



4000 Series User Guide

for Switch Engine Version 32.7.1

9038074-00 Rev. AB
May 2024



Copyright © 2024 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

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 (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



Table of Contents

Preface	4
Introduction to the 4000 Series User Guide	8
Getting Started	10
Managing the Switch	19
Configuring Stacked Switches	22
Common Commands	26
Software Licensing.....	54
Index	55



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings






Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic text</i>	Italic text indicates variable content.
[]	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.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member [member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)
[Release Notes](#)
[Hardware and Software Compatibility](#) for Extreme Networks products
[Extreme Optics Compatibility](#)
[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.

Help and Support

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

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions 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

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



Introduction to the 4000 Series User Guide

[Related Publications](#) on page 8

This guide is intended for use by network administrators who are responsible for installing and setting up 4000 Series switches. This is an abbreviated guide intended to highlight features, functionality, and operations specific to 4000 Series switches and is not intended to be a comprehensive guide about each feature of our software. For full, detailed information about Switch Engine software (which the 4000 Series supports), including detailed configuration material, helpful examples, and troubleshooting information, see the Switch Engine User Guide for this version.



Note

If the information in the release notes shipped with your switch differs from the information in this guide, follow the release notes.

Related Publications

Switch Engine Publications

- [Switch Engine 32.7.1 Command Reference Guide](#)
- [Switch Engine 32.7.1 Feature License Requirements](#)
- [Switch Engine and ExtremeXOS 32.7.1 EMS Messages Catalog](#)
- [Switch Engine 32.7.1 User Guide](#)
- [Switch Engine 32.7.1 Release Notes](#)
- [ExtremeXOS Quick Guide](#)
- [Extreme Hardware/Software Compatibility and Recommendation Matrices](#)
- [Extreme Optics Compatibility](#)
- [Switch Configuration with Chalet for ExtremeXOS 21.x and Later](#)
- [ACL Solutions Guide](#)
- [ExtremeXOS and Switch Engine SNMP Traps Reference](#)

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/open-source-declaration/.



Getting Started

- [Product Overview](#) on page 10
- [Software Required](#) on page 11
- [Modes of Operation](#) on page 11
- [Software and Feature Support](#) on page 11
- [ExtremeCloud™ IQ Agent Support](#) on page 12
- [Simple Switch Configuration with Chalet](#) on page 14
- [Cloning Switches](#) on page 15
- [Logging in to the Switch](#) on page 16
- [Port Numbering](#) on page 16

The Getting Started chapter is intended to help you learn about the features, functionality, and operations of 4000 Series switches in relation to the operating system software. You will find information about these switches, software version requirements, and other helpful software orientation information in this chapter.

Product Overview

This table lists the 4000 Series platforms that run the Switch Engine software.

Table 4: 4000 Series Switches

Switch Series	Switch Models
4120	4120-24MW-4Y 4120-48MW-4Y
4220	4220-8X 4220-12P-4X 4220-12T-4X 4220-24P-4X 4220-24T-4X 4220-48P-4X 4220-48T-4X 4220-4MW-8P-4X 4220-4MW-20P-4X 4220-8MW-40P-4X

Software Required

For information about which software version is required for each hardware switch model, see [ExtremeXOS and Switch Engine Software Support](#).

The features available on each switch are determined by the installed feature license and optional feature packs. For more information, see the [Switch Engine 32.7.1 Feature License Requirements](#) document.

Modes of Operation

The 4000 Series has been designed for easy-to-use cloud management which can be accessed through ExtremeCloud IQ or ExtremeCloud IQ - Site Engine. The 4000 Series takes advantage of Auto Provisioning through DHCP. CLI features are available for basic configuration, operation, and diagnostics and can be accessed through the Web (using Chalet), mobile apps (using Bluetooth), or through the console.

Available CLI Modes

There are two CLI modes that are available for use on 4000 Series switches:

- Basic CLI

The basic CLI provides access to a limited set of switch operating system commands. The basic CLI can be accessed through Web SSH, Telnet, SSH, the Chalet Terminal, SSH proxy, and the Bluetooth Dongle.

- Full CLI

The full CLI provides access to all of the switch operating system commands. The full CLI is only available through ExtremeCloud IQ or ExtremeCloud IQ - Site Engine.

Software and Feature Support

The switch operating system software supports stacking and static routing. The switch operating system software **does not** support:

- VMAN
- Ring Protection Protocols (ERPS, EAPS, ESRP)
- OAM (BFD)
- Legacy Features like IDM , XNV
- AVB
- L3 Routing Protocols (RIP , OSPF , BGP ,IS-IS)

Supported Features

The following features are supported:

EDP	Link Fault Signaling	IPv4 –L2 unicast and multicast switching
Fabric Attach	ELSM	IPv4 Directed broadcast
Identity Management	ACLs	IPv6 – L2 unicast switching
LLDP	CPU Dos Protect	IPv4 and IPv6 Nettools
VLANs (except Protocol based VLANs)	SNMPv3	IPv4 – Unicast and multicast routing – static routes
Jumbo Frames	SSH2 – Server & Client	IPv4 DAD
QoS – egress Shaping	RADIUS	IPv6 Unicast routing – static routes
LAG	Network login	IPv6 DAD
Software Redundant Port	IP Security	PBR for IPv4
STP (dot1d , dot1s , dot1w)	Static IGMP	PBR for IPv6
sFlow	Static MLD	Python script Execution
CLEAR flow	IGMP v1/v2/v3 snooping	Node Alias
CLI scripting	UDP forwarding	All Show commands
Web based Device management	UDP BOOTP Relay forwarding	All Debug commands
CEP detection	Multicast VLAN registration	Switch operational commands (cp / rm / mv)
DHCP v4	MVRP – VLAN Topo management	Switch Management (SSH / SNMP)
DHCP v6	CFM	VLAN Aggregation
User VRs and VRFs	Y.1731	Multinetting for forwarding

ExtremeCloud™ IQ Agent Support

4000 Series switches require management by ExtremeCloud IQ or ExtremeCloud IQ Site Engine. Currently, device discovery, basic monitoring, and visibility into homogenous stacking are supported.

Switch Engine also has the ability to configure an optional user-defined virtual router (VR) and address of the server for ExtremeCloud IQ agent to connect to. These values are used instead of any auto-detected values.

In addition, users can configure the IQ Agent HTTP Proxy server IP and port, and define the username and password, if required.

To configure a server VR, VLAN Management, or address, use the following command:

```
configure iqagent server [vr [[vr-name | none] | [ vr_name vlan vlan-name]] | none] | ipaddress [fqdn | ip_address| none]]
```

To configure the HTTP proxy, use the following command:

```
configure iqagent http-proxy [ipaddress [fqdn | ip_address] port port_number | user user_name password [encrypted encrypted_password | password] | none]
```

You can enable or disable the IQ Agent with the following commands:



Important

Disabling IQ Agent prevents all access to ExtremeCloud IQ. Any current activity with ExtremeCloud IQ, including remote SSH sessions, are disconnected immediately. Re-enabling IQ Agent can only occur by using the enable command by either console or Telnet or SSH access. Disabling IQ Agent deactivates automatic DHCP access on VLAN Mgmt, which is required for Zero-Touch Provisioning (ZTP).

```
enable iqagent
```

```
disable iqagent
```

To view information about IQ Agent, use the following command:

```
show iqagent discovery
```

For more information about ExtremeCloud IQ, go to <https://www.extremenetworks.com/support/documentation/extremecloud-iq/>.

Table 5: Supported Platforms

Switch Series	Switch Models
4120	4120-24MW-4Y 4120-48MW-4Y
4220	4220-8X 4220-12P-4X 4220-12T-4X 4220-24P-4X 4220-24T-4X 4220-48P-4X 4220-48T-4X 4220-4MW-8P-4X 4220-4MW-20P-4X 4220-8MW-40P-4X

IQ Agent and ExtremeCloud IQ Communication

After the IQ Agent is enabled, communication forms between the IQ Agent and extremecloudiq.com by secure HTTPS communication using destination TCP port 443. Communication between the IQ Agent and ExtremeCloud IQ occurs every 30 seconds, which includes check-in to ExtremeCloud IQ for actions, and includes CPU, memory, FDB information, Syslog, and ports statistics information. Note that data plane traffic is not sent to ExtremeCloud IQ by the IQ Agent.

Note that Telnet and SSH do not permit access to 'hivemanager' account, which the IQ Agent creates for its own purpose and uses it for all cloud-initiated SSH connections through local host, so logging on to this account through Telnet or SSH is not allowed.

IQ Agents use SNMPv2 (enabled only for internal requests) to monitor the status of the switch.

Distributed Denial of Service Support for IQ Agent

Distributed Denial of Service (DDoS) support for IQ Agent installs a filter on HTTPS L4 ports to set a CPU queue (QoS 5) that separates IQ Agent traffic from other IP exceptions. This new ACL redirects TCP traffic with source port 443 (default HTTPS port) to CPU queue 5. The IQ Agent system ACL is installed or uninstalled along with the L3 Unicast Miss (L3UCMiss) filter.

Automation of this feature is supported on all Universal switches.

You can also manually install the ACL to redirect IQ Agent traffic to CPU queue 5 on smaller switches with 8 ACL slices by running the following command:

```
# configure access-list iqagent.pol any

iqagent.pol:
entry iqagent_cpu5 {
  if {
    protocol tcp;
    source-port 443;
  } then {
    traffic-queue cpu_q_5;
  }
}
```

Simple Switch Configuration with Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch. Chalet removes the need to know and remember commands in a CLI environment. Viewable on desktop and mobile with a quick login and intuitive navigation, Chalet features an Quick Setup mode for configuring a switch in a few simple steps. Basic data surrounding port utilization, power, and Quality of Service (QoS) are available, and more advanced users can configure multiple VLANs, and create Access Control Lists (ACLs).

Chalet helps you interact with the switch outside of a CLI environment and allows you to easily:

- Configure the switch for the first time without the use of a console cable.
- Create and upload files to and from the switch.
- Install software images and modules directly on the switch.
- View status and details of the switch and its slots and ports.
- Analyze power efficiency of power supplies, fans, and PoE ports.
- Create VLANs and ACL policies.
- Enable and disable multiple features, including QoS, auto-negotiation, and flooding.
- View recent system events.
- View device topology (stacked switches only).
- Manage users, including defining global and individual security policies.

**Note**

Beginning with version 31.4, access to the switch through Chalet is limited to only Admin users. Read-only users do not have access to the switch through the Chalet interface. This restriction is included due to security concerns.

For instructions about setting up, logging in, configuring, and monitoring your switch, see [Switch Configuration with Chalet for ExtremeXOS 21.x and 22.x](#).

Cloning Switches

Switch Engine switches provide a script called `clone.py` that allows you to clone one switch's setup to another switch in the following scenarios:

- **Within a stack**
- **Standalone to standalone**
- **Standalone to stack**
- **Standalone to USB**

The `clone.py` script copies the following:

- All content under:
 - `/boot`
 - `/exos`
 - `/alt/boot`
 - `/alt/exos`
 - (optionally) `/usr/local/cfg`
- Specific NVRAM contents:
 - Boot selector
 - CLI banner
 - Failsafe username,password, and action

Limitations

- Cloning to a standalone switch using a stacking master as the source does not make the standalone switch a stacking master. The configuration cloned from a stacking master to the standalone switch is ignored by the operating system.
- ONIE to non-ONIE or non-ONIE to ONIE cloning cannot be performed.
- Clone application does not connect through VR-USER.
- If the clone primary is started and stopped, the configuration dirty bit is set.

Supported Platforms

Cloning is supported on all 4000 Series platforms.

Logging in to the Switch

Perform the following tasks to log in to the switch.

1. The initial login prompt appears as follows:

```
(Pending-AAA) login:
```

At this point, the failsafe account is now available, but the normal AAA login security is not.

2. Wait for the following message to appear:

```
Authentication Service (AAA) on the master node is now available for login.
```

At this point, the normal AAA login security is available.

3. Press **[Enter]**.

Whether or not you press **[Enter]**, after you see the login prompt, you can perform a normal logon.

The following prompt appears: login

After you have successfully logged on, the following information about successful and unsuccessful logons appears:

```
There have been 26 successful logins since last reboot and 0 failed logins since last successful login
Last Successful Login was on: Thu Apr 23 17:16:08 2020
```

Port Numbering

The operating system software runs on stand-alone switches.



Note

The keyword **a11** acts on all possible ports; it continues on all ports even if one port in the sequence fails.

Stand-alone Switch Numerical Ranges

On ExtremeSwitching switches, the port number is simply noted by the physical port number.

Separate the port numbers by a dash to enter a range of contiguous numbers, and separate the numbers by a comma to enter a range of non-contiguous numbers:

- `x-y`—Specifies a contiguous series of ports on a stand-alone switch.
- `x,y`—Specifies a non-contiguous series of ports on a stand-alone switch.
- `x-y,a,d`—Specifies a contiguous series of ports and a non-contiguous series of ports on a stand-alone switch.
- `Port:Channel`—For 4120 channelized ports. For example, `49:4` maps to Port 49, Channel 4.

SummitStack Numerical Ranges

On SummitStack switches, the port number is a combination of the slot number and the port number.

The nomenclature for the port number is as follows: `slot:port`

For example, if there is a switch in slot 2 of the stack with a total of four ports, the following ports are valid:

- `2:1`
- `2:2`
- `2:3`
- `2:4`

You can also use wildcard combinations (*) to specify port combinations.

The following wildcard combinations are allowed:

- `slot:*`—Specifies all ports on a particular switch in the stack.
- `slot:x-slot:y`—Specifies a contiguous series of ports on a range of switches in the stack.
- `slot:x-y`—Specifies a contiguous series of ports on a particular switch in the stack.
- `slota:x-slotb:y`—Specifies a contiguous series of ports on a SummitStack node and end on another node.
- `Slot:Port:Channel`—For 4120 channelized ports. For example, `2:49:4` maps to Slot 2, Port 49, Channel 4.

Assigning Slot:Port Notation on Standalone Switches

You can configure a standalone system as a slotted system, which allows for commands which had 'slot' arguments to be visible and take in a valid slot number of '1', along with any port arguments specified in 'slot':port' notation. In turn, any command output would specify 'slot' information and ports displayed in 'slot':port' notation.

To assign slot:port notation to a standalone switch, use the following command:

```
configure system ports notation [slot:port | slot/port]
```

The CLI prompt for the switch changes to show that you have changed it to slot:port notation. For example:

```
Slot-1 5420F-48P-4XE.1
```



Managing the Switch

[4000 Series Switch Management Overview](#) on page 19

This chapter provides summary information about how to use your 4000 Series switch using Switch Engine. This chapter contains information about the ExtremeXOS Shell, system redundancy, power supply management, user authentication, Telnet, and hitless failover support, as well as and usage information.

4000 Series Switch Management Overview

This chapter describes how to use the operating system to manage the switch. It also provides details on how to perform the following various basic switch functions:

- Access the command line interface (CLI) by connecting a terminal (or workstation with terminal-emulation software) to the console port.
- Access the switch remotely using TCP/IP through one of the switch ports, or through the dedicated 10/100 unshielded twisted pair (UTP) Ethernet management port. Remote access includes:
 - Telnet using the CLI interface
 - Secure Shell (SSH2) using the CLI interface
 - access using an SNMP manager
- Download software updates and upgrades.

The switch supports the following number of concurrent user sessions:

- One console session
- Eight shell sessions
- Eight Telnet sessions
- Eight Trivial File Transfer Protocol (TFTP) sessions
- Eight SSH2 sessions
- Six XML sessions

Managing the Switch with Bluetooth Devices

You can manage 4000 Series switches using Bluetooth with mobile devices or laptops. Bluetooth is enabled by default.

Supported Platforms

Switch: 4000 Series switches.

Adapters: Dongles with a common Bluetooth controller (Cypress CY20702). Vendors with CY20702 pluggable and CC&C (USB-BT-400). 4000 Series switches also support the Extreme Networks Bluetooth 5.0 dongle (XN-USB-BT500-ADAPTER).

Limitations

- Stacking with Bluetooth is not supported. Currently, access to a slot connected with a Bluetooth device is supported, but other slots cannot be accessed.
- No security procedures are initiated for Bluetooth connectivity.
- Only a specific list of Bluetooth dongles is supported.
- Only one Bluetooth adapter is enabled per card. Other adapters will be in powered off state.

Using Bluetooth

Bluetooth users/clients can access switches using either the global IP address or link local IP address. The Bluetooth interface is assigned with the global IP address (192.168.1.1/24 or 172.16.1.1/24). DHCP server runs on the Bluetooth interface. This is mainly to serve Bluetooth clients with DHCP support. After a Bluetooth connection is established, all Bluetooth clients are allocated IP addresses from this pool (192.168.1.2–192.168.1.20 or 172.16.1.1–172.16.1.20). For Bluetooth clients that do not support DHCP, you can use the link local IP address for accessing the switch. Range is 169.254.1.1–169.254.1.8.

To set up a Bluetooth device to manage a switch:

1. Insert a supported dongle into the USB port of the switch.
2. If needed (Bluetooth is enabled by default), ensure that Bluetooth capability, discovery, and pairing are all enabled. using the following command:

```
enable switch bluetooth {discovery | pairing }
```

You can check Bluetooth status using the `show switch bluetooth [statistics | inventory]` command.

3. If needed, enable Bluetooth on the desired Bluetooth device (phone or laptop).
4. To initiate pairing, do one of the following:
 - Press and hold the **mode** button for approximately 5 seconds.
 - Press the pairing button on the dongle.

The Bluetooth Status LED blinks green while pairing is in progress, and then becomes solid green when Bluetooth is connected.



Note

4120 Series switches have a Bluetooth status LED. The 4220 Series switches do not have a Bluetooth status LED.

Bluetooth Commands

To enable Bluetooth capabilities, use the following command:

```
enable switch bluetooth {discovery | pairing }
```

To disable Bluetooth capabilities, use the following command:

```
disable switch bluetooth {discovery | pairing }
```

To clear Bluetooth devices, use the following command:

```
clear switch bluetooth device [all | address]
```

To show Bluetooth information, use the following command:

```
show switch bluetooth [statistics | inventory]
```



Configuring Stacked Switches

[Verifying the Configuration](#) on page 22

A stack consists of a group of up to eight switches that are connected to form a ring. The stack offers the combined port capacity of the individual switches. But it operates as if it were a single switch, making network administration easier.

Stacking is facilitated by the SummitStack feature – part of the ExtremeXOS Edge license.

For descriptions of the supported configurations for stacking, considerations for planning a stack, and instructions for setting up the hardware, see the *Stacking* topic in the *hardware installation guide* for your switch. Also see the *Configuring Stacked Switches* topic in the *user guide* for your version of the switch operating system. We recommend that you read these topics before installing the switches that will make up the stack.

Verifying the Configuration

To verify that your stack is configured as you intended, log into the master node and issue any or all of the following commands.

- [show stacking](#) on page 23
- [show stacking configuration](#) on page 23
- [show slot](#) on page 24
- [show stacking detail](#) on page 24
- [show stacking stack-ports](#) on page 25

These commands are also helpful when debugging problems with your stack.



Note

The examples in the following sections show a stack consisting of four switches.

show stacking

The `show stacking` command displays the stack topology along with each node's slot number, state, and role (master, backup, or standby).

```
Slot-1 Stack.1 # show stacking
Stack Topology is a Ring
Active Topology is a Ring
Node MAC Address      Slot  Stack State  Role      Flags
-----
*00:04:96:9c:e4:39  1     Active       Master    CA-
00:04:96:9b:c1:34  2     Active       Backup    CA-
00:04:96:9e:5c:76  3     Active       Standby   CA-
00:04:96:9c:53:b6  4     Active       Standby   CA-
* - Indicates this node
Flags: (C) Candidate for this active topology, (A) Active Node
       (O) node may be in Other active topology
```

In the command output, note that:

- The asterisk (*) that precedes the node MAC address indicates the node to which you are logged in. The node MAC address is the address that is factory assigned to the stackable switch.
- The slot number shown is the number currently in use by the related node. Because slot number configuration only takes effect during node initialization, a change in configured value alone does not cause a change to the slot number in use.
- If a node role has not yet been determined, the node role indicates <none>. In a ring topology, the node on which this command is executed is always the first node displayed. In a daisy chain, the ends of the daisy chain are the first and last nodes displayed.
- Even though the stack topology could be a ring, the active topology could be a daisy chain because it does not contain every node in the stack topology.
- If the node on which this command is being executed is not active, the stacking topology is replaced with a line similar to this one:

```
This node is not in an Active Topology.
```
- It is possible for a node to be in stabilizing or waiting state and still be in the active topology.

show stacking configuration

The `show stacking configuration` command displays a summary of the stacking configuration for all nodes in the stack.

```
Slot-1 Stack.3 # show stacking configuration
Stack MAC in use: 02:04:96:9c:e4:39
Node          Slot      Alternate
MAC Address   Cfg Cur  Prio Mgmt IP / Mask  Alternate Gateway  Flags  Lic
-----
*00:04:96:9c:e4:39  1    1    Auto <none> <none> <none> CcEeMm-Nn --
00:04:96:9b:c1:34  2    2    Auto <none> <none> <none> CcEeMm-Nn --
00:04:96:9e:5c:76  3    3    Auto <none> <none> <none> --EeMm-Nn --
00:04:96:9c:53:b6  4    4    Auto <none> <none> <none> --EeMm-Nn --
* - Indicates this node
Flags: (C) master-Capable in use, (c) master-capable is configured,
       (E) Stacking is currently Enabled, (e) Stacking is configured Enabled,
```

```

(M) Stack MAC in use, (m) Stack MACs configured and in use are the same,
(i) Stack MACs configured and in use are not the same or unknown,
(N) Enhanced protocol is in use, (n) Enhanced protocol is configured,
(-) Not in use or not configured
License level restrictions: (C) Core, (A) Advanced edge, or (E) Edge in use,
(c) Core, (a) Advanced edge, or (e) Edge configured,
(-) Not in use or not configured

```

In the command output, note especially the values in the **Flags** column:

- All nodes should have the Ee, Mm, and Nn flags active.
- Additionally, the master and backup nodes should have the Cc flags active.

(The meanings of the flags are displayed at the bottom of the table in the command output.)

show slot

The `show slot` command shows the states of the nodes as they move from the empty to operational state.

```

Slot-1 Stack.2 # show slot
Slots      Type              Configured          State              Ports
-----
Slot-1     5520-12MW-36W          Operational         48
Slot-2     5520-12MW-36W          Operational         48
Slot-3     5520-12MW-36W          Operational         48
Slot-4     5520-12MW-36W          Operational         48
Slot-5                                     Empty              0
Slot-6                                     Empty              0
Slot-7                                     Empty              0
Slot-8                                     Empty              0

```

show stacking detail

The `show stacking {node-address node_address | slot slot_number} detail` command displays a full report about a particular node.

```

Slot-1 Stack.33 # show stacking slot 1 detail
Stacking Node 00:04:96:26:6b:ec information:
Current:
Stacking : Enabled
Role : Master
Priority : Automatic
Slot number : 1
Stack state : Active
Master capable? : Yes
Stacking protocol : Enhanced
License level restriction : <none>
In active topology? : Yes
Factory MAC address : 00:04:96:26:6b:ec
Stack MAC address : 02:04:96:26:6b:ec
Alternate IP address : <none>
Alternate gateway : <none>
Stack Port 1:
State : Operational
Blocked? : No
Control path active? : Yes

```



```

Selection : Alternate (23)
Stack Port 2:
State : Operational
Blocked? : Yes
Control path active? : Yes
Selection : Native
Configured:
Stacking : Enabled
Master capable? : Yes
Slot number : 1
Stack MAC address : 02:04:96:26:6b:ec
Stacking protocol : Enhanced
License level restriction : <none>
Stack Port 1:
Selection : Alternate (23)
Stack Port 2:
Selection : Native

```

In the command output, note that:

- If you issue `show stacking detail` without a `node-address` or `slot` parameter, the output is generated for all nodes in the stack topology.
- The `slot` parameter is available only in stacking mode. The `node-address` parameter is always available.
- Current information represents stacking states and configured values that are currently in effect. Configured information is that which takes effect at node reboot only.
- The node's role can be Primary, Backup, Standby, or none.
- License level restrictions are Base or Premier.

show stacking stack-ports

The `show stacking stack-ports` command displays the states of each stacking port in the stack. This information can help you verify that all ports are properly connected and operational.

```

Slot-1 Stack.5 # show stacking stack-ports
Stack Topology is a Ring
Slot Port Select Node MAC Address Port State Flags Speed
-----
*1 1 27 00:04:96:9c:e4:39 Operational C- 10G
*1 2 28 00:04:96:9c:e4:39 Operational CB 10G
2 1 27 00:04:96:9b:c1:34 Operational CB 10G
2 2 28 00:04:96:9b:c1:34 Operational C- 10G
3 1 15 00:04:96:9e:5c:76 Operational C- 10G
3 2 16 00:04:96:9e:5c:76 Operational C- 10G
4 1 15 00:04:96:9c:53:b6 Operational C- 10G
4 2 16 00:04:96:9c:53:b6 Operational C- 10G
* - Indicates this node
Flags: (C) Control path is active, (B) Port is Blocked

```

In the command output, a state other than `Operational` indicates a potential problem. Check the physical connections and the software configuration for the ports in question.



Common Commands

This section discusses common commands you can use to manage the switch.

Commands specific to a particular feature may also be described in other chapters of this guide. For a detailed description of the commands and their options, see the [Switch Engine 32.7.1 Command Reference Guide](#).

Table 6: Common Commands

Command	Description
<code>cat {--number -n } {--number-nonblank -b } {--show-ends -E } {--show-tabs -T } {--show-nonprinting -v }</code>	Displays the contents of various text files that may be created, edited, or otherwise visible in the user-visible file system.
<code>clear [license license-info] [software port-speed]</code>	
<code>clear access-list {dynamic} counter {countername} {any ports port_list vlan vlan_name} {ingress egress} meter {meter_name} [any ports [all port_list] vlan vlan_name]</code>	Clears the specified access list counters.
<code>clear account [all name lockout]</code>	Re-enables an account that has been locked out (disabled) for exceeding the permitted number failed login attempts. This was configured by using the <code>configure account [all name] password-policy lockout-on-login-failures [on off]</code> command.
<code>clear bootprelay ipv6 prefix-delegation snooping [{ipv6-prefix} ipv6_prefix ipv6-prefix all] [{vlan} vlan_name vlan all]</code>	Clears information about a snooped IPv6 delegate prefix on a or all VLANs.
<code>clear cdp neighbor [device id device_id all] counters {ports ports_list}</code>	Clears the CDP neighbor information.

Table 6: Common Commands (continued)

Command	Description
clear counters vr <i>vpn-vrf-name</i>	Clears all switch statistics and port counters, including port packet statistics, bridging statistics, IP statistics, and log event counters.
clear counters cfm session missed-hellos { <i>domain_name</i> { <i>association_name</i> { {ports <i>port_list</i> } { end-point [up down] } } } } { current history both } segment <i>segment_name</i> segment all frame-delay segment all frame-loss segment <i>segment_name</i> frame-loss mep <i>mep_id</i>	This command clears counters for current or historical cfm session missed-hellos.
clear counters edp {ports <i>ports</i> }	Clears the counters associated with .
clear counters fdb mac-tracking [<i>mac_addr</i> all]	Clears the event counters for the MAC-tracking feature.
clear counters flowmon	This command clears all groups.
clear counters identity-management	Clears the identity management feature counters.
clear counters iparp	Clears all the IPARP counters.
clear mvrp counters { event packet } {ports [<i>port_list</i> all]}	Clears MVRP statistics.
clear counters policy	Clears policy rule usage statistics.
clear counters ports { <i>port_list</i> all } { <i>port_list</i> all } protocol filter	Clears the counters associated with the ports.
clear counters stp [{ all diagnostics domains ports]}	Clears, resets all statistics and counters.
clear counters wred ecn	Clears Explicit Congestion Notification (ECN) counters statistics for all ports.
clear counters xml-notification { all <i>target</i> }	Clears the statistics counters.
clear cpu-monitoring { process <i>name</i> }	Clears, resets the CPU utilization history and statistics stored in the switch.
clear dns cache	Clears the Domain Name System (DNS) cache entries.
clear dns cache analytics entries { vr } <i>vr_name</i> }	Clears the Domain Name System (DNS) cache analytics entries for a virtual router (VR).

Table 6: Common Commands (continued)

Command	Description
clear elsm ports <i>port_list</i> auto-restart <i>port_list</i> counters	Clears one or more ELSM-enabled ports that are in the Down-Stuck state.
clear esrp counters <i>esrpDomain</i> sticky <i>esrpDomain</i> neighbor	Clears the statistics gathered by for all ESRP domains on the switch.
clear igmp counters group { <i>grpipaddress</i> } {{ vlan } <i>name</i> } snoping {{ vlan } <i>name</i> }	Clears Internet Group Management Protocol (IGMP) counters.
clear inline-power stats ports [all <i>port_list</i>]	Clears the inline statistics for the selected port to zero.
clear iparp { <i>ip_addr</i> { vr <i>vr_name</i> } vlan <i>vlan_name</i> vr <i>vr_name</i> } { refresh }	Removes dynamic entries in the IP ARP table.
clear ip nat counters vlan { <i>vlan_name</i> }	Clears the Network Address Translation (NAT) VLAN counters.
clear ip-security dhcp-snooping entries { vlan } <i>vlan_name</i> source-ip-lockdown entries ports [<i>ports</i> all] arp validation violations anomaly-protection notify cache { slot [<i>slot</i> all]}	Clears the binding entries present on a .
clear ipv6 dad {{ vr } <i>vr_name</i> { <i>ipaddress</i> } vr all { vlan } <i>vlan_name</i> } { counters }	Clears the counters for the DAD feature.
clear l2pt counters { vlan <i>vlan_name</i> { ports <i>port_list</i> }} { vman <i>vman_name</i> { ports <i>port_list</i> }} {[vlan <i>vlan_name</i> {{ vxlan { vr <i>vr_name</i> } rtep <i>rtep_ipv4</i> }}} {[vppls <i>vppls_name</i> { peer <i>ipaddress</i> } vpws <i>vpws_name</i>]}	Clears L2PT counters.
clear lacp counters	Clears the counters associated with Link Aggregations Control Protocol (LACP).
clear lldp neighbors [all port <i>port_list</i>]	Clears the neighbor information collected for one or all ports on the switch.
clear log { static messages [memory-buffer nvr am]}	Clears the log messages in memory and NVRAM.

Table 6: Common Commands (continued)

Command	Description
<code>clear mac-locking station [all {mac station_mac_address} {first-arrival static} {ports port_list}]</code>	Clears MAC lock station information.
<code>clear mld counters {{vlan} vlan_name}</code>	Clears MLD statistics counters.
<code>clear neighbor-discovery cache ipv6 {ipv6address {vr vr_name} vlan vlan_name vr vr_name} refresh {ipv6address {vr vr_name} vlan vlan_name vr vr_name} refresh</code>	Deletes a dynamic entry from the neighbor cache.
<code>clear netlogin state {port port_list}</code>	Clears and initializes the network login sessions on a port.
<code>clear nodealias { ports [port_list all] alias-id alias_id }</code>	This command clears alias entries out of the Node Alias feature database. You can clear information by specified port(s) or alias ID. Node Alias discovers information about the end systems on a per-port basis. Information from packets from end systems, such as VLANID, source MAC address, source IP address, protocol, etc. are captured in a database that can be queried.
<code>clear ports [port_list all] link-flap- detection counters [port_list all] link-flap- detection status [all port_list port_group] rate-limit flood out-of-profile {disabled-ports} {status counter}</code>	Clears the counters related to port link-flapping.
<code>clear session [history sessId all]</code>	Terminates a Telnet or SSH2 session from the switch.
<code>clear slot slot</code>	Clears a slot of a previously assigned module type.
<code>clear snmp notification-log [counters entries] [default name hex hex_name]</code>	
<code>clear switch bluetooth device [all address]</code>	Clears either all paired Bluetooth devices or a particular paired device.
<code>clear stpd stpd_name ports port_list protocol-migration</code>	Resets the partner Spanning Tree Protocol version to the configured version.
<code>clear vlan vlan_name dhcp-address- allocation [[all {offered assigned declined expired}] ipaddress]</code>	Removes addresses from the allocation table.

Table 6: Common Commands (continued)

Command	Description
<pre>configure account [all name] password-policy min-length [num_characters none] [all name] password-policy lockout-on-login-failures [on off] [all name] password-policy lockout-time-period [num_mins until-cleared]</pre>	<p>Configures a user account password. Passwords can have a minimum of 0 character and can have a maximum of 32 characters. Passwords are case-sensitive. User names are not case-sensitive.</p>
<pre>configure auto-provision cloud- connector server [vr (vr_name none) ipaddress (ip_address none)]</pre>	<p>Configures the either the virtual router or the IP address for the Cloud Connector to use.</p>
<pre>configure banner</pre>	<p>Configures the banner string. You can configure a banner to be displayed before login or after login. You can enter up to 24 rows of 79-column text that is displayed before the login prompt of each session.</p>
<pre>configure cli password prompting- only [on off]</pre>	<p>This command allows you to configure prompting (with no echo) for all passwords, secrets, or keys.</p>
<pre>configure diagnostics privilege [admin user]</pre>	<p>This command configures the user privilege level needed to view diagnostic results.</p>
<pre>configure dns-client add [domain- suffix domain_name name-server ip_address {vr vr_name}]</pre>	<p>Adds a domain suffix to the domain suffix list or a name server to the available server list for the DNS client.</p>
<pre>configure dns-client delete [domain-suffix domain_name name- server ip_address {vr vr_name}]</pre>	<p>Deletes a domain suffix from the domain suffix list or a name server from the available server list for the DNS client.</p>
<pre>configure fabric attach management-vlan [vlan_id vlan_name untagged none forward [on off]]</pre>	<p>Specifies the VLAN advertised to Fabric Attach clients for them to use as the management VLAN.</p>
<pre>configure fabric attach management-vlan ports [port_list all] forward [on off]</pre>	<p>Configures the Fabric Attach management VLAN propagation on a specific port.</p>
<pre>configure fabric attach ports [port_list all] enable disable]</pre>	<p>Configures the Fabric Attach state per port.</p>
<pre>configure fabric attach ports [port_list all] authentication [disable enable key {key default encrypted encrypted_key}]</pre>	<p>Configures Fabric Attach authentication.</p>
<pre>configure fabric attach uplink [port none]</pre>	<p>Configures the uplink port for and enables Fabric Attach standalone proxy operation.</p>

Table 6: Common Commands (continued)

Command	Description
configure fabric attach zero-touch-client <i>client</i> [vlan [<i>vlan_name</i> <i>vlan_id</i>] [nsi <i>nsi</i> isid <i>isid</i>] { priority [<i>priority</i> dot1p]} { enable disable } none] enable disable]	Configures the Fabric Attach Zero Touch Client.
configure failsafe-account {[deny permit] [all control serial ssh { vr <i>vr-name</i> } telnet { vr <i>vr-name</i> }]}	Configures a name and password for the failsafe account, or restricts access to specified connection types.
configure cli idle-timeout <i>minutes</i>	Configures the time-out for idle console, SSH2, and Telnet sessions.
configure instant-port profile <i>profile_name</i> [assign unassign (ports <i>port_list</i>)]	Configures an Instant Port profile.
configure iqagent http-proxy [ipaddress [<i>fqdn</i> <i>ip_address</i>] port <i>port_number</i> user <i>user_name</i> password [encrypted <i>encrypted_password</i> <i>password</i>] none]	Configures the IQ Agent HTTP Proxy server IP and port, and defines the username and password if required.
configure iqagent server [vr [[<i>vr-name</i> none] [<i>vr_name</i> vlan <i>vlan-name</i>]] ipaddress [<i>fqdn</i> <i>ip_address</i> none]]	Configures the optional user-defined virtual router (VR) and address for the server for ExtremeCloud™ IQ Agent to connect to.
configure iproute delete default [<i>ipv6Gateway</i> <i>ipv6ScopedGateway</i>] { vr <i>vr_name</i> }	Deletes a default gateway from the routing table.
configure ip-security dhcp-snooping information check	Enables the relay agent option (option 82) checking in the server-originated packets.
configure ip-security dhcp-snooping information circuit-id port-information <i>port_info</i> port <i>port</i>	Configures the port information portion of the circuit ID.
configure ip-security dhcp-snooping information circuit-id vlan-information <i>vlan_info</i> [dynamic { vlan } <i>vlan_name</i> all]	Configures the info portion of the circuit ID of a VLAN.
configure ip-security dhcp-snooping information option	Enables the relay agent option (option 82).
configure ip-security dhcp-snooping information policy [drop keep replace]	Configures the relay agent option (option 82) policy.

Table 6: Common Commands (continued)

Command	Description
<code>configure lacp member-port <i>port</i> priority <i>port_priority</i></code>	Configures the member port of an LACP to ensure the order that ports are added to the aggregator. The lower value you configure for the port's priority, the higher priority that port has to be added to the aggregator.
<code>configure log display <i>severity</i> {only}</code>	Configures the real-time log-level message to display.
<code>configure log messages privilege [admin user]</code>	This command configures the minimum user account level needed to view logs.
<code>configure log target [console memory-buffer primary-node backup-node nvram session syslog [all <i>ipaddress</i> {udp-port {<i>udp_port</i>}} <i>ipPort</i> ipaddress tls-port {<i>tls_port</i>}] {vr <i>vr_name</i>} {local0...local7}] filter <i>filter-</i> <i>name</i> {severity <i>severity</i> {only}}</code>	Associates a filter to a target. In a stack, this command is applicable only to Master and Backup nodes. This command is not applicable to standby nodes.
For console display, session, memory buffer, and NVRAM targets: <code>configure log target [console session memory-buffer nvram] format [timestamp [seconds hundredths none]] [date [dd-Mmm-yyyy yyyy-mm-dd Mmm- dd mm-dd-yyyy mm/dd/yyyy dd-mm-yyyy none]] {event-name [component condition none]} {process-name} {severity} {source- line} {host-name}</code> For Syslog targets: <code>configure log target syslog [all <i>ipaddress</i> {udp-port {<i>udp_port</i>}} <i>ipPort</i> ipaddress tls-port {<i>tls_port</i>}] {vr <i>vr_name</i>} {local}format [timestamp [seconds hundredths none]] [date [dd-Mmm-yyyy yyyy-mm-dd Mmm- dd mm-dd-yyyy mm/dd/yyyy dd-mm-yyyy none]] {event-name [component condition none]} {severity} {priority} {host-name} {source-line} {tag-id} {tag-name}</code>	Configures the formats of the displayed message, on a per-target basis. In a stack, this command is applicable only to Master and Backup nodes and not applicable to the standby nodes.
<code>configure log target syslog [all <i>ipaddress</i> {udp-port {<i>udp_port</i>}} <i>ipPort</i> ipaddress tls-port {<i>tls_port</i>}] {vr <i>vr_name</i>} {local0...local7} from <i>source-ip-</i> <i>address</i></code>	This command specifies the source-ip-address to use when sending log messages to the Syslog server. The Syslog server's IP address along with the ipPort and local facility (a tuple) identify which Syslog server target is to be configured.

Table 6: Common Commands (continued)

Command	Description
<code>configure log target [console memory-buffer nvram primary-node backup-node session syslog [all ipaddress {udp-port {udp_port}} ipPort ipaddress {tls-port {tls_port}}] {vr vr_name} {local0 ... local7}] match [any match-expression]</code>	Associates a match expression to a target. In a stack, this command is applicable only on a Master and Backup nodes. This command is not applicable for standby nodes.
<code>configure mirror {mirror_name} add [{vlan} vlan_name vlan vlan_id] {ingress [port port {ingress}] ip-fix port port vlan [vlan_id vlan_name] {ingress}}</code>	Specifies mirror source filters for an instance.
<code>configure mirror add ports port_list anomaly</code>	Mirrors detected anomaly traffic to the mirror port.
<code>configure mirror {mirror_name} delete [{vlan} vlan_name vlan vlan_id] {port port} ip-fix port port vlan [vlan_id vlan_name]</code>	Deletes mirror source filters for an instance.
<code>configure ntp key keyid [trusted not-trusted]</code>	Specifies whether an NTP key is trusted or not trusted.
<code>configure ntp local-clock none</code>	Removes the internal local clock from the clock source list.
<code>configure ntp local-clock stratum stratum_number</code>	Configures the internal local clock with a stratum number. The stratum number defines the distance from the reference clock. The lower the number, the closer the switch is to the reference clock.
<code>configure ntp restrict-list [add delete] network {mask} [permit deny] {{vr} vr_name}</code>	Restricts a host or block of client IP addresses from getting NTP service. When NTP is enabled over a , an NTP server is configured, or a broadcast NTP server is in a VLAN, the VLAN's IP block or NTP server's IP address is automatically added into the system with a permit action.
<code>configure ntp [server peer] add [ip_address ipv6_address host_name] {key keyid} {option [burst initial-burst]} {{vr} vr_name}</code>	Configures an NTP server or peer.
<code>configure ntp [server peer] delete [ip_address ipv6_address host_name]</code>	Removes an NTP server or peer from external clock source lists.
<code>configure ports port_list {medium [copper fiber]} auto off speed speed duplex [half full]</code>	Manually configures the port speed and duplex setting of one or more ports on a switch.

Table 6: Common Commands (continued)

Command	Description
<code>configure ports auto 1G-optics-in-10G-ports [on off]</code>	Configures the default 1 Gbps auto-negotiation mode to enabled or disabled (the default) when 1 Gbps optics are inserted in 10 Gbps ports.
<code>configure ports port_list {medium [copper fiber]} auto off speed speed duplex [half full]</code>	Manually configures port speed and duplex setting configuration on one or more ports on a switch.
<code>configure ports port_list {medium [copper fiber]} auto on [{speed speed} {duplex [half full]}] [{duplex [half full]} {speed speed}]</code>	Enables autonegotiation for the particular port type.
<code>configure ports port_list description-string string</code>	Configures a description string setting up to 255 characters.
<code>configure ports port_list display-string string</code>	Configures a user-defined string for a port or group of ports.
<code>configure ports port_list forward-error-correction [off on [c174 c191]]</code>	Enables/disables IEEE Forward Error Correction (FEC) Clause 74 or 91 modes.
<code>configure ports [port_list all] partition [1x100G 1x40G 2x50G 4x10G 4x25G]</code>	Partitions 100G and 40G ports into multiple partition speeds, and partitions 25G ports into a single 10G port for supported Universal platforms.
<code>configure ports port_list [{tagged tag} vlan vlan_name {tagged} vlan vlan_list] [limit-learning number {action [blackhole stop-learning]} lock-learning unlimited-learning unlock-learning]</code>	Configures virtual ports for limited or locked MAC address learning.
<code>configure sharing port slot slot distribution-list [port_list add port_list all]</code>	Adds ports to a load-sharing, or link aggregation, group. By using link aggregation, you use multiple ports as a single logical port. Link aggregation also provides redundancy because traffic is redistributed to the remaining ports in the if one port in the group goes down.
<code>configure slot slot description [slot_description none]</code>	Adds or removes a descriptive name to a slot.
<code>configure slot slot module module_type</code>	Configures a slot for a particular type of node.
<code>configure slot slot_number restart-limit num_restarts</code>	Configures the number of times a slot can be restarted on a failure before it is shut down.
<code>configure snmp [sysContact sysContact sysName sysName sysLocation sysLocation]</code>	

Table 6: Common Commands (continued)

Command	Description
<pre>configure snmp add community [readonly readwrite] alphanumeric_string [encrypted enc_community_name community name hex hex_community_name] store-encrypted</pre>	Adds a read or read/write community string.
<pre>configure snmp delete community [readonly readwrite] [all community_name alphanumeric_string hex hex_community_name encrypted enc_community_name]</pre>	Deletes a read or read/write community string.
<pre>configure snmp syscontact sysContact v</pre>	Configures the name of the system contact.
<pre>configure snmpv3 add access [[hex hex_group_name] group_name] {sec-model [snmpv1 snmpv2c usm]} {sec-level [noauth authnopriv priv]} {read- view [[hex hex_read_view_name] read_view_name]} {write-view [[hex hex_write_view_name]] write_view_name]} {notify-view [[hex hex_notify_view_name]] notify_view_name]} {volatile}</pre>	Creates (and modifies) a group and its access rights.
<pre>configure snmpv3 add community [[hex hex_community_index] community_index] [encrypted name community_name name [[hex hex_community_name] community_name] {store- encrypted}] user [[hex hex_user_name] user_name] {tag [[hex transport_tag] transport_tag]} {volatile}</pre>	Adds an SNMPv3 community entry.
<pre>configure snmpv3 add filter [[hex hex_profile_name] profile_name] subtree object_identifier {/ subtree_mask} type [included excluded] {volatile}</pre>	Adds a filter to a filter profile.
<pre>configure snmpv3 add filter- profile [[hex hex_profile_name] profile_name] param [[hex hex_param_name]] param_name] {volatile}</pre>	Associates a filter profile with a parameter name.
<pre>configure snmpv3 add group [[hex hex_group_name] group_name] user [[hex hex_user_name] user_name] {sec-model [snmpv1 snmpv2c usm]} {volatile}</pre>	Adds a user name (security name) to a group.

Table 6: Common Commands (continued)

Command	Description
<pre>configure snmpv3 add mib-view [[hex hex_view_name] view_name] subtree object_identifier {subtree_mask} {type [included excluded]} {volatile}</pre>	Adds (and modifies) a MIB view.
<pre>configure snmpv3 add notify [[hex hex_notify_name] notify_name] tag [[hex hex_tag] tag] {type [trap inform]}{volatile}</pre>	Adds an entry to the snmpNotifyTable.
<pre>configure snmpv3 add target- addr [[hex hex_addr_name] addr_name] param [[hex hex_param_name] param_name] ipaddress [ip_address ipv4- with-mask ip_and_tmask] [ipv6_address ipv6-with-mask ipv6_and_tmask]] {transport-port port_number} {from [src_ip_address src_ipv6_address]} {vr vr_name} {tag-list [tag_list hex hex_tag_list]} {volatile}</pre>	Adds and configures an SNMPv3 target address and associates filtering, security, and notifications with that address.
<pre>configure snmpv3 add target- params [[hex hex_param_name] param_name]user [[hex hex_user_name] user_name] mp- model [snmpv1 snmpv2c snmpv3] sec-model [snmpv1 snmpv2c usm] {sec-level [noauth authnopriv priv]} {volatile}</pre>	Adds and configures SNMPv3 target parameters.
<pre>configure snmpv3 add user [hex hex_user_name user_name] {engine-id engine_id} {authentication [md5 sha] {localized-key auth_localized_key hex hex_auth_password auth_password} {privacy {des aes {128 192 256}} {localized-key priv_localized_key hex hex_priv_password priv_password} }} {volatile}</pre>	Adds (and modifies) an SNMPv3 user.
<pre>configure snmpv3 add user [[hex hex_user_name] user_name] {engine-id engine_id}clone-from [[hex hex_user_name] user_name] {engine-id clone_from_engine_id}</pre>	Creates a new user by cloning from an existing SNMPv3 user.

Table 6: Common Commands (continued)

Command	Description
<code>configure snmpv3 delete access [all-non-defaults {[hex hex_group_name] group_name} {sec-model [snmpv1 snmpv2c usm] sec-level [noauth authnopriv priv]}]}</code>	Deletes access rights for a group.
<code>configure snmpv3 delete community [all {[hex hex_community_index] community_index} {name [[hex hex_community_name] community_name]}]</code>	Deletes an SNMPv3 community entry.
<code>configure snmpv3 delete group {[hex hex_group_name] group_name} user [all-non-defaults {[hex hex_user_name] user_name} {sec-model [snmpv1 snmpv2c usm]}]}</code>	Deletes a user name (security name) from a group.
<code>configure snmpv3 delete mib-view [all-non-defaults {[hex hex_view_name] view_name} {subtree object_identifier}]</code>	Deletes a MIB view.
<code>configure snmpv3 delete notify {[hex hex_notify_name] notify_name} all-non-defaults]</code>	Deletes an entry from the snmpNotifyTable.
<code>configure snmpv3 delete filter [all [hex hex_profile_name] profile_name] {subtree object_identifier}]</code>	Deletes a filter from a filter profile.
<code>configure snmpv3 delete filter-profile [all [hex hex_profile_name] profile_name] {param [hex hex_param_name] param_name}]</code>	Removes the association of a filter profile with a parameter name.
<code>configure snmpv3 delete target-addr {[hex hex_addr_name] addr_name} all]</code>	Deletes SNMPv3 target addresses.
<code>configure snmpv3 delete target-params {[hex hex_param_name] param_name} all]</code>	Deletes SNMPv3 target parameters.
<code>configure snmpv3 delete user [all [hex hex_user_name] user_name] {engine-id engine_id}]</code>	Deletes an existing SNMPv3 user.
<code>configure snmpv3 engine-id hex_engine_id</code>	Configures the SNMPv3 snmpEngineID.
<code>configure snmpv3 target-addr [hex hex_addr_name] addr_name] retry retry_count</code>	Configures SNMPv3 INFORM notification retries.

Table 6: Common Commands (continued)

Command	Description
configure sntp-client [primary secondary] <i>host-name-or-ip</i> { vr <i>vr_name</i> }	Configures an NTP server for the switch to obtain time information.
configure ssh2 access-profile [<i>access_profile</i> [[add rule] [first [[before after] <i>previous_rule</i>]]] delete rule none]	Configures SSH2 to use an policy or ACL rule for access control.
configure ssh2 dh-group minimum [1 14 16 18]	Configures the minimal supported Diffie-Hellman group.
configure ssh2 disable [cipher [<i>cipher</i> all] mac [<i>mac</i> all]]	Disables ciphers/Message Authentication Codes (MACs) for use with SSHv2.
configure ssh2 disable { pk-alg [<i>pkalg_name</i> all]}	Disables DSA/RSA X509v3 public key algorithms.
configure ssh2 enable [cipher [<i>cipher</i> all] mac [<i>mac</i> all]]	Configures the required ciphers/Message Authentication Codes (MACs) with SSHv2.
configure ssh2 enable { pk-alg [<i>pkalg_name</i> all]}	Enables DSA/RSA X509v3 public key algorithms.
configure ssh2 idletimeout [none <i>minutes</i>]	This command configures idle-timeout for SSH/SFTP connections.
configure ssh2 key {pregenerated}	Generates the SSH2 host key.
configure ssh2 key algorithm [ssh-rsa rsa-sha2-256 rsa-sha2-512]	Generates the Secure Shell 2 (SSH2) server host key.
configure ssh2 login-grace-timeout <i>seconds</i>	For the SSH server, configures a timeout period for a login attempt.
configure ssh2 rekey [time-interval [<i>time_interval</i> none] data-limit [<i>data_size</i> default]]	Sets SSHv2 session rekeying interval by specifying a time interval value and/or amount of transferred data.
configure ssh2 secure-mode [on off]	This command (secure-mode on) disables the weak ciphers and macs in SSH server and client.
configure ssh2 x509v3 ocsp [on off]	Enables or disables Online Certificate Status Protocol (OCSP) check for SSH2 x509v3 authentication.
configure ssh2 x509v3 ocsp nonce [on off]	Enables or disables the Online Certificate Status Protocol (OCSP) nonce for SSH2 x509v3 authentication.
configure ssh2 x509v3 ocsp override [<i>url</i> none]	This command configures one HTTP Online Certificate Status Protocol (OCSP) override URL for an SSH2 x509v3 authentication.
configure ssh2 x509v3 ocsp signer ocsp-nocheck [on off]	Enables or disables Online Certificate Status Protocol (OCSP) signer's ocsp-nocheck for SSH2 x509v3 authentication.

Table 6: Common Commands (continued)

Command	Description
<code>configure ssh2 x509v3 radius-password-auth [on off]</code>	Enables or disables password authentication using RADIUS for SSH2 x509v3 publication-key authentication.
<code>configure ssh2 x509v3 username overwrite [on off]</code>	Enables or disables authentication username configuration to use the Principal Name in the certificate as the username.
<code>configure ssh2 x509v3 username strip-domain [on off]</code>	Enables or disables authentication username configuration to strip the domain name for SSH2 x509v3 publication-key authentication.
<code>configure ssh2 x509v3 username use-domain [domain_name none]</code>	Enables or disables authentication username configuration with a domain name using RADIUS for SSH2 x509v3 publication-key authentication.
<code>configure ssl certificate hash-algorithm hash_algorithm</code>	This command configures the hash algorithm.
<code>configure ssl privkey pregenerated</code>	Obtains the pre-generated private key from the user.
<code>configure ssl certificate pregenerated { {csr-cert}pregenerated {ocsp {on off}}}</code>	Obtains the pre-generated certificate from the user.
<code>configure ssl certificate privkeylen length country code organization org_name common-name name</code>	Creates a self-signed certificate and private key that can be saved in the EEPROM.
<code>configure ssl csr privkeylen length country code organization org_name common-name name</code>	Generates certificate signing request (CSR) and private key.
<code>configure stacking alternate-ip-address [ipaddress netmask ipNetmask] gateway automatic configure stacking [node-address node-address slot slot_number] alternate-ip-address [ipaddress netmask ipNetmask] gateway</code>	Configures an alternate management IP address, subnetwork, and gateway.
<code>configure stacking easy-setup</code>	This command provides an easy way to initially configure the stacking parameters of all nodes in a new stack.
<code>configure stacking {node-address node-address slot slot-number} license-level license_restriction</code>	Allows you to restrict the license level at which the node operates.

Table 6: Common Commands (continued)

Command	Description
<code>configure stacking {node-address <i>node-address</i> slot <i>slot-number</i>} mac-address</code>	Selects a node in the stack whose factory assigned MAC address is to be used to form the stack MAC address. The formed address is then configured on every node in the stack topology.
<code>configure stacking [node-address <i>node_address</i> slot <i>slot_number</i>] master-capability [on off]</code>	The command configures a node to be allowed to operate as either a backup or master, or prevents a node from operating as either. The command controls the setting on the specified node only.
<code>configure stacking {node-address <i>node-address</i> slot <i>slot_number</i>} priority [<i>node_pri</i> automatic]</code>	Configures a priority value to be used to influence master and backup election.
<code>configure stacking node-address <i>node_address</i> slot-number <i>slot_number</i></code>	Configures a slot number on one or all nodes in the stack topology.
<code>configure stacking-support auto- discovery [disable enable]</code>	Enables or disables stacking auto-discovery.
<code>configure stacking-support stack- port [<i>stack-ports</i> all] selection [native {V40 V80 V160 V200 V320 V400 {alternative- configuration help}} alternate]</code>	Selects the switch ports and speed for stack communications.
<code>configure stpd <i>stpd_name</i> add [{vlan} <i>vlan_name</i> vlan <i>vlan_list</i>] ports [all <i>port_list</i>] {dot1d emistp pvst-plus}</code>	Adds all ports or a list of ports within a to a specified .
<code>configure stpd <i>stpd_name</i> delete [{vlan} <i>vlan_name</i> vlan <i>vlan_list</i>] ports [all <i>port_list</i>]</code>	Deletes one or more ports in the specified from an .
<code>configure stpd <i>stpd_name</i> mode [dot1d dot1w mstp [cist msti <i>instance</i>]]</code>	Configures the operational mode for the specified domain.
<code>configure stpd <i>stpd_name</i> ports active-role disable <i>port</i></code>	Allows a port to be selected as an alternate or backup port.
<code>configure stpd <i>stpd_name</i> ports active-role enable <i>port</i></code>	Prevents a port from becoming an alternate or backup port.
<code>configure stpd <i>stpd_name</i> ports auto-edge [on off] <i>port_list</i></code>	Enables and disables auto-edge detection.
<code>configure {stpd} <i>stpd_name</i> ports edge-safeguard disable <i>port_list</i> {bpdu-restrict} {recovery-timeout {<i>seconds</i>}}</code>	Disables the edge safeguard loop prevention on the specified RSTP or edge port.

Table 6: Common Commands (continued)

Command	Description
<code>configure {stpd} <i>stpd_name</i> ports edge-safeguard enable <i>port_list</i> {bpdu-restrict} {recovery-timeout {<i>seconds</i>}}</code>	Enables the edge safeguard loop prevention on the specified RSTP or edge port.
<code>configure {stpd} <i>stpd_name</i> ports bpdu-restrict [enable disable] <i>port_list</i> {recovery-timeout {<i>seconds</i>}}</code>	Configures BPDU Restrict.
<code>configure stpd <i>stpd_name</i> ports cost [auto <i>cost</i>] <i>port_list</i></code>	Specifies the path cost of the port in the specified .
<code>configure stpd <i>stpd_name</i> ports link-type [[auto broadcast point-to-point] <i>port_list</i> edge <i>port_list</i> {edge-safeguard [enable disable] {bpdu-restrict} {recovery-timeout <i>seconds</i>}}</code>	Configures the ports in the specified as auto, broadcast, edge, or point-to-point link types.
<code>configure stpd <i>stpd_name</i> ports loop-protect [on off] <i>port_list</i></code>	Enables and disables loop protect on a port.
<code>configure stpd <i>stpd_name</i> ports loop-protect partner [capable incapable] <i>port_list</i></code>	Configures whether the link partner is capable of the loop protect feature.
<code>configure stpd <i>stpd_name</i> ports mode [dot1d emistp pvst-plus] <i>port_list</i></code>	Configures the encapsulation mode for the specified port list. v
<code>configure stpd <i>stpd_name</i> ports port-priority <i>priority</i> <i>port_list</i></code>	Specifies the port priority of the port in the specified .
<code>configure stpd <i>stpd_name</i> ports priority <i>priority</i> <i>port_list</i></code>	Specifies the port priority of the port in the specified .
<code>configure stpd <i>stpd_name</i> priority <i>priority</i></code>	Specifies the bridge priority of the .
<code>configure stpd <i>stpd_name</i> priority-mode [dot1d dot1t]</code>	Sets bridge priority values.
<code>configure stpd <i>stpd_name</i> ports restricted-role disable <i>port_list</i></code>	Disables restricted role on the specified port inside the core network.
<code>configure stpd <i>stpd_name</i> ports restricted-role enable <i>port_list</i></code>	Enables restricted role on the specified port inside the core network.
<code>configure stpd <i>stpd_name</i> ports restricted-tcn [on off] <i>port_list</i></code>	Restricts the propagation of Topology Change Notification (TCN) BPDUs on the specified port.
<code>configure stpd <i>stpd_name</i> tag <i>stpd_tag</i></code>	Assigns an StpdID to an .
<code>configure sys-recovery-level [all none]</code>	Configures a recovery option for instances where an exception occurs in the software.

Table 6: Common Commands (continued)

Command	Description
<code>configure syslog add [ipaddress {udp-port {udp_port}} ipPort ipaddress tls_port {tls_port}] {vr vr_name} [local0...local7]</code>	Configures the remote Syslog server host address, and filters messages to be sent to the remote Syslog target.
<code>configure syslog delete [ipaddress {udp-port {udp_port}} ipPort ipaddress tls_port {tls_port}] {vr vr_name} [local0...local7]] all {local0...local7} {vr vr_name}] configure syslog delete host name/ip {: udp-port} [local0...local7]</code>	Deletes a remote Syslog server address.
<code>configure syslog [all ipaddress {tls-port tls_port}] {vr vr_name} {local} reference-identifier reference_identifier</code>	Specifies the remote Syslog server certificate reference identifier.
<code>configure syslog tls ocsp [on off]</code>	Enables or disables Online Certificate Status Protocol (OCSP) check for Transport Layer Security (TLS) connections to remote Syslog servers.
<code>configure syslog tls ocsp nonce [on off]</code>	Enables or disables Online Certificate Status Protocol (OCSP) nonce for Transport Layer Security (TLS) connections to remote Syslog servers.
<code>configure syslog tls tls override [url none]</code>	This command configures one HTTP Online Certificate Status Protocol (OCSP) override URL for Transport Layer Security (TLS) connections to a remote Syslog server.
<code>configure syslog tls ocsp signer ocsp-nocheck [on off]</code>	Enables or disables Online Certificate Status Protocol (OCSP) signer's ocsp-nocheck for Transport Layer Security (TLS) connections to remote Syslog servers.
<code>configure syslog tls tcp-user-timeout [seconds default]</code>	Specifies the maximum time that transmitted data may remain unacknowledged before TCP closes the connection to avoid loss of logging to TLS Syslog server.
<code>configure time month day year hour min sec</code>	Configures the system date and time. The format is as follows:mm dd yyyy hh mm ss The time uses a 24-hour clock format. You cannot set the year earlier than 2003 or past 2036.

Table 6: Common Commands (continued)

Command	Description
<code>configure timezone</code>	Configures the time zone information to the configured offset from GMT time. The format of GMT_offset is \pm minutes from GMT time. The autodst and noautodst options enable and disable automatic Daylight Saving Time change based on the North American standard. Additional options are described in the Switch Engine 32.7.1 Command Reference Guide
<code>configure [{ vlan } <i>vlan_name</i> vlan <i>vlan_id</i>] ipaddress [<i>ipaddress</i> {<i>ipNetmask</i>} ipv6-link-local {eui64} <i>ipv6_address_mask</i>]</code>	Configures an IP address and subnet mask for a .
<code>configure [{vlan} <i>vlan_name</i> vlan <i>vlan_list</i>] add ports [<i>port_list</i> all] {tagged <i>tag</i> untagged} {{stpd} <i>stpd_name</i>} {dot1d emistp pvst-plus}}</code>	Adds one or more ports in a .
<code>configure [{vlan} <i>vlan_name</i> vlan <i>vlan_id</i>] add ports <i>port_list</i> private-vlan translated</code>	Translation from network tag to each subscriber VLAN tag is done by default in a private VLAN.
<code>configure [{vlan} <i>vlan_name</i> vlan <i>vlan_list</i>] delete ports [all <i>port_list</i>]</code>	Deletes one or more ports in a .
<code>configure {vlan} <i>vlan_name</i> tag <i>tag</i> {remote-mirroring}</code>	Assigns a unique 802.1Q tag to the .
<code>configure [{vlan} <i>vlan_name</i> vlan <i>vlan_id</i>] ipaddress [<i>ipaddress</i> {<i>netmask</i>} {<i>ipNetmask</i>} ipv6-link-local {eui64} <i>ipv6_address_mask</i>]</code>	Assigns an IPv4 address and an optional subnet mask or an IPv6 address to the . Beginning with ExtremeXOS 11.2, you can specify IPv6 addresses. You can assign either an IPv4 address, and IPv6 address, or both to the VLAN. Beginning with ExtremeXOS 11.3, you can use this command to assign an IP address to a specified VMAN and enable multicasting on that VMAN.
<code>cp <i>old_name</i> <i>new_name</i></code>	Copies a file from the specified file system or relative to the current working directory to another file on the specified file system or relative to the current working directory.

Table 6: Common Commands (continued)

Command	Description
<code>create account</code>	Creates a user account. This command is available to admin-level users and to users with command authorization. The username is between 1 and 32 characters and is not case-sensitive. The password is between 0 and 32 characters and is case-sensitive. For user names, only alphanumeric, dash (-), and underscore (_) characters may be used. Any text after a hashtag (#) in a password is ignored. It has to be enclosed in "<double quotes>" if the hashtag is to be made part of the special character password.
<code>create log message text</code>	This command logs an event using the text provided as the message.
<code>create vlan [vlan_name {tag tag} vlan_list] {description vlan-description} {vr name}</code>	Creates a named .
<code>create vlan [{ vlan} vlan_name vlan vlan_list] {description vlan-description} {vr name}</code>	Creates a VLAN.
<code>delete account name</code>	Deletes a user account.
<code>delete instant-port profile profile_name</code>	Deletes an instant-port profile.
<code>delete [{ vlan} vlan_name vlan vlan_list]</code>	Deletes a VLAN.
<code>disable auto-provision</code>	Disables the auto provision capability.
<code>disable auto-provision cloud-connector</code>	Stops the Cloud Connector process on the switch.
<code>disable bootp {ipv4} dhcp {ipv4 ipv6}] vlan [vlan all]</code>	Disables the generation and processing of BOOTP packets on a to obtain an IP address for the VLAN from a BOOTP server.
<code>disable clear-flow</code>	
<code>disable cli prompting</code>	Disables CLI prompting for the session.
<code>disable cli config-logging</code>	Disables logging of CLI commands to the Syslog.
<code>disable cli paging</code>	Disables pausing of the screen display when a show command output reaches the end of the page.
<code>disable cli idle-timeout</code>	Disables the timer that disconnects all sessions. After being disabled, console sessions remain open until the switch is rebooted or until you log off. Telnet sessions remain open until you close the Telnet client. SSH2 sessions time out after 61 minutes of inactivity.

Table 6: Common Commands (continued)

Command	Description
<code>disable cli write-permission</code>	Disables access to the full CLI on 4120 Series and 4220 Series switches.
<code>disable igmp snooping {vlan} name fast-leave</code>	Disables the snooping fast leave feature on the specified .
<code>disable igmp snooping {forward-mcrouter-only with-proxy vlan name}</code>	Disables snooping.
<code>disable inline-power ports [all port_list]</code>	Shuts down power currently provided to all ports or to specified ports.
<code>disable ipforwarding ipv6 [{vlan} vlan_name vlan vlan_list] tunnel tunnel_name vr vr_name}</code>	Disables routing for one or all interfaces. If no argument is provided, disables routing for all interfaces on the current VR or VRF.
<code>disable ip-security dhcp-snooping [dynamic {vlan} vlan_name] ports [all ports]</code>	Disables snooping on the switch.
<code>disable iqagent</code>	Disables the ExtremeCloud™ IQ Agent.
<code>disable led locator { slot [slot all]}</code>	Disables the front panel LEDs from flashing on a switch.
<code>disable log display</code>	Disables the sending of messages to the console display. In a stack, this command is applicable only to Master and Backup nodes and not applicable to the standby nodes.
<code>disable log target [console memory-buffer nvram primary-node backup-node session syslog [all ipaddress udp-port {udp_port} ipPort ipaddress tls_port {tls_port}] {vr vr_name} {local0 ... local7}]</code>	Stops sending log messages to the specified target. In a stack, this command is applicable only to Master and Backup nodes and not applicable to the standby nodes.
<code>disable loopback-mode [{vlan} vlan_name vlan vlan_list]</code>	Disallows a to be placed in the UP state without an external active port. This allows (disallows) the VLANs routing interface to become active.
<code>disable mac-locking</code>	Disables MAC locking globally on the switch.
<code>disable mirror [mirror_name all]</code>	Disables a mirror instance.
<code>disable mld snooping {with-proxy vlan name}</code>	Disables MLD snooping.
<code>disable netlogin ports ports [{dot1x} {mac} {web-based}]</code>	Disables network login on a specified port for a particular method.
<code>disable netlogin [{dot1x} {mac} {web-based}]</code>	Disables network login modes.

Table 6: Common Commands (continued)

Command	Description
<code>disable ntp authentication</code>	Disables NTP authentication globally on the switch.
<code>disable ntp broadcast-client {{vr} vr_name}</code>	Disables an NTP broadcast client on the switch.
<code>disable ntp {vlan} vlan-name broadcast-server</code>	Prevents NTP from sending broadcast messages to a .
<code>disable ntp [{vlan} vlan-name all] {{vr} vr_name}</code>	Disables NTP on a .
<code>disable ntp vr vr_name</code>	This command disables NTP from the specified VR.
<code>disable sharing port</code>	Disables a load-sharing group of ports, also known as a .
<code>disable snmp access {snmp-v1v2c snmpv3}</code>	Selectively disables on the switch.
<code>disable snmp access vr [vr_name all]</code>	Selectively disables access on virtual routers.
<code>disable snmp community [encrypted enc_community_name community_name alphanumeric-community-string hex hex_community_name]</code>	Disables community strings on the switch.
<code>disable snmpv3 default-group</code>	Disables SNMPv3 default-group access on the switch.
<code>disable snmpv3 community [community_index hex hex_community_index]</code>	This command disables a community entry specified by the community index.
<code>disable snmp access {snmp-v1v2c snmpv3}</code>	Selectively disables on the switch.
<code>disable ssh2</code>	Disables SSH2 access to the switch.
<code>disable snmp-client</code>	Disables the client.
<code>disable stacking {node-address node-address}</code>	This command disables the stacking on one or all nodes in the stack topology.
<code>disable stacking-support</code>	This command disables the stacking-support option on a switch with dual-purpose hardware.
<code>disable stpd {stpd_name}</code>	Disables the protocol on a particular or for all STPDs.
<code>disable stpd stpd_name auto-bind [{vlan} vlan_name vlan vlan_list]</code>	Disables the ability to automatically add ports to an when they are added to a member .
<code>disable stpd stpd_name ports [all port_list]</code>	Disables on one or more ports for a given .

Table 6: Common Commands (continued)

Command	Description
<code>disable tech-support collector</code>	Disables the tech support feature.
<code>disable telnet</code>	Disables external Telnet services on the system.
<code>disable web http</code>	Disables the hypertext transfer protocol (HTTP) access to the switch on the default port (80).
<code>disable web https</code>	Disables the secure socket layer (SSL) access to the switch on the default port (443).
<p>Using TFTP: <code>download [url url {vr vrname} image [active inactive] [[hostname ipaddress] filename {{vr} vrname} {block-size block_size}] {partition} {install {reboot}}</code></p> <p>To download an image to a stack: <code>download image [[hostname ipaddress] filename {{vr} vrname} {block-size block_size}] {partition} {install {reboot}}</code></p>	<p>Downloads a new version of the ExtremeXOS software image or a new VOSS image when changing the switch's network operating system.</p> <p>The image file can be downloaded using TFTP (which is not a secure method), or SFTP and SCP2 (which are secure methods). The procedure using TFTP begins above and using SFTP/SCP2.</p>
<code>download ssl ipaddress certificate {ssl-cert trusted-ca oosp-signature-ca {csr-cert {oosp [on off]}} file_name privkey key_file</code>	<p>Permits downloading of certificate file(s) from files stored on a TFTP server.</p> <p>Permits downloading of a private key from files stored in a TFTP server.</p>
<code>eject usb-device</code>	Ensures that USB 2.0 storage device can be safely removed from the switch.
<code>enable auto-provision cloud-connector</code>	Starts the Cloud Connector process on the switch.
<code>enable bootp {ipv4} dhcp {ipv4 ipv6}] vlan [vlan all]</code>	Enables BOOTP for one or more VLANs.
<code>enable cli config-logging</code>	Enables the logging of CLI configuration commands to the Syslog for auditing purposes. The default setting is disabled.
<code>enable cli paging</code>	Enables pausing of the screen display when show command output reaches the end of the page. The default setting is enabled.
<code>enable cli idle-timeout</code>	Enables a timer that disconnects all sessions (Telnet, SSH2, and console) after 20 minutes of inactivity. The default setting is enabled.
<code>enable cli write-permission</code>	Enables access to the full CLI on 4120 Series and 4220 Series switches.

Table 6: Common Commands (continued)

Command	Description
<code>enable igmp snooping {forward-mcrouter-only {vlan} name with-proxy vr vrname} {vlan} name fast-leave</code>	Enables snooping on one or all s.
<code>enable inline-power ports [all port_list]</code>	Enables power currently provided to all ports or to specified ports.
<code>enable ipforwarding {ipv4 broadcast} {vlan vlan_name} {ipv4 broadcast} {vlan vlan_list} {ipv4 tunnel tunnel_name} {ipv4 ipv6(vr vr_name)} {ipv6 (vlan vlan_list)} {ipv6 (vlan vlan_name tunnel tunnel_name)}</code>	Enables IPv4 routing or IPv4 broadcast forwarding for one or all s. If no argument is provided, enables IPv4 routing for all s that have been configured with an IP address on the current VR or VRF.
<code>enable iqagent</code>	Enables the ExtremeCloud™ IQ Agent.
<code>enable ip-security dhcp-snooping [dynamic {vlan} vlan_name] ports [all ports] violation-action [drop-packet {[block-mac block-port] [duration duration_in_seconds permanently] none}]] {snmp-trap}</code>	Enables DHCP snooping for the specified VLAN and ports.
<code>enable led locator {timeout [seconds none]} {pattern [alternating flash-all high-to-low scanner]} {slot [slot all]}</code>	Configures the front panel LEDs to flash so a switch can be easily located in a crowded lab/data center.
<code>enable license {software} key install license file filename {slot slot} (for universal platforms only)</code>	Enables a particular software feature license. Specify <i>key</i> as a 10 or 14 digit hexadecimal value. The command <code>unconfigure switch {all}</code> does not clear licensing information. This license cannot be disabled once it is enabled on the switch.
<code>enable log display</code>	Enables a running real-time display of log messages on the console display. In a stack, this command is applicable only to Primary and Backup nodes. You cannot run this command on standby nodes.

Table 6: Common Commands (continued)

Command	Description
enable log target [console memory-buffer nvr am primary-node backup-node session syslog [all <i>ipaddress</i> udp-port { <i>udp_port</i> } <i>ipPort</i> <i>ipaddress</i> tls_port { <i>tls_port</i> }] { vr <i>vr_name</i> { local0 ... local7 }]	Starts sending log messages to the specified target.
enable loopback-mode vlan [<i>vlan_name</i> <i>vlan_list</i>]	Allows a to be placed in the UP state without an external active port. This allows (disallows) the VLANs routing interface to become active.
enable mac-locking	Enables MAC locking globally on the switch.
enable mirror <i>mirror_name</i>	Enables a mirror instance.
enable mld snooping {{ vlan } <i>vlan_name</i> }	Enables MLD snooping on the switch.
enable netlogin [{ dot1x } { mac } { web-based }]	Enables network login authentication modes.
enable netlogin ports <i>ports</i> [{ dot1x } { mac } { web-based }]	Enables NetLogin on a specified port for a particular authentication method.
enable ntp authentication	Enables NTP authentication globally on the switch.
enable ntp broadcast-client {{ vr } <i>vr_name</i> }	Enables an NTP broadcast client on the switch.
enable ntp { vlan } <i>vlan-name</i> broadcast-server { key <i>keyid</i> }	Enables NTP to send broadcast messages with or without a key to a .
enable ntp [{ vlan } <i>vlan-name</i> all] {{ vr } <i>vr_name</i> }	Enables NTP on a .
enable ntp vr <i>vr_name</i>	This command enables and configures NTP for the specified VR.
enable sharing <i>port</i> grouping <i>port_list</i> { algorithm [address-based { L2 L3 L3_L4 custom } port-based]} {resilient-hashing [on off]} {distribution-mode [all local-slot port-lists]} {lacp health-check }	Enables the switch to configure port link aggregation, or load sharing. By using link aggregation, you use multiple ports as a single logical port. Link aggregation also provides redundancy because traffic is redistributed to the remaining ports in the if one port in the group goes down. LACP allows the system to dynamically configure the LAGs.
enable snmp access { snmp-v1v2c snmpv3 }	Selectively enables access on the switch.
enable snmp access vr [<i>vr_name</i> all]	Selectively enables access on virtual routers.

Table 6: Common Commands (continued)

Command	Description
enable snmp community [encrypted <i>enc_community_name</i> <i>community_name</i> <i>alphanumeric-</i> <i>community-string</i> hex <i>hex_community_name</i>	Enables community strings.
enable snmpv3 community [<i>community_index</i> hex <i>hex_community_index</i>]	This command enables a community entry specified by the community index.
enable snmp-client	Enables the client.
enable ssh2 { access-profile [<i>access_profile</i> none]} { port <i>tcp_port_number</i> } { vr [<i>vr_name</i> all default]}	Enables SSH2 sessions. By default, SSH2 is disabled. When enabled, SSH2 uses TCP port number 22.
enable stacking { node-address <i>node-address</i> }	This command enables stacking on one or all nodes.
enable stacking-support	This command enables a switch with dual-purpose hardware to participate in a stack.
enable stpd { <i>stpd_name</i> } ports [all <i>port_list</i>] auto-bind [{ vlan } <i>vlan_name</i> vlan <i>vlan_list</i>]	Enables the protocol for one or all STPDs.
enable tech-support collector	Enables the tech support feature.
enable telnet	Enables Telnet access to the switch. By default, Telnet uses TCP port number 23.
enable web http	Enables hypertext transfer protocol (HTTP) access to the switch on the default HTTP port (80).
enable web https	Enables secure socket layer (SSL) access to the switch on the default port (443).
hidden load commands < <i>module_name</i> >	
history	Displays the commands entered on the switch.
install firmware { force } { slot <i>slot-number</i> }	This command upgrades the ExtremeSwitching Universal platforms using images from the installed Switch Engine package.
install image [inactive <i>filename</i> <i>local-file</i>] { <i>partition</i> } { slot <i>slotid</i> } { reboot }	Installs a new version of the ExtremeXOS software image.
mv <i>old_name</i> <i>new_name</i>	Moves a file from the specified file system or relative to the current working directory to another file on the specified file system or relative to the current working directory.

Table 6: Common Commands (continued)

Command	Description
<pre>ping mac <i>mac</i> port <i>port</i> {domain} <i>domain_name</i> {association} <i>association_name</i></pre> <p>The ping, or loopback message (LBM), goes from the MEP configured on the port toward the given MAC address.</p>	Allows you to ping on the Layer 2 level throughout the specified domain and MA.
<pre>reboot {[time <i>mon day year</i> <i>hour min sec</i>] cancel} {slot <i>slot-number</i>} node-address <i>node- address</i> stack-topology {as- standby} all} rolling}</pre>	Reboots the switch, bridge port extenders (BPEs), or SummitStack in the specified slot at a specified date and time.
<pre>restart ports [all <i>port_list</i>]</pre>	Resets autonegotiation for one or more ports by resetting the physical link.
<pre>run diagnostics [extended normal] }</pre>	Runs normal or extended diagnostics on the switch or node, and stacking ports. This command is not supported in stacking mode, but if you issue the show diagnostics command from the master node, it will show the diagnostic results for all the nodes.
<pre>run failover {force}</pre>	Causes a user-specified node failover.
<pre>run provisioning</pre>	Allows you to change management access to your device and to enhance security.
<pre>save configuration {primary secondary <i>existing- config</i> <i>new-config</i>} automatic {every <i>minutes</i> {primary secondary <i>existing-config</i> <i>new-config</i>} never}</pre>	Saves the current configuration from the switch's runtime memory to non-volatile memory.
<pre>scp2 {cipher <i>cipher</i>} {mac <i>mac</i>} {compression [on off]} {port <i>portnum</i>} {vr <i>vr_name</i>} <i>user</i> [<i>hostname</i> <i>ipaddress</i>]:<i>remote_file</i> <i>local_file</i></pre> <p>Or</p> <pre>scp2 {cipher <i>cipher</i>} {mac<i>mac</i>} {compression [on off]} {port <i>portnum</i>} {vr <i>vr_name</i>} <i>local_file</i> <i>user</i> [<i>hostname</i> <i>ipaddress</i>]:<i>remote_file</i></pre>	<p>The first command initiates an SCP2 client session to a remote SCP2 server and copies a configuration or policy file from the remote system to the switch.</p> <p>The second command initiates an SCP2 client session to a remote SCP2 server and copies a configuration or policy file from the switch to a remote system.</p>
<pre>show banner {after-login before- login}</pre>	Displays the user-configured banner.
<pre>ssh2 {cipher <i>cipher</i>} {mac <i>mac</i>} {port <i>portnum</i>} {compression [on off]} {user <i>username</i>} {<i>username</i>} [<i>host</i> <i>ipaddress</i>] {<i>remote command</i>} {vr <i>vr_name</i>}</pre>	Initiates an SSH2 client session to a remote SSH2 server.

Table 6: Common Commands (continued)

Command	Description
<code>synchronize {slot slotid}</code>	The synchronize command replicates all saved images and configurations from the master node to the backup or target node on a SummitStack.
<code>synchronize stacking {node-address node_address slot slot_number}</code>	This command copies certain NVRAM based configuration parameters to the target node.
<code>traceroute mac mac {up-end-point} port port {domain} domain_name {association} association_name {ttl ttl}</code>	Enables you to trace the routed path between the switch and a destination endstation.
<code>unconfigure snmp [sysContact sysName sysLocation]</code>	Allows you to send out a Link Trace Message (LTM) for the specified MA from the MEP configured on the port for the specified MAC address to the end of the MA.
<code>unconfigure ip-security dhcp-snooping information option</code>	Disables the relay agent option (option 82).
<code>unconfigure ip-security dhcp-snooping information check</code>	Disables the relay agent option (option 82) checking in the server-originated packets.
<code>unconfigure ip-security dhcp-snooping information circuit-id port-information ports [port_list all]</code>	Unconfigures the port information portion of the circuit ID.
<code>unconfigure ip-security dhcp-snooping information circuit-id vlan-information [dynamic {vlan} vlan_name all]</code>	Unconfigures the info portion of the circuit ID of a VLAN.
<code>unconfigure ip-security dhcp-snooping information policy</code>	Unconfigures the relay agent option (option 82) policy.
<code>unconfigure ip-security dhcp-snooping information remote-id</code>	Removes the relay agent remote ID.
<code>unconfigure log target [console memory-buffer nvram session syslog [all ipaddress {udp-port} {udp_port}} ipPort ipaddress {tls-port} {tls_port}] {vr vr_name} {local0...local7}] format</code>	Resets the log target format to its default values.
<code>unconfigure ports port_list description string port_list description string port_list display-string</code>	Unconfigures a description string setting. Clears the user-defined display string from one or more ports.
<code>unconfigure slot slot</code>	Clears a slot of a previously assigned module type.

Table 6: Common Commands (continued)

Command	Description
unconfigure ssl certificate [trusted-ca ocsp-signature-ca] [<i>file_name</i> all]	Removes a trusted CA certificate or OCSP response signature CA certificate from the switch.
unconfigure stacking { node-address <i>node_address</i> slot <i>slot_number</i> }	This command resets most stacking parameters to the default or unconfigured values.
unconfigure stacking-support	This command resets the stacking parameters configured with commands that use the stacking-support keyword.
unconfigure stpd { <i>stpd_name</i> }	Restores default values to a particular or all STPDs.
unconfigure switch { all } Or unconfigure switch erase all nvr am	Resets all switch parameters (with the exception of defined user accounts, and date and time information) to the factory defaults. If you specify the keyword all , the switch erases the currently selected configuration image in flash memory and reboots. As a result, all parameters are reset to default settings.
unconfigure [{ vlan } <i>vlan_name</i> vlan <i>vlan_list</i>] ipaddress	Removes the IP address of the or a VMAN. With no parameters, the command removes the primary IPv4 address on the specified VLAN. Using the IPv6 parameters, you can remove specified IPv6 addresses from the specified VLAN.
uninstall image <i>fname</i> <i>partition</i> { msm <i>slotid</i> } { reboot } On a SummitStack, use: uninstall image <i>fname</i> <i>partition</i> { slot <i>slot number</i> } { reboot }	Uninstalls an ExtremeXOS software package. Also uninstalls a VOSS image when staged for installation on the next reboot.
upload configuration [<i>hostname</i> <i>ipaddress</i>] <i>filename</i> { vr <i>vr-name</i> } { block-size <i>block_size</i> }	Uploads the current configuration in ASCII format to a TFTP server on your network.
use configuration <i>file-name</i>	Configures the switch to use a previously saved configuration on the next reboot.
use image { partition } <i>partition</i> { slot <i>slotid</i> }	Configures the switch to use a saved image on the next reboot.



Software Licensing

Extreme Networks software may contain software from third party sources that must be licensed under the specific license terms applicable to such software. Applicable copyright information is provided below.

Copyright (c) 1995-1998 by Cisco Systems, Inc.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies of the software and supporting documentation, the name of Cisco Systems, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior notice be given in supporting documentation that modification, permission, and copying and distribution is by permission of Cisco Systems, Inc.

Cisco Systems, Inc. makes no representations about the suitability of this software for any purpose. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

MD5C.C - RSA Data Security, Inc., Message-Digest Algorithm

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

\$Id: md5c.c,v 1.2.4880.1 2005/06/24 01:47:07 lindak Exp \$ This code is the same as the code published by RSA Inc. It has been edited for clarity and style only.



Index

A

announcements 6, 7

B

banner
string 30

C

common commands (table) 26
console
maximum sessions 19
conventions
notice icons 4
text 4

D

documentation
feedback 7
location 5, 6
Documentation, related 8, 9

F

feedback 7

M

Management Switch Fabric Module, *see* MSM
modular switch
port number 17
MSM
console sessions 19

N

notices 4

O

Open Source Declaration 8, 9

P

port
lists 16
numbers and ranges 16

port (*continued*)

wildcard combinations 17
product announcements 6, 7

S

sessions
console 19
maximum number of 19
software requirements for switches 11
stacking
verifying configuration 22–25
SummitStack configuration 22
support, *see* technical support
switch
software requirement 11
switch management
overview 19
user sessions 19
switch series, table 10

T

technical support
contacting 6, 7

U

user sessions 19
see also sessions

W

warnings 4
wildcard combinations, port 17