-Use	New Config	Enforce
LC1	36X100G	4	OPEN	CLOSED	ENABLE	ENABLE	YES

In this example, the left latch screw (Latch (L)) is not properly installed, latch detection is enabled (Config In-Use) and enforced (Enforce).

3. Disable latch detection on line card 1.

```
device# latch-detection disable linecard 1
```

Latch-Detection is disabled on Linecard 1. **Please reboot the system.**

4. Verify the new configuration for line card 1.

```
device# show latch-detection linecard 1
```

slot	Module Type	Ver	Latch(L)	Latch(R)	Config In-Use	New Config	Enforce
LC1	36X100G	4	OPEN	CLOSED	ENABLE	DISABLE	YES

The latch detection configuration on the system (New Config) is now disabled. However, the latch detection configuration in use (Config In-Use) is still enabled and latch detection is still enforced (Enforce). The new latch detection configuration is only applied to the line card after a system reboot.

5. To detect and apply the new system latch detection configuration on the line card, reboot the system.

- After reboot, verify the configuration.

```
device# show latch-detection linecard 1
```

slot	Module Type	Ver	Latch(L)	Latch(R)	Config In-Use	New Config	Enforce
LC1	36X100G	4	OPEN	CLOSED	DISABLE	DISABLE	NO

The latch detection configuration (Config In-Use) on the line card is now disabled and latch detection (Enforce) is no longer enforced.

- Display slot information for the device.

```
device# show slots
```

Slot	Type	Description	ID	Status
M1	MM v1	Management Module	179	ENABLED
M2	MM v3	Management Module	179	ENABLED
S1	SFM8 v6	Switch Fabric Module	187	ENABLED
S2	SFM8 v6	Switch Fabric Module	187	ENABLED
S3	SFM8 v6	Switch Fabric Module	187	ENABLED
S4	SFM8 v6	Switch Fabric Module	187	ENABLED
S5				VACANT
S6				VACANT
L1	LC36x100G v4 72-port 10GE card		180	ENABLED
L2				VACANT
L3				VACANT
L4				VACANT
L5				VACANT
L6				VACANT
L7				VACANT
L8	LC36x100G v3 36-port 100GE card		181	LOADING

Despite having a damaged left latch screw, L1 comes up because latch detection is now disabled.

Chassis and host names

A device can be identified by its IP address or by its host name and chassis name. You can customize the host name and chassis name. You can also change the default chassis IPv4 or IPv6 address.

Customizing chassis and host names

Brocade recommends that you customize the chassis name for each device. Some system logs identify the device by its chassis name; if you assign a meaningful chassis name, logs are more useful. You can also configure the host name.

To customize the chassis name and host name, perform the following steps:

- In privileged EXEC mode, enter global configuration mode.

```
device# configure terminal
```

- Configure the chassis name.

```
device(config)# switch-attributes chassis-name SLX-market1
```

A chassis name can be from 1 through 30 characters long, must begin with a letter, and can contain letters, numbers, and underscore characters.

The default chassis name is SLX9850-# where # is the number of slots in the chassis.

3. Configure the host name.

```
device(config)# switch-attributes host-name SLX-mrkt
SLX-mrkt(config)#
```

This example changes the host name to SLX-mrkt and it is displayed in the prompt.

A host name can be from 1 through 30 characters long. It must begin with a letter, and can contain letters, numbers, and underscore characters. The default host name is SLX.

4. Exit global configuration mode.

```
SLX-mrkt(config)# exit
```

5. Verify the configuration.

```
SLX-mrkt# show running-config switch-attributes
switch-attributes chassis-name SLX-market1
switch-attributes host-name SLX-mrkt
!
```

The following configuration is an example of the previous steps.

```
device# configure terminal
device(config)# switch-attributes chassis-name SLX-market1
device(config)# switch-attributes host-name SLX-mrkt
SLX-mrkt(config)#
```

Changing the chassis IP address

If you need to move the device to a different subnet, you can change the default IPv4 or IPv6 address of the device chassis.

To change the chassis IP address, perform the following steps:

1. In privileged EXEC mode, enter global configuration mode.

```
device# configure terminal
```

2. Configure the chassis address.

```
device(config)# chassis virtual-ip 10.11.12.13/20
```

If you want to reset the address to the initial address for the chassis, use the **no** form of this command.

3. Verify the configuration.

```
device# show running-config chassis
chassis virtual-ip 10.11.12.13/20
!
```

The following configuration is an example of the previous steps.

```
device# configure terminal
device(config)# chassis virtual-ip 10.11.12.13/20
```

System clock

The operation of the device does not depend on the date and time and the Brocade device with an incorrect date and time value functions properly. However, since logging, error detection, and troubleshooting use the date and time, you should set the clock correctly.

NOTE

You can set the system clock if there are no NTP servers configured. Otherwise, an active NTP server, if configured, automatically updates and overrides the system clock.

Setting the clock

The Brocade device allows you to manually set the system clock. The time counter setting is retained across power cycles.

To set the clock, perform the following step:

1. In privileged EXEC mode, set the date and time.

```
device# clock set 2016-07-07 12:30:45
```

This example sets the time and date to 12:30:45 on July 07, 2016.

2. Enter global configuration mode.

```
device# configure terminal
```

3. Change the time zone.

```
device(config)# clock timezone America/Bogata
```

This example changes the time zone to the region of America and the city of Bogata.

The following configuration is an example of the previous steps.

```
device# clock set 2016-07-07 12:30:45
device# configure terminal
device(config)# clock timezone America/Bogata
```

Management VRFs

Virtual Routing and Forwarding (VRF) is a technology that controls information flow within a network, isolating the traffic by partitioning the network into different logical VRF domains.

All management services on the Brocade device are VRF aware. The management services can select a particular VRF to reach a remote server based on a VRF. The VRFs are management (mgmt-vrf), default (default-vrf), and user defined (user-vrf).

By default, the device creates a VRF for management named mgmt-vrf and, all manageability services are accessible through this VRF. Multiple instances of IP services can be instantiated in multiple VRFs. For example, SSH can be in more than one VRF. IP services can have up to five VRF instances.

VRF reachability

The Brocade device supports the VRF reachability service. Reachability determines which VRF contains the routing information needed to reach the application servers. For example, when you configure an SSH server, you can configure the VRF information for the VRF context to resolved the SSH server route.

VRF reachability indicates the details of the VRF for servicing requests from the clients. It also indicates the clients specifying the VRF for reaching a source to ensure that the management packets are serviced or routed in a server VRF domain.

These two types of reachability services are also referred to as device-initiated and server-based services.

VRF reachability for device-initiated services

The following table lists the device-initiated services and associated commands that VRF reachability supports.

TABLE 5 Device-initiated services and associated commands that VRF reachability supports

Service	VRF-related command	Additional information
Firmware download	firmware download [default-config] ftp scp sftp [use-vrf vrf-name]...	Uses TCP IPv4 or IPv6. By default, mgmt-vrf is used and a user-defined VRF is optional.
Logging server	logging syslog-server { ipv4 ipv6 address } [use-vrf vrf-name]	Uses TCP UDP IPv4 or IPv6.
NTP	ntp server ip-address [use-vrf vrf-name]	Uses NTP UDP IPv4.
Openflow active controller	openflow controller name ip address ip-address [use-vrf vrf-name]	Uses OpenFlow TCP IPv4. By default, mgmt-vrf is used and a user defined VRF is optional.
RADIUS	radius-server host host-name [use-vrf vrf-name]	Uses UDP IPv4 or IPv6
sFlow	[no] sflow collector ipv4/ipv6 address port-number [use-vrf vrf-name] [no] sflow source-interface interface-type interface-number	Uses sFlow UDP IPv4 or IPv6. In the case of the sflow source-interface command, the VRF of the specified interface is used. NOTE Any given interface can belong to only one VRF at any given time.
SNMP notification	snmp-server host ip-address [use-vrf vrf-name] snmp-server v3host ip-address [use-vrf vrf-name]	Uses SNMP UDP IPv4 or IPv6. By default, mgmt-vrf is used to send the SNMP notifications.
Support save	copy support { ftp scp } [use-vrf vrf-name] ...	Uses TCP IPv4 or IPv6. By default, mgmt-vrf is used and a user-defined VRF is optional.
TACACS+	tacacs-server host host-name [use-vrf vrf-name]	Uses TCP IPv4 or IPv6

All these implementations use forward referencing of the VRF name in the **use-vrf** option, unless noted. At runtime when making the socket connection, the VRF ID by name must be resolved. If it does not resolve, it will result in a connection error.

VRF reachability for server-based services

The server services running on the Brocade device must listen to the requests in all the VRFs or a specified VRF and send the response back to the client in the same VRF where the request arrived. Thus, the services can come through any in-band interface bound to any VRF.

Each server-based service can have a maximum of six VRF instances including mgmt-vrf. The following table lists the server services and associated commands that VRF reachability supports.

NOTE

The SNMP server listens on all VRFs and sends the response back on the same VRF where the request arrived.

HTTP and HTTPS are mutually exclusive on the Brocade device and both will not be enabled in different VRFs.

TABLE 6 Server-based services and associated commands that VRF reachability supports

Service	VRF-related command	Additional information
HTTP	<code>[no] http server [use-vrf vrf-name] [shutdown]</code>	By default, the HTTP service is associated and started on mgmt-vrf and default-vrf. A user-defined VRF is optional.
SSH	<code>[no] ssh server [use-vrf vrf-name] shutdown</code>	By default, the SSH service is associated and started on mgmt-vrf and default-vrf. A user-defined VRF is optional.
Telnet	<code>[no] telnet server [use-vrf vrf-name] shutdown</code>	By default, the Telnet service is associated and started on mgmt-vrf and default-vrf. A user-defined VRF is optional.

Telnet and SSH limitations and considerations

Telnet and SSH limitations and considerations are as follows:

- By default, SSH and Telnet services are associated and started on mgmt-vrf and default-vrf.
- You cannot remove mgmt-vrf from the SSH and Telnet services.
- Telnet and SSH server can be enabled on a maximum number of 6 VRFs.
- When you use the **ssh** or **telnet server shutdown** command without a user-defined VRF, the service is shut down on mgmt-vrf only.
- Standby MM has support for mgmt-vrf. Starting SSH and Telnet service on a user-defined VRF does not have an impact on the standby MM until it becomes active.

NOTE

By default, SSH and Telnet service on the standby MM is disabled, use the **ssh** or **telnet server standby enable** command to enable standby access through SSH and Telnet.

- SSH and Telnet Services started on VRF context is applicable for both IPv4 and IPv6 addresses.
- A maximum of 32 user logins are allowed in the device. These sessions are a cumulative count of login sessions through SSH and Telnet across all the configured VRFs.

Zero Touch Provisioning

Zero Touch Provisioning (ZTP) is an automated process utilizing the DHCP process for firmware download and setting up the device configuration.

The ZTP process eliminates the need to login manually to the console to bring up the device with the correct firmware and required configuration. When the device is in the factory default configuration, ZTP can start automatically upon device bootup.

This process reduces the time taken for firmware download, device configuration . All switches download the same firmware and configuration script from the ZTP configuration file.

The following configuration considerations apply to Zero Touch Provisioning:

- ZTP is not supported for customers who do not use DHCP.
- ZTP supports only DHCPv4.
- The DHCP server must be configured with options 66 and 67 to set the ZTP configuration file.
- ZTP is triggered on a new device in the factory default state on an existing device using the **write erase** command.
- ZTP supports both in-band ports and management interface in the management VRF.
- After ZTP completes, all the in-band ports return to the default VRF state.
- To establish network connectivity, ZTP will retry indefinitely to establish a network connection among in-band ports and management interfaces until the firmware download completes, downloading all firmware packages before the device reboots.
- The interface is selected when it passes the sanity test. The order of selection is based on the response order of get option 66 or 67 during the DHCP server detection process.
- All the interfaces will be scanned in parallel to detect DHCP option 66 or 67.
- If ZTP is enabled and there is no DHCP server configured with option 66/67 for ZTP, the device will indefinitely try to discover a DHCP server. You will need to disable ZTP using the **dhcp ztp cancel** command and reboot the device before applying any configuration.
- Network connectivity over the management interface will have higher priority over in-band ports.
- ZTP is only supported in standalone mode.
- Customer configuration is supported with the Python script.
- The ZTP configuration file supports both a common setting and/or device specific settings.
- The ZTP progress is displayed on the serial console and saved in a log file.
- The DHCP client ID of the device must be set up on the device specific ZTP configuration file.
- The RASlog is disabled during the early stages of the ZTP process.
- Breakout ports are not supported because a device reboot is required.
- Only the default speeds (10G or 100G) on inband port are supported for the ZTP process.

Routing for Zero Touch Provisioning

The DHCP and FTP server may not be reachable by all the nodes in the IP Fabric. A route must be configured on the first level node with a connection to DHCP and FTP servers. ZTP must first be run on the first level using the Python script to enable iphelp to forward the traffic to the servers. The zero touch provisioning process can then run on the next level nodes. Eventually the farthest nodes can connect to the servers for ZTP.

Using zero touch provisioning

Follow these steps for zero touch provisioning in the standalone mode.

1. Establish a network connection with cable on one-to-multiple in-band ports or a management interface.
2. Power up the device in the factory default configuration or run the **write erase** command from the SLX CLI.

3. On device boot up, the Zero Touch Provisioning process performs the following actions:
 - a) Disables the RASlog to the serial output.
 - b) Enables in-band ports in the management VRF.
 - c) Detects a DHCP server with option 66 or 67 configured over a management interface and all in-band port interfaces.
 - d) Selects one interface not used before to assign the DHCP IP address.
 - e) Downloads the ZTP configuration file from the FTP server.
 - f) Validates the ZTP configuration file.
 - g) If required ZTP performs a firmware download or reboots the device. Firmware download reboots the device automatically.

In the current state the ZTP process will return to sub-step b. in the following situations:

- If there is a failure in any of the above-mentioned sub-steps from b. to g.
- If the device reboots from the CLI.
- If the device crashes.

On device bootup, the continuation of the ZTP process is indicated on the console. Wait for firmware commit to complete. If the firmware commit fails, the ZTP process aborts. If the script is enabled, the script is launched automatically.

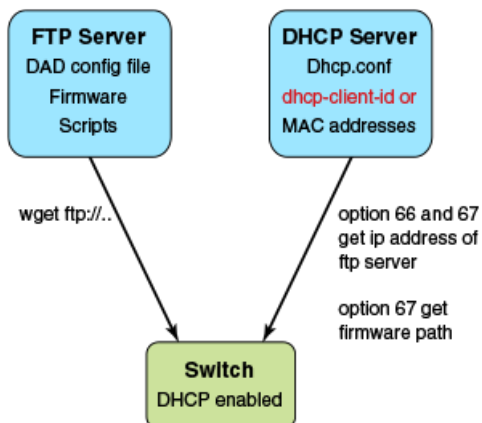
4. Enable the RAS log.

For more information and log outputs for canceling DHCP ZTP, refer to the *SLX-OS Command Reference Guide*.

ZTP configuration

To manage devices, the DHCP server and the FTP server must be set up to provide the environment.

FIGURE 1 ZTP configuration



DHCP server

DHCP Server version 4.2.4 is installed on Ubuntu 14.04 (Trusty) for development. The dhcpd.conf file must have option 66 (TFTP Server Name) and option 67 (Filename) set for ZTP. Option 66 is used for the FTP server IP address or host name. Option 67 is used for the ZTP configuration file path.

When the device starts the DHCP process, it sends the DHCP client ID to the DHCP server to get the IP address and option 66/67. The device then downloads the ZTP configuration file from the FTP server. To set up a different ZTP configuration file for different devices, the DHCP Client ID can be used in the dhcpd.conf. Whenever dhcpd.conf is changed, the dhcpd server must be restarted.

FTP server

vsFTP server version 3.0.2 is installed on Ubuntu 14.04 (Trusty) for development. The FTP server stores the ZTP configuration file, firmware, switch configuration file or Python script. The location of these configuration files under the FTP server base directory is flexible.

ZTP configuration script

The ZTP process can run the script to set up the device configuration automatically. For now, only the Python script is supported. The script takes no parameters.

The script can automate any command line including NOS CLI and Linux commands, such as configuration download command, “copy ftp://.... Running-config”.

ZTP configuration file

The ZTP configuration file has two configuration sections; common and device specific. The common section is shared by all the switches in the IP Fabric. The settings in switch-specific section can be used for a single switch or a group of switches with the DHCP client ID. If the host_client_id string matches the starting substring of the DHCP client ID of the switch, the switch-specific section is used by the switch.

Python script example

The following example shows a sample of the Python script:

```
#!/usr/local/python/3.3.2/bin/python3
import os
import sys, getopt

def main(argv):
    log.write("apply config\n")
    # change login banner
    CLI("conf ; banner login DAD ; end")
    # config download
    CLI("copy scp://root:brocade123@192.169.0.2/castorT.startup.cfg running-config")
if __name__ == "__main__":
    main(sys.argv[1:])
```

FTP server configuration file

The following example shows a sample of the FTP server configuration file.

```
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=NO
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=NO
tcp_wrappers=YES

#dad settings
anonymous_enable=YES
no_anon_password=YES
anon_root=/var/ftp
```

```

delay_failed_login=30
max_clients=100
anon_max_rate=8388608

```

DHCP server configuration file

The following example shows a sample of the DHCP server configuration file dhcp.conf

```

#ddns-update-style standard;
ddns-update-style interim;
ddns-ttl 600;
ignore client-updates; # Overwrite client configured FQHNs
ddns-domainname "infralab.com.";
ddns-rev-domainname "in-addr.arpa.";

option ntp-servers 192.168.0.2;
option domain-name-servers 192.168.0.2;
option domain-name "infralab.com.";
option domain-search "infralab.com";

default-lease-time 600;
max-lease-time 7200;

authoritative;

log-facility local7;

key "rndc-key" {
    algorithm hmac-md5;
    secret "dtBgNTAqZmwV5c4SueybjOvhe6OIqgacluQrzGBv504X4nIEBEEGWrf0lCnbFhuIJXGExNBjDdNSqgBMeNI8w==";
};

subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.100 192.168.0.200;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.0.255;
    zone 0.168.192.in-addr.arpa. {
        primary 192.168.0.2;
        key "rndc-key";
    }
    zone infralab.com. {
        primary 192.168.0.2;
        key "rndc-key";
    }
}
# cluster switches
group{
    option bootfile-name "/config/unified-cfg.min";
    option tftp-server-name "192.168.0.2";
    option routers 192.168.0.2;

    # sw0
    host sw0 {
        option dhcp-client-identifier = "BROCADE##SLX9240##EXG3342L00V";
        hardware ethernet 52:54:00:0E:95:8B;
        fixed-address 192.168.0.90;          # fixed ip address
    }
}

```

ZTP configuration file

The following has three sections - common, switch specific 1 and switch specific 2.

```

version=3
date=04/29/2016
supported_nos=17s.1.00 17r.1.00 17r.1.01 17s.1.0017

common_begin
vcsmode=SA
scriptcfgflag=2 #0-config file only, 1-script only, 2 both

```

```

script=/script/ztp.py
fwdir=/fw/slxos17s.1.00a_bld02
common_end

# model SXL9140 hosts
host_client_id=BROCADE##SLX9140
script=/script/Frredomlic.py
startup=/config/freedomlic.cfg
host_end

# model SXL9240 hosts
host_client_id=BROCADE##SLX9240
script=/script/dad2_new.py
startup=/config/cedarlic.cfg
host_end

# freedom
host_client_id=BROCADE##SLX9140##EXH3327M014
startup=/config/freedom_ospf.cfg
script=/script/FreedomZTP.py
host_end

# cedar
host_client_id=BROCADE##SLX9240##EXG3326M00P
startup=/config/cedar_ospf.cfg
script=/script/dad1_new.py
host_end

```

ZTP configuration file definitions

The following table contains the ZTP configuration file definitions.

TABLE 7 ZTP configuration file definitions

Variable description	Description
version	Only version 3 is supported.
date	The last modified date.
supported_nos	The release firmware version supporting the ZTP configuration file.
host_client_id, host_end	Host_client_id marks the beginning of the section host_end marks the end. User could set up the switch specific section with full dhcp client id or its prefix. Ex. <i>host_client_id=BROCADE##SLX9140##EXH3319M01J</i> <i>script=/script/dad1new.py</i> <i>host_end</i>
common_begin, common_end	The setting in the section will be shared by all switches.
vcsmode=SA	Only standalone mode is supported.
vcstimeout	If omitted, the default is 60 minutes. The timeout to wait for ZTP to complete configuration file download or Python script. If the configuration download process or Python script has issues, the zero touch provisioning process will stop the download after timeout and claim that ZTP is complete. You will need to increase the timeout if configuration download or Python script takes a long time to complete.
fwdir	Firmware path in the FTP server. For example <i>Fwdir=/fw/ slxoss17r.1.00_bld34</i> . If base directory of the FTP server is <i>/var/ftp</i> , then the absolute path of firmware in ftp server is located at <i>/var/ftp/fw/ slxoss174.1.00_bld34</i> .

TABLE 7 ZTP configuration file definitions (continued)

Variable description	Description
startup	The path to the switch configuration file in the FTP server. If omitted, the switch will take the default configuration. The value can be "default" or user configuration file.
scriptcfgflag	The default is 0, when not specified. The meaning of the value is: 0 - only use startup, script is ignored 1 - only use script, startup is ignored
script	The device configuration Python script file.

Example of Zero Touch Provisioning in a two node topology

The following section describes Zero Touch Provisioning IP routing in a two node topology.

In figure 1 switch 1 Eth 0/8 has direct connection to the DHCP or FTP server. Switch 1 acts as a router for switch 2 to reach the DHCP or FTP server. A default route on switch 1 is configured on the server for traffic sent from the DHCP server to reach switch 2 (see default route below). External access to DHCP sever is on Eth 0. There are two configurations for switch 1 - one is set up on Eth 0/8 by the DHCP server for ZTP to establish a connection to the DHCP server to download the ZTP configuration file, the other is set up by the Python script to configure the switch 1 as router Eth 0/8 and Eth 0/3 for switch 2. DHCP relay is configured on Eth 0/3 in switch 1 for DHCP requests from switch 2. Switch 1 Eth 0/8 and Eth 0/3 have to be in different subnets.

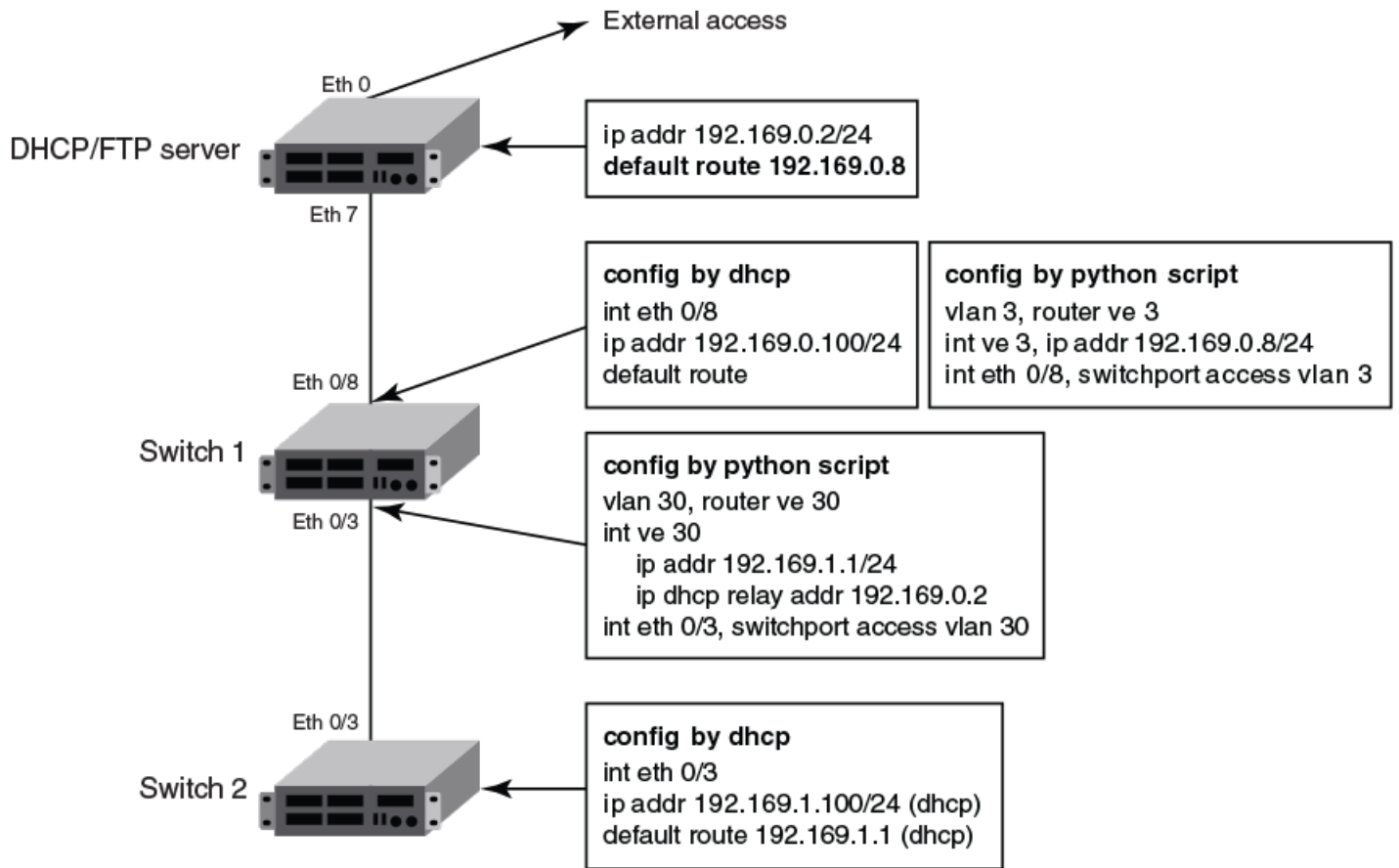
NOTE

The Python script for switch 1 should be manually tested to verify the routing set up before starting ZTP for switch 2.

DHCP server configuration will have two subnet address pools based on the DHCP client id. "level_1" for Switch 1 and "level_2" for switch 2.

```
class "level_1" {
  match if option dhcp-client-identifier = "BROCADE##SLX9140##EXH3319M01J"; <EXH3319M01J is the device
  serial number>
}
class "level_2" {
  match if option dhcp-client-identifier = "BROCADE##SLX9140##EXH3314M00L"; <EXH3314M00L is the device
  serial number>
}
subnet 192.169.0.0 netmask 255.255.255.0 {
  pool {
    allow members of "level_1";
    range 192.169.0.100 192.169.0.200;
  }
  option bootfile-name "/config/ztp.cfg";
  option tftp-server-name "192.169.0.2";
  option routers 192.169.0.2;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.169.0.255;
}
subnet 192.169.1.0 netmask 255.255.255.0 {
  pool {
    allow members of "level_2";
    range 192.169.1.100 192.169.1.200;
  }
  option bootfile-name "/config/ztp.cfg";
  option tftp-server-name "192.169.0.2";
  option routers 192.169.1.1; ip address as routers in level 2 subnet
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.169.1.255;
}
```

FIGURE 2 ZTP two node topology



Configuration file example

```

version=3
date=04/29/2016
supported_nos=17s.1.00 17r.1.00

common_begin
vcsmode=SA
fwdir=/bld/Nightly_nos_fusion_davinci_dev_160822_0600/dist
scriptcfgflag=2 #0-config file only, 1-script only, 2 both
script=/script/ztp.py
common_end

# model SXL9140 hosts
host_client_id=BROCADE##SLX9140 □ for Switch 2
startup=/config/startup.cfg
host_end

# switch 1 as router node
host_client_id=BROCADE##SLX9140##EXH3319M01J
startup=/config/freedom1_ospf.cfg
host_end

```

Configuration flow

- Enable ZTP on the inband port only by creating file `/etc/fabos/ztp.enable` with `echo \-l > /etc/fabos/ztp.enable`
- Run the **write erase** from the CLI on both switch 1 and switch 2 simultaneously.
- Switch 1 behaves as a single node ZTP.
- Switch 2 is held up with detecting the DHCP server with option 66 or 67 until ZTP on switch 1 succeeds, so that the static route is configured successfully. If switch 1 fails, switch 2 will wait indefinitely.

MAC address aging

MAC addresses that are dynamically learned are stored in MAC address table. The MAC address aging feature provides a mechanism to flush out the dynamic MAC addresses that remain inactive for a specified period.

The aging time of dynamic MAC address entries can be configured using the **mac-address-table aging-time** command. The MAC aging time can be configured to a value from 60 through 86400 seconds. By default, the aging time of dynamic MAC address entries is 300 seconds. The configured MAC aging time is applied to all MAC addresses in the system. You can disable the MAC address aging by specifying the aging time as 0 (zero).

NOTE

MAC address aging configuration per VLAN is not supported.

TCAM application-resource monitoring

Ternary Content Addressable Memory (TCAM) is specialized memory that stores complex tabular data and supports very rapid parallel lookups.

TCAM is used for storing different application filtering rules. These can be either L2, L3, or L4 control protocols. TCAM resources are used at different stages of the packet processor pipeline for providing the functionality. Some examples are:

- VT stage for inlif id
- TT stage for termination
- FWD stage for IPv6, IPv4 MC
- ACL - Ingress, Egress

A single lookup is performed on per packet per TCAM bank. It is possible to hit multiple TCAM banks for a single packet and the priority among the entries is selected based on either priority mode or interleaved mode. In priority mode bank1, entry1 takes precedence as compared to bank2, entry2. In interleaved mode minimal line entry is selected and first if both lines are equal. Associative data is 24b/48b when a TCAM bank is configured as 4K/2Kx80b/160b. When two TCAM banks are configured as 2K/128x320b model AD is 96b.

TABLE 8 TCAM Ingress and Egress details

TCAM	12 TCAM banks and 4 Small banks. 3 key arrangement options per bank
TCAM (Shared by Ingress and Egress)	256 entries per small banks
	4K entries of 80bit
	2K entries of 160bit
	2K entries of 320bit

TABLE 8 TCAM Ingress and Egress details (continued)

TCAM	12 TCAM banks and 4 Small banks. 3 key arrangement options per bank
	Concatenate two banks for a wider Key. The result options are:
	24bit
	48bit
	96bit
	Accesses: 1 per packet per bank

TCAM library-resource monitoring

The same TCAM hardware resources are shared by multiple applications, for example: Openflow, IPv4 ACL. So, monitoring and reporting the threshold status for each of the applications at hardware is not possible. TCAM software library is created to abstract this single hardware resource shared by multiple applications.

To support this capability of TCAM, each resource has to go through the TCAM library code path of resource allocation to achieve monitoring.

Based on the allocation via TCAM library, resource usage statistics are collected and RAS logs are generated and associated with the specific TCAM application resources with flags as critical, warning and info. Shared/fixed comment is present in the logs to reflect shared/fixed TCAM hardware resource by applications.

Hardware profiles

A variety of hardware profiles optimize ASIC resources for counters, port-channels, routes, and Ternary Content-Addressable Memory (TCAM)-allocation.

NOTE

When you change a hardware profile, the supported scale numbers remain the same with respect to the configuration even if hardware may not be able to fulfill them. This ensures that the same protocol and interface information remain valid with all hardware profile settings.

TCAM profiles

TCAM profiles enable you to optimize TCAM resources according to your system requirements.

TCAM is used by various forwarding applications. A TCAM profile supports a specified group of forwarding applications.

The following TCAM profiles are currently supported:

- default: Optimizes resources with basic support for all applications.
- layer2-optimised-1: Optimizes resources for Layer 2 ACL applications and VPLS endpoints.
- multicast-profile: Optimizes resources for IPv6 multicast. Layer 2 is also supported.
- npb-optimised-1: Optimizes resources for the Network Packet Broker (NPB) application.
- openflow-optimised-1: Optimizes resources for Openflow Layer 2 alone, IPv4 Layer 3 alone, and Layer 2 and Layer 3 simultaneously.
- openflow-optimised-2: Optimizes resources for Openflow Layer 2, IPv4 Layer 3, Layer 2 and Layer 3 simultaneously, and Layer 2 with metered action.

- openflow-optimised-3: Optimizes resources for Openflow Layer 2, IPv4 Layer 3, Layer 2 and Layer 3 simultaneously, and IPv6 with metered action.
- vxlan-ext: Optimizes resources for Vxlan transit and termination, and GRE tunnel.

Specifying a TCAM profile

Follow these steps to specify a TCAM profile.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter the **hardware** command to enable hardware configuration mode.

```
device(config)# hardware
```

3. Enter the **profile tcam** command to specify an ACL profile.

```
device(config-hardware)# profile tcam layer2-optimised-1
```

This optimizes resources for Layer 2 ACL applications and VPLS endpoints.

4. Enter the **reload system** command to reboot the device.

```
device# reload system
```

ATTENTION

The system must be rebooted following this configuration.

TCAM sharing

Under supported TCAM profiles, you can enable sharing of TCAM resources for each security ACL or PBR ACL applied to multiple ports.

When TCAM sharing is enabled, it applies to ports that are associated with one ASIC. Port-to-ASIC association varies with SLX-OS devices, as follows:

- Brocade SLX 9540: All ports share the same ASIC.
- Brocade SLX 9850: Refer to the "Association of ports to ASICs" tables in the *SLX 9850 Router Technical Specifications*.

No TCAM profile provides simultaneous support for all five flavors of TCAM sharing. The following table displays which and how many TCAM-sharing flavors are supported for each TCAM profile:

TABLE 9 TCAM-sharing support matrix

TCAM profile	Maximum sharing-flavors	Layer 2 ACL TCAM-sharing	IPv4 ACL TCAM-sharing	IPv4 PBR TCAM-sharing	IPv6 ACL TCAM-sharing	IPv6 PBR TCAM-sharing
default	4	Yes	Yes	Yes	Yes	Yes
layer2-optimised-1	4	Yes	Yes	Yes	Yes	Yes
multicast-profile	3	Yes	Yes	Yes	No	No
npb-optimised-1	3	Yes	Yes	Yes	No	No

TABLE 9 TCAM-sharing support matrix (continued)

TCAM profile	Maximum sharing-flavors	Layer 2 ACL TCAM-sharing	IPv4 ACL TCAM-sharing	IPv4 PBR TCAM-sharing	IPv6 ACL TCAM-sharing	IPv6 PBR TCAM-sharing
openflow-optimised-1	2	Yes	Yes	Yes	Not available	Not available
openflow-optimised-2	2	Yes	Yes	Yes	Not available	Not available
openflow-optimised-3	3	Yes	Yes	Yes	No	No
vlan-ext	4	Yes	Yes	Yes	Yes	Yes

ACLs and rules per ASIC

TCAM sharing helps to increase supported ACL rules if an ACL is applied to multiple ports of the same ASIC. The following table displays the configuration scale limits per ASIC.

TABLE 10 ASIC scale limits

ACL type	Maximum ACLs supported	Maximum rules in each ACL	Maximum filters configurable per ACL type
MAC-ACL	2048	2048	100K
IPv4-ACL	2048	2048	100K
IPv6-ACL	2048	2048	100K

- Maximum of 6K ACL tables can be created per system (2K of MAC-ACL, 2K of IPv4-ACL and 2K of IPv6-ACL).
- Maximum of 300K rules can be configured per system (100K rules of MAC-ACL, 100K rules of IPv4-ACL and 100K rules of IPv6-ACL).

ACLs supported for each TCAM profile

The below table displays the scale limits per profile per ASIC scale.

TABLE 11 Scale limits per profile per ASIC scale limits

	Entry type	Ingress	Egress
Default profile	L2 ACL	2038 (dedicated)	2038 (dedicated)
	IPv4 ACL	6134 (shared)	2038 (dedicated)
	IPv6 ACL		Not supported
NPB-profile-1	L2 ACL	6134 (shared)	2038 (dedicated)
	IPv4 ACL		2038 (dedicated)
	IPv6 ACL	4086 (dedicated)	Not supported
IPv4 VxLAN (Extended profile)	L2 ACL	2038 (dedicated)	1014 (dedicated)
	IPv4 ACL	4086 (dedicated)	1014 (dedicated)
	IPv6 ACL	2038 (dedicated)	Not supported
L2 optimized	L2 ACL	6134 (shared)	1014 (dedicated)
	IPv4 ACL		1014 (dedicated)
	IPv6 ACL	2038 (dedicated)	Not supported

TABLE 11 Scale limits per profile per ASIC scale limit\s (continued)

	Entry type	Ingress	Egress
Openflow-optimized-1/Openflow-optimized-2	L2 ACL	8182 (shared)	1014 (dedicated)
	IPv4 ACL		1014 (dedicated)
	IPv6 ACL	Not supported	Not supported
Openflow-optimized-3	L2 ACL	6134 (shared)	1014 (dedicated)
	IPv4 ACL		1014 (dedicated)
	IPv6 ACL	4086 (dedicated)	Not supported

Enabling TCAM sharing

Follow these steps to enable TCAM sharing.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter the **hardware** command to enable hardware configuration mode.

```
device(config)# hardware
```

3. Enter the **profile tcam** command to specify the TCAM-sharing profile or profiles that you require.

```
device(config-hardware)# profile tcam cam-share l3-v4-ingress-acl l3-v6-ingress-acl
```

Counter profiles

Counter profiles optimize counters. Common Infrastructure leveraged by applications, to take care of statistics subsystem programming.

Counter Engines (CEs) are used for Application Statistics.

Counting sources are:

- Ingress: InLIF, Ingress PMF(iACL)
- Egress: OutLIF, Egress PMF(eACL)

Counter Profiles determine the amount of CEs each counting source receives.

Each counter profile defines:

- Counter Engine (CE) distribution across counting sources.
- Counter Engine (CE) mode - Hit counter or Forward and Drop Counter.

The following table displays the list of counter profiles.

TABLE 12 Counter profiles

Profile	Recommended applications
Default	VLAN and BD local switching, MCT
Counter-profile-1	Ingress ACL, OF, Egress ACL
Counter-profile-2	OF, MPLS, VPLS, VLL, MCT
Counter-profile-3	MPLS, VPLS, VLL, MCT
Counter-profile-4	Ingress ACL, VPLS, Egress ACL

Specifying a counter profile

Follow these steps to optimize a specific counter profile.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter the **hardware** command to enable hardware configuration mode.

```
device(config)# hardware
```

3. Enter the **profile counter** command, specifying a counter profile.

```
device(config-hardware)# profile counters counter-profile-2
```

Hardware profile show commands

There are several show commands that display hardware-profile information, as listed in the following table.

TABLE 13 Hardware profile show commands in the *Command Reference*

Command	Description
show hardware profile	Displays details of the all current hardware profiles. You can also display TCAM-sharing details, or details for a specific TCAM, counter, or LAG profile.
show hw route-info	Displays the route-info counters.

Management Module High Availability

- Management module HA overview..... 61

Management module HA overview

High availability (HA) is supported on management modules (MMs).

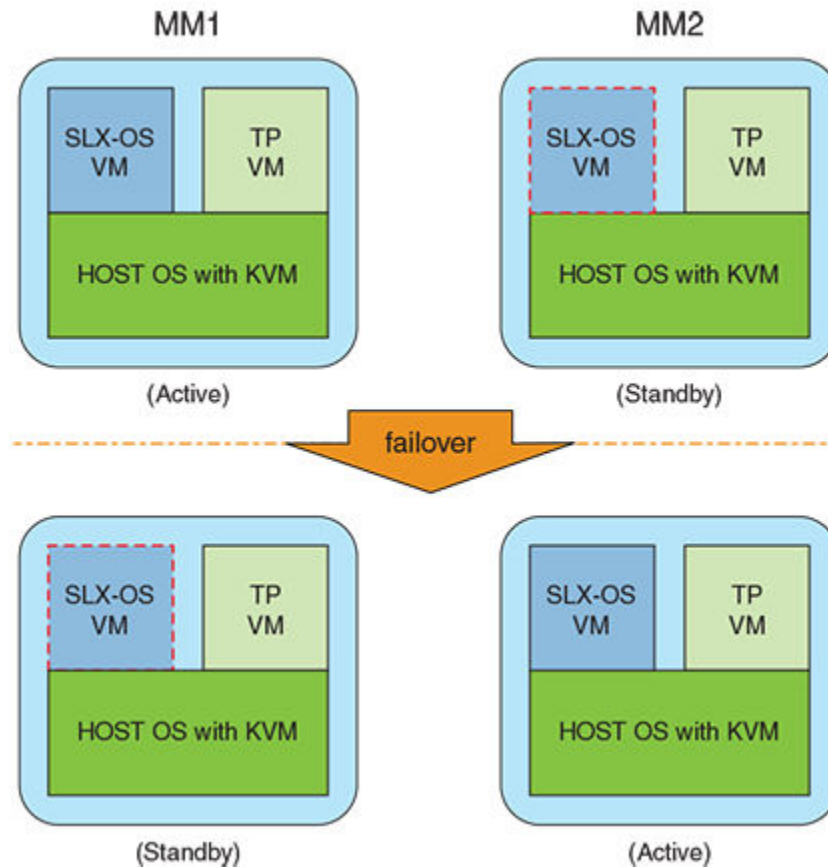
NOTE

High availability is not supported for In-Service Software Upgrade (ISSU).

The following figure shows the management module failover (MMFO) process on a device with two management modules; MM1 and MM2.

Initially, the SLX-OS VM on MM1 is active. On failover, the SLX-OS VM on the standby module (MM2) becomes active and the SLX-OS VM on MM1 reboots as standby.

FIGURE 3 Management module failover



A controlled MMFO occurs when you execute a command on the active MM to instigate the failover. A MMFO that occurs for any other reason is uncontrolled.

Normally, when MMFO occurs, active and standby MMs are synchronized. However, it is possible that for some reason the active and standby MMs are not synchronized when MMFO occurs. MM behavior upon failover is dependant on whether or not the active and standby MMs are synchronized and is shown in separate columns in the following tables that describe controlled and uncontrolled MMFOs. In these tables, the term "cold recovery" indicates that line cards are rebooted and traffic is disrupted on MMFO and the term "warm recovery" describes a hitless failover in which line cards are not rebooted and traffic is not disrupted on MMFO. When HA failover occurs, there may be a ping loss of 4 - 5 milliseconds.

A variety of HA commands are available on the device in privileged EXEC mode:

- The **show ha** command displays the management module status.
- The **ha failover** command forces the active management module to fail over. The standby management module will take over as the active management module. This command is only available in a modular chassis system.
- The **reload system** command reboots the entire chassis. This command is supported only on the active management module. This command is not supported on the standby management module. Both management modules must be in sync for the HA reboot operation to succeed.
- The **ha sync start** command enables HA state synchronization after an **ha sync stop** command has been invoked.

The following table shows commands that trigger controlled MMFO. It shows the impact of each command on active and standby MMs when the active and standby modules are synchronized and when they are not synchronized.

The **ha failover** command is the recommended method of executing a controlled MMFO.

TABLE 14 MM behavior in a controlled MMFO

Command	HA in sync		HA not in sync	
	Active MM	Standby MM	Active MM	Standby MM
reload	SLX-OS VM reboot itself can cause a cold recovery on the standby SLX-OS VM. Running-config will be used in new active.	SLX-OS VM self-reboot.	Prompt user to do 'reload system'.	SLX-OS VM self-reboot.
reload standby	Reboots standby SLX-OS VM.	SLX-OS VM self-reboot.	Reboots standby SLX-OS VM.	SLX-OS VM self-reboot.
reload system	Reboot chassis (including SLX-OS, TPVM and Host OS on both MMs) and retain mastership. Startup-config will be used.	Not allowed.	Reboot chassis (including SLX-OS, TPVM and Host OS on both MMs) and retain mastership. Startup-config will be used.	Not allowed.
ha failover	Reboots active SLX-OS VM and causes a warm recovery on the standby SLX-OS VM.	Not allowed.	Not allowed.	Not allowed.

The following table describes events that cause uncontrolled MMFO. It shows the impact of each event on active and standby MMs when the active and standby modules are synchronized and when they are not synchronized.

TABLE 15 MM behavior in an uncontrolled MMFO

Event	HA in sync		HA not in sync	
	Active MM	Standby MM	Active MM	Standby MM
Panic on active MM SLX-OS	Reboots active SLX-OS VM and causes a warm recovery on standby SLX-OS VM.	Not applicable.	Reboot Active SLX-OS VM and retain mastership. Startup- config will be used. Standby SLX-OS VM is rebooted.	Not applicable.

TABLE 15 MM behavior in an uncontrolled MMFO (continued)

Event	HA in sync		HA not in sync	
Pull out active MM	Causes a warm recovery on standby SLX-OS VM.	Not applicable.	Reboot standby SLX-OS VM and it will boot up in active. Startup- config will be used.	Not applicable.

Traffic forwarding features support for HA

Traffic forwarding features that support high availability (HA) are not disrupted when a switchover occurs between the active and standby management modules (MMs). Features that do not support HA may be disrupted.

The following traffic forwarding features support high availability (HA) and traffic is not disrupted upon MM switchover.

TABLE 16 Traffic forwarding features that support HA

Traffic forwarding feature	Note
802.1x	
BGP and BGP(v6) - NSF/GR	
CAM profiles	Supports HA without any traffic loss.
CFM/802.1ag	
Insight Architecture	Requires two guest virtual machines and applications that run independently on the active and standby MMs.
IPv4 and IPv6 forwarding	Requires routing protocols that support HA such as OSPF, BGP, ISIS GR, or NSR.
IP over MPLS	Requires: <ul style="list-style-type: none"> • Routing protocols that support HA • LDP graceful restart (GR) enabled
ISIS and ISIS(v6) - NSR	
L2 ACL, IPv4 ACL, IPv6 ACL, IPv4 rACL, IPv6 rACL, IPv4 PBR, IPv6 PBR, VXLAN visibility	Supports HA without any traffic loss.
LACP	
Layer-2 forwarding	
Layer-2 multicast	
MPLS transit LSR	LDP GR must be enabled.
OSPFv2 - NSF/GR , NSR	
OSPFv3 - NSR	
QoS-mutation features (CoS, DSCP, MPLS EXP)	Supports HA without any traffic loss.
SFLOW and rate-limiting features (port-based, BUM, and ACL-based)	Supports HA without any traffic loss.
UDLD	
VLAN and bridge-domain local switching, VLAN MAC port security	Supports HA without any traffic loss.
VPLS, VLL (using LDP tunnel as the transport mechanism)	LDP graceful restart (GR) must be enabled. <p>NOTE VPLS or VLL configurations that use RSVP LSPs do not support HA and traffic disruption may occur.</p>
VRF-LITE	
xSTP	

The following traffic forwarding features do not support HA; active management module failover may result in traffic disruption. However, normal operation resumes once the switchover is complete and when sessions or protocols are re-established.

TABLE 17 Traffic forwarding features that do not support HA

Traffic forwarding feature	Note
All multicast features	After MM failover, traffic disruptions may occur until the IP routing table is rebuilt, IGMP or PIM states are rebuilt, and the hardware is reprogrammed.
VRRP/E	Traffic disruption may occur in the scenario where: <ol style="list-style-type: none"> 1. The active MM is master 2. The remote node becomes master 3. The standby MM comes up and becomes master again There is no traffic disruption when the active MM is backup.
GRE (IPv4 and IPv6)	Traffic disruption occurs when the tunnel goes down and comes back up.
Openflow	During MM failover, flows are deleted. Flows are reinstalled after the switchover is complete.
MCT (for Layer 2 and Layer 3 traffic)	
Applications statistics	Counters are reset to zero upon MM failover.
VPLS, VLL (using RSVP LSPs)	

SLX-OS and Linux Shell Interoperability

• Overview	65
• Executing Linux shell commands from SLX-OS.....	66
• Executing scripts from SLX-OS.....	66
• Accessing the Linux shell from SLX-OS.....	67
• Executing SLX-OS commands from the Linux shell.....	68
• Escalating Linux permissions to root.....	69
• Saving and appending show command output to a file.....	69
• Logs of Linux shell activities.....	70

Overview

The SLX-OS supports interoperability between the SLX-OS CLI and the SLXVM Linux shell.

As an SLX-OS user with admin permissions, you can perform the following tasks:

- Running permitted Linux commands and scripts from the SLX-OS CLI
- Accessing the SLXVM Linux shell, and:
 - Running permitted Linux commands and scripts. However, if you have access to the root password, you can then escalate your permissions, by using the **su root** Linux command.
 - Running SLX-OS configuration and show commands.
 - Running scripts that contain multiple SLX-OS commands.

Limitations

- By default, only the Bash shell is supported. With Linux root permissions, you can install a different shell, such as the C shell or KornShell. However, shell-activity logging is supported only for the Bash shell.
- If you open multiple Bash sessions, the Linux shell timeout is applicable only on the current Bash session.
- If you run Linux commands as part of the script or through a file, the device logs the script or file execution. It does not log the commands.
- If you use the **cli_run** command to execute SLX-OS CLI **show** commands from the shell, pagination is not supported.
- At the SLX-OS CLI, a window resizing issue occurs when you execute Linux commands such as **top** using the **oscmd** command. Brocade recommends that you execute these commands from the Linux shell.
- Although as an SLX-OS admin, you have permissions to run the following commands from the Linux shell, you do not have permissions to run them—from the SLX-OS CLI—appended to the **oscmd** command.
 - **bash**
 - **script**
 - **vi**
 - **vim**
- Do not modify SLX-OS user accounts from the Linux shell. For information on modifying user accounts, refer to the *Brocade SLX-OS Security Configuration Guide for Brocade SLX 9540 and Brocade SLX 9850*.

Executing Linux shell commands from SLX-OS

You can execute a Linux command from the SLX-OS CLI, appended to `oscmd`.

In the following example, the Linux `ps -ef` command lists the process status.

```
device# oscmd ps -ef
UID      PID  PPID  C  STIME TTY          TIME CMD
root      1    0    0  Jul24 ?          00:00:04 /sbin/init
root      2    0    0  Jul24 ?          00:00:00 [kthreadd]
root      3    2    0  Jul24 ?          00:00:00 [migration/0]
root      4    2    0  Jul24 ?          00:00:03 [ksoftirqd/0]
root      5    2    0  Jul24 ?          00:00:00 [migration/1]
root      6    2    0  Jul24 ?          00:00:03 [ksoftirqd/1]
root      7    2    0  Jul24 ?          00:00:00 [migration/2]
root      8    2    0  Jul24 ?          00:00:02 [ksoftirqd/2]
root      9    2    0  Jul24 ?          00:00:00 [migration/3]
root     10    2    0  Jul24 ?          00:00:02 [ksoftirqd/3]
root     11    2    0  Jul24 ?          00:00:00 [migration/4]
root     12    2    0  Jul24 ?          00:00:02 [ksoftirqd/4]
root     13    2    0  Jul24 ?          00:00:00 [migration/5]
root     14    2    0  Jul24 ?          00:00:03 [ksoftirqd/5]
root     27    2    0  Jul24 ?          00:00:00 [cpuset]
root     28    2    0  Jul24 ?          00:00:01 [khelper]
root     31    2    0  Jul24 ?          00:00:00 [netns]
root     34    2    0  Jul24 ?          00:00:00 [async/mgr]
root    270    2    0  Jul24 ?          00:00:00 [sync_supers]
root    272    2    0  Jul24 ?          00:00:00 [bdi-default]

...

root      8kblockd/6]182    1  0  Jul24 ?          00:00:00 /usr/sbin/inetd
root      8237    1  0  Jul24 ?          00:00:00 /usr/sbin/sshd
admin    27536 27535  0 04:19 pts/4    00:00:00 ps -ef
```

Executing scripts from SLX-OS

From the SLX-OS CLI, you can execute scripts that you copied to flash memory or created in the SLXVM Linux shell.

Downloading a script to the SLX-OS device

After writing and testing a user-defined script file, copy it from an accessible network location to the flash memory of the SLX-OS device.

```
device# copy ftp://MyUserID:MyPassword@10.10.10.10//<copy_script.sh> flash://copy_script.sh
```

After copying the script to the device, verify that the script file is displayed with the list of files in the flash memory of the device.

```
device# dir
total 24
drwxr-xr-x  2 root    sys      4096 Oct 26 15:22 .
drwxr-xr-x  3 root    root     4096 Oct  1 1970 ..
-rw-r--r--  1 root    root     1051 Oct 24 16:09 copy_script.sh
-rw-r--r--  1 root    root      207 Oct 24 16:09 create_vlans.py
-rw-r--r--  1 root    sys      557 Oct 26 10:37 defaultconfig.novcs
-rw-r--r--  1 root    sys      778 Oct 26 10:37 defaultconfig.vcs

1922789376 bytes total (828317696 bytes free)
```

If the copied script does not have executable permissions, you need to assign executable permissions from the SLXVM Linux shell. Note that you need root access for this action, as described in "Escalating Linux permissions to root."

```
[root@SLX]# cd /var/config/vcs/scripts/
[root@SLX]# chmod 755 copy_script.sh
```

```
[root@SLX]# ls -lart copy_script.sh
-rwxr-xr-x 1 root root 1051 Oct 24 16:09 copy_script.sh
```

You can also display the contents of a script file.

```
device# show file copy_script.sh
```

Creating scripts in the Linux shell

You can create scripts by using the Linux shell **vi** editor, as in the following example.

```
device# start-shell
Entering Linux shell for the user: admUser
[admUser@SLX]# cd scripts
[admUser@SLX]# vi create_script.sh
```

After you write the script, make sure that it exists in the `/fabos/users/admin/script` directory and is executable under Linux.

```
[admUser@SLX]# pwd
/fabos/users/admin/scripts
```

Running scripts from the SLX-OS CLI

You can run scripts directly from SLX-OS CLI. Enter **oscmd** followed by the name of the script.

```
device# oscmd my_script
```

Accessing the Linux shell from SLX-OS

With admin-level permissions, you can access the SLXVM Linux shell from the SLX-OS CLI, by using the **start-shell** command.

NOTE

Inside the SLXVM Linux shell, you can execute commands that do not require root permissions. To escalate your permissions, refer to "Escalating Linux permissions to root".

1. To access the SLXVM Linux shell, enter the **start-shell** command.

```
device# start-shell
Entering Linux shell for the user: admUser
[admUser@SLX]#
```

2. Enter Linux commands and run scripts as needed. You can also run SLX-OS commands from the Linux shell.
3. To exit the shell and return to the SLX-OS CLI, enter **exit**.

```
[admUser@SLX]# exit
```

Upon exiting, the following message appears and you return to the SLX-OS CLI prompt.

```
exit
Exited from Linux shell
device#
```

Executing SLX-OS commands from the Linux shell

From the SLXVM Linux shell, you can execute a single SLX-OS command or a file that contains a series of such commands.

1. To execute an SLX-OS command, enter the Linux **cli_run -c** command.

```
[admUser@SLX]# cli_run -c "show ip interface brief" | grep Port-channel > /tmp/interface
```

In the previous example, the output of **show ip interface brief** is redirected to the `/tmp/interface` file.

2. Display the contents of the file to verify the redirection.

```
[admUser@SLX]# cat /tmp/interface
Port-channel 1          unassigned          administratively down    down
Port-channel 2          unassigned          administratively down    down
```

3. To execute a file containing multiple SLX-OS commands, enter the Linux **cli_run -f** command.

```
[admUser@SLX]# cli_run -f /tmp/slxcli_cmd_file > /tmp/newfile
```

In this example, `slxcli_cmd_file` contains the following commands:

```
[admUser@SLX]# cat /tmp/slxcli_cmd_file
show ssh server status
conf t
router bgp
local-as 23
capability as4-enable
```

NOTE

Make sure that each command is on a new line.

4. Display the contents of the target file to verify that it contains the redirected output.

```
[admUser@SLX]# cat /tmp/newfile
Welcome to the Brocade SLX-OS Software
admin connected from 127.0.0.1 using console on SLX
SLX# show ssh server status | nomore
VRF-Name: mgmt-vrf      Status: Enabled
VRF-Name: default-vrf  Status: Enabled
device# conf t
Entering configuration mode terminal
Current configuration users:
admin console (cli from 10.70.4.183) on since 2017-01-31 05:49:59 terminal mode
device(config)# router bgp
device(config-bgp-router)# local-as 23
device(config-bgp-router)# capability as4-enable
device(config-bgp-router)#
```

Escalating Linux permissions to root

In the SLXVM Linux shell, you can escalate your default admin access to root access (password protected).



CAUTION

A user with SLXVM Linux-shell root permissions can—unintentionally or maliciously—execute commands that can render the SLX-OS inoperable.

1. From the SLX-OS CLI prompt, enter **start-shell** to access the SLXVM Linux shell.

```
device# start-shell
Entering Linux shell for the user: admUser
[admUser@SLX]#
```

You can now execute commands that do not require root permissions.

2. To escalate your permissions, enter the Linux **su root** command.

```
[admUser@SLX]# su root
Password:
```

3. Enter the root password.

```
Password:
```

After successful login, the following warning is displayed:

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
[root@SLX]#
```

4. Enter Linux commands and run scripts as needed.

You can also run SLX-OS commands from the Linux shell.

5. To exit root level and return to the default SLXVM Linux shell, enter **exit**.

```
[root@SLX]# exit
exit
[admUser@SLX]#
```

6. To exit the default SLXVM Linux shell and return to the SLX-OS CLI, enter **exit**.

```
[admUser@SLX]# exit
exit
Exited from Linux shell
device#
```

Saving and appending show command output to a file

For output of a **show** command saved or appended to a file, the **oscmd** command enables you to display the file.

1. Save the **show** command output to a file.

```
device# show ssh server status | save status
```

In this example, the **show ssh server status** output is saved to the status file.

2. Display the contents of the file with the Linux **cat** command.

```
device# oscmd cat status
VRF-Name: mgmt-vrf      Status: Enabled
VRF-Name: default-vrf  Status: Enabled
```

3. Append the **show** output to an existing file.

```
device# show ip interface brief | last 5 | append status
```

In this example, the **show ip interface brief** output is appended to the status file.

4. Display the contents of the file with the Linux **cat** command.

```
device# oscmd cat status
VRF-Name: mgmt-vrf      Status: Enabled
VRF-Name: default-vrf  Status: Enabled
Ethernet 2/58           unassigned   default-vrf  administratively down    down
Ethernet 2/59           unassigned   default-vrf  administratively down    down
Ethernet 2/60           unassigned   default-vrf  administratively down    down
Ethernet 2/125(I)       unassigned   default-vrf  administratively down    down
Ethernet 2/126(I)       unassigned   default-vrf  administratively down    down
```

Logs of Linux shell activities

By default, SLX-OS logs users entering the SLXVM Linux shell, commands executed in that shell, and users exiting from the Linux shell back to the SLX-OS CLI.

Linux shell user entry and exit logs

SLX-OS uses RASLOG to log entries when the user enters and exits the Linux shell. If you configure a remote Syslog server, the same logs can also be seen on that server.

From privileged EXEC mode, use the **show logging raslog** command to display the RASLOG entries.

- When a user enters the Linux shell, the **show logging raslog** command displays an SH-1001 message.

```
device# show logging raslog

2016/06/25-06:42:54, [SH-1001], 1547, M1 | Active, INFO, SLX, SLXVM Linux shell login information:
User [admUser]. Login Time : Sat Jun 25 06:42:54 2016
```

- When a user exits the Linux shell, the **show logging raslog** command displays an SH-1002 message.

```
device# show logging raslog

2016/06/25-06:43:59, [SH-1002], 1548, M1 | Active, INFO, SLX, Event: exit, Status: success, Info:
User [admUser] successfully exited from SLXVM Linux shell. Exit Time: Sat Jun 25 06:43:59 2016
```

NOTE

An SH-1003 message indicates failure to log in to the Linux shell.

Linux shell command execution logs

Command activities at the Linux shell are logged locally in the `/var/log/shell_activity.log` file and remotely on a Syslog server.

When a user executes a command at the Linux shell, the `shell_activity.log` file includes SH-1005 messages:

```
[admUser@SLX]# tail -f /var/log/shell_activity.log

shell: [log@1588 value="SHELL"][timestamp@1588 value="2017-12-14T11:17:03"][msgid@1588 value="SH-1005"]
[severity@1588 value="INFO"][swname@1588 value="SLX9850-8"][arg0@1588 value="no" desc="root access"]
[arg1@1588 value="admin" desc="username"] BOM Executed command at Linux shell : pwd
shell: [log@1588 value="SHELL"][timestamp@1588 value="2017-12-14T11:17:18"][msgid@1588 value="SH-1005"]
[severity@1588 value="INFO"][swname@1588 value="SLX9850-8"][arg0@1588 value="no" desc="root access"]
[arg1@1588 value="admin" desc="username"] BOM Executed command at Linux shell : ls
```

NOTE

The `/var/log/shell_activity.log` file is rotated every thirty minutes if it goes over 2 MB in size. The old version of the file is compressed; a maximum of four rotated files can exist at the same time.

Configuring remote logging of Linux shell activities

By default, SLX-OS logs Linux shell commands both locally (in `/var/log/shell_activity.log`) and remotely, on the Syslog server.

From SLX-OS CLI, you can perform the following tasks to control the logging of commands executed at the Linux shell to a remote Syslog server. These tasks do not affect the local logging.

NOTE

Changes of the `log-shell stop` and `log-shell start` commands are applicable only on new Linux shell sessions.

1. To disable remote logging, enter `log-shell stop`.

```
device# log-shell stop
```

Local logging of user activities continues.

2. To restart remote logging, enter `log-shell start`.

```
device# log-shell start
```

3. To check the remote logging status, enter `log-shell status`.

```
device# log-shell status
```

When remote logging is enabled, the following message is displayed.

```
Linux shell activity logging : Enabled
```


Guest OS for TPVM

- VM access management.....73
- Insight interface and TPVM.....79
- TPVM.....93

TPVM, or Third-Party Virtual Machine, is a general server that resides on BrocadeSLX-OS devices. The guest OS that accesses it is different from SLX-OS.

VM access management

This section addresses how the Brocade SLX 9850 and the Brocade SLX 9540 access the Third-Party Virtual Machine (TPVM).

Brocade SLX 9850 VM access management

The Brocade SLX 9850 has data plane access for Third-Party Virtual Machine (TPVM) applications through the insight interface.

Port-channels are not created by default as in previous releases. The user can configure any port-channel as an insight port-channel. The ports that connect to TPVM are x/125 to MM1 and x/126 to MM2. The user must create a port-channel and enable the insight interface under that. This provides flexibility to use any port-channel as an insight port-channel.

Overview

The Brocade SLX 9850 allows you to access its internal host and virtual machine (VM) operating systems on the management module (MM), and the host and VM operating systems on the line cards.

The MM consist of the following operating systems:

- SLXVM OS—The Linux VM on the MM (active or standby)
- TPVM OS—Third-party VM on the MM (active or standby)
- MM host OS—Hypervisor Kernel-based Virtual Machine (KVM) that hosts the VM on the MM

A line card (LC) consists of the following operating systems:

- LCVN OS—Linux VM on LC
- Host OS—Hypervisor KVM that hosts the VM on the LC

Default credentials for the hosts

The following table provides the default user credentials to access the hosts of the operating systems on the MM and line cards. It also provides the commands to change the passwords.

TABLE 18 Default credentials for the hosts

Host name	Default user login	Default password	Changing the password
SLXVM	root	fibranne	From the SLXVM shell, the passwd command
	admin	password	From the SLXVM CLI, the username command with RBAC rules
	user	password	
LCVM	root	fibranne	Same default passwords as in the SLXVM

TABLE 18 Default credentials for the hosts (continued)

Host name	Default user login	Default password	Changing the password
	admin	password	
	user	password	
MM HOST-OS	root	fibranne	From the SLXVM shell, use the hostadm update_passwd command
LC HOST-OS	root	fibranne	Same default password as in the MM host OS
TPVM	root	fibranne	From the SLXVM shell, use the tpvmadm update_passwd command

NOTE

LCVM users are independent of the SLXVM users. Users from SLXVM will not be synched to the LCVM. The following example changes the password for the admin user on the LCVM.

```
LCVM1:L2/0: >/bin/passwd admin
Enter new UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
LCVM1:L2/0: >
```

VM access

You can access the VMs and host operating systems through the SLX-OS CLI, SLXVM OS shell or the serial console.

SLX-OS CLI to VM access

The SLX-OS CLI allows you to access to the following:

- SLXVM shell by using the **start-shell** command
- LCVM and MM host OS through a Telnet or SSH session

When you log into the SLX-OS CLI, you can use the default admin or user credentials. Non-default users are authenticated through AAA.

The following example shows Telnet access to the SLX-OS CLI with admin credentials.

```
client# telnet 10.24.12.71
Trying 10.24.12.71...
Connected to 10.24.12.71.
Escape character is '^]'.
SLX login: admin
Password:
SECURITY WARNING: The default password for at least
one default account (root, admin and user) have not been changed.

Welcome to the Brocade SLX Operating System Software
admin connected from 10.70.5.113 using telnet on device
device#
```

The default SLX-OS prompt is SLX#. However, throughout this guide, the device# is used as the prompt.

To exit the session, enter **exit**.

Using the serial console to access the MMVM, MM host OS, or TPVM

Within the MM, the shortcut keys shown in the following table allow access to the MMVM, MM host OS, or TPVM operating systems.

TABLE 19 Shortcut keys

Operating system	Shortcut keys
Host OS	Ctrl-Y1
MMVM OS	Ctrl-Y2
TPVM	Ctrl-Y3

Serial console to host OS access example

```
device# Ctrl-Y1
Ubuntu 14.04 LTS HOST ttyS0

HOST login: root
Password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.14.17 x86_64)
...
root@HOST:~#
```

Serial console to MMVM shell access example

```
device# Ctrl-Y2
[admin@SLX]#
```

Serial console to TPVM access example

From the MMVM shell, start TPVM.

```
[admin@SLX]# tpmadm install
Installation starts. To check the status, run 'tpvmadm show'
[admin@SLX]# tpmadm show
TPVM is installed but not running, and AutoStart is disabled on this host.
[admin@SLX]# tpmadm start
start succeeds
[admin@SLX]#
```

Authenticate and access the TPVM shell prompt.

```
[admin@SLX]# Ctrl-Y3
TPVM login: root
Password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)
...
root@TPVM:~#
root@TPVM:~# exit
```

```
Ubuntu 14.04.3 LTS TPVM ttyS0
```

```
TPVM login:
```

To return to the MMVM CLI shell prompt, enter **Ctrl-Y2**.

Accessing the Linux shell from SLX-OS

With admin-level permissions, you can access the SLXVM Linux shell from the SLX-OS CLI, by using the **start-shell** command.

NOTE

Inside the SLXVM Linux shell, you can execute commands that do not require root permissions. To escalate your permissions, refer to "Escalating Linux permissions to root".

1. To access the SLXVM Linux shell, enter the **start-shell** command.

```
device# start-shell
Entering Linux shell for the user: admUser
[admUser@SLX]#
```

2. Enter Linux commands and run scripts as needed. You can also run SLX-OS commands from the Linux shell.
3. To exit the shell and return to the SLX-OS CLI, enter **exit**.

```
[admUser@SLX]# exit
```

Upon exiting, the following message appears and you return to the SLX-OS CLI prompt.

```
exit
Exited from Linux shell
device#
```

Accessing LCVm from the SLX-OS CLI

You can access the LCVm on a line card from the SLX-OS CLI from a Telnet or an SSH session. In the LCVm shell, you can execute any LC command.

In the following example, a Telnet session is used to access the LCVm on line card 2.

```
device# telnet lc2_vm1 vrf mgmt-vrf
/fabos/cliexec/vrfgcmd 0 /usr/bin/telnet lc2_vm1 23
Trying 127.2.1.4...
Connected to lc2_vm1.
Escape character is '^]'.
Ubuntu 14.04 LTS
LCVM1 login: admin
Password:
LCVM1:L2/0: >
LCVM1:L2/0: >exit
logout
Connection closed by foreign host.
device#
```

The default LCVm OS shell prompt for LC2 VM1 is LCVm1:L2/0: >.

In the following example, an SSH session is used to access the LCVm on line card 2.

```
device# ssh lc2_vm1 vrf mgmt-vrf -l admin
The authenticity of host 'lc2_vm1 (127.2.1.4)' can't be established.
ECDSA key fingerprint is d7:d9:56:82:28:5c:58:71:90:5a:e2:ec:d7:f7:db:18.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'lc2_vm1' (ECDSA) to the list of known hosts.
admin@lc2_vm1's password:
LCVM1:L2/0: >
LCVM1:L2/0: >exit
logout
Connection to lc2_vm1 closed.
device#
```

In the previous examples, use **exit** to terminate the session and return back to the parent shell.

Accessing an MM host-OS shell from the SLX-OS CLI

You can access the MM host-OS shell from the SLX-OS CLI from a Telnet or an SSH session.

In the following example, a Telnet session is used to access the MM2 host-OS shell.

```
device# telnet mm1_kvmm vrf mgmt-vrf
/fabos/cliexec/vrfgcmd 0 /usr/bin/telnet mm1_kvmm 23
Trying 127.2.0.1...
Connected to mm1_kvmm.
Escape character is '^]'.
Ubuntu 14.04 LTS
HOST login: root
Password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.14.17 x86_64)
* Documentation: https://help.ubuntu.com/
System information as of Wed Aug 3 12:41:01 PDT 2016
System load: 0.08          Memory usage: 0%    Processes:      164
Usage of /:  14.6% of 9.72GB  Swap usage:  0%    Users logged in: 0
```

```

=> There is 1 zombie process.
Graph this data and manage this system at:
  https://landscape.canonical.com/
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
root@HOST:~#

```

In the following example, an SSH session is used to access the MM2 host-OS shell.

```

device# ssh mm1_kvm vrf mgmt-vrf -l root
The authenticity of host 'mm1_kvm (127.2.0.1)' can't be established.
ECDSA key fingerprint is d5:ba:cc:d4:57:03:e4:b2:6f:ca:d2:dd:4c:40:5d:60.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mm1_kvm' (ECDSA) to the list of known hosts.
root@mm1_kvm's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.14.17 x86_64)
 * Documentation:  https://help.ubuntu.com/
System information as of Thu Aug  4 10:41:47 PDT 2016
System load:  0.81          Users logged in:   0
Usage of /:   14.7% of 9.72GB   IP address for eth1: 127.2.0.1
Memory usage: 54%           IP address for br0:  10.24.12.77
Swap usage:  0%             IP address for virbr0: 192.168.122.1
Processes:   164
Graph this data and manage this system at:
  https://landscape.canonical.com/
Last login: Thu Aug  4 10:41:47 2016 from cp0_vm1
root@HOST:~#

```

In the previous examples, use **exit** to terminate the session and return back to the parent shell.

SLXVM shell to another MM or LC VM access

The SLXVM Linux shell allows you access another MM or the LC VM by using their host names and credentials through a Telnet or SSH session. The following table lists the hosts and addresses, and the session type in which the SLXVM shell can access them through the Ethernet 1 backplane.

TABLE 20 Hosts, addresses, and session types for the SLXVM shell

Host name	Description	IP address	SLXVM accessibility
slxvm1_vm	MM1 SLXVM	127.2.1.1	Telnet or SSH
slxvm2_vm	MM2 SLXVM	127.2.1.2	Telnet or SSH
lc1_vm1 through lc8_vm1	LC1 through LC8 LCVM	127.2.1.3 through 127.2.1.10	Telnet or SSH
slxvm1_kvm	SLXVM1 host OS	127.2.0.1	SSH only
slxvm2_kvm	SLXVM2 host OS	127.2.0.2	SSH only
lc1_kvm through lc8_kvm	LC1 through LC8 host OS	127.2.0.3 through 127.2.0.10	SSH only

The following example shows Telnet access of LC1 VM from the SLXVM shell.

```

[admin@SLX]# telnet lc1_vm1
Trying 127.2.1.3...
Connected to lc1_vm1.
Escape character is '^]'.
Ubuntu 14.04 LTS

LCVM1 login: admin
Password:
LCVM1:L1/0: >

```

In the following example, SSH is used to access LC1 VM from the SLXVM shell.

```
[admin@SLX]# ssh lc1_vm1 -l admin
admin@lc1_vm1's password:
LCVM1:L1/0: >
LCVM1:L1/0: >
```

Serial console to VM access

The serial console on the MM allows access to the following:

- SLXVM OS
- MM host OS
- TPVM
- LCVM
- LC host OS

On the MM, initial authentication occurs at the SLX-OS CLI prompt.

```
SLX login: admin
Password:

SECURITY WARNING: The default password for at least
one default account (root, admin and user) have not been changed.

Welcome to the Brocade SLX Operating System Software
admin connected from 127.0.0.1 using console on SLX
device#
```

Each OS requires its own credentials.

Using the serial console to access the MMVM, MM host OS, or TPVM

From the SLX-OS CLI on the serial console, you use a remote console to access the LCVM and LC host OS.

After you access the LCVM, you can use the **Ctrl-Y1** shortcut key to access the LC host OS.

The following shortcut keys are available on the line card to move between the LCVM and LC host OS.

Operating system	Shortcut keys
LC host OS	Ctrl-Y1
LCVM	Ctrl-Y2

The following example shows console access to LCVM on line card 2.

```
device# # rconsole.sh 2
Connecting to Linecard L2
Connecting to /dev/ttyS1, speed 9600
Escape character: Ctrl-\ (ASCII 28, FS): enabled
Type the escape character followed by C to get back,
or followed by ? to see other options.
-----

Ubuntu 14.04 LTS LCVM1 ttyS0

LCVM1 login: admin
Password:
LCVM1:L2/0: >
```

To access the LC host OS, use **Ctrl-Y1**.

To return to the LCVM CLI shell prompt, enter **Ctrl-Y2**.

TPVM address assignment

TPVM has an Ethernet 0 and 1 interfaces. Ethernet 0 (eth0) is enabled and its IP address is configured using DHCP.

On the SLXVM, the `tpvmadm show_ipaddr` command configures the address.

If DHCP is not available, you can use the serial console to log in as root, and use standard Ubuntu (14.04 LTS) commands to configure the IP address for eth0 interface.

Eth1 is connected to the Insight interface and allows packet monitoring.

Brocade SLX 9540 VM access management

The Brocade SLX 9540 has data plane access for Third-Party Virtual Machine (TPVM) applications through the insight interface.

On the Brocade SLX 9540, one the front-panel ports (port 0/48) is shared with the insight interface (port 0/125) through a hardware switch controlled by a CLI. Either the native port or the insight interface is operational at any given time. By default, port 0/48 is operative. When insight mode is configured, interface 0/48 is deleted dynamically and interface 0/125 is created, and all configurations under interface 0/48 are deleted.

Insight interface and TPVM

The insight interface is a port that provides data plane access for Third-Party Virtual Machine (TPVM) applications.

TPVM, or Third-Party Virtual Machine, is a general server that resides on Brocade SLX-OS devices. The guest OS that access it is different from SLX-OS.

On some platforms, insight interfaces can be configured by the user to connect the line card (LC) packet processors and the management module (MM) backplane switches running on both of the MM1 and MM2 CPUs. On other platforms, support for TPVM can be a front-panel port that is shared with the insight interface through a hardware switch, by means of a CLI command.

The following table details support for the insight interface on Brocade SLX platforms.

TABLE 21 Insight interface support on Brocade SLX platforms

Brocade SLX device	Support for insight interface
SLX 9850	On line card ports 1/125 and 1/126
SLX 9540	On port 0/48 (insight interface 0/125 is created)

The following section addresses the management details of using the insight interface port on Brocade SLX devices that support it. For the details of TPVM applications supported on all Brocade SLX devices, refer to "TPVM" later in this chapter.

Insight interface

Insight interface supported features

Insight interface port-channel supports the following third-party features and hardware.

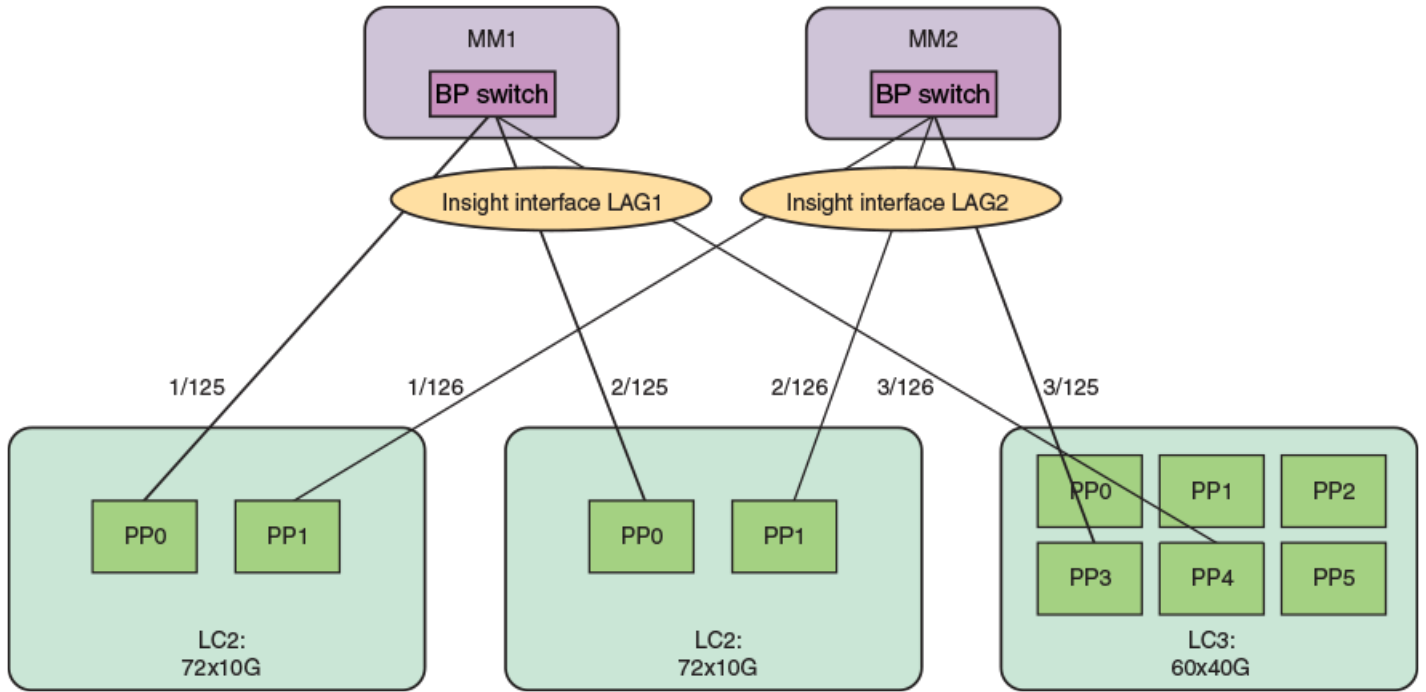
Insight interface supports the standard features seen in other front end interfaces including:

- Port and ACL-based mirroring destination
- QoS and rate shaping

Insight interface internal connectivity

LAG based modeling handles the failover of a linear program (LP) module.

FIGURE 4 High level view of insight interface ports and port-channels



Insight interface data path

The insight interface port is provided as a pre-existing port-channel interface to which all the insight interfaces on the LC are automatically added during system boot.

The port-channel 1 interface and the port-channel 2 interface are created as default LAGs in the system for MM1 and MM2 respectively. These are visible to you, configured with default settings, and are static LAGs only. All other options on the LAG are disabled. Insight interface ports and port-channels work independently with each providing up to 20 GB bandwidth for applications running on MM1 and MM2.

Insight interface port-channel creation, addition, or deletion is similar to the standard port-channel creation, addition, or deletion except it is programmatically invoked during system initialization and the insight interfaces on the LC are automatically and statically associated with the insight interface port-channel on the MM.

For example, when the LC in slot 1 comes online, the insight interface LAG port on the LC interface ethernet 1/125 is statically associated with the insight interface LAG interface port-channel 1 on MM1. Similarly interface ethernet 1/126 is statically associated with the insight interface LAG interface port-channel 2 on MM2.

Insight interface physical ports

There are two insight interface ports per line card (LC).

One of the insight interface ports is connected to a TPVM on Management Module (MM) 1 and the other is hard-wired to the TPVM port on MM2.

TABLE 22 Insight interface ports mapping:

LC type	LC port	LC tower	Destination
36x100 GB	1/125	3	MM1
	1/126	4	MM2
72x10 GB	1/125	0	MM1
	1/126	1	MM2

Consider the following when configuring insight interface:

- Link detection and reporting are the same as in regular front ports.
- The regular front ports are in an administratively down state by default. However, the insight interface ports are in an administratively up state.
- Forward error correction (FEC) between the media-independent interface (MII) and physical medium attachment (PMA) layers is enabled.
- 10 GB KR auto negotiation is enabled on BP switches and line card packet processor ports for insight interface ports.

Configuring the insight interface

Do the following to configure the insight interface on any port-channel. Port-channels 1 and 2 are not created by default.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter the **hardware** command to enter hardware configuration mode.

```
device(config)# hardware
```

3. Enter the **connector** command to specify a slot and port.

```
device(config-hardware)# connector 0/48
```

4. Enter the **insight mode** command to enable the insight interface on a port-channel, and exit to global configuration mode.

```
device(connector-0/48)# insight mode
```

5. Exit to global configuration mode.

```
device(connector-0/48)# exit
```

6. In global configuration mode, specify a port-channel.

```
device(config)# interface port-channel 22
```

7. In interface subtype configuration mode, enter the **insight enable** command and (optionally) specify a management module to enable insight support on the port-channel.

```
device(config-Port-channel-22)# insight enable mmid 1
```

This example specifies MM 1.

8. Enable the interface.

```
device(config-Port-channel-22)# no shutdown
```

9. Use the **show interface port-channel** and the **show port-channel** commands to confirm the configuration, as in the following example.

```

device# show interface port-channel 22
Port-channel 22 is up, line protocol is up
Hardware is AGGREGATE, address is 609c.9f5a.4558
  Current address is 609c.9f5a.4558
Interface index (ifindex) is 671088673
Minimum number of links to bring Port-channel up is 1
MTU 1548 bytes
LineSpeed Actual      : 10000 Mbit
Allowed Member Speed : 10000 Mbit
Priority Tag disable
Forward LACP PDU: Disable
Route Only: Disabled
Last clearing of show interface counters: 1d23h53m
Queueing strategy: fifo
Receive Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
  Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 0
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  5 packets, 380 bytes
  Unicasts: 0, Multicasts: 5, Broadcasts: 0
  Underruns: 0
  Errors: 0, Discards: 0
Rate info:
  Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Route-Only Packets Dropped: 0
Time since last interface status change: 00:00:21

device# show port-channel 22
Static Aggregator: Po 22
Aggregator type: Standard
Number of Ports: 1
Member ports:
  Eth 0/125  *

```

For the Brocade SLX 9850 series, slot IDs are x/125 and x/i26. For the Brocade SLX 9540, the slot ID is 0/125.

Inbound ACL-based mirroring

A Layer 2 or Layer 3 extended ACL permit filter must be configured to mirror the incoming matching traffic to a given port. You can also configure different mirror ports for different filters in the same ACL.

Enabling ACL-based port mirroring

Follow these high level steps to enable ACL-based port mirroring.

1. Create an ACL.
 - Traffic can only be selected using a permit clause.
 - The ACL can be bound to a physical port or a LAG.
 - The physical port or LAG interface should be configured as a switchport.
 - Configure the **mirror** keyword in an ACL filter to enable inbound ACL mirroring. This directs selected traffic to the mirrored port.

2. Associate the ACL mirror source and destination port. The mirror source port should be physical and the mirror destination port is either a physical port or a LAG port.
3. Bind the ACL to an interface.
4. Save the configuration.

Configuring inbound ACL-based mirroring to the insight interface

Follow these steps to configure inbound ACL-based mirroring.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Create an extended Layer 2 ACL.

```
device(config)# mac access-list extended macl
```

3. Configure the Layer 2 ACL for mirroring.

```
device(conf-macl-ext)# seq 10 permit host 0010.9400.0010 host 0010.9400.0014 vlan 20 count mirror
device(conf-macl-ext)# seq 20 permit host 0010.9400.0011 host 0010.9400.0015 vlan 20 count mirror
device(conf-macl-ext)# seq 30 permit host 0010.9400.0012 host 609c.9f01.58cb vlan 21 count mirror
device(conf-macl-ext)# seq 40 permit host 0010.9400.0013 host 609c.9f01.58cb vlan 22 count mirror
device(conf-macl-ext)# seq 50 permit any any count mirror
```

4. Return to global configuration mode.

```
device(conf-macl-ext)# exit
```

5. Create an extended IPv4 ACL.

```
device(config)# ip access-list extended ipv4acl
```

6. Configure the IPv4 ACL for mirroring.

```
device(conf-ipv4acl-ext)# seq 10 permit ip host 11.12.13.14 any count mirror
```

7. Return to global configuration mode.

```
device(conf-ipv4acl-ext)# exit
```

8. Associate the ACL destination mirror port.

```
device(config)# acl-mirror source ethernet 4/1 destination port-channel 1
```

9. Enter configuration mode for the source mirror port.

```
device(config)# interface ethernet 1/4
```

10. Bind the Layer 3 IP ACL to the source mirror port.

- a) Bind the Layer 2 ACL to the source mirror port.

```
device(conf-if-eth-4/1)# mac access-group macl in
```

- b) Bind the IPv4 ACL to the source mirror port.

```
device(conf-if-eth-4/1)# ip access-group ipv4acl in
```

- Return to privileged exec mode.

```
device(conf-if-eth-4/1)# end
```

- Verify the configuration.

```
device# show statistics access-list interface ethernet 4/1 in
mac access-list macl on Ethernet 4/1 at Ingress (From User)
seq 10 permit host 0010.9400.0010 host 0010.9400.0014 vlan 20 count mirror (105555094236 frames)
seq 20 permit host 0010.9400.0011 host 0010.9400.0015 vlan 20 count mirror (105555103123 frames)
seq 30 permit host 0010.9400.0012 host 609c.9f01.58cb vlan 21 count mirror (105555072247 frames)
seq 40 permit host 0010.9400.0013 host 609c.9f01.58cb vlan 22 count mirror (105555083432 frames)
seq 50 permit any any count mirror (0 frames)
```

- Save the configuration.

```
device# copy running-config startup-config
```

Inbound ACL-based mirroring to the insight interface configuration example (Layer 2)

```
device# configure terminal
device(config)# mac access-list extended macl
device(conf-macl-ext)# seq 10 permit host 0010.9400.0010 host 0010.9400.0014 vlan 20 count mirror
device(conf-macl-ext)# seq 20 permit host 0010.9400.0011 host 0010.9400.0015 vlan 20 count mirror
device(conf-macl-ext)# seq 30 permit host 0010.9400.0012 host 609c.9f01.58cb vlan 21 count mirror
device(conf-macl-ext)# seq 40 permit host 0010.9400.0013 host 609c.9f01.58cb vlan 22 count mirror
device(conf-macl-ext)# seq 50 permit any any count mirror
device(conf-macl-ext)# exit
device(config)# acl-mirror source ethernet 4/1 destination port-channel 1
device(config)# interface ethernet 1/4
device(conf-if-eth-4/1)# mac access-group macl in
device(conf-if-eth-4/1)# end
device# show statistics access-list interface ethernet 4/1 in
device# copy running-config startup-config
```

NOTE

Only the Layer 2 ACL creation is shown in this example.

Insight interface port-channel

This section addresses details of the insight interface port on different Brocade SLX platforms.

Brocade SLX 9850

- Port-channels are not created by default.
- Ports connected to TPVM are still x/125 and x/126 to MM1 and MM2.
- The user can configure any port-channel as an insight port-channel.
- The user must create a port-channel and enable insight interface under that. This provides the flexibility to use any port-channel as an insight port-channel.
- An existing port-channel (with existing member ports) cannot be made an insight interface port-channel.

The following is an example configuration.

```
device(config)# interface port-channel 43
device(config-Port-channel-43)# insight enable mmid1 or mmid2
device(config-Port-channel-43)# no shutdown
```

Brocade SLX 9540

- Either front-port 0/48 or the insight interface port 0/125 can exist at a given time, as these ports share the same ASIC port.
- By default, 0/48 is created.
- Insight mode can be configured by means of the **connector 0/48** command. A port-channel cannot be made an insight port-channel until insight interface mode is enabled on connector 0/48. Similarly, insight mode cannot be removed on connector 0/48 until the connector is unbound from the insight port-channel.
- Upon insight mode configuration, interface 0/48 is dynamically deleted and 0/125 is created.
- All the configurations under interface 0/48 are deleted upon insight mode configuration.
- An existing port-channel (with existing member ports) cannot be made an insight interface port-channel.

The following is an example configuration.

```
device(config)# hardware
device(config-hardware)#
device(config-hardware)# connector 0/48
device(config-connector-0/48)# [no] insight mode
device(config)# interface port-channel 22
device(config-Port-channel-22)# insight enable
```

Insight interface LC recovery

During link aggregation group (LAG) member failover, when the primary LC is powered down:

- There is a disassociation of the primary insight interface from the insight interface port-channel.
- There is an automatic selection of another insight interface LC as the primary insight interface port-channel.
- The port-channel stays up during the LC transition.

Insight interface traffic management and QoS

From a traffic management perspective, QoS for insight interface is similar to QoS for a regular port. The difference is the QoS configuration is applied to an insight interface LAG (port-channel) instead of an interface.

Consider the following when you configure this feature:

- The TM supports egress scheduling, rate shaping, WRED, and ingress buffer management for insight interface.
- TM egress scheduling and shaping for the insight interface must be configured under a port-channel interface.
- The QoS configuration is automatically applied to all ports in the port-channel.
- Follow the same configuration procedures for ingress buffer management and WRED as you would with a standard port.

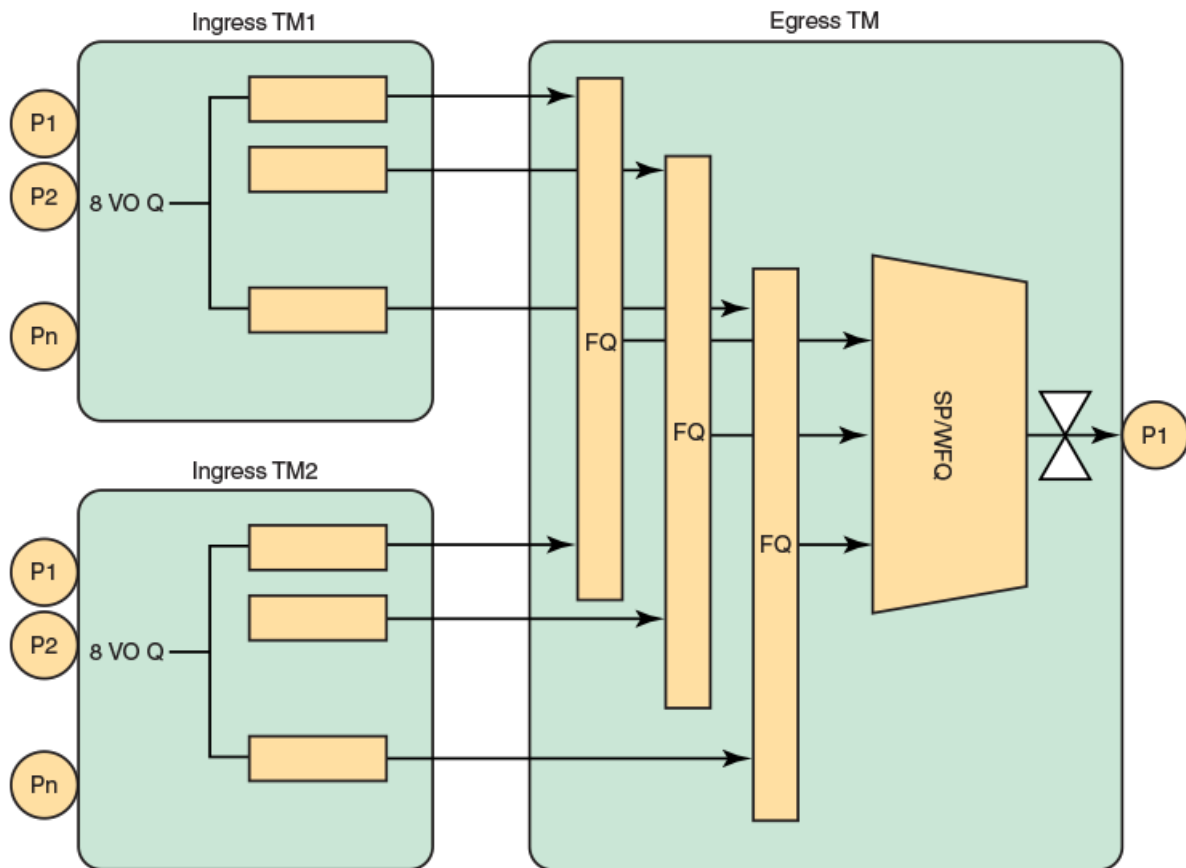
QoS egress scheduling

QoS egress scheduling works under the following rules, restrictions, and limitations:

- You must use a credit request/grant mechanism to perform egress scheduling QoS.
- The maximum credit size is 1024 Bytes.
- For each egress port there are 8 Virtual Output Queues (VOQs) allocated on each ingress transmit module (TM) core to support 8 priorities.
- Egress scheduling supports strict priority (SP), weighted fair queue (WFQ), and mixed mode scheduling.
- You can specify weighted for each VOQ only in WFQ mode.
- Fair queue (FQ) scheduling between VOQs from different TMs and with the same priority is permitted.

The figure below illustrates a QoS egress scheduling scheme.

FIGURE 5 QoS egress scheduling scheme



In the figure above P1 is the insight interface.

See the topic [Configuring QoS egress scheduling](#) on page 87.

QoS rate shaping

QoS rate shaping allows you to limit egress traffic to a specified rate.

Rate shaping works under the following rules and limitations:

- If there is a higher data rate than the configured shaping rate, traffic is kept at the ingress VOQ.
- The ingress TM tail drops packets if the queue is full.
- Accuracy is +/- 3%.
- Configuration granularity is 1KB.

Configuring QoS egress scheduling

Follow the below steps to configure QoS egress scheduling.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter interface configuration mode for port-channel 1.

```
device(config)# interface port-channel 1
```

3. Specify the option for strict priority mode to determine strict priority queues.

```
device(port-channel-1)# qos queue scheduler strict-priority 4
```

There are seven traffic classes. Specify the weight for the priority If the priority is in WFQ mode.

4. Return to privileged exec mode.

```
device(port-channel-1)# end
```

5. Verify the configuration.

```
device# show qos interface port-channel 1
```

6. View the VOQ statistics.

```
device# show tm voq-stat ingress-device ethernet 1/15 egress-port ethernet 1/125
```

```
VOQ-Counters:
```

```
=====
```

```
Priority 0
```

```
-----
EnQue Pkt Count                0
EnQue Bytes Count              0
Total Discard Pkt Count        0
Total Discard Bytes Count      0
Current Queue Depth            0
Maximum Queue Depth since Last read 0
```

```
Priority 1
```

```
-----
EnQue Pkt Count                0
EnQue Bytes Count              0
Total Discard Pkt Count        0
Total Discard Bytes Count      0
Current Queue Depth            0
Maximum Queue Depth since Last read 0
```

```
Priority 2
```

```
-----
EnQue Pkt Count                0
EnQue Bytes Count              0
Total Discard Pkt Count        0
Total Discard Bytes Count      0
Current Queue Depth            0
Maximum Queue Depth since Last read 0
```

```
Priority 3
```

```
-----
EnQue Pkt Count                0
EnQue Bytes Count              0
Total Discard Pkt Count        0
Total Discard Bytes Count      0
Current Queue Depth            0
Maximum Queue Depth since Last read 0
```

```
Priority 4
```

```
-----
EnQue Pkt Count                0
EnQue Bytes Count              0
Total Discard Pkt Count        0
Total Discard Bytes Count      0
Current Queue Depth            0
Maximum Queue Depth since Last read 0
```

```
Priority 5
```

```
-----
EnQue Pkt Count                0
EnQue Bytes Count              0
Total Discard Pkt Count        0
Total Discard Bytes Count      0
Current Queue Depth            0
Maximum Queue Depth since Last read 0
```

```
Priority 6
```

```
-----
EnQue Pkt Count                0
EnQue Bytes Count              0
Total Discard Pkt Count        0
Total Discard Bytes Count      0
Current Queue Depth            0
Maximum Queue Depth since Last read 0
```

```
Priority 7
```



```

-----
EnQue Pkt Count          0
EnQue Bytes Count       0
Total Discard Pkt Count 0
Total Discard Bytes Count 0
Current Queue Depth     0
Maximum Queue Depth since Last read 0

```

7. Save the configuration.

```
device# copu running-config startup-config
```

QoS egress scheduling configuration example

```

device# configure terminal
device(config)# interface port-channel 1
device(port-channel-1)# qos queue scheduler strict-priority 4
device(port-channel-1)# end
device# show qos interface port-channel 1
device# show tm voq-stat ingress-device ethernet 1/15 egress-port ethernet 1/125
device# copy running-config startup-config

```

Troubleshooting port-mirroring

Follow these high level steps to troubleshoot port-mirroring.

1. MAC counters on source and destination interfaces can be verified by running the command : **show interface ethernet slot/port**.

NOTE

This command is specific to the LC, it can be executed only on an LC console and not on a MM.

2. To see if there are any packet drops, check the PP counters by running the command: **show ppc statistics device slot/port**.

NOTE

This command is specific to the LC, it can be executed only on an LC console and not on a MM.

3. To see if packets are sent to a destination queue, VOQ counters can be verified by running the command: **show tm voq-stat destination slot/port**.
4. MMVM commands include:
 - a. **show interface port-channel [1 | 2]** (MM1) or 2 (MM2)
 - b. **show port-channel**
 - c. **show interface stats [brief | detail]**
 - d. **show interface ethernet slot/125** (MM1)
 - e. **show interface ethernet slot/126** (MM2)

Troubleshooting port-mirroring

Use these example in debugging port mirroring.

Configuring port mirroring from interface 1/2 to 1/1.

```
device(config)# monitor session 1
device(config-session-1)# source ethernet 1/2 destination ethernet 1/1 direction rx
```

Display the MAC counters on the ingress interface:

```
device# show interface ethernet 1/2
Ethernet 1/2 is up, line protocol is up (connected)
Receive Statistics:
  1000 packets, 128000 bytes
  Unicasts: 1000, Multicasts: 0, Broadcasts: 0
...
(Output is truncated)
```

Display the MAC counters on the mirrored interface:

```
device# show interface ethernet 1/1 (Output is trimmed for brevity)
Ethernet 1/1 is up, line protocol is up (connected)
Transmit Statistics:
  1000 packets, 128000 bytes
  Unicasts: 1000, Multicasts: 0, Broadcasts: 0
  Underruns: 0
...
(Output is truncated)
```

Display the destination virtual output queuing (VOQ) counters:

```
device# show tm voq-stat destination 1/1
VOQ-Counters:
Priority 1:
EnQue Pkt Count          1000
EnQue Bytes Count       148000
Total Discard Pkt Count 0
Total Discard Bytes Count 0
```

NOTE

This command can be used to check if the packets are received by the destination VOQ.

SLX-OS VM commands

Use these commands on the Brocade device to help troubleshoot the VM.

Display general interface information

```
device# show interface stats brief
```

Interface	Packets		Error		Discards		CRC
	rx	tx	rx	tx	rx	tx	
Po 1	16	2	0	0	0	0	0
Po 2	0	0	0	0	0	0	0
Eth 1/1	0	0	0	0	0	0	0
Eth 1/125	8	3	0	0	0	0	0
Eth 1/126	0	0	0	0	0	0	0

Display port-channel information

```
device# show interface port-channel 1
Port-channel 1 is up, line protocol is up
```

```

Hardware is AGGREGATE, address is 748e.f88f.5ffd
  Current address is 748e.f88f.5ffd
Description: Insight port-channel on MM1
Interface index (ifindex) is 671088641
Minimum number of links to bring Port-channel up is 1
MTU 2500 bytes
LineSpeed Actual      : 10000 Mbit
Allowed Member Speed  : 10000 Mbit
Priority Tag disable
IPv6 RA Guard disable
Last clearing of show interface counters: 03:43:52
Queueing strategy: fifo
Receive Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
  Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 0
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  Underruns: 0
  Errors: 0, Discards: 0
Rate info:
  Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 03:43:52

```

```

device# show interface port-channel 2
Port-channel 2 is up, line protocol is down (link protocol down)
Hardware is AGGREGATE, address is 0027.f817.1438
  Current address is 0027.f817.1438
Description: Insight port-channel on MM2
Interface index (ifindex) is 671088642
Minimum number of links to bring Port-channel up is 1
MTU 2500 bytes
LineSpeed Actual      : Nil
Allowed Member Speed  : 10000 Mbit
Priority Tag disable
IPv6 RA Guard disable
Last clearing of show interface counters: 03:45:17
Queueing strategy: fifo
Receive Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
  Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 0
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  Underruns: 0
  Errors: 0, Discards: 0
Rate info:
  Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 03:45:18

```

```

device# show running-config interface port-channel 1
interface Port-channel 1
  no vlag ignore-split
  description Insight port on MM1
  no shutdown

```

```

device# show running-config interface port-channel 2
interface Port-channel 2

```

```
description Insight port on MM1
shutdown
```

```
device# show port-channel
Static Aggregator: Po 1
Aggregator type: Standard
Eth 1/125
Eth 4/125
Static Aggregator: Po 2
Aggregator type: Standard
Eth 1/126
Eth 4/126
```

Optional keywords are **summary**, **detail**, and **load-balance**.

Display Ethernet interface information

```
device# show interface ethernet 1/125
Ethernet 1/125 is up, line protocol is down (link protocol down)
Hardware is Ethernet, address is 0027.f817.12fe
Current address is 0027.f817.12fe
Pluggable media not present
Interface index (ifindex) is 4704206921
MTU 2500 bytes
LineSpeed Actual      : Nil
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
IPv6 RA Guard disable
Last clearing of show interface counters: 03:46:22
Queueing strategy: fifo
Receive Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
  Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 0
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  Underruns: 0
  Errors: 0, Discards: 0
Rate info:
  Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 03:46:22
```

```
device# show interface ethernet 1/126
Ethernet 1/126 is up, line protocol is down (link protocol down)
Hardware is Ethernet, address is 0027.f817.12ff
Current address is 0027.f817.12ff
Pluggable media not present
Interface index (ifindex) is 4704239690
MTU 2500 bytes
LineSpeed Actual      : Nil
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
IPv6 RA Guard disable
Last clearing of show interface counters: 03:47:28
Queueing strategy: fifo
Receive Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
  Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 0
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
```

```

0 packets, 0 bytes
Unicasts: 0, Multicasts: 0, Broadcasts: 0
Underruns: 0
Errors: 0, Discards: 0
Rate info:
  Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 03:47:27

```

TPVM

TPVM enables users to run applications such as Docker Container, syslog server, SNMP server, and RESTful applications, among others. TPVM runs as a separate, independent virtual machine (VM), sharing the host CPU, RAM, hard disk drive, and management resources with SLX-OS.

Brocade devices are shipped with the TPVM firmware, but it is not installed by default.

Supported third-party applications, packages, and hardware

Note the following basic support and limitations for TPVM.

Third-party applications

- Packet capture applications
- RESTful support to access SLX-OS

Third-party packages

- Packages installed by default on the TPVM
- RESTful application: Chrome browser – GUI RESTful access
- RESTful application: cURL – Command line RESTful access
- Tcpdump: Command line packet-capture utility
- Tshark: Command line packet-capture utility
- Wireshark: GUI packet-capture utility
- Datadog or Splunk – External analytics software service

NOTE

Brocade SLX-OS provides support for built-in applications (third-party packages shipped with the SLX-OS) that are listed in the *Brocade SLX-OS Management Configuration Guide*.

- Brocade is committed to providing limited support for the interoperability of these applications with Brocade application interfaces.
- Brocade does not provide support for the application configuration, functionality, or deficiencies.
- Brocade does not provide any support for applications not listed in the *Brocade SLX-OS Management Configuration Guide*.

Hardware

The TPVM has 4 GB of RAM and 256GB of solid-state disk (SSD) memory, which limits the amount of data captured through packet capture applications. To overcome this limitation, Brocade provides support for the Network File System (NFS) mount of an external drive.

perfSONAR

perfSONAR (Performance focused Service Oriented Network monitoring ARchitecture) is an open-source, active network measurement toolkit that provides federated coverage of paths and helps establish end-to-end user expectations.

To identify network problems, it is important to compare active measurements against predefined notions of successful networks. Performance probes are placed in paths of interest, such as campus network endpoints, demarcations between networks, within carrier points of presence, at exchange points, and near data resources such as storage and computing elements.

To provide measurement baselines, some 2000 perfSONAR instances are deployed worldwide, representing around 300 domains, and many of which are available for the open testing of key measures of network performance. This global infrastructure helps to identify and isolate problems as they occur, making the role of supporting network users easier for engineering teams, and increasing productivity in the use of network resources.

perfSONAR provides a uniform interface that allows for the scheduling of measurements, storage of data in uniform formats, and scalable methods to retrieve data and generate visualizations. This extensible system can be modified to support new metrics, with a variety of ways to present data.

perfSONAR features

perfSONAR supports the following features and tools:

- Active measurement with scheduled tests
- Tools: Bwctl (lperf, iperf3, Nuttcp tests), ping, OWAMP tests (one-way latency), traceroute, tracepath
- Visualizations of stored data (MadDash)
- Directory service (to find perfSONAR instance around the world)

TPVM deployment considerations

Although SLX-OS allows perfSONAR to run on TPVM, it is recommended that this application be run on a dedicated server to mitigate risks posed by the VM environment, for the following reasons:

1. *Time keeping:* Some virtualization environments implement clock management as a function of the hypervisor and VM communication channel, rather than using a stabilization daemon such as NTP. This could result in timing skipping forward or backward, making it generally unpredictable for measurement.
2. *Data path:* Additional hypervisor layers can cause undesired latency.
3. *Resource management:* Because VMs share physical hardware and might get swapped, this might introduce additional errors in network performance measurements.

Reason (2) is mitigated in TPVM deployments by directly assigning the insight interface to the VM.

Reason (3) can be potentially mitigated by pinning one or more CPU cores to the VM.

Reason (1) can also be mitigated, such as by running NTP between guest and host, but this still not provide sufficient accuracy.

The perSONAR development team has identified several use cases that can work in VM environments, provided the known issues are mitigated. However, the high-speed throughput and OWAMP tests do not perform well.

ARP sponge

ARP sponge is an application that snoops on ARP packets on the Virtual Private LAN Service (VPLS) domain.

ARP sponge listens for ARP traffic. When the number of ARP requests for a certain IP address exceeds a threshold, ARP sponge sends out an ARP reply for that address that uses its own MAC address. This is achieved by using the insight LAG to the bridge domain as an AC endpoint. All ARP traffic received by the VPLS instance is flooded to the insight LAG as well.

TPVM installation and management

TPVM installation and a variety of management details are described.

Installation

The TPVM firmware is shipped with the Brocade device and it is stored in the SLXVM filesystem. The user executes the **tpvm install** command to install it. During the subsequent firmware download, the TPVM firmware in the SLXVM filesystem is updated to be the same as the SLXVM firmware version. However, the user must run the **tpvm install** command again to re-install it. Otherwise, the currently running TPVM image is not changed.

ATTENTION

The installation is disruptive, and any data saved on the TPVM partition is erased. You must save any data manually before executing the **tpvm install** command.

Initially, the TPVM firmware stored in the SLXVM /ftpboot directory matches the version created by the netinstall process. However, in subsequent firmware downloads the TPVM firmware can be from different distributions.

After the installation, you can start and stop the image by means of the **tpvm start** and **tpvm stop** commands, respectively. To start the TPVM image automatically in subsequent reboots, use the **tpvm launch-on-boot enable** command. (TPVM may not come up if there are any issues with booting SLXVM.)

Once the TPVM image is running, you can download user-specific applications by copying them to the TPVM partition and starting them manually.

To uninstall the TPVM image and release its resources, use the **tpvm uninstall** command.

ATTENTION

When TPVM is re-installed, any user applications are deleted.

Resources and default XML configuration

TPVM runs the Linux 3.19 64-bit kernel. It has 4 GB of RAM, with a second SSD dedicated to it, and it shares one of the four CPU cores with SLXVM. Note that the host runs a different version of Linux (3.14 64-bit kernel). XML is used as the file format for storing the total configuration, including domain, network, storage, and other elements, and is used by QEMU/Libvirt to instantiate TPVM. That file cannot be edited by the user.

Resource usage

QEMU is a multithreaded application that creates multiple virtual CPUs (VCPUs) for TPVM to use the Linux kernel's symmetric multiprocessing (SMP) capabilities on a multicore system. QEMU creates one thread per VCPU and there is a single I/O thread. The VCPU threads execute guest code, and the I/O thread waits on select calls for disk I/O. The threads run in lock-step fashion with a mutually exclusive semaphore. From the Linux host perspective, TPVM appears as a process. All commands to check TPVM resources and control TPVM are executed from the host and have administrative (root) restrictions.

To check TPVM resource utilization, use the following commands:

- `ps aux | grep TPVM`
- `top -p pid`
- `cat /proc/ pid /*`

Console access

A console daemon runs on the host and opens a console connection to TPVM. The user can switch the console connection among host, SLXVM, and TPVM by pressing the following key sequences, respectively.

- Host: **Ctrl + y + 2**
- SLXVM: **Ctrl + y + 2**
- TPVM: **Ctrl + y + 3**

NOTE

By default, the console is connected to SLXVM.

TPVM can be accessed through the eth0 (management) interface. The eth0 interface connects to the outside network through the host physical interface, which makes it appear as a normal host to the rest of the network. SSH or Telnet access to TPVM is provided through the IP address of the eth0 interface configured on TPVM.

IP and MAC address management

The assignment of a TPVM IP address to a management interface uses DHCP by default. However, the user can also assign a static address and a default gateway to the TPVM eth0 interface by using the `ifconfig` command. See [Assigning a static IP address on the TPVM Linux OS](#) on page 109.

Communication between TPVM and SLXVM

An HTTP RESTful interface is provided for accessing the running configuration, interface statistics, interface states, and all system-related information. TPVM is prepackaged with a RESTful client to support, for example, cURL (command line RESTful access utility), to extract information from SLXVM. cURL uses HTTP methods (such as GET, PUT) to extract and modify configuration information so long as the requesting user is authenticated correctly.

The following example shows a simple request format from TPVM:

```
curl -s -u admin:password http://ip-addr/rest/config/running/ . . .
```

In addition to cURL, Advanced Rest Client, a Chrome-based RESTful client application, is prepackaged inside TPVM and is accessed through a browser interface.

Both HTTP and HTTPS secure access are enabled.

NFS mount support

TPVM supports the NFS mount of an external drive to support the storage of captured data.

Packages support and applications

No configuration is needed on TPVM to support RESTful access with cURL and Google-chrome.

In addition, TPVM comes with Tcpcdump, Tshark, and Wireshark prepackaged to support packet capture.

Users or administrators can use the **apt-get** command with options to upgrade, update, purge, or remove (to downgrade to an older version). In addition, applications can be downloaded to provide a development environment that allows users or administrators to build their own applications, development tools (gdb, glibc (e.g. ANSI-C and POSIX), and gcc) for C/C++ . Similarly, python development tools can also be downloaded.

Containers

The following container binaries have been tested with TPVM:

- Docker container: docker-1.13.0
- Linux container: LXC 1.0

The above binaries do not come prepacked with TPVM. Use the **wget** or **apt-get** commands to install, upgrade, or downgrade Docker and Linux container binaries or packages in TPVM.

Using the *tpvmadm* command

This administrative command is available at the SLX-OS shell and is invoked by means of the **oscmd** command (on the Brocade SLX 9850) or the **start-shell** command (on the Brocade SLX 9540). This command requires root privileges.

The **tpvmadm** command, in privileged EXEC mode, allows you to manage TPVM with a variety of subcommands that do the following:

- Install, start, stop, and uninstall TPVM
- Specify the default behavior when SLX-OS boots
- Add or remove disks and show the disk information
- Print out IP addresses set on TPVM
- Change the root password on TPVM
- Use the **help** keyword for details on all options

NOTE

The optional keywords **mm1** and **mm2** are for management module (MM) support only on the Brocade SLX 9850.

To install TPVM if it is not already installed:

```
SLX# tpvmadm install
Installation starts. To check the status, run 'tpvm status'
```

To uninstall TPVM if it is installed:

```
SLX# tpvmadm uninstall
uninstallation succeeds
```

To force the clearing of installation or uninstallation errors by means of the **-f** keyword:

```
SLX# tpvmadm uninstall -f
uninstallation succeeds
```

To start TPVM if it is not running:

```
SLX# tpvmadm start
start succeeds
```

To stop TPVM if it is running:

```
SLX# tpvmadm stop
stop succeeds
```

To start TPVM at the next reboot of SLX-OS (without the need for the **start** keyword):

```
SLX# tpmadm enable_on_boot
enable_on_boot succeeds
```

To prevent TPVM from starting at the next reboot of SLX-OS:

```
SLX# tpmadm disable_on_boot
disable_on_boot succeeds
```

NOTE

In this case, the **tpvmadm start** command is required to enable TPVM.

To display the current status of TPVM or any errors:

```
SLX# tpmadm show
TPVM is running, and AutoStart is disabled on this host.
```

To add a new disk to TPVM, where the syntax is as follows:

```
tpvmadm add_disk <disk_name|auto> <disk_size> [ mm1 | mm2 ]
```

disk_name: The disk name added to TPVM.

Note. The disk name must be the next disk if it's not 'auto'. For example, if the last disk added to the system is 'vdb', the disk name must be 'vdc'. When 'auto' is used, the system automatically assigns the next disk name.

disk_size: Any positive number.

Also the following suffix can be added to the end.

```
b or B for bytes
k or K for KiB bytes
m or M for MiB bytes
g or G for GiB bytes
```

Note. When no suffix is used, the size is taken as GiB bytes. For example, '5' means '5g'.

```
SLX# tpmadm add_disk auto 10g
add_disk succeeds
```

```
SLX# tpmadm add_disk vdd 512m
add_disk succeeds
```

NOTE

The maximum number of disks supported is currently 3. If the number of allocated disks exceeds this number, the **add_disk** keyword fails. Also, the total disk capacity is limited to 100 Gbytes on the Brocade SLX 9850 and 50 Gbytes on the Brocade SLX 9540. If you exceed this limit when you create a disk, the **add_disk** keyword fails.

To remove an additional disk from TPVM, where the syntax is as follows:

```
tpvmadm remove_disk <disk_name|auto> [ mm1 | mm2 ]
```

disk_name: The disk name removed from TPVM.

The name must be 'vd[b-x]' or 'auto'

Note. When 'auto' is passed, the system removes the latest disk automatically.

Otherwise, the disk name must be the last disk added to the system.

For example, if the last disk added to the system is 'vdx', the disk removed from the system must be this disk, 'vdx'.

```
SLX# tpmadm remove_disk auto
'umount' is needed before this disk is removed. Continue? [y/n]: y
remove_disk succeeds
```

```
SLX# tpmadm remove_disk vdc
'umount' is needed before this disk is removed. Continue? [y/n]: y
remove_disk succeeds
```

ATTENTION

If the disk is mounted, it must be unmounted before it is removed from the system. Otherwise, the next added disk will be labeled incorrectly. If this happens, TPVM must be rebooted to recover.

To clear errors by means of the `-c <error>` keywords, where the error in this example is "add_disk":

```
SLX# tpmadm add_disk auto 10g
add_disk failed

SLX# tpmadm show
TPVM had runtime error(s) -- these error(s) seem not fatal, and the operation(s) could be retryable
add_disk: virsh vol-create-as failed. error detail: error: Failed to create vol vde error: operation
failed: the number of volumes goes beyond the maximum

TPVM is running, and AutoStart is disabled on this host.

SLX# tpmadm show -c add_disk
TPVM is running, and AutoStart is disabled on this host.
```

NOTE

The runtime error can be also removed automatically when the same subcommand succeeds.

To display disk information, where the syntax is as follows:

```
tpvmadm show_disk <disk_name|all> [ mm1 | mm2 ]

disk_name: The disk name whose information is shown.
           The name must be 'vd[b-x]' or 'all'
Note. When 'all' is passed, the information about all disks is shown.

SLX# tpmadm show_disk all
disk: vdb
Capacity: 70.00 GiB
Allocation: 196.00 KiB

disk: vdc
Capacity: 30.00 GiB
Allocation: 196.00 KiB

total:
Capacity: 100.00 GiB
Allocation: 100.00 GiB
Available: 0.00 B

sw0:FID128:root> tpmadm show_disk vdb
disk: vdb
Capacity: 70.00 GiB
Allocation: 196.00 KiB

total:
Capacity: 100.00 GiB
Allocation: 100.00 GiB
Available: 0.00 B
```

To display IPv4 and IPv6 addresses that are configured on TPVM, in this example on MM1:

```
SLX# tpmadm show_ipaddr mm1
[ TPVM running on MM1 ]
IPv4:
eth0 10.24.7.80
IPv6:
eth0 fe80::5054:ff:fe9c:446d
eth1 fe80::7:d0ff:fe02:100
```

NOTE

The `show_ip_addr` keyword requires the `qemu-guest-agent` package on TPVM. If this package is removed, the keyword fails.

To change the root password on TPVM, in this example on MM2:

```
SLX# tpmadm update_passwd mm2
root password: <enter a new root password here..>
re-enter root password: <enter the root password again..>
update_passwd succeeds
```

To view all options by using the **help** keyword:

```
SLX# tpmadm help
Usage: tpmadm sub-command [ options ] [ mm1 | mm2 ]
sub-command:
    install          install TPVM
    uninstall        uninstall TPVM

    start            start TPVM
    stop             stop TPVM

    add_disk         add a new disk to TPVM
    remove_disk      remove the disk from TPVM
    show_disk        show the disk information on TPVM

    enable_on_boot   enable to start TPVM at boot
    disable_on_boot  disable to start TPVM at boot

    show_ipaddr      show TPVM IP address(es)
    update_passwd    update the TPVM root password

    show             show status or errors of TPVM
    help            show sub-command usage

run 'tpmadm help <sub-command>' for detail
```

Using the *tpvm* command

The **tpvm** command is available at the SLX-OS CLI on a device or active management module (MM), but it does not require root privileges as does the **tpmadm** command. It otherwise provides the same functionality as that command.

The **tpmadm** command, in privileged EXEC mode, allows you to manage TPVM with a variety of subcommands that do the following:

- Install, start, stop, and uninstall TPVM
- Specify the default behavior when SLX-OS boots
- Add or remove disks and show the disk information
- Print out IP addresses set on TPVM
- Change the root password on TPVM
- Use the help keyword for details on all options

NOTE

The optional keywords **blade mm1** and **blade mm2** are for management module (MM) support only on the Brocade SLX 9850.

To install TPVM if it is not already installed, with the following syntax:

```
tpvm install [ blade <MM1 | MM2> ]

SLX# tpvm install
Installation starts. To check the status, run 'tpvm show status'
```

NOTE

Used without the **blade** keyword, this command installs TPVM on a device that does not have blades.

To uninstall TPVM if it is installed, with the following syntax:

```
tpvm uninstall [ force ] [ blade <MM1 | MM2> ]

force: clear installation or uninstallation error(s) then try to uninstall (forcefully)

SLX# tpvm uninstall
uninstallation succeeds
```

To force the clearing of installation or uninstallation errors by means of the **force** keyword:

```
SLX# tpvmadm uninstall
TPVM uninstallation failed

SLX# tpvm uninstall force
uninstallation succeeds
```

To start TPVM if it is not running, with the following syntax:

```
tpvm start [ blade <MM1 | MM2> ]

SLX# tpvm start
start succeeds
```

To stop TPVM if it is running, with the following syntax:

```
tpvm stop [ blade <MM1 | MM2> ]

SLX# tpvm stop
stop succeeds
```

To start TPVM at the next reboot of SLX-OS (without the need for the **start** keyword), with the following syntax:

```
tpvm auto-boot enable [ blade <MM1 | MM2> ]

SLX# tpvm auto-boot enable
```

To prevent TPVM from starting at the next reboot of SLX-OS, with the following syntax:

```
tpvm auto-boot disable [ blade <MM1 | MM2> ]

SLX# tpvm auto-boot disable
auto-boot disable succeeds
```

NOTE

In this case, the **tpvm start** command is required to enable TPVM.

To display the current status of TPVM or any errors, with the following syntax:

```
tpvm show status [ clear-tag <tag name> ] [ blade <MM1 | MM2> ]

clear-tag: clear the runtime error when the 'command' ran

SLX# tpvm show status
TPVM is running, and AutoStart is disabled on this host.
```

To clear errors by means of the **clear-tag**<tag name> keywords, where the error in this example is "vm_disks":

```
SLX# tpvm start
start succeeds

SLX# tpvm show status
TPVM had runtime error(s) -- these error(s) seem not fatal, and the operation(s) could be retryable
vm_disks: virsh list timed out. TPVM cannot transit to 'running' state

TPVM is installed but not running, and AutoStart is disabled on this host.

SLX# tpvm show status clear-tag vm_disks
TPVM is installed but not running, and AutoStart is disabled on this host.
```

NOTE

The runtime error can be also removed automatically when the same subcommand succeeds.

To add a new disk to TPVM, where the syntax is as follows:

```
tpvm disk add name <vd[b-x] | auto> size <number | number[bkmg]> [ blade <MM1 | MM2> ]
```

name: The disk name added to TPVM.

The name must be 'vd[b-x]' or 'auto'.

Note. The disk name must be the next disk if it's not 'auto'. For example, if the last disk added to the system is 'vdb', the disk name must be 'vdc'. When 'auto' is used, the system automatically assigns the next disk name.

size: Any positive number.

Also the following suffix can be added to the end.

b or B for bytes

k or K for KiB bytes

m or M for MiB bytes

g or G for GiB bytes

Note. When no suffix is used, the size is taken as GiB bytes. For example, '5' means '5g'.

```
SLX# tpvm disk add name auto size 10g
disk add succeeds
```

```
SLX# tpvm disk add name vdd size 512m
disk add succeeds
```

NOTE

The maximum number of disks is currently 3. If the number of allocated disks exceeds this limit, the **add_disk** keyword fails.

Also, the total disk capacity is limited to 100 Gbytes on the Brocade SLX 9850 and 50 Gbytes on the Brocade SLX 9540. If you exceed this limit when you create a disk, the **add_disk** keyword fails.

To remove an additional disk from TPVM, where the syntax is as follows:

```
tpvm disk remove name <vd[b-x] | auto> [ blade <MM1 | MM2> ]

name: The disk name removed from TPVM.
      The name must be 'vd[b-x]' or 'auto'
      Note. When 'auto' is passed, the system removes the latest disk automatically.
      Otherwise, the disk name must be the last disk added to the system.
      For example, if the last disk added to the system is 'vdx', the disk removed from
the system must be this disk, 'vdx'.
SLX# tpvm disk remove name auto
'umount' is needed before this disk is removed. Continue? [y/n]: y
disk remove succeeds

SLX# tpvm disk remove name vdc
'umount' is needed before this disk is removed. Continue? [y/n]: y
disk remove succeeds
```

NOTE

If it is mounted, the disk must be unmounted before it is removed from the system. Otherwise, the next added disk will be labeled wrongly. If the system falls in this situation by mistake, TPVM must be rebooted to recover.

To display disk information, where the syntax is as follows:

```
tpvm show disk name <vd[b-x] | all> [ blade <MM1 | MM2> ]

name: The disk name whose information is shown.
      The name must be 'vd[b-x]' or 'all'
      Note. When 'all' is passed, the information about all disks is shown.
SLX# tpvm show disk
Value for 'name' : all
disk: vdb
Capacity: 10.00 GiB
Allocation: 196.00 KiB

total:
Capacity: 100.00 GiB
Allocation: 10.00 GiB
Available: 90.00 GiB

SLX# tpvm show disk name vdb
disk: vdb
Capacity: 10.00 GiB
Allocation: 196.00 KiB

total:
Capacity: 100.00 GiB
Allocation: 10.00 GiB
Available: 90.00 GiB
```

To display IPv4 and IPv6 addresses that are configured on TPVM, in this example on MM1, where the syntax is as follows:

```
tpvm show ip-address [ blade <MM1 | MM2> ]

SLX# tpvm show ip-address
[ TPVM running on MM1 ]
IPv4:
eth0 10.24.7.149
IPv6:
eth0 fe80::629c:9fff:fe01:fe43
eth1 fe80::7:d0ff:fe02:100
```

NOTE

The **show_ip_addr** keyword requires the *qemu-guest-agent* package on TPVM. If this package is removed, the keyword fails.

To change the root password on TPVM, in this example on MM2, where the syntax is as follows:

```
tpvm password [ blade <MM1 | MM2> ]

SLX# tpvm password blade mm2
root password: ****
re-enter root password: ****
password succeeds
```

Third Party Virtual Machine (TPVM) service port support

TPVM Service port can be used to share the traffic captured on Insight port with external analytics software services like Datadog or Splunk. The traffic files captured, for example, insight-traffic.cap can be shared with external analytics services over service port with variety of options like NFS mount or file transfer utilities.

Service port is accessible only from TPVM. It is visible as linux network device interface like **eth1**. Service port supports bi-directional traffic to share the data plane traffic captured from Insight port with external analytics services.

NOTE

By default, Service port is disabled. To enable the service port, use SLXOS TPVM command.

TPVM Service port configuration

After service port is enabled, **ifconfig -a** output in TPVM displays three ethernet interfaces and these are numbered **eth0**, **eth1** and **eth2**. Since, service port is hot-plugged into TPVM, the **ethX** interface assignment changes. This is due to the way linux assigns interface names based on the PCI scan order. The table below shows which **ethX** interface represents what port when service port is enabled or disabled.

TABLE 23 Service port assignment

Service port status	Management interface	Insight interface	Service port interface
Disabled	eth0	eth1	Not applicable
Enabled	eth0	eth2	eth1

To ensure consistent interface names as per the table, complete the below configuration while TPVM is running. This will setup TPVM to always assign **eth1** to Insight Port and **eth2** to service port.

1. Login as root on TPVM and edit/create the file: `/etc/udev/rules.d/75-persistent-net-generator.rules`
2. Add the following lines to the file -

```
ACTION=="add", SUBSYSTEMS=="pci",SUBSYSTEM=="net", ATTRS{device}=="0x15ab", NAME="eth1"
ACTION=="add", SUBSYSTEMS=="pci",SUBSYSTEM=="net", ATTRS{device}=="0x15a8", NAME="eth2"
```

3. Save the file and restart TPVM. This displays the configuration changes.

Port IP address configuration

TPVM IP address assignment to interfaces uses either 'static' or 'dhcp' assignment. Current TPVM assignment is as follows -

TABLE 24 TPVM IP address assignment

Ports	Interfaces
eth0	Management interface uses DHCP mechanism.

TABLE 24 TPVM IP address assignment (continued)

Ports	Interfaces
eth1	Insight interface uses static IP address assignment.
eth2	Service interface uses static or DHCP IP address assignment.

Using the `tpvm` command

Using the `tpvm` command to enable or disable service port.

To enable service port:

```
tpvm service-port enable [ blade <MM1 | MM2> ]
```

To enable TPVM service port:

```
tpvm service-port enable [ blade <MM1 | MM2> ]
```

```
SLX# tpvm service-port enable
TPVM service port is enabled
```

To disable TPVM service port:

```
no tpvm service-port enable [ blade <MM1 | MM2> ]
```

```
SLX# no tpvm service-port enable
TPVM service port is disabled.
WARNING: Disabling Service Port takes effect only after TPVM is restarted.
```

NOTE

Service port is disabled only after the TPVM is restarted.

Docker containers

This section addresses the installation and management of Docker containers.

Installation

Complete the following steps to install the latest version of Docker under TPVM.

1. Install and export the missing Gnu Privacy Guard (GPG) key.

```
gpg --keyserver hkp://keyserver.ubuntu.com:80 --recv 1397BC53640DB551
gpg --export --armor 1397BC53640DB551 | apt-key add -
```

2. Add `[arch=amd64]` before `http://d1.google.com/linux/chrome/deb/ stable main` in the `/etc/apt/sources.list.d/google-chrome.list` file.

3. Update the repository: **`apt-get -y update`**

4. Install the CA certificates: **`apt-get -y install apt-transport-https ca-certificates`**

5. Add the new GPG key for Docker: **`apt-key adv --keyserver hkp://p80.pool.sks-keyservers.net:80 --recv-keys 58118E89F3A912897C070ADB76221572C52609D`**

6. Create or update the `/etc/apt/sources.list.d/docker.list` file to contain the following string: `deb https://apt.dockerproject.org/repo ubuntu-trusty main`

7. Update the Advance Packaging Tool (APT) package index: **`apt-get -y update`**

8. Purge the old repository: **`apt-get -y purge lxc-docker`**

9. Verify that APT is pulling the Docker engine from the proper repository: **apt-cache policy docker-engine**
10. Install the Docker engine: **apt-get -y install docker-engine**
11. Start Docker service: **service docker start**
12. Verify the Docker installation by running the "hello-world" image: **docker run hello-world**

Docker Linux binaries can also be obtained from the following URL by means of the **wget** command:

- Docker script: <https://get.docker.com/>

After downloading the binaries, you extract the archive by using the **tar -xvzf docker-latest.tgz** command, which puts the binaries in a directory named `/docker` in the current location.

Depending upon the Docker engine version, you may have to set "execute" permission on the Docker daemon, by using the **chmod +x docker** command.

Docker requires the binaries to be installed in your host's \$PATH. For example, you can move these binaries to `/usr/bin`.

Starting Docker

Start Docker by using the **service docker start &** command.

The docker daemon always runs as the root user, and binds to a UNIX socket instead of to a TCP port. By default, that UNIX socket is owned by the user "root", and therefore is accessible by means of the **sudo** or **root** commands.

If you (or your Docker installer) create a UNIX group called "docker" and add users to it, then the docker daemon makes the ownership of the UNIX socket read/writable by the docker group when the daemon starts. The docker daemon must always run as the root user, but if you run the docker client as a user in the docker group, then you do not need to add **sudo** to all the client commands.

Upgrading Docker

To upgrade your manual installation of Docker, first kill the docker daemon by using the **killall docker** command.

Running and monitoring Docker containers

You can start, stop, and monitor Docker containers by using the **docker** command. The following table lists frequently used commands.

TABLE 25 Frequently used docker commands

Command	Description
docker help	Lists supported Docker commands
docker --version	Displays the Docker version
docker create image	Creates a new container
docker run -i -t ubuntu /bin/bash	Instantiates a Docker container with bash shell and console connection
docker ps -a	List all Docker containers
docker attach container-id	Attach to a running Docker container
docker start container-id	Start/restart a particular Docker container
docker stop container-id	Stop a particular Docker container
docker rm \$(docker ps -a -q)	Delete all Docker containers
docker rmi \$(docker images -q)	Delete all Docker images

Linux containers

This section addresses the installation of Linux and creating and managing containers.

Installation

LXC 1.0 was tested with TPVM. The `lxc` package can be installed as root by means of the `apt-get install lxc` command.

Your system will then have all the LXC commands, all LXC templates, and also the python3 binding should you want to script LXC.

Creating containers

You can create privileged or unprivileged containers. (Only privileged containers were tested for this release.)

Privileged containers are containers created by root and running as root. They can be created as follows: `sudo lxc-create -t download -n my-container`

This creates a new privileged container "my-container" on TPVM, using an image based on the download template. The download template contains a list of distributions, versions, and architectures to choose from. Good example templates would be "ubuntu" and "trusty".

Running and monitoring containers

Once the container is created, start it by using the `lxc-start -n my-container -d` command.

You can then confirm its status by using either of the following commands:

- `lxc-info -n my-container`
- `lxc-ls -f`

You can access the `my-container` console by using the `lxc-console -n my-container` command.

You get a shell inside the container by using the `lxc-attach -n my-container` command.

Once done, you can stop the container by using the `lxc-stop` command, and remove it by using the `lxc-destroy` command:

- `lxc-stop -n my-container`
- `lxc-destroy -n my-container`

To confirm connectivity, attach to one of the containers and check network access by pinging a server accessible from the host:

- `lxc-attach -n lxc1`
- `ping external-server`

Utilities installation and management

cURL

cURL is a command-line RESTful access utility. The following table lists useful installation and management commands.

TABLE 26 cURL commands

Command	Description
<code>sudo apt-get update</code>	Updates any dependency packages
<code>sudo apt-get install curl</code>	Installs the latest cURL package, or specifies a previous version number

TABLE 26 cURL commands (continued)

Command	Description
<code>sudo apt-get upgrade curl</code>	Upgrades to the latest cURL package

Google-chrome

Google-chrome is a graphical user interface RESTful access utility. The following table lists useful installation and management commands

TABLE 27 Google-chrome commands

Command	Description
<code>sudo apt-get update</code>	Updates any dependency packages
<code>sudo apt-get install google-chrome-stable</code>	Installs the latest Google-chrome package, or specifies a previous version number
<code>sudo apt-get upgrade google-chrome-stable</code>	Upgrades to the latest Google-chrome package

ifconfig and route

The **Ifconfig** and **route** utility commands are available by default in the Ubuntu/Debian package, and can be used without any additional package installation. The following table lists useful command options.

TABLE 28 ifconfig and route command options

Command	Description
<code>ifconfig eth0 Net-IP-Addr netmask <Net-IP-Addr-Mask></code>	Checks interface status and statistics
<code>route add -net Net-IP-Addr netmask Net-IP-Addr-Mask gw Gw-IP</code>	Adds a route
<code>route add default gw GW-IP</code>	Adds a default gateway

Ethtool

The Ethtool utility is used to get device information. The following table lists useful command options.

TABLE 29 Ethtool commands

Command	Description
<code>sudo apt-get update</code>	Updates any dependency packages
<code>sudo apt-get install ethtool</code>	Installs the latest Ethtool package, or specifies a previous version number
<code>sudo apt-get upgrade ethtool</code>	Upgrades to the latest Ethtool package

Tcpdump

Tcpdump is a command line utility that is used for packet capture by means of libpcap. The following table lists useful command options.

TABLE 30 Tcpdump commands

Command	Description
<code>sudo apt-get update</code>	Updates any dependency packages
<code>sudo apt-get install tcpdump</code>	Installs the latest Tcpdump package, or specifies a previous version number
<code>sudo apt-get upgrade tcpdump</code>	Upgrades to the latest Tcpdump package

Tshark

Tshark is a command line utility from the Wireshark community that is used for packet capture by means of libpcap. The following table lists useful command options.

TABLE 31 Tshark commands

Command	Description
<code>sudo apt-get update</code>	Updates any dependency packages
<code>sudo apt-get install tshark</code>	Installs the latest Tshark package, or specifies a previous version number
<code>sudo apt-get upgrade tshark</code>	Upgrades to the latest Tshark package

Wireshark

Wireshark is a GUI-based packet capture utility that is used for packet capture by means of libpcap. The following table lists useful command options.

TABLE 32 Wireshark commands

Command	Description
<code>sudo apt-get update</code>	Updates any dependency packages
<code>sudo apt-get install wireshark</code>	Installs the latest Wireshark package, or specifies a previous version number
<code>sudo apt-get upgrade wireshark</code>	Upgrades to the latest Wireshark package

Assigning a static IP address on the TPVM Linux OS

To use a static IP address, you add the static method for the interface in the file `/etc/network/interfaces`.

1. Get your current address, net mask, and broadcast.

```
device# ifconfig
...
eth0 Link encap:Ethernet HWaddr 00:0a:21:ff:45:2a
      inet addr:10.10.10.0 Bcast:10.10.10.255 Mask:255.255.255.0
      ...
```

The above example displays the first Ethernet interface identified as eth0.

2. Get your gateway and network

```
device# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.10.10.2 0.0.0.0 UG 100 0 0 eth0
172.16.77.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
```

Use flags `u` and `g` for the route gateway. The other IP address is the network IP.

3. Open the interfaces file.

```
device# sudo nano /etc/network/interfaces
```

Nano is the GNU version of the Pico text editor, use the editor of your choice.

4. Find the DHCP settings in the `interfaces` file, they will appear as text similar to the following:

```
...
auto eth0
iface eth0 inet dhcp
...
```

5. Replace the text seen in step 4 with the following.

```
...
auto eth0
iface eth0 inet static
address 10.0.0.100
netmask 255.255.255.0
gateway 10.0.0.0
...
```

The above example configures the first Ethernet interface identified as eth0.

6. Save the file and exit to the command prompt.
7. Make sure your name server IP address is your gateway IP address.

```
device# sudo nano /etc/resolv.conf
```

8. Restart the networking components.

```
device# sudo /etc/init.d/networking restart
```

9. If you want this as a permanent change, remove the DHCP client so it can no longer assign dynamic IP addresses.

```
device# sudo apt-get remove dhcp-client
```

10. Verify connectivity.

```
device# ping www.brocade.com
```

11. Manually enable the interface.

```
device# sudo ifup eth0
```

Network Time Protocol (NTP)

• Network Time Protocol overview	111
• Configuring NTP	113
• Authenticating an NTP server	115
• Displaying the active NTP server	116

Network Time Protocol overview

Network Time Protocol (NTP) maintains uniform time across all devices in a network. The NTP commands support the configuration of an external time server to maintain synchronization among all local clocks in a network.

To keep the time in your network current, it is recommended that each device have its time synchronized with at least one external NTP server.

Date and time settings

Brocade devices maintain the current date and time inside a battery-backed real-time clock (RTC) circuit. Date and time are used for logging events. Device operation does not depend on the date and time; a device with incorrect date and time settings can function correctly. However, because the date and time are used for logging, error detection, and troubleshooting, you should set them correctly.

Time zone settings

The time zone settings have the following characteristics:

- The setting automatically adjusts for Daylight Savings Time.
- Changing the time zone on a device updates the local time zone setup and is reflected in local time calculations.
- By default, all devices are in the Greenwich Mean Time (GMT) time zone (0,0).
- System services that have already started will reflect the time zone changes only after the next reboot.
- Time zone settings persist across failover for high availability.
- Time zone settings are not affected by NTP server synchronization.

Network Time Protocol Server Overview

An Network Time Protocol (NTP) server provides the correct network time on your device. NTP can be used to synchronize the time on devices across a network.

Network Time Protocol server is used to obtain the correct time from an external time source and adjust the local time in each connected device. When NTP server functionality is enabled, the NTP server starts listening on the NTP port for client requests and responds with the reference time. Up to five server addresses in IPv4 or IPv6 format can be configured. When you configure multiple NTP server addresses, the first obtainable address is set as the active NTP server. If there are no reachable time servers, then local device time is the default time until a new active time server is configured. when it has lost synchronization, NTP server operates in master mode to serve time using the local clock. Serving local clock can be enabled using the **ntp master** command.

The NTP server is stateless and will not maintain any NTP client information. Network time synchronization is guaranteed only when a common external time server is used by all devices.

Network Time Protocol Client Overview

The NTP client can be enabled when we configure one or more NTP servers/peers.

The NTP client maintains the server and peer state information as association. The server and peer association is mobilized at the startup or whenever user configures. These statically configured server/peer associations are not demobilized unless user removes the configuration. The symmetric passive association is mobilized upon arrival of NTP packet from peer which is not statically configured. These associations will be demobilized on error or timeout.

The NTP client operation can be summarized as follows:

1. When the device is booted, after system initialization polls all the servers and peers (both configured and dynamically learnt) with the configured poll interval.
2. The multiple samples of server/peer time related fields in the NTP packet is maintained in the association database.
3. The selection, cluster and combine algorithms, chooses the most accurate and reliable server/peer as system peer.

NOTE

Refer, RFC 5905.

4. The reference time from the system peer is used for system time synchronization.
5. The NTP client increases poll interval exponentially from minimum poll interval to maximum poll interval value after clock stabilizes.

After the system peer is chosen, the system time is synchronized using one of the following ways:

1. If the system time differs by less than 128 milliseconds with the system peer, then the system clock is adjusted slowly towards the system peer time reference time.
2. If the system time is greater than 128 milliseconds with the system peer, then the system clock is stepped to the system peer reference time. The time related information stored in the server/peer association database is cleared as they are no more valid.

Network Time Protocol Associations

NTP work in one or more association modes.

The following modes are the NTP polling based associations:

1. NTP server
2. NTP client
3. NTP peer

NTP Server

The server mode requires no prior client configuration. It responds to client mode NTP packets. The **ntp master** command is used to set the device to operate in server mode when it has lost the synchronization

NTP Client

When the system is operating in the client mode, it polls all configured NTP servers and peers. The device selects a host from all the polled NTP servers to synchronize. To configure the NTP servers and peers individually, use **server** and **peer** commands.

NTP Peer

NTP peer mode is intended for configurations where a group of devices operate as mutual backups for each other. If one of the devices lose a reference source, the time values can flow from the surviving peers to all the others.

The NTP peer can operate in:

- **Symmetric Active** - When the peer is configured using the peer command.
- **Symmetric Passive** - Dynamically learnt upon arrival of a NTP packet from the peer which is not configured. The symmetric passive

Network Time Protocol Authentication

The NTP can be configured to provide cryptographic authentication of messages with the clients/peers, and with its upstream time server.

NTP supports symmetric key scheme for authentication. The scheme uses MD5 key hash algorithm. The key-id and the calculated digest form the Message Authentication Code (MAC). When authentication is enabled on the server, it is expected that the client's request message should have valid MAC. If authentication of the client message fails, NTP replies with crypto-NAK packet.

Enabling NTP authentication

To enable Network Time Protocol (NTP) strict authentication, use the authenticate command. To disable the function, use the no form of this command.

```
device(config)# ntp authenticate
```

Syntax: [no] ntp authenticate

Defining an authentication key

To define an authentication key for Network Time Protocol (NTP), use the authentication-key command. To remove the authentication key for NTP, use the no form of this command.

```
device(config)# ntp authentication-key key-id 1 md5 moof
```

Syntax: [no] ntp authentication-key key-id [md5] keystring

The valid key-id parameter is 1 to 65535.

The md5 keyword specifies the message authentication support that is provided using the Message Digest 5 Algorithm.

Configuring NTP

After setting the date and time on a device, the local time on a device can be synchronized with an Network Time Protocol (NTP) server.

The date and time are set in privileged EXEC mode and only have to be configured once per device because the value is written to nonvolatile memory. After the basic time information is set up, an NTP server is configured to allow the local time to be synchronized across the network.

1. Set the date and time for the device.

```
device# clock set 2016-08-06T12:15:00
```

2. Access global configuration mode.

```
device# configure terminal
```

3. Set the time zone for the device.

```
device(config)# clock timezone America/Los_Angeles
```

4. Return to privileged EXEC mode.

```
device(config)# exit
```

5. Display the local date, time, and time zone for the device.

```
device# show clock  
2017-02-09 12:15:00 America/Los_Angeles
```

6. Enter global configuration mode.

```
device# configure terminal
```

7. Synchronize the local time with an external source accessible from a user-specified VRF named myvrf.

```
device(config)# ntp server 192.168.10.1 use-vrf myvrf
```

8. Exit to global configuration mode.

```
device(config)# exit
```

9. Exit to privileged EXEC mode.

```
device(config)# exit
```

10. Display the active NTP server IP address.

```
device# show ntp status  
Clock is synchronized, stratum 3, reference clock is 192.168.128.5  
precision is 2**24  
reference time is CC38EC6A.8FCCA1C4 (10:10:02.561 JST Fri Jan 20 2017 )  
clock offset is -1.051 msec, root delay is 174.060 msec  
root dispersion is 172.37 msec, peer dispersion is 0.10 msec  
system poll interval is 32, last update was 19 sec ago  
NTP server mode is enabled, NTP client mode is enabled  
NTP master mode is disabled, NTP master stratum is 8
```

In the following example, the date, time and time zone are set on a device and verified. The local device is configured to synchronize the local time with an external NTP server at a specific IP address, accessible from a user-specified VRF named myvrf.

```
device# clock set 2017-02-09 12:15:00
device# configure terminal
device(config)# clock timezone America/Los_Angeles
device(config)# exit
device# show clock
2017-02-09 12:15:00 America/Los_Angeles
device# configure terminal
device(config)# ntp server 192.168.10.1 use-vrf myvrf
device(config)# exit
device(config)# exit
device# show ntp status
Clock is synchronized, stratum 3, reference clock is 192.168.128.5
precision is 2**24
reference time is CC38EC6A.8FCCA1C4 (10:10:02.561 JST Fri Jan 20 2017 )
clock offset is -1.051 msec, root delay is 174.060 msec
root dispersion is 172.37 msec, peer dispersion is 0.10 msec
system poll interval is 32, last update was 19 sec ago
NTP server mode is enabled, NTP client mode is enabled
NTP master mode is disabled, NTP master stratum is 8
```

Authenticating an NTP server

An authentication key can be created for the purpose of authenticating an external Network Time Protocol (NTP) server.

This task demonstrates how to create an authentication key and associate the key to an NTP server.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Create an authentication key ID and key string.

```
device(config)# ntp authentication-key 33 md5 check
```

Up to five NTP authentication keys can be configured and each key ID must be unique.

3. Synchronize the local time with an external source, an NTP server, accessible by the management VRF. Associate the key to the NTP server.

```
device(config)# ntp server 192.168.10.1 key 33
```

4. Exit to global configuration mode.

```
device(config)# exit
```

5. Exit to privileged EXEC mode.

```
device(config)# exit
```

In the following example, an authentication key with an ID of 33 is created and the local time on the device is synchronized with an external NTP server at the IP address of 192.168.10.1.

```
device# configure terminal
device(config)# ntp authentication-key 33 md5 check
device(config)# ntp server 192.168.10.1
device(config)# server-192.168.10.1 key 33
device(config)# exit
device(config)# exit
```

Displaying the active NTP server

Information about the currently active NTP server can be displayed. When an NTP server has been configured, the server IP address is displayed. If an NTP server is not configured or the server is unreachable, the output displays LOCL (for local device time).

Only the local NTP server information is displayed.

NTP server status when an NTP server is not configured

The following example shows the local device NTP status when an NTP server is not configured:

```
device# show ntp status
Clock is synchronized, stratum 9, reference clock is 127.127.1.0
precision is 2**-24
reference time is ddddebd8.6c995cf9 ( 6:36:10.1821990137 GMT Fri Dec 15 2017)
clock offset is 0.0000 msec, root delay is 0.0000 msec
root dispersion is 11.1813 msec, peer dispersion is 10.0000 msec
system poll interval is 64, last clock update was 17 sec ago

NTP server mode is enabled, NTP client mode is enabled
NTP master mode is enabled, NTP master stratum is 8
```

NTP server status when an NTP server is configured

The following example shows the status of a configured NTP server:

```
device# show ntp status
Clock is synchronized, stratum 3, reference clock is 192.168.128.5
precision is 2**24
reference time is CC38EC6A.8FCCA1C4 (10:10:02.561 JST Fri Jan 20 2017 )
clock offset is -1.051 msec, root delay is 174.060 msec
root dispersion is 172.37 msec, peer dispersion is 0.10 msec
system poll interval is 32, last update was 19 sec ago

NTP server mode is enabled, NTP client mode is enabled
NTP master mode is disabled, NTP master stratum is 8
```

SNMP

• SNMP overview.....	117
• Configuring SNMPv2.....	120
• Configuring SNMPv3.....	121
• Configuring an SNMP server context to a VRF.....	122
• Offline SNMP ifIndex generation tool.....	123

SNMP overview

Simple Network Management Protocol (SNMP) is a set of application layer protocols for managing complex networks. Devices within a network use SNMP to send messages, called protocol data units (PDUs), to different parts of a network.

Network management using SNMP requires three components:

- **SNMP manager**—Typically, network management systems (NMS) that manage networks by monitoring the network parameters, and optionally, setting parameters in managed devices. The SNMP manager communicates to the devices within a network using the SNMP protocol.
- **SNMP agent**—Software that resides in the managed devices in the network, and collects and stores data from these devices. Each device hosts an SNMP agent. The agent receive requests from the SNMP manager and responds with the requested data. In addition, the agent can asynchronously alert the SNMP manager about events by using special PDUs called traps.

Multiple instances of the same MIB module can support a single SNMP agent by mapping a specific key called a context name to a virtual routing and forwarding (VRF) instance created within the Brocade device.

- **Management Information Base (MIB)**—Hierarchical database where SNMP agents in the managed devices store the data about these devices. The MIB is structured on the standard specified in the RFC 2578 [Structure of Management Information Version 2 (SMIv2)].

An SNMP manager can issue read or write operations to retrieve and use the MIB objects to manage and monitor devices on the network. However, the MIB structure determines the scope of management access allowed by a device.

The SNMP server on the Brocade device supports SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2), and SNMP version 3 (SNMPv3).

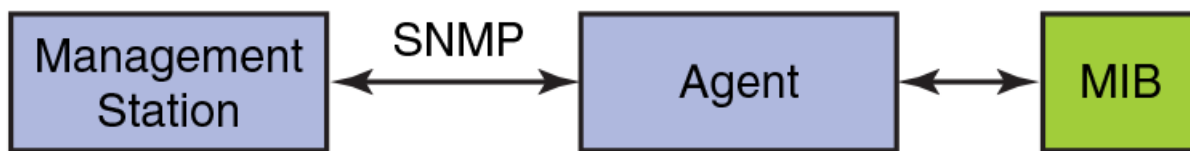
- SNMPv1 and SNMPv2 use community strings associated to SNMP groups. The group maps the user to MIB objects called SNMP views. The views restrict the access of the MIB OIDs .
- SNMPv3 provides additional security through authenticated users associated with groups to restrict the access of MIBs for SNMP requests through SNMP views.

Also, the device supports the configuration of trap hosts as a trap recipient to receive filtered traps based on their severity level, and optionally receive SNMP communication through a VRF.

Basic SNMP operation

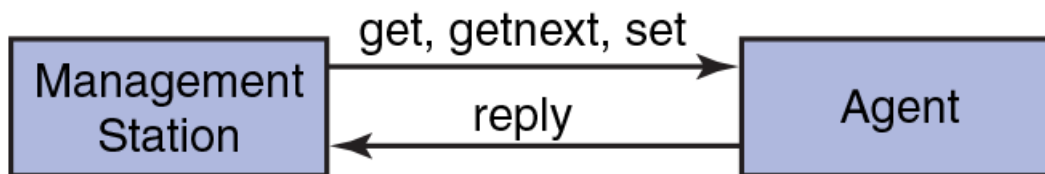
Every Brocade device carries an *agent* and management information base (MIB), as shown in the next figure. The agent accesses information about a device and makes it available to an SNMP network management station.

FIGURE 6 SNMP structure



When active, the management station can "get" information or "set" information when it queries an agent. SNMP commands, such as **get**, **set**, **getnext**, and **getresponse**, are sent from the management station, and the agent replies once the value is obtained or modified as shown in the next figure. Agents use variables to report such data as the number of bytes and packets in and out of the device, or the number of broadcast messages sent and received. These variables are also known as managed objects. All managed objects are contained in the MIB.

FIGURE 7 SNMP query



The management station can also receive *traps*, unsolicited messages from the device agent if an unusual event occurs as shown in the next figure.

FIGURE 8 SNMP trap



The agent can receive queries from one or more management stations and can send traps to up to six management stations.

SNMP community strings

SNMP versions 1 and 2 use community strings to restrict SNMP access.

You associate the community string with an SNMP group to restrict the access of MIBs for SNMPv1 and SNMPv2c requests. You can configure a total of 256 read-only and read-write community strings on the device.

The software automatically encrypts SNMP community strings. Users with read-only access or who do not have access to management functions in the CLI cannot display the strings. For users with read-write access, the strings are encrypted in the CLI.

By default, you cannot perform any SNMP Set operations until you configure a read-write community string.

SNMP groups

SNMP groups map the SNMP user for SNMPv3 and the community for the SNMPv1 and SNMPv2 to SNMP views.

You can configure each group with any or all of the following views:

- Read view with read-only access
- Write view with read-write access
- Notify view to filter notifications to be encrypted and sent to target hosts

SNMP users that are mapped to a group with SNMP views use its views for access control.

SNMP users

SNMP version 3 (RFC 2570 through 2575) introduces a User-Based Security model (RFC 2574) for authentication and privacy services. This model provides a user that is associated with security information for authentication of its generated SNMP messages.

SNMP version 3 also supports View-Based Access Control Mechanism (RFC 2575) to control access at the PDU level. It defines mechanisms for determining whether to allow access to a managed object in a local MIB by a remote principal. You can create and associate SNMPv3 users with configured SNMP groups to use the group views for access control.

SNMP views

SNMP views are named groups of MIB objects that you can associate with groups to limit access by community strings and users for viewing and modifying the SNMP statistics and system configuration. With SNMP views, you can create or remove the access to a MIB object for inclusion or exclusion from viewing from user access.

SNMP views reference MIB objects using object names. It represents the hierarchical location of the object in the MIB tree. You associate the views with each group to restrict or allow access to the OIDs. You can create a maximum of 10 views on the device.

SNMP server hosts

On the Brocade device, the SNMP server host serves as a trap receiver to ensure that all SNMP traps sent by the device go to the same SNMP trap receiver or set of receivers, typically one or more host devices on the network.

For an SNMPv3 trap, you associate a SNMPv3 host with the SNMP users. When you specify the host, you also specify a community string for SNMPv1 and SNMPv2. The Brocade device sends all the SNMP traps to the specified hosts and includes the specified community string. Then, administrators can filter for traps from a Brocade device based on IP address or community string.

Multiple SNMP server context to VRF mapping

A single SNMP agent can support multiple instances of the same MIB module by the mapping of the context name to a virtual routing and forwarding (VRF) instance created within the device.

You map each VRF with a specific context name. The context name identifies the VRF and fetches the MIB details of the mapped VRF from the underlying modules. For example, the OSPF-MIB returns the queried OSPF-MIB object values pertaining to the default VRF (default-vrf).

For SNMPv1 and SNMPv2, the mapping of the context is with the community. This mapping is in addition to mapping of the context with the VRF. The SNMP agent supports 256 contexts to support context-to-VRF mapping.

For SNMPv3, you only need to map the context with the VRF. The SNMPv3 request PDU itself provisions for the context. Only one context is allowed for each VRF instance.

Configuring SNMPv2

SNMPv1 and SNMPv2 use community strings to restrict SNMP access. When you associate it with an SNMP group, you can restrict the access of MIBs for SNMPv1 and SNMPv2c requests.

To configure SNMPv2, perform the following steps.

1. In privileged EXEC mode, enter global configuration mode.

```
device# configure terminal
```

2. Configure the location and contact information for the SNMP server.

```
device(config)# snmp-server location "Building 3 Room 214" contact "Operator 12345"
```

This example changes the default location from BrocadeTcsHyd to "Building 3 Room 214" and default contact information from BrocadeCommunicationSystem to "Operator 12345".

The double quotes allows you to enter the string with spaces.

3. Add an SNMP view to restrict or allow access to the MIB OIDs.

```
device(config)# snmp-server view view2 1.3.6.1 included
```

This example adds the SNMP view2 view entry with included permission to allow access for the MIB 1.3.6.1 object ID ('internet').

4. Add an SNMP group.

```
device(config)# snmp-server group admin v2c write view2 notify view2
```

This example adds the admin group for SNMPv2 and maps the read-write access and notify views to view2.

5. Add an SNMP community string and associate it with a group.

```
device(config)# snmp-server community comm1 group admin
```

This example adds the comm1 community string and associates it with the admin group to access the MIBs for SNMPv2c requests.

6. Configure the SNMP trap host associated with community string.

```
device(config)# snmp-server host 10.32.147.6 comm1 version 2c severity-level Warning
```

This example configures 10.32.147.6 as a trap recipient with SNMPv2c on the default target port 162 and associates the comm1 community string.

7. Enable the traps.

```
device(config)# snmp-server enable trap
```

8. Access privileged EXEC mode.

```
device(config)# exit
```


9. Verify the configuration.

```
device# show running-config snmp-server
snmp-server contact "Operator 12345"
snmp-server enable trap
snmp-server location "Building 3 Room 214"
snmp-server community comm1 group admin
snmp-server group admin v2c write view2 notify view2
snmp-server host 10.32.147.6 comm1 version 2c
severity-level Warning
!
```

The following example shows the previous steps to configure SNMPv2.

```
device# configure terminal
device(config)# snmp-server location "Building 3 Room 214" contact "Operator 12345"
device(config)# snmp-server view view2 1.3.6.1 included
device(config)# snmp-server group admin v2c write view2 notify view2
device(config)# snmp-server community comm1 group admin
device(config)# snmp-server host 10.32.147.6 comm1 version 2c severity-level Warning
device(config)# snmp-server enable trap
```

Configuring SNMPv3

SNMPv3 uses SNMP users to restrict SNMP access. When you map an SNMP user to an SNMP group, you can restrict the access of MIBs for SNMP requests through an SNMP view.

To configure SNMPv3, perform the following steps.

1. In privileged EXEC mode, enter global configuration mode.

```
device# configure terminal
```

2. Configure the contact information for the SNMP server.

```
device(config)# snmp-server contact "Network Management group - Contact # 123-123-1234"
```

This example changes the default contact information from Field Support to "Network Management group - Contact # 123-123-1234".

The double quotes allows you to enter the string with spaces.

3. Configure the location information for the SNMP server.

```
device(config)# snmp-server location "South Room, Rack-11"
```

This example changes the default location from End User Premise to "South Room, Rack-11".

The double quotes allows you to enter the string with spaces.

4. Add an SNMP view to restrict or allow access to the MIB OIDs.

```
device(config)# snmp-server view view2 1.3.6.1 included
```

This example adds the SNMP view2 view entry with included permission to allow access for the MIB 1.3.6.1 object ID ('internet').

5. Add an SNMP group.

```
device(config)# snmp-server group group1 v3 priv write view2 notify view2
```

This example adds the group1 group for SNMPv3 and maps the read-write access and notify views to view2.

6. Add an SNMP user and associate it with a group.

```
device(config)# snmp-server user user2 groupname group1 auth md5 auth-password private123 priv DES
priv-password public123
```

This example adds the user2 user and associates it with the group1 group to access of MIBs for SNMPv3 requests. For SNMPv3 users, the passwords for **auth-password** and **priv-password** keywords are encrypted while storing to the persistent memory or displaying it back to the user. You can configure either with a plain-text password or an encrypted password. In both cases, the **show running-config** command displays the passwords as encrypted.

7. Configure the SNMPv3 trap host associated with an SNMP user.

```
device(config)# snmp-server v3host 10.26.3.166 user2 severity-level Info udp-port
4425
```

This example configures 10.26.3.166 as an SNMPv3 trap recipient host on the target port 4425 and associates the user2 user.

The global SNMPv3 host can be associated with global SNMPv3 users only. You cannot create an SNMPv3 host in a global configuration by associating it with local SNMPv3 users.

8. Enable the traps.

```
device(config)# snmp-server enable trap
```

9. Access privileged EXEC mode.

```
device(config)# exit
```

10. Verify the configuration.

```
device# show running-config snmp-server
snmp-server contact "Network Management group - Contact # 123-123-1234"
snmp-server enable trap
snmp-server location "South Room, Rack-11"
snmp-server group group1 v3 priv write view2 notify view2
snmp-server user user2 groupname group1 md5 auth-password private123 priv DES priv-password public123
snmp-server v3host 10.26.3.166 user2
severity-level Info
udp-port 4425
!
snmp-server view view2 1.3.6.1 included
```

The following example shows the previous steps to configure SNMPv3.

```
device# configure terminal
device(config)# snmp-server contact "Network Management group - Contact # 123-123-1234"
device(config)# snmp-server location "South Room, Rack-11"
device(config)# snmp-server view view2 1.3.6.1 included
device(config)# snmp-server group group1 v3 priv write view2 notify view2
device(config)# snmp-server user user2 groupname group1 md5 auth-password private123 priv DES priv-password
public123
device(config)# snmp-server v3host 10.26.3.166 user2 severity-level Info udp-port 4425
device(config)# snmp-server enable trap
```

Configuring an SNMP server context to a VRF

A single SNMP agent can support multiple instances of the same MIB module by mapping the context name to a virtual routing and forwarding (VRF) instance created within the device. The SNMP context name is used to identify the VRF and fetch the MIB details of the mapped VRF from the underlying modules.

To configure an SNMP server context to a VRF for SNMPv1 or SNMPv2, perform the following steps.

NOTE

For SNMPv3, use the **snmp-server context** command only. The SNMPv3 request PDU itself has the provision for the context name as input.

ATTENTION

SNMP SET requests work only on the default VRF.

1. In privileged EXEC mode, enter global configuration mode.

```
device# configure terminal
```

2. Map the context with the community.

```
device(config)# snmp-server community public groupname admin
```

3. Create a context and map it with a VRF.

```
device(config)# snmp-server context mycontext vrf myvrf
```

4. Map the community to the context.

```
device(config)# snmp-server mib community-map public context mycontext
```

5. Verify the configuration.

```
device# show running-config snmp-server
...
snmp-server community public groupname admin
snmp-server context mycontext vrf myvrf
...
snmp-server mib community-map public context mycontext
```

The following example shows the previous steps for the configuration.

```
device# configure terminal
device(config)# snmp-server community public groupname admin
device(config)# snmp-server context mycontext vrf myvrf
device(config)# snmp-server mib community-map public context mycontext
```

Offline SNMP ifIndex generation tool

On Brocade SLX Router, SNMP Management Information Base (MIB) uses Interface Index (ifIndex) to assign a unique identifying value to each interface.

The ifIndex is encoded per interface type and the assigned value is used if any information needs to be polled for a particular interface. The offline SNMP ifIndex generation tool which is developed based on Python, provides a means to find out the ifIndexes associated with various interfaces. This tool can run on any platform (SLX Router, Linux, or Windows) wherever the Python package is installed. The script is available on SLX Router at `/fabos/cliexec/ifindex_gen.py`. If you want to run it on a Linux or Windows platform, you may have to modify the first line in the script to point to the location of the Python binary on the platform.

Generating ifIndexes for various interfaces

ifIndex can be generated offline for various interface types such as physical interface, LAG (port-channel) interface, VE interface, loopback interface, tunnel interface and Management interface.

To generate ifIndex for a specific interface, perform the following steps.

1. Enter SLX-OS Linux shell from privileged EXEC mode.

```
device# start-shell
```

2. Retrieve syntax to find available options to generate ifIndex.

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -h
usage: ifindex_gen.py [-h] -i INTF_TYPE [-t LC_TYPE] [-m MODE] [-s SLOT]
                    [-p PORT] [-sp SUB_PORT] [-lp LAG_PORT]
                    [-vb VE_BRIDGE_ID] [-vi VE_INTF_ID] [-tt TUNNEL_TYPE]
                    [-ti TUNNEL_ID] [-lbi LB_INTF_ID] [-mi MGMT_INTF_ID]
                    [-d DISP_MODE]

arguments:
-h, --help            show this help message and exit
-i INTF_TYPE          Interface type: [phy (physical) | lag | ve | tunnel | lb
                    (loopback) | mgmt (management)]
-t LC_TYPE            LC type: [72x10G | 36x100G]
-m MODE              PortGroup Mode: [40g | 100g] (required when LC type is
                    36x100G)
-s SLOT              Slot #: [1-8]
-p PORT              Port #: [1-72] for 72x10G, [1-60] for 36x100G LC type
-sp SUB_PORT          Sub Port #: [1-4] for break-out ports (required when LC
                    type is 36x100G, PortGroup Mode is 40g and break-out is
                    enabled)
-lp LAG_PORT          LAG Port #: [1-512]
-vb VE_BRIDGE_ID     VE Bridge ID: [0-255]
-vi VE_INTF_ID       VE Interface ID: [1-4096]
-tt TUNNEL_TYPE      Tunnel type: [vxlan | gre | nvgre | mpls]
-ti TUNNEL_ID        Tunnel ID: [1-1024]
-lbi LB_INTF_ID      Loopback Interface ID: [1-255]
-mi MGMT_INTF_ID     Management Interface ID: [1-2]
-d DISP_MODE         Output Display Mode: [bin | dec | hex | all] (default:
                    dec)
```

Note: The parameters -t, -m, -s, -p, and -sp are the sub-options specific to physical interface.

3. Generate ifIndex for a specific interface. In this example, ifIndex is generated for a physical interface.

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i physical -t 72x10G -s 2 -p 65 -d all
Decimal : 413171855
Hex      : 18a0808f
Binary   : 00011000101000001000000010001111
```

Configuration examples for generating ifIndexes offline

The following examples provide details on how ifIndexes can be generated for various interface types.

Physical interfaces with LC type 72x10G

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i physical -t 72x10G -s 2 -p 65 -d all
Decimal : 413171855
Hex      : 18a0808f
Binary   : 00011000101000001000000010001111
```

Physical interfaces with LC type 36x100G (100g mode)

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i phy -t 36x100G -m 100g -s 3 -p 1 -d all
Decimal : 415285249
```

```
Hex      : 18c0c001
Binary  : 00011000110000001100000000000001
```

Physical interfaces with LC type 36x100G (40g mode) non-breakout

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i phy -t 36x100G -m 40g -s 3 -p 8 -d all
Decimal : 207683777
Hex     : 0c6100c1
Binary  : 00001100011000010000000011000001
```

Physical interfaces with LC type 36x100G (40g mode) breakout

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i phy -t 36x100G -m 40g -s 3 -p 15 -sp 1 -d all
Decimal : 207741442
Hex     : 0c61e202
Binary  : 00001100011000011110001000000010
```

LAG (Port-channel) interface

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i lag -lp 1 -d all
Decimal : 671088641
Hex     : 28000001
Binary  : 00101000000000000000000000000001
```

VE interface

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i ve -vi 10 -d all
Decimal : 1207959562
Hex     : 4800000a
Binary  : 010010000000000000000000000001010
```

Tunnel interfaces

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i tunnel -tt mpls -ti 2 -d all
Decimal : 2092957698
Hex     : 7cc00002
Binary  : 01111100110000000000000000000010
```

Loopback interface

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i lb -lbi 20 -d all
Decimal : 1476395028
Hex     : 58000014
Binary  : 0101100000000000000000000000010100
```

Management interface

```
[admin@SLX]# /fabos/cliexec/ifindex_gen.py -i mgmt -mi 2 -d all
Decimal : 805306370
Hex     : 30000002
Binary  : 001100000000000000000000000000010
```


LLDP

- [LLDP overview.....](#) 127
- [Configuring and managing LLDP.....](#) 129

LLDP overview

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP) enhances the ability of network management tools to discover and maintain accurate network topologies and simplify LAN troubleshooting in multi-vendor environments. To efficiently and effectively operate the various devices in a LAN you must ensure the correct and valid configuration of the protocols and applications that are enabled on these devices. With Layer 2 networks expanding dramatically, it is difficult for a network administrator to statically monitor and configure each device in the network.

Using LLDP, network devices such as routers and switches advertise information about themselves to other network devices and store the information they discover. Details such as device configuration, device capabilities, and device identification are advertised. LLDP defines the following:

- A common set of advertisement messages.
- A protocol for transmitting the advertisements.
- A method for storing the information contained in received advertisements.

NOTE

LLDP runs over the data-link layer which allows two devices running different network layer protocols to learn about each other.

LLDP information is transmitted periodically and stored for a finite period. Every time a device receives an LLDP advertisement frame, it stores the information and initializes a timer. If the timer reaches the time to live (TTL) value, the LLDP device deletes the stored information ensuring that only valid and current LLDP information is stored in network devices and is available to network management systems.

Layer 2 topology mapping

The LLDP protocol lets network management systems accurately discover and model Layer 2 network topologies. As LLDP devices transmit and receive advertisements, the devices store information they discover about their neighbors. Advertisement data such as a neighbor's management address, device type, and port identification is useful in determining what neighboring devices are in the network.

NOTE

The Brocade LLDP implementation supports up to two neighbors.

The higher level management tools, such as the Brocade Network Advisor, can query the LLDP information to draw Layer 2 physical topologies. The management tools can continue to query a neighboring device through the device's management address provided in the LLDP information exchange. As this process is repeated, the complete Layer 2 topology is mapped.

In LLDP the link discovery is achieved through the exchange of link-level information between two link partners. The link-level information is refreshed periodically to reflect any dynamic changes in link-level parameters. The basic format for exchanging information in LLDP is in the form of a type, length, value (TLV) field.

LLDP keeps a database for both local and remote configurations. The LLDP standard currently supports three categories of TLVs. Brocade's LLDP implementation adds a proprietary Brocade extension TLV set. The four TLV sets are described as follows:

- Basic management TLV set — This set provides information to map the Layer 2 topology and includes the following TLVs:
 - Chassis ID TLV — Provides the ID for the switch or router where the port resides. This is a mandatory TLV.
 - Port ID TLV—Provides a unique identifiable information of the port. The Port ID could be one of the following: MAC address, Network address, Interface name of the port. On the SLX-OS, the interface name of the port is provided. This is a mandatory TLV.
 - Port description TLV — Provides a description of the port in an alphanumeric format. If the LAN device supports RFC-2863, the port description TLV value equals the "ifDescr" object. This is an optional TLV.
 - System name TLV — Provides the system-assigned name in an alphanumeric format. If the LAN device supports RFC-3418, the system name TLV value equals the "sysName" object. This is an optional TLV.
 - System description TLV — Provides a description of the network entity in an alphanumeric format. This includes system name, hardware version, operating system, and supported networking software. If the LAN device supports RFC-3418, the value equals the "sysDescr" object. This is an optional TLV.
 - System capabilities TLV — Indicates the primary functions of the device and whether these functions are enabled in the device. The capabilities are indicated by two octets. The first octet indicates Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and Station, respectively. The second octet is reserved. This is an optional TLV.
 - Management address TLV — Indicates the addresses of the local switch. Remote switches can use this address to obtain information related to the local switch. This is an optional TLV.
- IEEE 802.1 organizational TLV set — This set provides information to detect mismatched settings between local and remote devices. A trap or event can be reported once a mismatch is detected. This is an optional TLV. This set includes the following TLVs:
 - Port VLANID TLV — Indicates the port VLAN ID (PVID) that is associated with an untagged or priority tagged data frame received on the VLAN port.
 - PPVLAN ID TLV — Indicates the port- and protocol-based VLAN ID (PPVID) that is associated with an untagged or priority tagged data frame received on the VLAN port. The TLV supports a "flags" field that indicates whether the port is capable of supporting port- and protocol-based VLANs (PPVLANs) and whether one or more PPVLANs are enabled. The number of PPVLAN ID TLVs in a Link Layer Discovery Protocol Data Unit (LLDPDU) corresponds to the number of the PPVLANs enabled on the port.
 - VLAN name TLV — Indicates the assigned name of any VLAN on the device. If the LAN device supports RFC-2674, the value equals the "dot1QVLANStaticName" object. The number of VLAN name TLVs in an LLDPDU corresponds to the number of VLANs enabled on the port.
 - Protocol identity TLV — Indicates the set of protocols that are accessible at the device's port. The protocol identity field in the TLV contains a number of octets after the Layer 2 address that can enable the receiving device to recognize the protocol. For example, a device that wishes to advertise the spanning tree protocol includes at least eight octets: 802.3 length (two octets), LLC addresses (two octets), 802.3 control (one octet), protocol ID (two octets), and the protocol version (one octet).
- IEEE 802.3 organizational TLV set — This is an optional TLV set. This set includes the following TLVs:
 - MAC/PHY configuration/status TLV — Indicates duplex and bit rate capabilities and the current duplex and bit rate settings of the local interface. It also indicates whether the current settings were configured through auto-negotiation or through manual configuration.
 - Power through media dependent interface (MDI) TLV — Indicates the power capabilities of the LAN device.
 - Link aggregation TLV — Indicates whether the link (associated with the port on which the LLDPDU is transmitted) can be aggregated. It also indicates whether the link is currently aggregated and provides the aggregated port identifier if the link is aggregated.
 - Maximum Ethernet frame size TLV — Indicates the maximum frame size capability of the device's MAC and PHY implementation.

LLDP configuration guidelines and restrictions

Follow these LLDP configuration guidelines and restrictions when configuring LLDP:

- Brocade's implementation of LLDP supports standard LLDP information.
- Mandatory TLVs are always advertised.
- The exchange of LLDP link-level parameters is transparent to the other Layer 2 protocols. The LLDP link-level parameters are reported by LLDP to other interested protocols.

Configuring and managing LLDP

The following sections discuss working with the Link Layer Discovery Protocol (LLDP) on Brocade devices.

Understanding the default LLDP

The following table lists the default LLDP configuration. Consider this when making changes to the defaults.

TABLE 33 Default LLDP configuration

Parameter	Default setting
LLDP global state	Enabled
LLDP receive	Enabled
LLDP transmit	Enabled
Transmission frequency of LLDP updates	30 seconds
Hold time for receiving devices before discarding	120 seconds

Disabling LLDP globally

LLDP is enabled globally by default. You can disable LLDP globally without changing any other aspect of the LLDP configuration.

To globally disable LLDP, perform the following steps:

1. From privileged EXEC mode, access global configuration mode.

```
device# configure terminal
```

2. Access LLDP configuration mode.

```
device(config)# protocol lldp
```

3. Disable LLDP globally.

```
device(config-lldp)# disable
```

4. Verify the configuration.

```
device(config-lldp)# do show running-config protocol lldp
protocol lldp
 system-description Brocade BR-SLX9850-4 Router
 disable
!
```

The following configuration is an example of the previous steps to disable LLDP.

```
device# configure terminal
device(config)# protocol lldp
device(config-lldp)# disable
```

If required, re-enable LLDP.

```
device(config-lldp)# no disable
```

Configuring LLDP global parameters

When LLDP is enabled, the default values of its parameters are set. You can change the configuration of these parameters in LLDP configuration mode.

Specifying a system name for the Brocade device hardware

The global system name for LLDP is useful for differentiating between devices. By default, the host name from the chassis/entity management information base is used. By specifying a descriptive system name, you may find it easier to distinguish the device with LLDP. The following example changes the system name to Brocade_Alpha.

```
device(conf-lldp)# system-name Brocade_Alpha
```

Specifying an LLDP system description

The default system description depends on the device type. For example, the default description for a Brocade SLX 9850-4 router is Brocade BR-SLX9850-4 Router.

Brocade recommends that you use the operating system version for the description or use the description from the chassis/entity management information base (MIB).

Do not use special characters, such as #!@, as part of the system name and description. The following example specifies the IT_1.6.2_LLDP_01 system description.

```
device(conf-lldp)# system-description IT_1.6.2_LLDP_01
```

Specifying a user description for LLDP

A user description for LLDP is for network administrative purposes and is not seen by neighboring devices. The following example specifies the Brocade-LLDP-installed-jan-25 description.

```
device(conf-lldp)# description Brocade-LLDP-installed-jan-25
```

Enabling and disabling the receiving and transmitting of LLDP frames

By default both transmit and receive for LLDP frames is enabled.

- The following example enables only receiving of LLDP frames.

```
device(conf-lldp)# mode rx
```

- The following example enables only transmitting of LLDP frames.

```
device(conf-lldp)# mode tx
```

Configuring the transmit frequency of LLDP frames

The default transmit frequency of LLDP frames is 30 seconds. You can change the frequency from 4 to 180 seconds. The following example changes the frequency to 45 seconds.

```
device(conf-lldp)# hello 45
```

Configuring the hold time for receiving devices

By default, four consecutive LLDP hello packets can be missed before removing the neighbor information. You can configure from 1 to 10 consecutive LLDP hello packets that can be missed before removing the neighbor information. The following example configures the 6 consecutive LLDP hello packets.

```
device(conf-lldp)# multiplier 6
```

Advertising the optional LLDP TLVs

By default, the port description and system name are advertised

You can advertise the rest of the optional LLDP TLVs. The following example advertises the management address, capabilities, name and description of the device, and user-configured port.

```
device(conf-lldp)# advertise optional-tlv management-address port-description system-capabilities system-name system-description
```

Configuring the advertisement of LLDP organizationally-specific TLVs

You have the option of advertising dot1.tlv and dot3.tlv. The following example advertise dot1.tlv.

NOTE

Brocade does not recommend advertising dot1.tlv and dot3.tlv LLDPs if your network contains Converged Network Adapters (CNAs) from non-Brocade vendors. Functionality problems can occur.

```
device(conf-lldp)# advertise dot1-tlv
```

Configuring LLDP profiles

SLX 9240 supports 128 active profiles and SLX 9140 supports 72 active profiles. When you configure a profile, its default parameters are from the global LLDP configuration.

1. In privileged EXEC mode, access global configuration mode.

```
device# configure terminal
```

2. Enter LLDP configuration mode.

```
device(config)# protocol lldp
```

3. Configure the profile name.

```
device(conf-lldp)# profile UK_LLDP_IT
```

4. Specify a description for the profile.

```
device(conf-lldp-profile-UK_LLDP_IT)#description standard_profile_by_Jane
```

- Configure the transmission frequency of LLDP updates.

```
device(conf-lldp-profile-UK_LLDP_IT)# hello 10
```

- Configure the hold time for receiving devices.

```
device(conf-lldp-profile-UK_LLDP_IT)# multiplier 2
```

- Advertise the optional LLDP TLVs.

```
device(conf-lldp)# advertise optional-tlv system-name
```

- Advertise the LLDP organizationally-specific TLVs.

```
device(conf-lldp-profile-UK_LLDP_IT)# advertise advertise dot1-tlv
```

NOTE

Brocade does not recommend advertising dot1.tlv and dot3.tlv LLDPs if your network contains CNAs from non-Brocade vendors. Functionality problems can occur.

- Return to privileged EXEC mode.

```
device(conf-lldp-profile-UK_LLDP_IT)# end
```

- Verify the configuration.

```
device# show running-config protocol lldp profile
profile UK_LLDP_IT
hello 10
multiplier 2
advertise dot1-tlv
advertise option-tlv system-name
description standard_profile_by_Jane
```

The following configuration is an example of the previous steps.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# profile UK_LLDP_IT
device(conf-lldp-profile-UK_LLDP_IT)# description standard_profile_by_Jane
device(conf-lldp-profile-UK_LLDP_IT)# hello 10
device(conf-lldp-profile-UK_LLDP_IT)# multiplier 2
device(conf-lldp-profile-UK_LLDP_IT)# advertise option-tlv system-name
device(conf-lldp-profile-UK_LLDP_IT)# advertise advertise dot1-tlv
```

Configuring an LLDP profile to an interface

You can assign only one LLDP profile to an interface. If you do not use the **lldp profile** option at the interface level, the interface uses the global LLDP configuration.

To configure LLDP interface-level command options, perform the following steps.

- In privileged EXEC mode, access global configuration mode.

```
device# configure terminal
```

- Access the interface configuration mode.

```
device(config)# interface Ethernet 1/8
```

3. Apply an LLDP profile to the interface.

```
device(conf-if-eth-1/8)# lldp profile network_standard
```

4. Return to privileged EXEC mode.

```
device(conf-if-eth-1/8)# end
```

5. Save the running-config file to the startup-config file.

```
device# copy running-config startup-config
```

The following configuration is an example of the previous steps.

```
device# configure terminal
device(config)# interface Ethernet 1/8
device(conf-if-eth-1/8)# lldp profile network_standard
```

Displaying LLDP information

The **show lldp** command allows you to display the following information:

- LLDP status
- LLDP neighbor information
- LLDP statistics

Displaying LLDP status

To display the global LLDP status, use the **show lldp** command.

```
device# show lldp
LLDP Global Information
system-name: SLX
system-description: Brocade BR-SLX9850-4 Router
description: Brocade-LLDP
State: Enabled
Mode: Receive/Transmit
Advertise Transmitted: 30 seconds
Hold time for advertise: 120 seconds
Tx Delay Timer: 1 seconds
Transmit TLVs: Chassis ID Port ID
                TTL Port Description
                System Name
```

To display LLDP status for an Ethernet interface, use the **show lldp interface ethernet** command.

```
device# show lldp interface ethernet 1/18
LLDP information for Eth 1/18
State: Enabled
Mode: Receive/Transmit
Advertise Transmitted: 30 seconds
Hold time for advertise: 120 seconds
Tx Delay Timer: 1 seconds
Transmit TLVs: Chassis ID Port ID
                TTL Port Description
                System Name
```

Displaying LLDP neighbor information

To display the LLDP neighbor information, use the **show lldp neighbors** command. This command allows you to display the information for all Ethernet interfaces, a specific interface, or detailed neighbor information.

The following example displays the LLDP neighbor information for all interfaces.

```
device# show lldp neighbors
Local Port  Dead Interval  Remaining Life  Remote Port ID  Remote Port Descr  Chassis ID      Tx  Rx
System Name
Eth 1/18    120              102            Ethernet 2/25   Eth 2/25           768e.f807.6000  653 652 R6
Eth 1/21    120              108            Ethernet 1/21   Eth 1/21           768e.f807.6000  653 652 R6
Eth 1/40    120              110            Ethernet 1/50   Eth 1/50           768e.f807.6000  653 650 R6
Eth 1/43    120              102            Ethernet 2/51   Eth 2/51           768e.f807.6000  653 652 R6
Eth 1/50    120              102            Ethernet 2/23   Eth 2/23           768e.f807.6000  653 611 R6
```

The following example displays the LLDP neighbor information for Ethernet interface 1/18.

```
device# show lldp neighbors interface ethernet 1/18
Local Port  Dead Interval  Remaining Life  Remote Port ID  Remote Port Descr  Chassis ID      Tx  Rx
System Name
Eth 1/18    120              115            Ethernet 2/25   Eth 2/25           768e.f807.6000  655 654 R6
```

The following example displays the detailed LLDP neighbor information for Ethernet interface 1/18.

```
device# show lldp neighbors interface ethernet 1/18 detail
Neighbors for Interface Eth 1/18

MANDATORY TLVs
=====
Local Interface: Eth 1/18 (Local Interface MAC: 768e.f805.5816)
Remote Interface: Ethernet 2/25 (Remote Interface MAC: 768e.f807.610d)
Dead Interval: 120 secs
Remaining Life : 118 secs
Chassis ID: 768e.f807.6000
LLDP PDU Transmitted: 656 Received: 655

OPTIONAL TLVs
=====
Port Interface Description: Eth 2/25
System Name: R6
```

Displaying LLDP statistics

To display the LLDP statistics for all interfaces or a specific interface, use the **show lldp statistics** command.

The following example displays the statistics for Ethernet interface 1/18.

```
device# show lldp statistics interface ethernet 1/18
LLDP Interface statistics for Eth 1/18
Frames transmitted: 659
Frames Aged out: 0
Frames Discarded: 0
Frames with Error: 0
Frames Recieved: 657
TLVs discarded: 0
TLVs unrecognized: 0
```

If you do not include the **interface ethernet** option, the command displays the statistics for all interfaces.

Clearing LLDP-related information

You can clear LLDP neighbor and statistic information for all interfaces or a specified interface.

To clear LLDP-related information, perform the following steps.

1. In privileged EXEC mode, clear the LLDP neighbor information.

```
device# clear lldp neighbors
```

This example clears the LLDP neighbor information for all interfaces.

2. Clear the LLDP statistics on an interface.

```
device# clear lldp statistics interface ethernet 1/8
```

This example clears the LLDP transmit and receive counters on the Ethernet interface 1/8.

3. Clear the LLDP statistics for all interfaces.

```
device# clear lldp statistics
```


Password Recovery

- [Recovering the admin password from the root account.....](#) 137
- [VM root password recovery for Brocade SLX 9850.....](#) 137

Recovering the admin password from the root account

If you lose access to the SLX-OS admin account but you have access to the root account for the device, you can recover the password.

Perform the following steps to reset the admin password from the root account.

1. Open a session to access the device.
2. Log in as root.
3. Start the SLX-OS CLI.

```
[root@device]# slxcli
device#
```

4. Access global configuration mode.

```
device# configure terminal
```

5. Reset the admin password.

```
device(config)# username admin password password
```

In this example, the admin password is reset to the default value of password.

You can now use the admin account to manage the admin and user passwords by using normal password-management procedures.

VM root password recovery for Brocade SLX 9850

By default, the root account on the virtual machine (VM) for Brocade SLX 9850 is disabled. To log into root, you can log into the SLX-OS CLI and enable the root account from global configuration mode by using **root enable** command. In rare cases, SLX-OS CLI may not be available to enable the root account.

The ability to enable the root account and recover the root credentials (password) depends on the uboot environment variable. When the variable is set, it executes the root recovery logic based on the parameter set. The variable is not preserved across reboot. Every time a reboot occurs, the root account is disabled by default and this variable has to be set again to enable it unless the root account was not enabled from global configuration mode.

The root account access availability determines the method for password recovery:

- When the root account is disabled and the SLX-OS CLI is not available, you must recover the root login account. The password is also recovered.
- When the root account is enabled but you forget the password, you must recover the VM root password.

NOTE

The default password for the root account on the VM is fibranne.

Recovering the VM root login account

When you need to recover the VM root password, and the root account is disabled and SLX-OS CLI is not available, you must recover the VM root login account.

- To perform the recovery process on the active or standby management module (MM), you must have access to the console prompt.
- To perform the process on line cards (LCs), you can either use the direct console access if present or use remote console from the MM to access the LC console.

For VM root login recovery, perform the following steps.

1. Reboot the active MM, standby MM, or LC for which you are trying to recover the root credentials.

```
# reboot
Press Esc during reboot.
Hit ESC to stop autoboot: 0
FPGA f6000720 -> 0x12
```

```
1) Start system.
2) Recover password.
3) Enter command shell.
```

```
Option?
```

2. Choose option 3 to access the uboot prompt.

```
Option? 3
=>
```

The uboot prompt appears.

3. Define the root login value for the root recover environment variable.

```
=> setenv VM_Root_Recover RootLogin
=>
```

This step sets the VM_Root_Recover variable with the RootLogin value.

4. Save the variable to flash memory.

```
=> saveenv
Saving Environment to SPI Flash...
SF: Detected W25Q128BV @ 0:0 with page size 256 Bytes, erase size 64 KiB, 32 KiB, 4 KiB, total 16 MiB
Erasing SPI flash...Writing to SPI flash...
Erasing SPI flash...Writing to SPI flash...done
=>
```

5. Boot the MM or LC.

```
=> boot
6912784 bytes read in 152 ms (43.4 MiB/s)
Valid Boot Flag
Setup Size = 0x00004400
Magic signature found
Using boot protocol version 2.0c
Linux kernel version 3.14.17 (raop@hql-ub-ecbld-373) #1 SMP Thu Jul 7 19:43:15 UTC 2016
```

The root account is now enabled. You can login with the default password.

If the SLX-OS CLI is available, you can recover the the active MM root account by using the SLX-OS CLI **root enable** command.

Recovering the VM root password

If you forgot the password for the VM root account, you can recover the default password.

- To perform the recovery process on the active or standby management module (MM), you must have access to the console prompt.
- To perform the process on line cards (LCs), you can either use the direct console access if present or use remote console from the MM to access the LC console.

For VM root password recovery, perform the following steps.

1. Reboot the active MM, standby MM, or LC for which you are trying to recover the root credentials.

```
# reboot
Press Esc during reboot.
Hit ESC to stop autoboot: 0
FPGA f6000720 -> 0x12

1) Start system.
2) Recover password.
3) Enter command shell.
```

Option?

2. Choose option 3 to access the uboot prompt.

```
Option? 3
=>
```

3. Define the root password value for the root recovery environment variable.

```
=> setenv VM_Root_Recover RootPasswd
=>
```

This step sets the VM_Root_Recover variable with the RootPasswd value.

4. Save the variable to flash memory.

```
=> saveenv
Saving Environment to SPI Flash...
SF: Detected W25Q128BV @ 0:0 with page size 256 Bytes, erase size 64 KiB, 32 KiB, 4 KiB, total 16 MiB
Erasing SPI flash...Writing to SPI flash...
Erasing SPI flash...Writing to SPI flash...done
=>
```

5. Boot the MM or LC.

```
=> boot
6912784 bytes read in 152 ms (43.4 MiB/s)
Valid Boot Flag
Setup Size = 0x00004400
Magic signature found
Using boot protocol version 2.0c
Linux kernel version 3.14.17 (raop@hq1-ub-ecbld-373) #1 SMP Thu Jul 7 19:43:15 UTC 2016
```

You can now login as root with the default password of fibranne.

Python Event-Management and Scripting

- Python under Brocade operating systems 141
- Python scripts 143
- Python event-management 148
- Troubleshooting event-management..... 151
- Event-management show commands 151

Python under Brocade operating systems

The Python interpreter installed with supported Brocade operating systems enables you to access a Python shell or to launch Python scripts. You can also define event handlers that run such scripts automatically upon specified conditions.

NOTE

SLX-OS is among the Brocade operating systems that support Python.

Python overview

Python is a high-level scripting language that also supports object-oriented programming. If you have previous programming experience, you can quickly learn how to write useful, simple Python scripts.

NOTE

For Python resources, refer to <http://python.org>.

Working interactively in the Python shell

Use this procedure to access a Python shell, within which you can use Python commands that call and manipulate Brocade operating system commands.

NOTE

The Python shell is accessible only to admin-role users.

Python syntax is case-sensitive.

1. In privileged EXEC mode, enter **python** to access the Python shell.

```
device# python
```

The `device#` prompt changes to a Python prompt:

```
device# python
Python 3.4.0 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
```

2. To exit the Python shell and return to the Brocade operating system prompt, enter either:
 - `exit()`
 - `Ctrl-D`

- To run a Brocade operating system command from within the Python shell, enter the CLI () command.

```
>>> cmd_show_running_ve = CLI('show running-config interface ve')
!Command: show running-config interface ve
!Time: Mon Aug 22 16:53:13 2016
```

The statement entered above does two things:

- Runs the **show running-config interface ve** command and displays the result.
- Assigns that command to a Python variable named `cmd_show_running_ve`

- To run a series of Brocade operating system commands from within the Python shell, separate the commands with `\n`.

```
>>> cmd_config_ve = CLI('configure \n interface ve 101-103')
!Command: configure
interface ve 101-103
!Time: Mon Aug 22 16:53:13 2016
```

NOTE

There is a difference between running a sequence of Brocade operating system CLI commands in the Python shell rather than in the standard Brocade operating system interface. Whereas in the standard interface the result of a command is persistent, in the Python shell each CLI () statement is independent of any preceding ones.

In the following example, the lines beginning with **#** are added for explanation.

```
device# python
Python 3.4.0 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_show_running_ve = CLI('show running-config interface ve')
!Command: show running-config interface ve
!Time: Mon Aug 22 16:53:13 2016

% No entries found.
# The SLX-OS show running-config interface ve command is run,
# and that command is assigned to the Python variable cmd_show_running_ve.

>>> cmd_config_ve = CLI('configure \n interface ve 101-103')
# A series of three commands are run and assigned to the Python variable cmd_config_ve.
!Command: configure
interface ve 101-103
!Time: Mon Aug 22 16:53:13 2016

>>> cmd_show_running_ve.rerun()
# The rerun() function appended to cmd_show_running_ve gives the following output:
!Command: show running-config interface ve
!Time: Mon Aug 22 16:53:13 2016

interface Ve 101
shutdown
!
interface Ve 102
shutdown
!
interface Ve 103
shutdown
!
!
```

Python scripts

Python scripts enable you to manipulate and launch Brocade operating system commands, taking advantage of the power and flexibility of Python. Such scripts also support event handling.

The topics in this section guide you through the process of writing and testing Python scripts, copying them to supported devices, and running them with the **python** command from the command line.

Guidelines for writing Python scripts

The guidelines for writing Python scripts to run under SLX-OS are as follows:

- Although previous experience programming in Python is helpful, experience in other high-level languages is enough to get you started with simple Python scripts.
- The Python developer either needs experience with SLX-OS CLI or access to a resource with such experience.
- To help decide which editor or integrated development environment (IDE) to use, refer to <http://www.python.org>.
- Make sure that the appropriate version of the Python interpreter is installed on your development computer. For the current version of SLX-OS, install Python 3.4.0.
- Make sure that in the *Brocade SLX-OS Command Reference* you are familiar with the **python** and the **CLI()** topics.
- One of the first statements in the script should be `from CLI import CLI`. This enables the `CLI()` command, by which Python can interact with SLX-OS.
- Write the Python script and save it, with a `.py` suffix. Valid filenames range from 4 through 32 characters (including the suffix). The first character must be alphabetic.

NOTE

For additional sample scripts, refer to [Python scripts and run-logs](#) on page 145.

Testing Python-script statements

While developing a Python script, you can test Brocade operating system calls by entering them in the device Python command shell. After the script is stable, you copy it to the device and then test it further by running it from the command line.

1. In privileged EXEC mode, enter the **python** command to access the Python shell.

```
device# python
Python 3.4.0 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

Note that the `device#` prompt changed to a `>>>` Python prompt:

2. Enter the script statements one at a time, verifying that they run as expected.

```
>>> cmd_config_ve = CLI('configure \n interface ve 101-103')
!Command: configure
  interface ve 101-103
!Time: Mon Aug 22 16:53:13 2016
```

3. Make corrections as needed.

Copying Python files to the device

After writing and testing a Python script file, use one of these topics to copy it to device flash memory.

Copying a file from a USB device

Use this topic to copy a file from a USB stick to a Brocade device .

ATTENTION

The only supported USB device for this task is the Brocade USB stick shipped with the device.

1. Copy the Python script file to the USB stick.
2. Insert the USB stick into the device USB port and enter the **usb on** command.
3. In privileged EXEC mode, enter the **copy** command to copy the Python file from the USB stick to the device flash memory.

```
device# copy usb://pythscript1.py flash://pythscript1.py
```

4. To display a list of files in the device flash memory, enter the **dir** command.

```
device# dir
total 32
drwxr-xr-x 2 251 1011 4096 Aug 26 08:44 .
drwxr-xr-x 3 251 1011 4096 Jul 20 07:50 ..
-rw-r--r-- 1 root root 1051 Mar 24 16:09 create_po.py
-rw-r--r-- 1 root sys 695 Aug 23 21:18 defaultconfig.cluster
-rw-r--r-- 1 root root 410 Aug 26 04:06 defaultconfig.standalone
-rw-r--r-- 1 root root 10042 Aug 4 00:01 ospfnsrl.cfg
-rw-r--r-- 1 root root 410 Aug 26 01:28 startup-config

16908197888 bytes total (10226114560 bytes free)
```

5. To display the contents of a Python file copied into the device flash memory, enter the **show file** command.

```
device# show file pythscript1.py
```

Downloading a file from a network

Use this topic to download a file from a network location to the Brocade device.

1. Make sure that the Python script file is uploaded to an accessible network location.
2. In privileged EXEC mode, enter the **copy** command to copy the Python file from the network location to the device flash memory.

```
device# copy ftp://MyUserID:MyPassword@10.10.10.10//pythscript1.py flash://pythscript1.py
```

For other file-transfer options, refer to the *Brocade SLX-OS Command Reference copy* topic.

3. To display a list of files in the device flash memory, enter the **dir** command.

```
device# dir
total 32
drwxr-xr-x 2 251 1011 4096 Aug 26 08:44 .
drwxr-xr-x 3 251 1011 4096 Jul 20 07:50 ..
-rw-r--r-- 1 root root 1051 Mar 24 16:09 create_po.py
-rw-r--r-- 1 root sys 695 Aug 23 21:18 defaultconfig.cluster
-rw-r--r-- 1 root root 410 Aug 26 04:06 defaultconfig.standalone
-rw-r--r-- 1 root root 10042 Aug 4 00:01 ospfnsrl.cfg
-rw-r--r-- 1 root root 410 Aug 26 01:28 startup-config

16908197888 bytes total (10226114560 bytes free)
```


- To display the contents of a Python file copied into the device flash memory, enter the **show file** command.

```
device# show file pythscript1.py
```

Running Python scripts from the command line

The facility to run Python scripts from the Brocade operating system command line enables you to execute complex and repetitious tasks with accuracy and efficiency. This facility also enables you to validate scripts intended for event management.



CAUTION

Make sure that you test Python scripts according to standard quality assurance practices before deploying them.

In privileged EXEC mode, enter the **python** command, specifying the Python script file that you want to run.

```
device# python create_po.py
```

After the script runs, the SLX-OS prompt displays.

NOTE

The create_po.py script is discussed in "Script for assigning interfaces to port channels (create_po.py)."

Python scripts and run-logs

This section contains sample SLX-OS Python scripts and run-logs.

Script for assigning interfaces to port channels (create_po.py)

The create_po.py script is an example for automating common configuration tasks.

Script (create_po.py)

This script runs the relevant **show running-config** commands before and after the following actions:

- VLAN configuration
- Port-channel configuration
- Adding interfaces to port channels

NOTE

Lines beginning with # are annotations.

```
#Required in all scripts for SLX-OS:
from CLI import CLI
```

```
slots = [1, 2]
interfaces = [40, 41, 42, 43]
port_channel = 10
vlan_range = "101-105"
```

```
# Runs show running-config int vlan before the configuration, and assigns this SLX-OS
# command to a Python variable named cmd_show_running_vlans.
cmd_show_running_vlans = CLI("show running-config vlan")
```

```
# Configures VLANs. {} is a placeholder for the format (arg1, arg2, ... argN) variables:
cmd_configure_vlans = CLI("config \n vlan {}".format(vlan_range))
```

```
# Reruns show running-config int vlan, following definition of new VLANs:
```

```

cmd_show_running_vlans.rerun()

# Reruns show running-config int po, following configuration changes:
cmd_show_running_port_channels.rerun()

# Runs show running-config:
cmd_show_running = CLI("show running-config")

```

Run-log (create_po.py)

A log upon running create_po.py was as follows:

```

device# python create_po.py
!Command: show running-config vlan
!Time: Mon Aug 22 18:33:03 2016

vlan 1
!
vlan dot1q tag native

!Command: config
vlan 101-105
!Time: Mon Aug 22 18:33:03 2016

!Command: show running-config vlan
!Time: Mon Aug 22 18:33:03 2016

vlan 1
!
vlan 101
!
vlan 102
!
vlan 103
!
vlan 104
!
vlan 105
!
vlan dot1q tag native

!Command: show running-config int po
!Time: Mon Aug 22 18:33:03 2016

interface Port-channel 1
description Insight port-channel on MM1
shutdown
!
interface Port-channel 2
description Insight port-channel on MM2
shutdown
!

!Command: config
int po 10
switchport
switchport mode trunk
switchport trunk allowed vlan add 101-105
switchport trunk tag native-vlan ; no shut
!Time: Mon Aug 22 18:33:03 2016

!Command: show running-config int po
!Time: Mon Aug 22 18:33:04 2016

interface Port-channel 1
description Insight port-channel on MM1
shutdown

```

```
!  
interface Port-channel 2  
description Insight port-channel on MM2  
shutdown  
!  
interface Port-channel 10  
switchport  
switchport mode trunk  
switchport trunk allowed vlan add 101-105  
switchport trunk tag native-vlan  
no shutdown  
!  
  
!Command: config  
int eth 1/40  
channel-group 10 mode active type standard  
no shut  
!Time: Mon Aug 22 18:33:04 2016  
  
  
!Command: show running-config int eth 1/40  
!Time: Mon Aug 22 18:33:04 2016  
  
interface Ethernet 1/40  
channel-group 10 mode active type standard  
lACP timeout long  
no shutdown  
!  
  
!Command: config  
int eth 1/41  
channel-group 10 mode active type standard  
no shut  
!Time: Mon Aug 22 18:33:04 2016  
  
  
!Command: show running-config int eth 1/41  
!Time: Mon Aug 22 18:33:05 2016  
  
interface Ethernet 1/41  
channel-group 10 mode active type standard  
lACP timeout long  
no shutdown  
!  
  
!Command: config  
int eth 1/42  
channel-group 10 mode active type standard  
no shut  
!Time: Mon Aug 22 18:33:05 2016  
  
  
!Command: show running-config int eth 1/42  
!Time: Mon Aug 22 18:33:05 2016  
  
interface Ethernet 1/42  
channel-group 10 mode active type standard  
lACP timeout long  
no shutdown  
!  
  
!Command: config  
int eth 1/43  
channel-group 10 mode active type standard  
no shut  
!Time: Mon Aug 22 18:33:05 2016  
  
  
!Command: show running-config int eth 1/43  
!Time: Mon Aug 22 18:33:05 2016  
  
interface Ethernet 1/43
```

```

channel-group 10 mode active type standard
lACP timeout long
no shutdown
!
<output truncated>

```

Script illustrating the `.get_output` function (`get_output.py`)

The `.get_output` function returns—as a list—the output of the SLX-OS CLI commands assigned to a Python object.

Script (`get_output.py`)

This script displays a list of firmware version per slot.

```

#Required in all scripts for SLX:
from CLI import CLI
# Import the Python Regular Expressions (re) module:
import re
# Create Python objects:
slot_firmware = {}

cmd_show_ver = CLI("show ver", False)
# Using .get_output(), assign the result of show ver to a Python object named output:
output = cmd_show_ver.get_output()
for line in output:
    found = re.search(r'^(\S+)\s+(\S+)\s+(\S+)\s+ACTIVE.*$', line, re.M)
    if found:
        slot_firmware[found.group(1)] = found.group(3)

print("SLOT_FIRMWARE:\n")
for key in slot_firmware:
    print("\t", key, "\t=> ", slot_firmware[key])

```

Run-log (`create_po.py`)

A log upon running `get_output.py` was as follows:

```

device# python get_output.py
SLOT_FIRMWARE:
  L2/0 => 16r.1.01dsadanan_slxos_16r.1.x_maint_01
  L1/0 => 16r.1.01dsadanan_slxos_16r.1.x_maint_01
  M1   => 16r.1.01dsadanan_slxos_16r.1.x_maint_01

```

Python event-management

Python event management enables you to specify a Python script that runs automatically upon specified conditions.

You specify which RASlog message triggers the script.

Configuring an event-handler profile

Use this procedure to create an event-handler profile, define one or more triggers for it, and specify a Python script that runs upon one or more trigger events.

1. Enter **configure terminal** to access global configuration mode.

```
device# configure terminal
```

2. Enter the **event-handler** command.

```
device(config)# event-handler eventHandler1
```

3. For each trigger that you need for a profile, enter the **trigger** command.

```
device(config-event-handler-eventHandler1)# trigger 1 raslog LOG-1001
```

The trigger event is RASlog message #LOG-1001.

4. Enter the **action python-script** command to specify a Python script that runs when the event-handler is triggered.

```
device(config-event-handler-eventHandler1)# action python-script example.py
```

5. To add an event-handler-profile description, enter **description**, followed by the description text.

```
device(config-event-handler-eventHandler1)# description This is a sample description.
```



CAUTION

Make sure that you test Python scripts according to standard quality assurance practices before deploying them.

The following example includes all of the steps.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)# trigger 1 raslog LOG-1001
device(config-event-handler-eventHandler1)# action python-script example.py
device(config-event-handler-eventHandler1)# description This is a sample description.
```

The following example defines a trigger that uses POSIX extended REGEX to search for a match within a specified RASlog message ID.

```
device# configure terminal
device(config-event-handler-eventHandler1)# event-handler eventHandler2
device(config-event-handler-eventHandler2)# trigger 1 raslog NSM-1003 pattern Interface Ethernet 1/[1-9] is link down
```

RASlog message NSM-1003 includes "**interface** *interface-name* is link down", indicating that an interface is offline because the link is down. The REGEX searches within such a message for an interface from 1/1 through 1/9.

Activating an event-handler

Use this procedure to activate one or more event-handlers on the device. If a trigger specified in the event-handler profile occurs, a designated Python script runs.

1. Enter **configure terminal** to access global configuration mode.

```
device# configure terminal
```

2. Enter the **event-handler activate** command, specifying the event handler that you are activating.

```
device(config)# event-handler activate eventHandler1
```

3. To activate an additional event handler, enter the **event-handler activate** command, specifying the additional event handler.

```
device(config-activate-eventHandler1)# event-handler activate eventHandler2
```

4. To de-activate an event handler, enter the **no event-handler activate** command

```
device(config-activate-eventHandler2)# no event-handler activate eventHandler2
```

The following example includes all of the activation steps.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# event-handler activate eventHandler2
```

Configuring event-handler options

After you activate an event handler, you can configure various options. For example, you can specify if the event-handler script runs more than once and how multiple triggers are handled.

1. Activate an event handler, as described in [Configuring an event-handler profile](#) on page 148:

```
device# configure terminal
device(config)# event-handler activate eventHandler1
```

2. To specify a delay from when a trigger is received until execution of the event-handler action, enter the **delay** command.

```
device(config-activate-eventHandler1)# delay 60
```

The above example specifies a delay of 60 seconds.

3. To specify multiple iterations of the action when a trigger is received:

- a) Enter the **iterations** command.
- b) To specify an interval between iterations, enter the **interval** command.

```
device(config-event-handler-eventHandler1)# iterations 3
device(config-activate-eventHandler1)# interval 30
```

The above example sets the number of iterations to 3 and specifies an interval of 30 seconds between each iteration.

4. To specify a maximum number of minutes to wait for an action script to complete execution, enter the **action-timeout** command.

```
device(config-activate-eventHandler1)# action-timeout 30
```

The example sets the timeout to 30 minutes.

5. To limit action-recurrence upon multiple trigger-events, enter one of the following commands:

- **trigger-mode only-once**—for the duration of a device configuration, the event-handler action is launched only once.
- **trigger-mode on-first-instance**—as long as the device is running, the event-handler action is launched only once. Following a device restart, the event-handler action can be triggered again.

```
device(config-activate-eventHandler1)# trigger-mode on-first-instance
```

6. If multiple triggers are defined, to specify that the action run only if all of the triggers occur, enter the **trigger-function AND time-window** command.

```
device(config-activate-eventHandler1)# trigger-function AND time-window 120
```

The above example specifies that the action run only if all triggers occur within 120 seconds.

Troubleshooting event-management

Use these topics to troubleshoot issues that arise during implementation of Python event-management.

Aborting an event-handler action

If needed, abort a Python script launched by an event-handler action.

1. In privileged EXEC mode, enter the **event-handler abort action** command.

```
device# event-handler abort action eh1
This operation will abort an event handler action that is currently running and may leave the device
in an inconsistent state. Do you want to continue? [y/n]:y
```

2. To confirm aborting the action, type *y*.

```
Operation completed successfully.
```

The Python script launched by the event-handler action is aborted.

Event-management show commands

There are several show commands that display event-management information, listed here with descriptions.

TABLE 34 Event-management show commands in the *Command Reference*

Command	Description
show event-handler activations	Displays operational data of activated event-handlers.
show running-config event-handler	Displays details of event-handler profiles defined on the device. You can display the results by Python-script action or trigger ID.