Command Line Interface Cross-Reference Guide

ExtremeXOS, EOS, VOSS, BOSS, Cisco IOS

Published: March, 2018

Version: 1.0

9035422-00

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, please see:
www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. Enduser license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit:
http://www.extremenetworks.com/support/contact/

For product documentation online, visit: https://www.extremenetworks.com/documentation/

Table of Contents

Introduction to the CLI Cross-Reference Guide

This guide describes common Command Line Interface (CLI) commands for ExtremeXOS, EOS, VOSS, BOSS, and Cisco IOS.

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word "enter" 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 "type."
[Key] names	Key names are written with brackets, such as [Return] 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]
Words in italicized type	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.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

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

Getting Help

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

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- Extreme Portal — Search the GTAC knowledgebase, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- The Hub — A forum for Extreme 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.

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

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

Using the Alias Command to Transition to ExtremeXOS

ExtremeXOS has an alias command that allows you use a term you prefer to execute any ExtremeXOS command, including any options, arguments, and redirection.

For example, you can create an alias named *set* for *configure* commands:

alias set "configure"

You can now substitute the command *set* for all *configure* commands. For example, you can type *set vlan vlan_name tag tag* instead of *configure vlan vlan_name tag tag*.

For more information about the ExtremeXOS alias command, see the latest *ExtremeXOS Command Reference*.

Switch Models and Versions Used

ExtremeXOS	System Type: X440-G2 version: 21.1.3.7 System Type: X460 version: 16.1.3.6
EOS	System Type: C5-Series version: 6.81.09.0001 System Type: 7100 Series version: 8.62.04.0001 System Type: S-Series version: 8.62.04.0001
VOSS	System Type: VSP7200 version: 6.1.0.0 System Type: VSP8000 version: 6.1.0.0 System Type: VSP4000

	version: 6.1.0.0

BOSS	System Type: ERS4900 version: 7.4.0 System Type: ERS5900 version: 7.4.0 System Type: ERS3600 version: 6.1.0.005

Cisco IOS	System Type: WS-C3560-48PS version: 12.2(55)SE6 System Type: WS-3750-X version: 12.2(55)SE

Connecting to, Logging In, and Clearing Configuration

Console Cable

	ExtremeXOS, VOSS, BOSS Cisco IOS	EOS
Terminal Emulation		
	Baud rate: 9600	Baud rate: 9600
	Data Bits: 8	Data Bits: 8
	Stop bit: 1	Stop bit: 1
	Parity: none	Parity: none
	Flow control: none	Flow control: none

RJ45 to DB9 Pinouts

Pin	RJ45	DB9
1		
2		
3		
4		
5		
6		
7		
8		
9		

Pin	RJ45	DB9
1		
2		
3		
4		
5		
6		
7		
8		
9		

Default Login

<table>
<tr><td>ExtremeXOS</td><td>Username: admin
Password: <no password>

<table><tr><th>Username</th><th>Password</th><th>Description</th></tr><tr><td>admin</td><td>N/A</td><td>super-user</td></tr><tr><td>user</td><td>N/A</td><td>read-only</td></tr></table></td></tr>
<tr><td>EOS</td><td>login: admin
password: <no password>

<table><tr><th>Username</th><th>Password</th><th>Description</th></tr><tr><td>admin</td><td>N/A</td><td>super-user</td></tr><tr><td>ro</td><td>N/A</td><td>read-only</td></tr><tr><td>rw</td><td>N/A</td><td>read-write</td></tr></table></td></tr>
<tr><td>VOSS</td><td>login: rwa

password: rwa

<table><tr><th>Username</th><th>Password</th><th>Description</th></tr><tr><td>rwa</td><td>rwa</td><td>read-write-all</td></tr><tr><td>rw</td><td>rw</td><td>read-write</td></tr><tr><td>ro</td><td>ro</td><td>read-only</td></tr><tr><td>l1</td><td>l1</td><td>layer 1</td></tr><tr><td>l2</td><td>l2</td><td>layer 2</td></tr><tr><td>l3</td><td>l3</td><td>layer 3</td></tr></table></td></tr>
<tr><td>BOSS</td><td>1. Connect to console serial port:
9600 baud, 8 data bits, 1 stop bit, No parity, No flow control, VT100 or ANSI
2. Type CTRL + y to wake up the port.
3. Enter – by default - No login credentials are needed.

If Password Security is set, default values are:

<table><tr><th>Username</th><th>Password</th><th>Description</th></tr><tr><td>RW</td><td>secure</td><td>read-write-all</td></tr></table></td></tr>
</table>

	RO user read-only **Note** ERS 4800 and earlier models offered two software images—Standard and Secure. • For the standard image, the default password for RO is *user,* and *secure* for RW. • For the secure software image, the default password for RO is *userpasswd,* and *securepasswd* for RW.
Cisco	No login credentials needed. *Switch>enable* *Switch#*

Clearing Switch Configuration

ExtremeXOS	EXAMPLE: *X440-8p# unconfigure switch all* *Restore all factory defaults and reboot? (y/N) Yes*
EOS	EXAMPLE: *C5(su)->clear config all* *This command will reset the entire system and clear its application and stacking configuration.* *Do you want to continue (y/n) [n]?y*
VOSS	EXAMPLE: *VSP4850# Delete config.cfg (then reboot switch) or alternatively,* *EXAMPLE:* *VSP4850# Configure Terminal* *VSP4850#boot config flags factorydefaults* *VSP4850# boot –y (Reboots the switch)* *This flags automatically resets to the default setting after the* *CPU restarts. If you change this flag, you must restart the switch*
BOSS	EXAMPLE: *3626GTS#boot default Reboot the stack/switch and use the factory default configurations* Or *3626GTS# restore factory-default -y*
Cisco	erase startup-config write erase EXAMPLE: *Switch>enable* *Switch#write erase <or erase startup-config>* *Erasing the nvram filesystem will remove all configuration files! Continue? [con firm]* *[OK]* *Erase of nvram: complete*

	Delete the VLAN information from Flash or NVRAM, and reload the switch. *Switch#delete flash:vlan.dat* *Delete filename [vlan.dat]?* *Delete flash:vlan.dat? [confirm]* *Switch#reload* *Proceed with reload? [confirm]* *#After reboot* *Would you like to enter the initial configuration dialog? [yes/no]: no*

Changing Passwords

ExtremeXOS	**configure account** <account-name> **password** EXAMPLE*:* *X440-8p# configure account admin password* *Current user's password: <password>* *New password: <password>* *Reenter password: <password>*
EOS	**set password** <username> EXAMPLE*:* *C5(su)->set password admin* *Please enter new password: <password>* *Please re-enter new password: <password>* *Password Changed.*
VOSS	**cli password** <WORD> <1-20> <level> EXAMPLES*:* In Configure Mode: *cli password WORD<1-20> layer1* *cli password WORD<1-20> layer2* *cli password WORD<1-20> layer3* *cli password WORD<1-20> read-only* *cli password WORD<1-20> read-write* *cli password WORD<1-20> read-write-all*
BOSS	**username** <WORD> <password> {ro | rw}

	EXAMPLE: In Configure Mode: *4826GTS-PWR+(config)#username RO password* - *Enter new password and confirm* *4826GTS-PWR+(config)#username RW password* - *Enter new password and confirm*
Cisco	enable password: **enable password** <password> console and telnet: **password** <password> EXAMPLE: Enable *Switch>enable* *Switch#configure terminal* *Switch(config)# enable password <password>* *Switch#write memory* Console *Switch(config)#line con 0* *Switch(config-line)#password <password>* *Switch(config-line)#login* *Switch(config-line)#end* *Switch#write memory* Telnet *Switch(config)# line vty 0 4* *Switch(config-line)#password <password>* *Switch(config-line)#login* *Switch(config-line)#end* *Switch#write memory*

Recovering Passwords

ExtremeXOS	GTAC Knowledge Home https://gtacknowledge.extremenetworks.com/ Search: ExtremeXOS password recovery.
EOS	GTAC Knowledge Home https://gtacknowledge.extremenetworks.com/ Search: What is the procedure to recover passwords on a SecureStack via the reset button. **set system password-resetbutton** {enable | disable} EXAMPLE:

	set system password-resetbutton enable
VOSS	Password recovery requires the assistance of Technical Support. Open a case at www.support.avaya.com. Support will be migrated to the Extreme Networks support website in calendar year 2018. The password recovery procedure involves a switch reboot.
BOSS	Password Recovery requires the assistance of Technical Support. Open a case at www.support.avaya.com. Support will be migrated to the Extreme Networks support website in calendar year 2018. The password recovery procedure involves a switch reboot.
Cisco	Hold down the green mode button during boot. *switch: flash_init* *switch: load_helper* *switch: rename flash:config.text flash:config.old* *switch: boot* *after the switch boots and you are at the enable prompt, type this:* *switch# rename flash:config.old flash:config.text* *Switch# copy flash:config.text system:running-config*

Recovering Passwords for ExtremeXOS SummitStacks

GTAC Knowledge Home
https://gtacknowledge.extremenetworks.com/

Search: ExtremeXOS password recovery.

If you have lost all admin passwords to the switch, use one of the recovery methods described in in these GTAC Knowledge articles.

- How to default a Summit switch when the password is unknown
- How to Recover an EXOS Switch and its Configuration Without the Password

If the switch is running 21.1 or later, you can use a one-time failsafe password to log in.

https://gtacknowledge.extremenetworks.com/articles/How_To/How-to-access-an-EXOS-switch-using-a-one-time-failsafe-password?q=exos+password+recovery&l=en_US&fs=Search&pn=1

Otherwise, use one of the following methods:

- Method 1: Creating an autoexec script
- Method 2: Transferring the XML config off and modifying it:

Both require the same initial steps.

Initial Steps: Reboot the Switch with a Default Configuration

1. Connect to the switch using a console connection.
2. Turn off, and then turn on the switch.
3. During the boot process press spacebar to enter the bootrom.

   Extreme Networks
   Alternate BootStrap Image
   Starting CRC of Default image
   Using Default image ...

   Extreme Networks

   Default BootLoader Image
   DRAM Post

   Press and hold the spacebar to enter the bootrom.

4. In the bootrom, type the following commands to select a default configuration to be booted:

   config none

   boot

The switch should boot with a factory default configuration. Username = admin, Password = none.

Method 1: Creating an Autoexec Script

1. Enter the vi editor to create an autoexec.xsf file: vi autoexec.xsf.
2. Press the i key to enter insert mode.
3. Type the following line, which creates a new user called "temp" with administrative privileges and a password of "*password*"
4. *create account admin temp password.*
5. Exit insert mode by pressing ESC, and then write the file and exit vi by typing :*wq.*
6. Reboot the switch by typing *reboot*, but do NOT save the configuration. Saving the configuration at this point overwrites the existing configuration with a blank one.
7. When the switch reboots, the autoexec.xsf script is executed, creating the new account.
8. Log in using the new account and make the appropriate changes to the other accounts to allow access. If the password for an account is unknown, the only way to change the password is to delete the account and re-create it.
9. Log out.
10. Ensure that the other accounts can now be used to log into the switch.
11. While logged in using a different account than one created in the script, delete the temp account and the autoexec.xsf script.

    delete account temp

    rm autoexec.xsf

    At this point, the switch should be back to its initial configuration, except for the passwords on the modified accounts.

Method 2: Transferring the XML Configuration and Modifying:

1. Once logged into the switch, configure an IP address on VLAN mgmt and connect a computer with a TFTP server.

   configure vlan mgmt ipaddress <SWITCH_IP>

2. Type *ls* to list files on the switch.
3. Use TFTP to transfer the original configuration file. Typically named "*primary.cfg*":

   tftp put <TFTP_SERVER_IP> primary.cfg

4. Save a new configuration file with the current factory default credentials

   save configuration nopassword

5. Use TFTP to transfer this file:

   tftp put <TFTP_SERVER_IP> nopassword.cfg

6. Use a text editor, such as Notepad++, to replace the password data:

   Primary.cfg:

   <account><name><![CDATA[admin]]></name><password><![CDATA[DlWbeK$OF3c54bLuRbBMtpy19rfP/]]></password><default_val>0</default_val><readwrite>1</readwrite></account>

   Nopassword.cfg:

   <account><name><![CDATA[admin]]></name><password><![CDATA[DlWRiK$y/1Cl8umtCcGlxaRAW8.m/]]></password><default_val>1</default_val><readwrite>1</readwrite></account>

   Primary.cfg:

   <account><name><![CDATA[admin]]></name><password><![CDATA[DlWRiK$y/1Cl8umtCcGlxaRAW8.m/]]></password><default_val>0</default_val><readwrite>1</readwrite></account>

7. Use TFTP to overwrite the configuration on the switch with the password edited version.

   tftp get <TFTP_SERVER_IP> primary.cfg force-overwrite

8. Use the new configuration:

   use configuration primary

   reboot

9. Log in to switch with admin/no password and verify that the expected configuration is present.

10. If not, transfer any other configuration (.cfg) files on the switch and repeat the process.

Note
To prevent losing access in the future, you can create a failsafe account with the command: *configure failsafe-account*.

Recovering EOS SecureStack Passwords

GTAC Knowledge Home

https://gtacknowledge.extremenetworks.com/

Search: What is the procedure to recover passwords on a SecureStack via the reset button.

Environment:

- Securestack
- C5 Series
- B5 Series
- Firmware All Versions

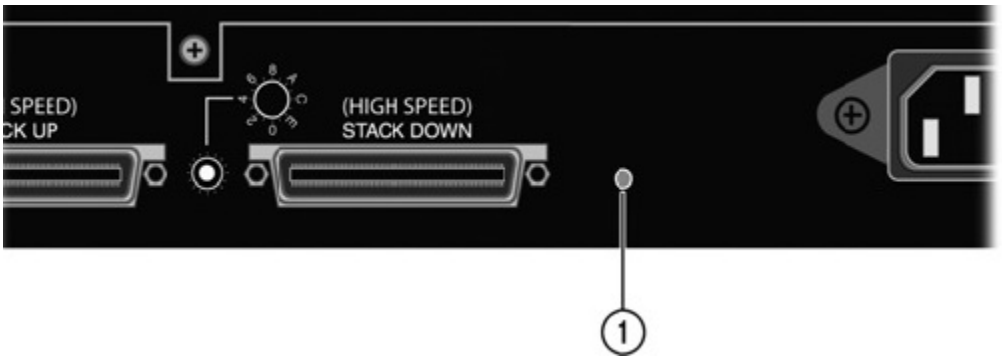


Figure 1. Password Reset Button

1. Connect a local console cable to the switch
2. While the switch is operational, press and hold the password reset button for 6 seconds; release after 6 seconds. This changes the login password to the default password and is indicated in the CLI.
3. Log in to the switch using the default password using the console port and assign a new password using the CLI.

The preceeding steps do not reset the system

Recovering VOSS and BOSS Passwords

Password recovery requires the assistance of Technical Support. Open a case at www.support.avaya.com. Support will be migrated to the Extreme Networks support website in calendar year 2018.

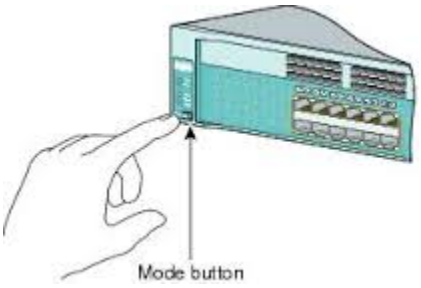
The password recovery procedure requires rebooting the switch.

Recovering Cisco IOS Passwords

Cisco Support Community

https://supportforums.cisco.com/discussion/11375006/3560-password-recovery-enabled-procedures

Hold down the green mode button during the boot process.



switch: flash_init

switch: load_helper

switch: rename flash:config.text flash:config.old

switch: boot

After the switch boots and you are at the enable prompt, type the following:

switch# rename flash:config.old flash:config.text

Switch# copy flash:config.text system:running-config

System Level Commands

Creating User Accounts

ExtremeXOS	**create account** [admin | user] account-name {encrypted password} EXAMPLE: *create account admin bob encrypted Extreme123*
EOS	**set system login** *username* [privilege *level*][enable | disable] **set password** *username* EXAMPLE: C5(su)->set system login bob super-user enable *C5(su)->set password bob* *Please enter new password: Extreme123* *Please re-enter new password: Extreme123* *Password Changed.*
VOSS	*{username} {password} {ro | rw}* EXAMPLE: *VSP4850> enable* *VSP4850# Configure Terminal* *VSP-4850:(config)#Bob Extreme123 rw*
BOSS	**username** <username> <password> {ro | rw} EXAMPLE: *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#username bob rw <enter>* *You are prompted for the password for the user just created* EXAMPLE: *5928GTS-PWR+>enable*

	5928GTS-PWR+#configure terminal *5928GTS-PWR+(config)#username add bob role-name rw password <enter> and confirm password when prompted*
Cisco	username *name* [privilege *level*] {nopassword | password *password* | password encryption-type *encrypted-password*} EXAMPLE*:* *>enable* *#config t* *(config)#username bob privilege 15 password Extreme123* *(config)#end*

Configuring the Switch Prompt

ExtremeXOS	configure snmp sysname *sysName* EXAMPLE*:* *configure snmp sysname switch-01*
EOS	set prompt prompt_string EXAMPLE*:* *C5(su)->set prompt switch-01*
VOSS	prompt *node name* EXAMPLE*:* *VSP4850> enable* *VSP4850# Configure Terminal* *VSP-4850:(config)#prompt switch-01*
BOSS	EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#snmp name Switch44*

	Switch44#(config)#
Cisco	h*ostname* *name* EXAMPLE*:* *Switch>enable* *Switch#config t* *Switch(config)#hostname switch-01* *Switch(config)#end*

Configuring Login Parameters

ExtremeXOS	configure cli max-failed-logins *num-of-logins* EXAMPLE*: configure cli max-login 2* configure cli max-sessions *num-of-sessions* EXAMPLE*: configure cli max-sessions 4* configure idletimeout *minutes* EXAMPLE*:* configure idletimeout 240
EOS	set system login *username* {super-user | read-write | read-only} {enable | disable}[allowed-interval *HH:MM HH:MM*] [allowed-days {[Sun] [Mon] [Tue] [Wed] [Thu] [Fri][Sat]}] [local-only {yes|no}] [aging *days*] [simultaneous-logins *logins*] [password *password*] EXAMPLE*:* *C5(su)->set system lockout attempts 2* set system login *username* {super-user | read-write | read-only} {enable | disable} [simultaneous-logins *logins*] EXAMPLE*:* *C5(su)->set system login admin super-user enable simultaneous-logins 4* set logout *timeout* EXAMPLE*: set logout 240*
VOSS	EXAMPLE*:*

	VSP4850> enable *VSP4850# Configure Terminal* *VSP-4850:(config)#cli timeout <30-65535>* *VSP-4850:(config)#default cli timeout (default is 900 seconds)* *Change the login prompt for CLI:* *VSP-4850:(config)#default login-message (default is "Login")* *VSP-4850:(config)#login-message WORD<1-1513>* *VSP-4850:(config)#no login-message* EXAMPLE*:* *VSP4850> enable* *VSP4850# Configure Terminal* *VSP-4850:(config)#login-message Logon* *Configure the number of supported rlogin sessions.* *VSP-4850:(config)#default max-logins* *VSP-4850:(config)#max-logins <0-8>* *VSP-4850:(config)#Default (The default is)* *VSP-4850:(config)#max-logins 4*
BOSS	EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#cli timestamp enable* *5928GTS-PWR+(config)#cli password serial ?* *local Use local password.* *none Disable password.* *radius Use RADIUS password authentication.*

	tacacs Use TACACS+ AAA services EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#cli password serial local* EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#cli password ?* *change Change radius password* *serial Enable/disable serial port password.* *telnet Enable/disable telnet and web password.*
Cisco	aaa local authentication attempts max-fail *number-of-unsuccessful-attempts* EXAMPLE*:* *Switch>enable* *Switch#config t* *Switch(config)#aaa new-model* *Switch(config)#aaa local authentication attempts max-fail 2(config)#aaa authentication login default local* *Switch(config)#end*

Configuring NTP

ExtremeXOS	configure ntp [server | peer] add [*ip_address* | *host_name*] {key *keyid*} {option[burst | initial-burst]} EXAMPLE*: configure ntp server add 134.20.16.35 Missouri key 5 option initial-burst*
EOS	set sntp server *ip-address* [precedence *precedence*] [key *key-id*] EXAMPLE*:*

	C5(su)->set sntp server 134.20.16.35 precedence 1 key 5
VOSS	*ntp server {A.B.C.D}* *ntp server {A.B.C.D} auth-enable* *ntp server {A.B.C.D} authentication-key <0-2147483647>* *ntp server {A.B.C.D} enable* *ntp server {A.B.C.D} source-ip* EXAMPLE*:* *VSP4850> enable* *VSP4850# Configure Terminal* *VSP-4850:(config)#ntp server 24.56.178.140* *VSP-4850:(config)#ntp server 24.56.178.140 enable*
BOSS	*ntp [authentication-key <1-2147483647> <WORD>] [interval <10-1440>] [server {A.B.C.D}* *{[enable] [auth-enable] [authentication-key <1-2147483647>]}] [sync-now]* *default sntp server primary* *no sntp server primary* *sntp server primary address {A.B.C.D} | [WORD]* EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#sntp server primary address 24.56.178.140* *5928GTS-PWR+(config)#sntp enable* *5928GTS-PWR+(config)#sntp sync-interval 1* *s5928GTS-PWR+(config)#ntp sync-now*
Cisco	ntp [server | peer] *[host_name | ip address] {**key** key_number}* EXAMPLE*:* *Switch>enable*

	#config t *Switch(config)#ntp authenticate* *Switch(config)ntp authentication-key 5 md5 Missouri* *Switch(config)ntp trusted-key 5* *Switch(config)ntp server 134.20.16.35 version 2* *Switch(config)#end*

Configuring SNMP

SNMPv1

ExtremeXOS	**configure snmp add community** [**readonly** | **readwrite**] *alphanumeric_string* [**encrypted** *enc_community_name* | *community name* | **hex** *hex_community_name*] **storeencrypted** EXAMPLE*:* *configure snmp add community readonly public1* *EXAMPLE:configure snmp add community readwrite private1*
EOS	**set snmp group** *groupname* **user** *user* **security-model** {**v1** | **v2c** | **usm**} [**volatile** | **nonvolatile**] EXAMPLE*:* *C5(su)->set snmp group public1 user RO security-model v1* *C5(su)->set snmp group private1 user RW security-model v1* **set snmp community** *community* [**securityname** *securityname*] [**context** *context*] [**transport** *transport*] [**volatile** | **nonvolatile**] EXAMPLE*:* *C5(su)->set snmp community public1 securityname public1* *C5(su)->set snmp community private1 securityname private1* **set snmp access** *groupname* **security-model** {**v1** | **v2c** | **usm**} [**noauthentication** | **authentication** | **privacy**] [**context** *context*] [**exact** | **prefix**] [**read** *read*] [**write** *write*] [**notify** *notify*] [**volatile** | **nonvolatile**] EXAMPLE*:*

	C5(su)->set snmp access public1 security-model v1 read *C5(su)->set snmp access private1 security-model v1 write*
VOSS	Default Pubic/Private community strings are enabled: *snmp-server host WORD<1-256> port <1-65535> v1 WORD<1-32>* EXAMPLE*:* *VSP4850> enable* *VSP4850# Configure Terminal* *VSP-4850:(config)#snmp-server host 10.10.10.10 port 161 v1 PUBLIC* *VSP-4850:(config)#snmp-server community public group readgrp index first secname readview* *VSP-4850:(config)#snmp-server community private group v1v2grp index second secname initialview* EXAMPLE*:* *VSP4850> enable* *VSP4850# Configure Terminal* *To change:* *VSP-4850:(config)#snmp-server community public* *VSP-4850:(config)#snmp-server community private* *VSP-4850:(config)#snmp-server community newpublic group readgrp index first secname readview* *VSP-4850:(config)#snmp-server community newprivate group v1v2grp index second secname* EXAMPLE*:* *VSP-4850:>enable* *VSP-4850:#configure terminal* *VSP-4850:(config)#snmp-server authentication-trap enable* *VSP-4850:(config)#snmp-server contact xxxx@company.com* *VSP-4850:(config)#snmp-server force-iphdr-sender enable*

	VSP-4850:(config)#snmp-server host 45.16.149.128 port 1 v1 SNMPv1 filter SNMPfilterv1
BOSS	EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#snmp-server enable* EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#snmp-server community ro (this changes the read-only string)* *At prompt, enter new RO community string name, and confirm* *5928GTS-PWR+(config)#snmp-server community rw (this changes the read-write string)* *At prompt, enter new RW community string name, and confirm* *5928GTS-PWR+(config)#snmp-server name MDF-SW1 (this changes the system prompt)* *5928GTS-PWR+(config)#snmp-server contact "Joe_Customer"* *5928GTS-PWR+(config)#snmp-server location "Boston"*
Cisco	snmp-server community string [view view-name] {ro | rw} [access-list] snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type] EXAMPLE*:* *Switch>enable* *Switch#config t* *Switch(config)snmp-server community public1 ro* *Switch(config)snmp-server community private1 rw* *Switch(config)snmp-server host 192.168.10.35 version 2c private1* *Switch(config)end*

SNMPv2

ExtremeXOS	**configure snmp add community** [**readonly** | **readwrite**] *alphanumeric_string* [**encrypted** *enc_community_name* | *community name* | **hex** *hex_community_name*] **storeencrypted** EXAMPLE*:* *configure snmp add community readonly public1* EXAMPLE*:* *configure snmp add community readwrite private1*
EOS	**set snmp group** *groupname* **user** *user* **security-model** {**v1** | **v2c** | **usm**} [**volatile** | **nonvolatile**] EXAMPLE*:* *C5(su)->set snmp group public1 user RO security-model v2c* *C5(su)->set snmp group private1 user RW security-model v2c* **set snmp community** *community* [**securityname** *securityname*] [**context** *context*] [**transport** *transport*] [**volatile** | **nonvolatile**] EXAMPLE*:* *C5(su)->set snmp community public1 securityname public1* *C5(su)->set snmp community private1 securityname private1* **set snmp access** *groupname* **security-model** {**v1** | **v2c** | **usm**} [**noauthentication** | **authentication** | **privacy**] [**context** *context*] [**exact** | **prefix**] [**read** *read*] [**write** *write*] [**notify** *notify*] [**volatile** | **nonvolatile**] EXAMPLE*:* *C5(su)->set snmp access public1 security-model v2c read* *C5(su)->set snmp access private1 security-model v2c write*
VOSS	Default Public/Private community strings are enabled: *snmp-server host WORD<1-256> port <1-65535> v1 WORD<1-32>* EXAMPLE*:* *VSP-4850:>enable*

	VSP-4850:#configure terminal *VSP-4850:(config)#snmp-server host 10.10.10.10 port 161 v1 PUBLIC* *VSP-4850:(config)#snmp-server community public group readgrp index first secname readview* *VSP-4850:(config)#snmp-server community private group v1v2grp index second secname initialview* EXAMPLE*:* *VSP-4850:>enable* *VSP-4850:#configure terminal* To change: *VSP-4850:(config)#snmp-server community public* *VSP-4850:(config)#snmp-server community private* *VSP-4850:(config)#snmp-server community newpublic group readgrp index first secname readview* *VSP-4850:(config)#snmp-server community newprivate group v1v2grp index second secname* EXAMPLE*:* *VSP-4850:>enable* *VSP-4850:#configure terminal* *S VSP-4850:(config)#snmp-server authentication-trap enable* *VSP-4850:(config)#snmp-server contact xxxx@company.com* *VSP-4850:(config)#snmp-server force-iphdr-sender enable* *VSP-4850:(config)#snmp-server host 45.16.149.128 port 1 v1 SNMPv1 filter SNMPfilterv1*
BOSS	EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#snmp-server enable* *5928GTS-PWR+(config)#snmp-server community ro (this changes the read-only string)*

	At prompt, enter new RO community string name, and confirm *5928GTS-PWR+(config)#snmp-server community rw (this changes the read-write string)* *At prompt, enter new RW community string name, and confirm* *5928GTS-PWR+(config)#snmp-server name MDF-SW1 (this changes the system prompt)* *5928GTS-PWR+(config)#snmp-server contact "Joe_Customer"* *5928GTS-PWR+(config)#snmp-server location "Boston*
Cisco	snmp-server community string [view view-name] {ro | rw} [access-list] snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type] EXAMPLE*:* *Switch>enable* *Switch#config t* *Switch(config)snmp-server community public1 ro* *Switch(config)snmp-server community private1 rw* *Switch(config)snmp-server host 192.168.10.35 version 2c private1* *Switch(config)end*

SNMPv3

ExtremeXOS	configure snmpv3 add user [hex *hex_user_name* | *user_name*] {engine-id *engine_id*}{ authentication [md5 | sha] [{auth-encrypted} localized-key *auth_localized_key*| {auth-encrypted} hex *hex_auth_password* | *auth_password*] {privacy {des |3des | aes {128 |192 |256}} [{privacy-encrypted} localized-key *priv_localized_key* | {privacy-encrypted} hex *hex_priv_password* | <priv_password>]} } {volatile} EXAMPLE*: conf snmpv3 add user EXTRadmin auth md5 extreme!!! privacy des extreme!!!* configure snmpv3 add group [[hex *hex_group_name*] | *group_name*] user [[hex *hex_user_name*] | *user_name*] {sec-model [snmpv1| snmpv2c | usm]} {volatile} EXAMPLE*:*

	conf snmpv3 add group EXTRgroup user EXTRadmin sec-model usm 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_nam*]] | *notify_view_name*]} {volatile} EXAMPLE: *conf snmpv3 add access EXTRgroup sec-model usm sec-level priv read-view defaultAdminView write-view defaultAdminView notify-view defaultAdminView*
EOS	set snmp group *groupname* user *user* security-model {v1 | v2c | usm} [volatile | nonvolatile] EXAMPLE: *C5(su)->set snmp group EXTRgroup user EXTRadmin security-model usm* set snmp access *groupname* security-model {v1 | v2c | usm} [noauthentication | authentication | privacy] [context *context*] [exact | prefix] [read *read*] [write *write*] [notify *notify*] [volatile | nonvolatile] EXAMPLE: set snmp access *EXTRgroup* security-model usm authentication exact read All write All notify All nonvolatile set snmp user *user* [remote *remoteid*] [encryption {des | aes}] [privacy *privpassword*] [authentication {md5 | sha}] [*authpassword*] [volatile | nonvolatile] EXAMPLE: C5(su)->set snmp user EXTRadmin authentication md5 extreme!!! encryption des privacy extreme!!!
VOSS	*User admin with full access, SHA pass-phrase levelnot, AES pass-phrase secret100* *User operator with read-only access, SHA pass-phrase levelset, AES pass-phrase secret99* *EXAMPLE:* *VSP-4850:>enable* *VSP-4850:#configure terminal*

	VSP-4850:(config)#snmp-server user operator group operators sha levelset aes secret99 *VSP-4850:(config)#snmp-server group operators "" auth-priv read-view root notify-view VSP-4850:(config)#snmp-server user admin group administrators sha levelnot aes secret100* *VSP-4850:(config)#snmp-server group administrators "" auth-priv read-view root write-view root notify-view root*
BOSS	This example creates two user names with read-only and read-write privileges, respectively, and sets a destination for a trap receiver: User names: operator (read-only) and admin (read-write) SHA pass-phrase: levelset and levelnot AES pass-phrase: secret99 and secret 100 view name: root trap destination: 192.168.221.19 EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#snmp-server enable* *5928GTS-PWR+(config)#snmp-server view root 1* *5928GTS-PWR+(config)#snmp-server user operator sha aes read-view root notify-view root* *- prompted for SHA passphrase "levelset" & confirm (no quotes)* *- prompted for AES pass-phrase "secret99" & confirm (no quotes)* *5928GTS-PWR+(config)#snmp-server user admin sha aes read-view root write-view root notify-view root* *- prompted for SHA passphrase "levelnot" & confirm (no quotes)* *- prompted for AES pass-phrase "secret100" & confirm (no quotes)* *5928GTS-PWR+(config)#snmp-server host 192.168.221.19 v3 auth admin*
Cisco	snmp-server group [groupname {v1 | v2c | v3{auth | noauth | priv}}] [read readview] [write writeview] [notify notifyview] [access access-list] EXAMPLE*:*

	Switch>enable *Switch#config t* *Switch(config)snmp-server group EXTRgroup v3 priv match exact read DefaultAdminView write DefaultAdminView notify DefaultAdminView* *(config)end* snmp-server user username [groupname remote ip-address [udp-port port] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password [priv des56 priv password]] [access access-list] EXAMPLE*:* *Switch>enable* *Switch#config t* *Switch(config)snmp-server user EXTRadmin EXTRgroup v3 auth md5 extreme!!!* *Switch(config) end*

Configuring Syslog

ExtremeXOS	configure syslog add [*ipaddress* | *ipPort*] {vr *vr_name*} [local0...local7] EXAMPLE*: configure syslog add 192.168.10.100 vr vr-default local1* 0 Emergency 1 Alert 2 Critical 3 Error 4 Warning 5 Notice 6 Informational 7 Debug
EOS	*s*et logging server *index* [ip-addr *ip-addr*] [facility *facility*] [severity *severity*][descr *descr*] [port *port*] [state {enable | disable}] EXAMPLE*:*

	C5(su)->set logging server 1 ip-addr 192.168.10.100 facility local1 state enable 1 Emergency 2 Alert 3 Critical 4 Error 5 Warning 6 Notice 7 Informational 8 Debug
VOSS	*syslog host <1-10>* *syslog host <1-10> address WORD<0-46>* *syslog host <1-10> enable* *syslog host <1-10> facility { local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 }* *syslog host <1-10> maperror { emergency | alert | critical | error | warning | notice | info | debug }* *syslog host <1-10> mapfatal { emergency | alert | critical | error | warning | notice | info | debug }* *syslog host <1-10> mapinfo { emergency | alert | critical | error | warning | notice | info | debug }* *syslog host <1-10> mapwarning { emergency | alert | critical | error | warning | notice | info | debug }* *syslog host <1-10> secure-forwarding mode none* *syslog host <1-10> secure-forwarding mode tls server-cert-name WORD<1-64>* *syslog host <1-10> severity { info | warning | error | fatal }* *syslog host <1-10> severity { info | warning | error | fatal } { info | warning | error | fatal }* *syslog host <1-10> severity { info | warning | error | fatal } { info | warning | error | fatal } { info | warning |* *error | fatal }*

	syslog host <1-10> severity { info | warning | error | fatal } { info | warning | error | fatal } { info | warning | *error | fatal } { info | warning | error | fatal }* *syslog host <1-10> udp-port <514-530>* *syslog host <1–10> secure-forwarding tcp-port <1025–49151>* EXAMPLE*:* *VSP-4850:>enable* *VSP-4850:#configure terminal* *VSP-4850:(config)#syslog enable* *VSP-4850:(config)#syslog host 1* *VSP-4850:(config)#syslog host 1address 10.10.10.10* *VSP-4850:(config)#syslog host 1enable* *VSP-4850:(config)#syslog host 1facility local7* *VSP-4850:(config)#syslog host1udp-port 514*
BOSS	*logging [disable] [enable] [level] {[critical] [informational] [none] [serious]} [nv-level]* *{[critical] [none] [serious]} [remote] {[address] {[A.B.C.D] [WORD]} [enable] [facility]* *{[daemon] [local0] [local1] [local2] [local3] [local4] [local5] [local6] [local7]} [level]* *{[critical] [informational] [none] [serious]} [secondary-address] {[A.B.C.D] [WORD]}}* *[volatile] {[latch] [overwrite]}* EXAMPLE*:* *5928GTS-PWR+>enable* *5928GTS-PWR+#configure terminal* *5928GTS-PWR+(config)#logging enable level informational* *l5928GTS-PWR+(config)#ogging remote address 10.10.10.10* *5928GTS-PWR+(config)#logging remote enable* *5928GTS-PWR+(config)#logging remote facility local7*

	5928GTS-PWR+(config)#logging remote level informational
Cisco	logging host [*host_name	ip_address]* logging trap [*0-7*] EXAMPLE*:* *Switch>enable* *Switch#config t* *Switch(config)#logging host 192.168.10.100* *Switch(config)#logging facility local1* *Switch(config)#logging trap 1* *Switch(config)#end*

Configuring DHCP Server (*Bootprelay*)

ExtremeXOS	**configure bootprelay add** *ip_address* {**vr** *vrid*} EXAMPLE*:* *configure bootprelay add 192.168.10.100* **configure bootprelay** [{**ipv4**} {**vlan** [*vlan_name*]} [**add** *ip_address* | **delete**[*ip_address*] | **all**]] | **ipv6** {**vlan** [*vlan_name*]} [**add** *ipv6_address* | **delete** [*ipv6_address* | **all**]] {**vr** [*vrid*]} EXAMPLE: configure bootprelay vlan purple add 192.168.10.100 **enable bootprelay** {{**vlan**} [*vlan_name*] | {{**vr**} *vr_name*} | **all** [{**vr**} *vr_name*]} EXAMPLE*:* *enable bootprelay vlan purple*
EOS	**ip helper-address** *address* EXAMPLE*:* *C5(su)->router* *C5(su)->router>enable* *C5(su)->router#configure* *C5(su)->router(Config)#interface vlan 100* *C5(su)->router(Config)#ip ip helper-address 192.168.10.100* *C5(su)->router(Config)#exit*
VOSS	**ip dhcp-relay fwd-path** *dhcp_server_address* EXAMPLE*:* *#configure terminal* *(config)#interface vlan 100* *(config-if)#ip dhcp-relay* *(config-if)#ip dhcp-relay fwd-path 192.168.10.100*
BOSS	**ip dhcp-relay fwd-path** *vlan_ip_address dhcp_server_address* EXAMPLE*:*

	#configure terminal *(config)#ip dhcp-relay fwd-path 192.168.50.1 192.168.10.100* *(config)#interface vlan 100* *(config-if)#ip dhcp-relay*
Cisco	ip helper-address *ip_address* EXAMPLE *>enable* *#config t* *(config)#interface vlan 100* *(config-if)#ip helper-address 192.168.10.100* *(config-if)#end*

Labeling Ports

ExtremeXOS	**configure port**s *port_list* **display-string** *string* EXAMPLE*: configure port 1 display-string Uplink-to-Core*
EOS	**set port alias** *port-string* [*name*] EXAMPLE*:* *C5(su)->set port alias ge.1.1 Uplink-to-Core*
VOSS	**name** *string* EXAMPLE*:* *#configure terminal* *(config)#interface gigabitEthernet 1/1* *(config-if)#name Uplink-to-Core*
BOSS	**name** *string* EXAMPLE*:* *#configure terminal* *(config)#interface ethernet 1/1* *(config-if)#name Uplink-to-Core*
Cisco	**description** *string* EXAMPLE*:* *Switch>enable* *Switch#config t* *Switch(config)#interface GigabitEthernet0/1* *Switch(config-if)#description Uplink-to-Core* *Switch(config-if)#end*

Configuring the Banner

ExtremeXOS	**configure banner** {**after-login** | { **before-login** } { **acknowledge** } | **before-login**{**acknowledge**} **save-to-configuration**}

	EXAMPLE: *configure banner before-login (enter)* *Welcome to Extreme (hit esc key)* EXAMPLE: *configure banner after-login (enter)* *Welcome to Extreme again (hit esc key)*
EOS	**set banner** {**login** | **motd**} EXAMPLE: C5(su)->set banner login “Welcome to Extreme” C5(su)->set banner motd “Welcome to Extreme again”
VOSS	**banner** *"string"* EXAMPLE: *#configure terminal* *(config)#banner custom* *(config)#banner "Welcome to Extreme"* *(config)#banner displaymotd* *(config)#banner motd "Welcome to Extreme again"*
BOSS	**banner <1-19>** "string" EXAMPLE: *#configure terminal* *(config)#banner custom* *(config)#banner 1 "Welcome to Extreme"*
Cisco	**banner motd** [*delimiting_character*] EXAMPLE: *Switch>enable* *Switch#config t* *Switch(config)#banner motd ^C*

	Welcome to Cisco *Switch(config)#end*

Enabling WEB/GUI

ExtremeXOS	**enable web http** **enable web https** (ssh module required) EXAMPLE: *enable web http*
EOS	**set webview** {**enable** [**ssl-only**] | **disable**} EXAMPLE*:* *C5(su)->set webview enable* *C5(su)->set ssl enabled* *C5(su)->set webview enable ssl-only*
VOSS	**web-server enable** (enables HTTPS access) **no web-server secure-only** (enables HTTP access) EXAMPLE: *#configure terminal* *(config)#web-server enable* *(config)#no web-server secure-only*
BOSS	**web-server enable** (enables HTTP access) **ssl** (enables HTTPS access) **https-only** (disables HTTP access) EXAMPLE: *#configure terminal* *(config)#web-server enable* *(config)#ssl* *(config)#https-only*

Cisco	EXAMPLE: *Switch>enable* *Switch#config t* *Switch(config)ip http server* *Switch(config)ip http secure-server* *Switch(config)end*

Configuring Remote Monitoring (RMON)

ExtremeXOS	**enable rmon** EXAMPLE: *enable rmon*
EOS	**set rmon stats** *{index} {port-string}* EXAMPLE: *set rmon stats 2 ge.1.1*
VOSS	**rmon stats** *index port* **owner** *ip-address* EXAMPLE: *#configure terminal* *(config)#rmon stats 1 1/1 owner 10.10.10.50*
BOSS	(RMON statistics are enabled by default)
Cisco	**rmon {native | promiscuous}** EXAMPLE: *Switch>enable* *Switch#config t* *Switch(config)Interface fasteth 0/0* *Switch(config)rmon native* *Switch(config)end*

Configuring Software/Image

Downloading New Images

ExtremeXOS	**download** [**url** url {**vr** vrname} | **image** [**active** | **inactive**] [[hostname | ipaddress] filename {{**vr**} vrname} {**block-size** block_size} | **memorycard** filename] {partition}} EXAMPLE: *download image 192.168.10.75 summitX-16.1.3.6.ExtremeXOS vr vr-default*
EOS	**copy** *source* {*destination* | **system:image**} EXAMPLE: *C5(su)->copy tftp://192.168.10.75/*c5_06.71.03.0007 *system:image*
VOSS	Use an FTP or SFTP client to copy the software image to the switch using the switch management IP address. Put the software image in the "/intflash" directory. If using FTP, make sure the ftp boot config flag is enabled. If using SFTP, make sure the ssh boot config flag is enabled Enable FTP boot config flag: EXAMPLE: *#configure terminal* *(config)#boot config flags ftpd* Enable SSH boot config flag and enable SSH globally EXAMPLE: *#configure terminal* *(config)#boot config flags ssh* *(config)#ssh*
BOSS	**download address** *tftp server address* **diag** *file-name* **no-reset** **download address** *tftp server address* **image** *file-name* EXAMPLE: *#configure terminal* *(config)#download address 192.168.10.75 diag 4000_58003_diag.bin no-reset*

	(config)#download address 192.168.10.75 image 4900_720213s.img
Cisco	**copy [/erase] [/verify | /noverify]** *source-url destination-url* EXAMPLE*:* *Switch>enable* *Switch#copy tftp flash:* *Address or name of remote host []?192.168.10.75* *Source filename []?test.bin* *Destination filename [test.bin]?* *……*

Selecting the Image to Run on the Switch

ExtremeXOS	**use image** {**partition**} *partition* {**slot** *slotid*} EXAMPLE*:* *use image secondary*
EOS	**set boot system** *filename* EXAMPLE: C5(su)->set boot system c5_06.71.03.0007
VOSS	**software add** *software-file-name* (Unpacks the software) **software activate** *software-version* (Copies software to bootflash) **boot -y** (Boot switch to load new software) EXAMPLE*:* *#software add VOSS7K.6.1.0.0.tgz* *#software activate VOSS7K.6.1.0.0.GA* *#boot -y*
BOSS	Download the image to the flash and boot the switch to activate the new image **boot**

	EXAMPLE*:* *#boot*
Cisco	**boot flash** *[flash-fs:][partition-number:][filename]* EXAMPLE*:* *Switch>enable* *Switch# Boot system flash:test.bin*

Managing the Switch Configuration

Saving Configurations

ExtremeXOS	**save configuration** {**primary** | **secondary** | *existing-config* | *new-config*} EXAMPLE*: save configuration (default primary.cfg)* EXAMPLE*: save configuration lab-test (save to lab-test.cfg)* To automatically save configurations periodically: ***save configuration automatic*** *{****every*** *minutes {****primary*** *| ****secondary*** *| existing-config | new-config} | ****never****}*
EOS	Configurations are automatically saved on single switch stacks. To save running configuration to all stack members: **save config** EXAMPLE*:* *C5(su)->save config* To save configuration in local directory: **show config** [**all** | *facility*] [**outfile** {**configs/***filename*}] EXAMPLE*:* *C5(su)->show config outfile configs/current.cfg (current.cfg must be used for the first save)*
VOSS	**save config** (saved to file name "config.cfg) **save config file** *file-name*

	EXAMPLE*:* *#save config* *#save config file lab-test.cfg*
BOSS	"Auto-save" is enabled by default, so running configurations are automatically saved. If "auto-save" is manually disabled, the running configuration must be manually saved. save config EXAMPLE*:* *#save config*
Cisco	copy [/erase] [/verify | /noverify] *source-url destination-url* EXAMPLE*:* *Switch>enable* *Switch#copy running-config startup-config* EXAMPLE*:* *Switch>enable* *Switch#copy running-config lab-test-config*

Booting Configurations

ExtremeXOS	**use configuration** [**primary** | **secondary** | *file_name*] EXAMPLE*: use configuration lab-test*
EOS	**configure** {directory | filename} EXAMPLE*:* *C5(su)->configure configs/lab-test* To append a configuration file to the existing running config without resetting the switch **configure** *directory/filename* **append** EXAMPLE*:* *C5(su)->configure configs/lab-test append*
VOSS	**boot config choice primary config-file file** *file-name* **boot config choice primary backup-config-file** *file-name* EXAMPLE*:* *#configure terminal* *(config)#boot config choice primary config-file lab-test*
BOSS	
Cisco	**copy [/erase] [/verify | /noverify]** *source-url destination-url* EXAMPLE*:* *Switch>enable* *Switch#copy lab-test-config running-config*

Backing Up Configurations

ExtremeXOS	**upload configuration** [*hostname* | *ipaddress*] *filename* {**vr** *vr-name*} EXAMPLE*: upload configuration 192.168.10.75 primary.cfg vr vr-default*
EOS	**copy** *source* {*destination* | filename}

	Options are a local file path in the configs directory, or the URL of a TFTP, SFTP, or SCP server. EXAMPLE: *C5(su)->copy configs/lab-test.cfg tftp://192.168.10.75/lab-test.cfg*
VOSS	The recommended best practice is to backup configurations using sFTP, since it is secure. Connect to the switch using an sFTP client, log in, and then upload the desired configuration file. You can also use FTP or TFTP to back up the configuration. **copy** file-name ip-address:filename EXAMPLE: *#copy config.cfg 134.141.68.198:config.cfg*
BOSS	**copy config tftp address** *ip-address* **filename** *file-name* **copy config sftp address** *ip-address* **filename** *file-name* **username** *username* EXAMPLE: *#copy config tftp address 192.168.10.75 filename lab-test.cfg*
Cisco	**copy system:running-config tftp:** [[[// location] / directory] / filename] **copy nvram:startup-config tftp:** [[[// location] / directory] / filename] **copy flash** [n] **:/ directory /startup-config** **tftp:** [[[// location] / directory] / filename] **copy system:running-config** **ftp:** [[[**//** [*username* [**:** *password*]**@**] *location*] **/** *directory*] **/** *filename*] **copy nvram:startup-config** **ftp:** [[[**//** [*username* [**:** *password*] **@**] *location*] **/** *directory*] **/** *filename*] EXAMPLE: *Switch>enable* *Switch#copy running-config tftp:* Address or name of remote host []? 192.168.10.75 Destination filename [2960]? backup_cfg_for_my_router !!!!!!!!!!!!!!!

Resetting to Factory Default Configuration

ExtremeXOS	unconfigure switch {all} EXAMPLE: *Unconfigure switch all*
EOS	clear config [all] EXAMPLE: *C5(su)->clear config all*
VOSS	boot config flags factorydefaults EXAMPLE: *>enable* *#configure terminal* *(config)#interface (config)#boot config flags factorydefaults* *(config)#save config* *(config)#reset -y*
BOSS	boot default EXAMPLE: *#boot default*
Cisco	erase startup-config write erase *Switch>enable* *Switch#write erase <or erase startup-config>* *Erasing the nvram filesystem will remove all configuration files! Continue? [con firm]* *[OK]* *Erase of nvram: complete* *Delete the VLAN information from Flash or NVRAM, and reload the switch.* *Switch#delete flash:vlan.dat* *Delete filename [vlan.dat]?* *Delete flash:vlan.dat? [confirm]* *Switch#reload*

Layer 1/Physical Commands

Configuring Port Duplex/Speed

ExtremeXOS	configure ports *port_list* {medium [copper | fiber]} auto off speed *speed* duplex [half | full] EXAMPLE*: configure port 1 auto off speed 100 duplex full*
EOS	set port negotiation *port-string* {enable | disable} EXAMPLE*:* *C5(su)->set port negotiation ge.1.1 enable* set port speed *port-string* {10 | 100 | 1000} EXAMPLE*:* *C5(su)->set port speed ge.1.1 100*
VOSS	interface gigabitEthernet *port_list* speed [10 | 100] duplex [full | half] EXAMPLE*:* *>enable* *#configure terminal* *(config)#interface gigabitethernet 1/1* *(config-if)# no auto-negotiate enable* *(config-if)#speed 100* *(config-if)#duplex full*
BOSS	interface ethernet *port_list* speed [10 | 100 | 1000 | 10000 | auto] duplex [auto | full | half] EXAMPLE*:* *>enable* *#configure terminal*

	(config)#interface ethernet 1/1 *(config-if)#speed 100* *(config-if)#duplex full*
Cisco	duplex [auto | full | half] speed [10 | 100 | 1000 | auto] EXAMPLE*:* *Switch>enable* *Switch#config t* *Switch(config)# interface GigabitEthernet0/1* *Switch(config-if)#duplex auto* *Switch(config-if)#speed auto* *Switch(config-if)#end*

Enabling/Disabling Port Configuration

ExtremeXOS	enable port [*port_list* | all] EXAMPLE*: enable port 1* disable port [*port_list* | all] EXAMPLE*: disable port 1*
EOS	set port enable *port-string* EXAMPLE*:* *C5(su)->set port enable ge.1.1* set port disable *port-string* EXAMPLE*:* *C5(su)->set port disable ge.1.1*
VOSS	interface gigabitEthernet *port_list* [shutdown | no shutdown]

	EXAMPLE: *>enable* *#configure terminal* *(config)#interface* *(config)#interface gigabitEthernet 1/1* *(config-if)#no shutdown*
BOSS	interface ethernet *port_list* [shutdown | no shutdown] EXAMPLE: *>enable* *#configure terminal* *(config)#interface* *(config)#interface ethernet 1/1* *(config-if)#no shutdown*
Cisco	no shut EXAMPLE: *Switch>enable* *Switch#configure terminal* *Switch(config)#interface GigabitEthernet0/1* *Switch(config-if)#no shut* *Switch(config-if)#end*

Partitioning Ports

ExtremeXOS	configure ports [*port_list* | all] partition [4x10G | 1x40G] EXAMPLE: *configure ports 49 partition 4x10G*
EOS	set port speed *port-string* {1000 | 10000 | 40000} Applicable to S-series, K-series, and 7100 switches EXAMPLE: *System(su)->set port speed fg.4.1 10000* A reset of the module is necessary for the changes to take affect EXAMPLE: *System(su)->reset system* *This command will reset the system and may disconnect your telnet session.* *Do you want to continue (y/n) [n]? y* *Resetting...* reset nemcpu *mod.nemcpu* Resets the CPU on an option module, where mod specifies the module in which the option module is installed and nemcpu specifies the location of the option module. Currently, this value can only be 1. EXAMPLE: *System(su)->reset nemcpu 4.1* *This command will reset NEM CPU 4.1.* *Do you want to continue (y/n) [n]? y* *Resetting NEM CPU 4.1 ...*
VOSS	interface gigabitEthernet *port_list* [channelize enable | no channelize enable] EXAMPLE: *>enable* *#configure terminal*

	(config)#interface gigabitEthernet 1/1 *(config-if)#channelize enable*
BOSS	N/A
Cisco	interface breakout module *slot* port *port-range* map 10g-4x *Switch>enable* *Switch#configure terminal* *(config)#interface breakout module 1 port 1-12 map 10g-4x* Note: Available on specific models.

Configuring Power over Ethernet (PoE)

ExtremeXOS	disable inline-power ports [all | *port_list*] EXAMPLE*: disable inline-power port 1* EXAMPLE*: enable inline-power port 1*
EOS	set port inlinepower *port-string* {[admin {off | auto}] [priority {critical | high | low}] [type *type*]} EXAMPLE*:* *set inlinepower detectionmode auto* Note: By default auto is enabled on all ports.
VOSS	interface gigabitEthernet *port_list* [poe-shutdown | no poe-shutdown] poe {poe-limit [3-32]} poe {poe-priority [critical | high | low]} EXAMPLE*:* *>enable* *#configure terminal* *(config)#interface gigabitEthernet 1/1*

	(config-if)#poe-shutdown
BOSS	interface ethernet *port_list* [poe-shutdown | no poe-shutdown] poe {poe-limit [3-32]} poe {poe-priority [critical | high | low]} poe {poe-power-up-mode [802.3af | 802.3at | high-inrush | pre-802.3at]} EXAMPLE*:* *>enable* *#configure terminal* *(config)#interface ethernet 1/1* *(config-if)# poe-shutdown*
Cisco	power inline { auto [max *max-wattage*] | never | static [max *max-wattage*]} EXAMPLE*:* Switch>*enable* *Switch#configure terminal* *Switch(config)# interface-range 0/1-0/48* *Switch(config-if)# power inline auto*

Configuring Port Mirroring

Configuring Local Mirrors

ExtremeXOS	create mirror *mirror_name* {to [port *port* | port_list *port_list* loopback-port *port*] { remote-tag *rtag* }} {description *mirror-desc*} EXAMPLE*: create mirror to port 1* configure mirror *mirror_name* add [vlan *name* |port *port* {ingress | egress | ingress-and-egress | anomaly}] EXAMPLE*: configure mirror test add port 2 ingress-and-egress* enable mirror *mirror_name* EXAMPLE*: enable mirror test*
EOS	set port mirroring {create | disable | enable} *source destination*} EXAMPLE*:* *C5(su)->set port mirroring create ge.1.1 ge.1.10* *C5(su)->set port mirroring enable ge.1.1 ge.1.10*
VOSS	mirror-by-port *instance number {1-479}* in-port *port* out-port *port* mode [both | rx | tx] enable EXAMPLE*:* *>enable* *#configure terminal* *(config)# mirror-by-port 1 in-port 1/1 out-port 1/10 mode both enable*
BOSS	port-mirroring *instance number {1-4}* [allow-traffic mode] mode [Adst | Asrc | AsrcBdst | AsrcBdstOrBsrcAdst | AsrcOrAdst | disable | ManytoOneRx | ManytoOneRxTx | ManytoOneTx | Xrx | XrxOrXtx | XrxOrYtx | XrxYtx | XrxYtxOrYrxXtx | Xtx] monitor-port *port* mirror-port-X *port* EXAMPLE*:* *>enable* *#configure terminal* *(config)# port-mirroring 1 mode xrxorxtx monitor-port 1/10 mirror-port-X 1/1*
Cisco	monitor session *session_number* source { interface *interface-id* | vlan *vlan-id } [, | -] [* both / rx / tx *]*

	monitor session *session_number* destination *{* interface *interface-id [, | -] [* encapsulation replicate*]}* EXAMPLE*:* *Switch>enable* *Switch #configure terminal* *Switch (config)monitor session 1 source interface fastEthernet0/1* *Switch (config)monitor session 1 destination interface fastEthernet0/10* *Switch (config)end*

Configuring Remote Mirrors

ExtremeXOS	create mirror *mirror_name* {to [port *port* | port_list *port_list* loopback-port *port*] { remote-tag *rtag* }} {description *mirror-desc*} EXAMPLE*: create mirror to port 1 remote-tag 200* configure mirror *mirror_name* add [vlan *name* |port *port* {ingress | egress | ingress-and-egress | anomaly}] EXAMPLE*: configure mirror test add port 2 ingress-and-egress* enable mirror *mirror_name* EXAMPLE*: enable mirror test*
EOS	Use the set mirror vlan command to assign a VLAN to be reserved for mirroring. If a mirrored VLAN is created, all mirrored traffic egresses VLAN tagged. All traffic on the mirror VLAN is flooded. EXAMPLE*:* *C5(su)->set mirror vlan 2* Alternative: SMON port mirroring support allows you to redirect traffic on ports remotely using SMON MIBs. To configure an SMON MIB port mirror, see the latest Configuration Guide.
VOSS	N/A
BOSS	Not supported on the ERS3600. port-mirroring *instance number {1-4}* [allow-traffic mode] mode [Adst | Asrc | AsrcBdst | AsrcBdstOrBsrcAdst | AsrcOrAdst | disable | ManytoOneRx |

	ManytoOneRxTx | ManytoOneTx | Xrx | XrxOrXtx | XrxOrYtx | XrxYtx | XrxYtxOrYrxXtx | Xtx] monitor-port *port* mirror-port-X *port* rspan-vlan *vlan id* EXAMPLE*:* *(config)# port-mirroring 1 mode xrxorxtx monitor-port 1/24 mirror-port-X 1/2 rspan-vlan 200*
Cisco	remote-span no monitor session { *session_number* | all | local |remote } monitor session *session_number* source {interface *interface-id* | vlan *vlan-id* } *[* , | - *]* *[* both| rx | tx *]* monitor session *session_number* destinationremote vlan *vlan-id* EXAMPLE*:* *Source Switch:* *Switch1# configure terminal* *Switch1(config)# vlan 200* *Switch1(config-vlan)# remote-span* *Switch1(config-vlan)# end* *!* *Switch1# configure terminal* *Switch1(config)# monitor session 1 source interface fastEthernet0/2 rx* *Switch1(config)# monitor session 1 destination remote vlan 200* *reflector-port fastEthernet0/24* *Destination Switch:* *Switch2# configure terminal* *Switch2(config)# vlan 200* *Switch2(config-vlan)# remote-span* *Switch2(config-vlan)# end* *!* *Switch2# configure terminal* *Switch2(config)# monitor session 1 source remote vlan 200*

	Switch2(config)# monitor session 1 destination interface fastEthernet0/3 *Switch2(config)# exit*

Layer 2 Commands

Configuring VLANs

Configuring Port-Based (Untagged)

ExtremeXOS	**create vlan** [vlan_name] **configure** [{**vlan**} *vlan_name* | **vlan** *vlan_list*] add ports [*port_list* | **all**] {**tagged** *tag* | **untagged**} EXAMPLE*:* *#create vlan data_100* *#configure vlan data_100 tag 100* *#configure vlan data_100 add port 1 untagged*
EOS	**set vlan create** *{vid}* **set vlan name** *{vlan-list} {vlan-name}* **set port vlan** *{port-string} {vid}* **modify-egress** EXAMPLE*:* *set vlan create 100* *set vlan name 100 data_100* *set port vlan ge.1.1 100 modify-egress*
VOSS	**vlan create** *{vlan id}* **name** *{name}* **type** [port-mstprstp {instance id} | protocol-mstprstp | {instance id} | pvlan-mstprstp {instance id} | spbm-bvlan **vlan members add** *{vlan id} {port_list}* EXAMPLE*:* *>enable* *#configure terminal* *(config)# vlan create 100 name data type port-mstprstp 0* *(config)# vlan members add 100 1/1*
BOSS	**vlan create** *{vlan id}* **name** *{name}* **type** [port | private-vlan | protocol | spbm-bvlan | spbm-switchedUni | voice-vlan] **vlan members add** *{vlan id} {port_list}*

	EXAMPLE: *>enable* *#configure terminal* *(config)# vlan create 100 name data type port* *(config)# vlan members add 100 1/1*
Cisco	**vlan** *vlan_number* **vlan name** *name* **switchport access vlan** *vlan_number* EXAMPLE: *Switch>enable* *Switch #configure terminal* *Switch (config)#vlan 100* *Switch (config-vlan#name data_100* *Switch (config-vlan)#exit* *Switch (config)#interface gigabitethernet0/1* *Switch (config-if)#switchport access vlan 20* *Switch (config-if)#end*

Configuring Tagged VLANs

ExtremeXOS	**create vlan** [vlan_name] **configure** [{**vlan**} *vlan_name* | **vlan** *vlan_list*] add ports [*port_list* | **all**] {**tagged** *tag* | **untagged**} EXAMPLE: *#create vlan data_100* *#configure vlan data_100 tag 100* *#configure vlan data_100 add port 1 tagged*
EOS	**set vlan create** *{vid}*

	set vlan name *{vlan-list} {vlan-name}* set vlan egress *{vid} {port-string}* tagged EXAMPLE*:* *set vlan create 100* *set vlan name 100 data_100* *set vlan egress 100 ge.1.1 tagged*
VOSS	vlan create *{vlan id}* name *{name}* type [port-mstprstp {instance id} | protocol-mstprstp | {instance id} | pvlan-mstprstp {instance id} | spbm-bvlan vlan members add *{vlan id} {port_list}* interface gigabitEthernet *{port_list}* encapsulation dot1q EXAMPLE*:* *>enable* *#configure terminal* *(config)# vlan create 100 name data type port-mstprstp 0* *(config)# vlan members add 100 1/1* *(config)# interface gigabitEthernet 1/1* *(config-if)# encapsulation dot1q*
BOSS	vlan create *{vlan id}* name *{name}* type [port | private-vlan | protocol | spbm-bvlan | spbm-switchedUni | voice-vlan] vlan members add *{vlan id} {port_list}* vlan ports *{port_list}* tagging tagAll EXAMPLE*:* *>enable* *#configure terminal* *(config)# vlan create 100 name data type port* *(config)# vlan members add 100 1/1*

	(config)#vlan ports 1/1 tagging tagAll
Cisco	vlan *vlan_number* vlan name *name* switchport trunk encapsulation dot1q switchport trunk allowed vlan *vlan_number* EXAMPLE*:* *Switch>enable* *Switch #configure terminal* *Switch (config)#vlan 100* *Switch (config-vlan#name data_100* *Switch (config-vlan)#exit* *Switch (config)#interface gigabitethernet0/1* *Switch (config-if)#switchport trunk encapsulation dot1q* *Switch (config-if)#switchport trunk allowed vlan 100* *Switch (config-if)#end*

Configuring Private VLANs

ExtremeXOS	create private-vlan *name* {vr *vr_name*} configure private-vlan *name* add network *vlan_name* configure private-vlan *name* add subscriber *vlan_name* {non-isolated} {loopback-port *port*} EXAMPLE*:* *create private-vlan companyx* *configure private-vlan companyx add network sharednet* *configure private-vlan companyx add subscriber restricted isolated*
EOS	set vlan name *{vid} {name}* set vlan constraint vlan-id *set-num* [shared | independent] EXAMPLE*:*

	S Chassis(rw)->set vlan name 100 PrimaryVlan *S Chassis(rw)->set vlan name 200 SecondaryVlan* *S Chassis(rw)->set port vlan ge.1.1-2 100* *S Chassis(rw)->set port vlan ge.1.3-4 200* *S Chassis(rw)->set vlan egress 100 ge.1.1-4 untagged* *S Chassis(rw)->set vlan egress 200 ge.1.1-2 untagged* *S Chassis(rw)->set vlan constraint 100 100 shared* *S Chassis(rw)->set vlan constraint 200 100 shared* *S Chassis(rw)->configure* *S Chassis(rw-config)->interface vlan 100* *S Chassis(rw-config-intf-vlan.0.100)->ip address 100.1.1.1/24 primary* *S Chassis(rw-config-intf-vlan.0.100)->secondary-vlan 200*
VOSS	vlan create {vlan id} type pvlan-mstprstp *{instance}* secondary *{secondary-vlan-id}* EXAMPLE*:* *>enable* *#configure terminal* *(config)# vlan create 100 type pvlan-mstprstp 0 secondary 200*
BOSS	vlan create *{vlan id}* type private-vlan secondary *{secondary-vlan-id}* EXAMPLE*:* *>enable* *#configure terminal* *(config)# vlan create 100 type private-vlan secondary 200*
Cisco	feature private-vlan private-vlan { community| isolated | primary } private-vlan association {[add] *secondary-vlan-list* | remove*secondary-vlan-list* } EXAMPLE*:*

	Switch>enable *Switch #configure terminal* *Switch(config)#feature private-vlan* *Switch (config)#vlan 100* *Switch (config-vlan)#private-vlan primary* *Switch (config-vlan)#exit* *Switch (config)#vlan 200* *Switch (config-vlan)#private-vlan community* *Switch (config)#vlan 100* *Switch (config-vlan)#private-vlan association 200* *Switch (config-vlan)#end*

Configuring EAPS

ExtremeXOS	**create eaps** <name> **configure eaps** <name> **mode** [master | transit] **configure eaps** <name> [primary | secondary] **port** <ports> **configure eaps** <name> **add control** {vlan} <vlan_name> **configure eaps** <name> **add protected** {vlan} <vlan_name> **enable eaps** {<name>} EXAMPLE*:* *create vlan EAPS-Control* *configure EAPS-Control tag 20* *configure EAPS-Control add ports 1,2 tagged* *configure EAPS-Control qosprofile QP8* *create vlan purple* *configure purple tag 30* *configure purple add ports 1,2 tagged*

	# Module eaps configuration. *create eaps Domain1* *configure eaps Domain1 mode master* *configure eaps Domain1 primary port 1* *configure eaps Domain1 secondary port 2* *configure eaps Domain1 add control vlan EAPS-Control* *configure eaps Domain1 add protected vlan purple* *enable eaps Domain1* **Note:** transit switch is configured the same except for mode = transit
EOS	*N/A*
VOSS	*N/A*
BOSS	*N/A*
Cisco	*N/A*

Configuring ERPS

ExtremeXOS	**create erps** ring-name **configure erps** ring-name **add control** {**vlan**} vlan_name **configure erps** ring-name **ring-ports [east | west]** port **configure erps** ring-name **protection-port** port **configure erps** ring-name **neighbor-port** port **configure erps** ring-name **add protected {vlan}** vlan_name EXAMPLE: (rpl owner switch) *create vlan "data"* *configure vlan data tag 10* *create vlan "erps1"*

	configure vlan erps1 tag 20 *configure vlan data add ports 1, 2 tagged* *configure vlan erps1 add ports 1, 2 tagged* *#ERPS* *enable erps* *create erps Ring-1* *configure erps Ring-1 add control vlan erps1* *configure erps Ring-1 ring-port east 1* *configure erps Ring-1 ring-port west 2* *configure erps Ring-1 protection-port 2* *enable erps Ring-1* *configure erps Ring-1 add protected vlan data* EXAMPLE*: (RPL neighbor switch)* *Same as above except port connecting to rpl owner would be* *"configure erps Ring-1 neighbor-port 1"* EXAMPLE*: (non-RPL switch)* *Same as above except no protected or neighbor port configured*
EOS	N/A
VOSS	N/A
BOSS	N/A
Cisco	N/A

Configuring LAGs

ExtremeXOS	**enable sharing** *port* **grouping** *port_list* {**algorithm** [**address-based** {**L2** | **L3** | **L3_L4** | **custom}** | **port-based** }]} {resilient-hashing [**on** | **off**]} {distribution-mode [**all** | **local-slot** | **port-lists**]} {lacp | **health-check**} EXAMPLE*:*

	enable sharing 1 grouping 1-2 algorithm address-based L2 lacp
EOS	**set lacp aadminkey** *{lag port} {lag id}* **set port lacp port** *{port-string}* **aadminkey** *{lag id}* **enable** **set lacp singleportlag enable** EXAMPLE*:* *set lacp aadminkey lag.0.1 100* *set port lacp port ge.1.1 aadminkey 100 enable* *set lacp singleportlag enable*
VOSS	[**no**] **mlt** <1-512> **mlt** <1-512> **vlan** <1-4059> **mlt** <1-512> **encapsulation dot1q** **show mlt** <1–512> Optional: **mlt** <1-512> **private-vlan** <isolated|promiscuous|trunk> **mlt** <1-512> **name** WORD<0-20> EXAMPLE*:* *Switch:1>enable* *Switch:1#config t* *Switch:1(config)# mlt 10* *Switch:1(config)#mlt 10 private-vlan isolated* *Switch:1(config)#mlt 10 encapsulation dot1q* *Switch:1(config)# mlt 10 vlan 20* *Switch:1(config)# mlt 10 enable*
BOSS	[**no**] **mlt** <1-32> [**name** TRUNKNAME<0-16>] [**enable** | **disable**] [**member** <portlist>] [**learning** {**disable** | **fast** | **normal**}] [**bpdu** {**all-ports** | **single-port**}] [**loadbalance** <**advance**|**basic**> Optionally, set the private VLAN type for the MLT:

	mlt <id> **private-vlan** <**isolated**|**promiscuous**|**trunk**> EXAMPLE*:* *Switch >enable* *Switch #config t* *Switch (config) # mlt 10 enable member 1/23,2/23*
Cisco	**channel-group** *channel* -group-number **mode { auto [non-silent] | desirable [non-silent] | on } | { active | passive } *** *LACP is used for this example for a single switch* EXAMPLE*:* *>enable* *# config t* *(config)# interface range gigabitethernet0/12-14* *(config-if-range)# switchport access vlan 10* *(config-if-range)# channel-group 3 mode active* *(config-if-range# end*

Configuring MLAGs

ExtremeXOS	**create mlag peer** peer_name { authentication [**md5 key** [**encrypted** encrypted_auth_key | auth_key]] } **configure mlag peer** peer_name **ipaddress** peer_ip_address {vr VR} **enable mlag port** port **peer** peer_name id identifier EXAMPLE*:* *(X440-SW1)* ISC Link Configuration. Port connecting MLAG peers. *create vlan ISC* *configure VLAN ISC tag 100* *configure ISC add port 24 tagged* *configure VLAN ISC ipaddress 10.10.10.1/24*

	MLAG Configuration *create mlag peer 440-SW2* *configure mlag peer 440-SW2 ipaddress 10.1.1.2* *enable mlag port 1 peer 440-SW2 id 1* *(X440-SW2)* ISC Link Configuration. Port connecting MLAG peers *create vlan ISC* *configure VLAN ISC tag 100* *configure ISC add port 24 tagged* *configure VLAN ISC ipaddress 10.10.10.2/24* MLAG Configuration *create mlag peer 440-SW1* *configure mlag peer 440-SW1 ipaddress 10.1.1.1* *enable mlag port 1 peer 440-SW id 1*
EOS	N/A
VOSS	Non-SPB Option for Split Multi-link Trunking utilizing Simplified vIST: When you enable Simplified vIST with the **virtual-ist enable** command, two VLANs are automatically created to support vIST. The VLAN IDs are: 4086 and 4087. SPBM must not be enabled on the vIST peers or any router that participates in the network. The following requires a switch reboot: **no boot config flags spbm-config-mode** Create the vIST: **vlan create** <2-4059> **type port-mstprstp** <0–63> **interface vlan** <1-4059> **ip address** <A.B.C.D/X> **virtual-ist peer-ip** <A.B.C.D> **vlan** <1-4059> **mlt** <1-512> **enable**

	mlt <1-512> member {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} mlt <1-512> encapsulation dot1q interface mlt <1-512> virtual-ist enable *Create the Split Multi Link Trunk:* mlt <1-512> enable mlt <1-512> member {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]} interface mlt <1-512> smlt *Assign customer VLAN to SMLT:* vlan create <2-4059> vlan mlt <vlan-id> <mlt-id> EXAMPLE*:* *Switch:1>enable* *Switch:1#configure terminal* *Switch:1(config)#no boot config flags spbm-config-mode* Save the configuration and reboot the switch. *Switch:1>enable* *Switch:1#configure terminal* *Switch:1(config)#virtual-ist peer-ip 50.1.1.14 vlan 50* *Switch:1(config)#mlt 3 enable* *Switch:1(config)#mlt 3 member 1/35,1/36* *Switch:1(config)#interface mlt 3* *Switch:1(config-if)#smlt* *Switch:1(config-if)#exit*

	Switch:1(config)#mlt 5 enable *Switch:1(config)#mlt 5 member 2/15,2/17* *Switch:1(config)#mlt 5 encapsulation dot1q* *Switch:1(config)#interface mlt 5* *Switch:1(config-if)#virtual-ist enable* *Switch:1(config-if)#exit* *Switch:1(config)#vlan create 50 type port-mstprstp 0* *Switch:1(config)#interface vlan 50* *Switch:1(config-if)#ip address 50.1.1.15 255.255.255.0 1* *Switch:1(config-if)#exit* *Switch:1(config)#vlan create 100* *Switch:1(config)#vlan mlt 100 3* *Switch:1(config)#interface vlan 100* *Switch:1(config-if)#ip address 100.1.1.15 255.255.255.0 2* *Switch:1(config-if)#exit*
BOSS	N/A
Cisco	*Cisco's implementation of MLAG uses vPC with limited model support to Nexus switching.*

Configuring LLDP

ExtremeXOS	**enable lldp ports** *[all | port_list] {receive-only | transmit-only}* EXAMPLE*: (most common options)* *configure lldp port all advertise system-name* *configure lldp port all advertise vendor-specific dot3 mac-phy* *configure lldp port all advertise vendor-specific med capabilities* *configure lldp port all advertise vendor-specific med power-via-mdi* *configure lldp port all advertise vendor-specific med policy application voice vlan <Vlan name> dscp 46*
EOS	**set lldp port status {tx-enable | rx-enable | both | disable}** {*port-string}* **set lldp port tx-tlv {[all] | [port-desc] [sys-name] [sys-desc] [sys-cap] [mgmt-addr] [vlan-id] [stp] [lacp] [gvrp] [mac-phy] [poe] [link-aggr] [max-frame] [med-cap] [med-pol] [med-loc] [med-poe] [enhanced-trans-config] [enhanced-trans-rec] [priority-flowctrl]}** *{port-string}* **set lldp port network-policy {all | voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} [state {enable | disable}] [tag {tagged | untagged}] [vid {vlan-id | dot1p}] [cos cos-value] [dscp dscp-value]** *{port-string}* EXAMPLE*:* *set lldp port status both ge.1.1* *set lldp port status both *.*.** **all port enabled*
VOSS	Transmission Parameters: [**default**] **lldp** [**tx-interval** <5–32768>|**tx-hold-multiplier** <2–10>] Port Parameters: [**default**|**no**] **lldp** [**port** {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]**status txAndrx** EXAMPLE*:* *Switch:1>enable* *Switch:1#configure terminal*

	Switch:1(config)#interface GigabitEthernet 1/23 *Switch:1(config-if)#lldp status txAndrx* *Switch:1(config-if)#exit* *Switch:1(config)#lldp tx-interval 31*
BOSS	Transmission Parameters: [**default**|**no**] **lldp** [**tx-interval** <5-32768>] [**tx-hold-multiplier** <2-10>] [**reinitdelay** <1-10>] [**tx-delay** <1-8192>] [**notification-interval** <5-3600>] [**med-fast-start** <1-10>] [**vendor-specific avaya** {**call-server** | **fileserver**}] Port Parameters: [**default**|**no**] **lldp port** <portlist> [**status** {**rxOnly** | **txAndRx** | **txOnly**}] [**config notification**] MED Policies: [**default**|**no**] **lldp med-network-policies** [**port** <portList>] {**voice**|**voice-signaling**} [**dscp** <0-63>] [**priority** <0-7>] [**tagging** {**tagged**|**untagged**}] [**vlan-id** <0-4094>] EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#default lldp* *Switch(config)#interface ethernet 1/23* *Switch(config-if)#lldp status txOnly* *Switch(config-if)#lldp med-network-polices voice dscp 46* *Switch(config-if)#exit*
Cisco	Global enable/disable **lldp run / no lldp run** (respectively) Interface enable/disable **lldp receive, lldp transmit / no lldp receive , no lldp transmit** (respectively) EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#lldp run*

Configuring CDP

ExtremeXOS	**enable cdp ports** [*port_list* | **all**] **disable cdp ports** *[port_list* | **all**] EXAMPLE*:* *enable cdp ports all* *disable cdp ports all*
EOS	**set ciscodp status {auto | enable | disable}** **set ciscodp port { [status {disable | enable}] [vvid { | none | dot1p | untagged}] [trust-ext {trusted | untrusted}] [cos-ext value] }** *{port-string}* EXAMPLE*:* *set ciscodp status enable* *set ciscodp port enable ge.1.1*
VOSS	[**no**] **lldp cdp enable** EXAMPLE*:* *Switch:1>enable* *Switch:1#configure terminal* *Switch:1(config)#interface GigabitEthernet 1/23* *Switch:1(config-if)#lldp cdp enable*
BOSS	N/A
Cisco	Global enable/disable **cdp run / no cdp run** (respectively) Interface enable/disable **cdp enable / no cdp enable** (respectively) EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#cdp run*

Configuring Spanning Tree

Configuring Spanning Tree Protocol (STP)

ExtremeXOS	**configure stpd** stpd_name **add** vlan vlan_name **ports** [all | port_list] {[dot1d |emistp | pvst-plus]} EXAMPLE*:* *configure stpd s0 add vlan purple ports 1-2 dot1d* *enable stpd s0*
EOS	**set spantree version {stp | mstp | stpcompatible | rstp}** EXAMPLE*:* *set spantree version rstp*
VOSS	Set STP Type (default is MSTP): **boot config flags spanning-tree-mode** {**rstp**|**mstp**} [**default**] **spanning-tree mstp** [**forward-time** <400-3000>] [**max-age** <600-4000>] [**max-hop** <100-4000>] [**pathcost-type** {**bits16**|**bits32**}] [**priority** <0-61440>] [**tx-holdcount** <1-10>] [**version** {**mstp**|**rstp**|**stp-compatible**}] [**msti** <1-63> **priority** <0-65535>] [**region config-id-sel** <0-255> **region-name** WORD<1-32> **region-version** <0-65535>] Configure Ethernet MSTP: [**default**|**no**] **spanning-tree mstp** [**cost** <1–200000000>] [**edge-port** <**false**|**true**>] [**force-port-state enable**] [**hello-time** <100–1000>] [**msti** <1–63>] [**p2p** {**auto**|**force-false**|**force-true**}] [**port** {slot/port[/sub-port]}] [**priority** <0–240>] [**protocol-migration** <**false**|**true**>] EXAMPLE*:* *Switch:1>enable* *Switch:1#configure terminal* *Switch:1(config)#spanning-tree mstp forward-time 500 max-age 3000 max-hop 200 pathcost-type bits32 priority 8192 tx-holdcount 10 version mstp* *Switch:1(config)# spanning-tree mstp msti 62 priority 4096* *Switch:1(config)# spanning-tree mstp cost 1 edge-port true force-portstate enable hello-time 100 p2p auto priority 2 protocol-migration true* *Switch:1(config)#interface GigabitEthernet 1/23* *Switch:1(config-if)#no spanning-tree mstp force-port-state enable*

	Switch:1(config-if)#exit
BOSS	Set STP Type (default is MSTP)(STPG is Avaya MSTP): **spanning-tree mode** {**mst** | **rstp** | **stpg**} [**default**] **spanning-tree MSTP** [**max-hop** <100 - 4000>][**forward-time** <4 - 30>] [**max-age** <6 - 40>][**pathcost-type** {**bits16** | **bits32**}] [**priority** {0000 | 1000 | 2000 | ... | F000}] [**tx-holdcount** <1 - 10>] [**version** {**stpcompatible** | **rstp**| **MSTP**}] [**add-vlan** <1 - 4094>] [**remove-vlan** <1 - 4094>] Configure Ethernet MSTP: [**default**] **spanning-tree MSTP** [**port** <portlist>] [**cost** <1 - 200000000>][**edgeport** {**false** | **true**}][**hello-time** <1 - 10>] [**learning** {**disable** | **enable**}][**p2p** {**auto** | **force-false** | **force-true**}][**priority** {00 | 10 | < | F0}] [**protocol-migration** {**false** | **true**}] [**instance-specific** <1-7>] EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#interface ethernet ALL* *Switch(config-if)# spanning-tree mstp port 1/1-49 learning enable* *Switch(config-if)# spanning-tree mstp port 1/50 learning disable* *Switch(config-if)#exit*
Cisco	**spanning-tree mode {pvst | mst | rapid-pvst}** EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#spanning-tree mode rapid-pvst*

Configuring Per-VLAN Spanning Tree Protocol (PVSTP)

ExtremeXOS	**configure stpd** stpd_name **add** vlan vlan_name **ports** [all | port_list] {[dot1d |emistp | pvst-plus]}
EOS	N/A. MSTP is standard for per-VLAN STP.

VOSS	N/A. MSTP is standard for per-VLAN STP.
BOSS	N/A. MSTP is standard for per-VLAN STP.
Cisco	**spanning-tree mode {pvst | mst | rapid-pvst}** EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#spanning-tree* mode pvst

Configuring Rapid Spanning Tree Protocol (RSTP)

ExtremeXOS	**configure stpd** stpd_name **add** vlan vlan_name **ports** [all | port_list] {[dot1d |emistp | pvst-plus]} EXAMPLE*:* *configure stpd s0 mode dot1w* *configure stpd s0 add vlan purple ports 1-2 dot1d* *enable stpd s0*
EOS	**set spantree version {stp | mstp | stpcompatible | rstp}** EXAMPLE*:* *set spantree version rstp*
VOSS	Set STP Type (default is MSTP): **boot config flags spanning-tree-mode** {rstp|mstp} [**default**|**no**] **spanning-tree rstp** [**forward-time** <400–3000>] [**group-stp enable**] [**hello-time** <100–1000>] [**max-age** <600–4000>] [**pathcost-type** <**bits16**|**bits32**>] [**priority** <0–61440>] [**tx-holdcount** <1–10>] [**version** <**rstp**|**stp-compatible**>] Configure Ethernet RSTP: [**default**|**no**] **spanning-tree rstp cost** <1–200000000> **edge-port** <**false**|**true**> **p2p** <**auto**|**force-false**|**force-true**> **priority** <0–240> **protocol-migration** <**false**|**true**> **stp enable** EXAMPLE*:*

	Switch:1>enable *Switch:1#configure terminal* *Switch:1(config)# spanning-tree rstp forward-time 1000 hello-time 200 maxage 4000 pathcost-type bits16 priority 4096 tx-holdcount 10 version rstp group-stp enable* *Switch:1(config)# interface gigabitEthernet 1/23* *Switch:1(config-if)# spanning-tree rstp cost 100 edge-port true p2p auto* *priority 32 protocol-migration true stp enable*
BOSS	Set STP Type (default is MSTP)(STPG is Avaya MSTP): **spanning-tree mode** {**mst** | **rstp** | **stpg**} [**default**] **spanning-tree rstp** [**forward-time** <4 - 30>] [**hello-time** <1 - 10>] [**max-age** <6 - 40>] [**pathcost-type** {**bits16** | **bits32**}] [**priority** {0000|1000|2000| ...| F000}] [**tx-holdcount** <1 - 10>] [**version** {**stpcompatible** | **rstp**}] Configure Ethernet RSTP: [**default**] **spanning-tree rstp** [**port** <portlist>] [**cost** <1 - 200000000>][**edgeport** {**false** | **true**}] [**learning** {**disable** | **enable**}] [**p2p** {**auto** | **force-false** | **force-true**}] [**priority** {00 | 10 | ... | F0}] [**protocol-migration** {**false** | **true**}] EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#interface ethernet ALL* *Switch(config-if)# spanning-tree rstp port 1/1-49 learning enable* *Switch(config-if)# spanning-tree rstp port 1/50 learning disable* *Switch(config-if)#exit*
Cisco	**spanning-tree mode {pvst | mst | rapid-pvst}** EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#spanning-tree mode rapid-pvst*

Configuring Multiple Spanning Tree Protocol (MSTP)

ExtremeXOS	**configure mstp region** regionName **configure stpd** stpd_name **mode** [dot1d | dot1w | mstp [cist | msti instance]] **configure stpd** stpd_name **priority** priority **enable stpd** stpd_name **auto-bind** vlan vlan_name EXAMPLE*:* *configure mstp region Test* *configure stpd s0 mode mstp cist* *configure stpd s0 priority 4096* *enable stpd s0 auto-bind vlan purple* *enable stpd s0*
EOS	**set spantree version {stp | mstp | stpcompatible | rstp}** EXAMPLE*:* *set spantree version mstp*
VOSS	Set STP Type (default is MSTP): **boot config flags spanning-tree-mode** {rstp|mstp} [**default**|**no**] **spanning-tree rstp** [**forward-time** <400–3000>] [**group-stp enable**] [**hello-time** <100–1000>] [**max-age** <600–4000>] [**pathcost-type** <**bits16**|**bits32**>] [**priority** <0–61440>] [**tx-holdcount** <1–10>] [**version** <**rstp**|**stp-compatible**>] Configure Ethernet RSTP: [**default**|**no**] **spanning-tree rstp cost** <1–200000000> **edge-port** <**false**|**true**> **p2p** <**auto**|**force-false**|**force-true**> **priority** <0–240> **protocol-migration** <**false**|**true**> **stp enable** EXAMPLE*:* *Switch:1>enable* *Switch:1#configure terminal*

	Switch:1(config)# spanning-tree rstp forward-time 1000 hello-time 200 maxage 4000 pathcost-type bits16 priority 4096 tx-holdcount 10 version rstp group-stp enable *Switch:1(config)# interface gigabitEthernet 1/23* *Switch:1(config-if)# spanning-tree rstp cost 100 edge-port true p2p auto* *priority 32 protocol-migration true stp enable*
BOSS	Set STP Type (default is MSTP)(STPG is Avaya MSTP): **spanning-tree mode** {**mst** | **rstp** | **stpg**} [**default**] **spanning-tree rstp** [**forward-time** <4 - 30>] [**hello-time** <1 - 10>] [**max-age** <6 - 40>] [**pathcost-type** {**bits16** | **bits32**}] [**priority** {0000|1000|2000| ...| F000}] [**tx-holdcount** <1 - 10>] [**version** {**stpcompatible** | **rstp**}] Configure Ethernet RSTP: [**default**] **spanning-tree rstp** [**port** <portlist>] [**cost** <1 - 200000000>][**edgeport** {**false** | **true**}] [**learning** {**disable** | **enable**}] [**p2p** {**auto** | **force-false** | **force-true**}] [**priority** {00 | 10 | ... | F0}] [**protocol-migration** {**false** | **true**}] EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#interface ethernet ALL* *Switch(config-if)# spanning-tree rstp port 1/1-49 learning enable* *Switch(config-if)# spanning-tree rstp port 1/50 learning disable* *Switch(config-if)#exit*
Cisco	**spanning-tree mode {pvst | mst | rapid-pvst}** EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#spanning-tree mode mst (mst is not compatible with mstp)*

Preventing Loops (Non-STP)

ExtremeXOS	**ELRP** **configure elrp-client periodic** *vlan_name* **ports** [*ports* | **all**] **interval** *sec* [**log** | **log-and-trap** | **trap**] {**disable-port** {**egress** | **ingress**} {**duration** {*seconds* } | **permanent** }} **configure elrp-client disable-ports** [**exclude** | **include**] [*ports* | **eapsring-ports**] **enable elrp-client** EXAMPLE*:* *configure elrp-client periodic marketing ports 3:2 interval 2 log disable-port duration 5* *configure elrp-client disable-ports exclude 2:1,2:3* *enable elrp-client*
EOS	N/A
VOSS	Uses SLPP (Simple Loop Prevention Protocol) **slpp port** {slot/port[/sub-port][-slot/port[/sub-port]][,...]}**packet-rx** [**packet-rx-threshold** <1-500>] **slpp enable** **slpp tx-interval** <500–5000> **slpp vid** <1-4059> EXAMPLE*:* *Switch:1>enable* *Switch:1#configure terminal* *Switch:1(config)# interface gigabitEthernet 1/23* *Switch:1(config-if)# slpp pack-rx-threshold 10* *Switch:1(config-if)# exit* *Switch:1(config)# interface vlan 2* *Switch:1(config-if)# slpp vid 2*

	Switch:1(config-if)# slpp enable *Switch:1(config-if)# exit*
BOSS	Uses SLPP (Simple Loop Prevention Protocol) Guard [**default** | **no**] **slpp-guard** [**port** <portlist>][**enable**][**timeout** {0| <10-65535>}] EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)# slpp-guard port 1/1-24 enable timeout 0* **Note**: SLPP packets are generated only on switches that are configured with SLPP, for example, ERS 5000 Series or ERS 8800. The switch does not support SLPP. When you enable SLPP Guard on the switch, it must be connected to another Avaya switch that supports SLPP, and SLPP must be enabled on that switch.
Cisco	N/A

Configuring Layer 2 Quality of Service (QoS)

ExtremeXOS	**create qosprofile** [QP2| QP3 | QP4 | QP5 | QP6 | QP7] **configure** vlan vlan_name {qosprofile} qosprofile **configure dot1p type** dot1p_priority {**qosprofile**} qosprofile **enable dot1p examination ports** [port_list | **all**] VLAN EXAMPLE: *Create vlan purple* *Create qosprofile qp5* *Configure vlan purple qosprofile qp5* 802.1p EXAMPLE: *Create qosprofile qp5* *Enable dot1p examination ports all (on by default)* *Configure dot1p type 4 qp5 (COS of 4 put into QP5)*

EOS	**set vlan create** *{vid}* **set vlan name** *{vlan-list} {vlan-name}* **set policy profile** {*profile-index}* [**name** *name*] [**pvid-status** {**enable** | **disable**}][*pvid* **pvid**] [**cos-status** {**enable** | **disable**}] [**cos** *cos*] [**egress-vlans** *egress-vlans*][**forbidden-vlans** *forbidden-vlans*] [**untagged-vlans** *untagged-vlans*][**precedence** *precedence-list*] [**append**] [**clear**] EXAMPLE*:* *Create your VLAN:* *set vlan create 7* *set vlan name 7 purple* Configure your purple policy profile for tagged frames: *set policy profile 1 name "purple" pvid-status enable pvid 7 cos-status enable cos 4 tagged-vlans 7* Create your CoS to TOS mappings: *set cos state enable* *set cos settings 4 tos-value 184* The CoS setting for CoS-4 applying DSCP value of EF to purple traffic.
VOSS	QoS by default is enabled on all NNI interfaces. Depending on the switch, QoS may still have to be enabled on the UNI interface, or filters must be used to provide end-to-end QoS. On the VSP 4000, VSP 8000, VSP 7200, and VSP 9000, the interface level parameters “802.1p-override disable”, “enable-diffserv enable”, and “no access-diffserv enable” are the default settings. On an UNI interface, this has the overall result of honoring p-bits for bridge traffic and DSCP values for routed traffic.
BOSS	By default, the QoS queues configured on the ERS platform is Queue Set 2 (2 queues). To map the queues one for one, set the Queue Set to 8 (8 queues): [**default**] **qos agent queue-set** <1-8> [**no**] **qos if-group name** <WORD> **class** {**trusted** | **untrusted** | **unrestricted** | **untrustedbasic** | **untrustedv4v6**} EXAMPLE*:* *Switch>enable* *Switch#configure terminal*

	Switch(config)# qos agent queue-set 8 *(requires reboot to take affect)* *Switch(config)# qos if-group name Voice class trusted* *Switch(config)# interface FastEthernet ALL* *Switch(config-if)# qos if-assign port all name Voice* *Switch(config-if)# exit*
Cisco	**mls qos trust** [**cos**| **dscp** | **ip-precedence**] **mls qos cos** {*default-cos* |**override** } EXAMPLE*:* *>enable* *Switch#configure terminal* *Switch(config)#mls-qos* *Switch(config)#interface fastethernet0/1* *Switch(config-if)#mls-qos trust cos* *Switch(config-if)#exit* *Switch(config)#mls-qos map cos-dscp 0 8 16 24 32 46 48 56*

Configuring Jumbo Frames

ExtremeXOS	**enable jumbo-frame ports** [**all** | *port_list*] **configure jumbo-frame-size** *framesize* **disable jumbo-frame ports** [**all** | *port_list*] EXAMPLE*:* *enable jumbo-frame ports all* *configure jumbo-frame-size 9216* *disable jumbo-frame ports all*
EOS	**set port jumbo {enable | disable}***[port-string]* EXAMPLE*:* *set port jumbo enable ge.1.1*

	There is no option to set the frame size - Max Frame Size: 9216
VOSS	sys mtu <1950|1522|9600> EXAMPLE*:* *Switch:1> enable* *Switch:1# configure terminal* *Switch:1#(config)# sys mtu 9600*
BOSS	[default | no] jumbo-frames [enable] [size <1519-9216>] EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)# jumbo-frames*
Cisco	system mtu jumbo *jumbo mtu size in bytes* EXAMPLE*:* *Switch#config t* *Switch(config)# system mtu jumbo 9216* *Switch(config)# end*

Configuring Layer 2 Security

Configuring MAC Locking

ExtremeXOS	configure ports port_list {tagged tag} vlan vlan_name [limit-learning number {action [blackhole | stop-learning]} | lock-learning | unlimited-learning | unlock-learning] EXAMPLES*:* *configure port 1 vlan "purple" lock-learning* *configure port 1 vlan "purple" learn-limit 1*
EOS	set maclock [enable | disable] *{port-string}* set maclock *{mac-address} {port-string}* [create | enable | disable]

	set maclock static *{port-string} {value. Value specifies the maximum number of static MAC addresses allowed per port. Valid values are 0 to 20.* **set maclock firstarrival** *{port-string} {value}. Value specifies the number of first arrival end station MAC addresses to be allowed connections to the port. Valid values are 0 to 600.* **set maclock agefirstarrival** *{port-string}* **[enable | disable]** *When enabled, first arrival MAC addresses that are aged out of the forwarding database will be removed from the associated port MAC lock.* EXAMPLE*:* *set maclock enable ge.1.1* *set maclock 0e-03-ef-d8-44-55 ge.1.2 create* *set maclock static ge.1.3 2* *set maclock firstarrival ge.1.4 6* *set maclock agefirstarrival ge.1.4 enable*
VOSS	[**default** | **no**] **mac-security limit-learning enable** [**default** | **no**] **mac-security limit-learning max-addrs** <1-32000> [**default** | **no**] **mac-security port** {slot/port[/sub-port][-slot/port[/sub-port]][,...]} **limit-learning enable** [**default** | **no**] **mac-security port** {slot/port[/sub-port][-slot/port[/sub-port]][,...]} **limit-learning maxaddrs** <1-32000> EXAMPLE*:* *Switch:1>enable* *Switch:1#configure terminal* *Switch:1(config)# interface gigabitEthernet 1/23* *Switch:1(config-if)# mac-security limit-learning enable* *Switch:1(config-if)# mac-security limit-learning max-addrs 1* *Switch:1(config-if)# exit*
BOSS	[**default** | **no**] **mac-security** [**auto-learning**]{[**aging-time** <0-65535>] | [**sticky**]} [**mac-address-table**] {[**address** <H.H.H>] {[**mlt-id** <1-32>] | [**port** <LINE>] | [**security-list** <1-128>]} | {[**stickyaddress** <H.H.H>] {[**mlt-id** <1-32>] | [**port** <LINE>]}}} [**mac-da-filter**] {[**add** <H.H.H>] | [**delete** <H.H.H>] | <H.H.H>]} [**disable**] [**enable**] [**intrusion-detect**] {[**disable**] | [**enable**] | [**forever**]}

	[intrusion-timer <0-65535>] [filtering] {[disable] | [enable]} [learning] {[disable] | [enable]} [learning-ports] {[add <LINE>] | [LINE] | [remove <LINE>]} [securitylist] [<1-128>] {[add <LINE>] | <LINE> | [remove <LINE>]} [snmp-lock] { [disable] | [enable]} EXAMPLE: *Switch(config)#mac-security auto-learning sticky* *Avaya recommends disabling autosave when sticky mac is enabled* *Switch(config)#mac-security enable* *Switch(config)#no autosave enable* *Switch(config)#copy config nvram* *Switch(config)#interface Ethernet 1/6-14* *Switch(config-if)#mac-security auto-learning enable* *Switch(config-if)#mac-security auto-learning max-addrs <1-25>* *Switch(config-if)#mac-security enable* *Switch(config-if)#exit*
Cisco	switchport port-security switchport port-security maximum *number_of_addresses* vlan *{vlan_ID | vlan_range}* switchport port-security mac-address [sticky] *mac_address* [vlan *vlan_ID*] (sticky or static MAC) EXAMPLE: *Switch>enable* *Switch# configure terminal* *Switch(config)#interface gigabitethernet0/1* *Switch(config-if)#switchport port-security* *Switch(config-if)#switchport port-security mac-address 0e-03-ef-d8-44-55*

Layer 3 Commands

Configuring VLAN IP Addresses

ExtremeXOS	**configure** [{**vlan**} *vlan_name* | **vlan** *vlan_id*] **ipaddress** [*ipaddress {netmask}* | {*ipNetmask*} | **ipv6-link-local** | {**eui64**} *ipv6_address_mask*] **unconfigure** [{**vlan**} *vlan_name* | **vlan** *vlan_list*] ipaddress EXAMPLE*:* *configure vlan accounting ipaddress 10.12.123.1/24* *unconfigure vlan accounting ipaddress*
EOS	**ip address** *{ip-address} {ip-mask}* **[secondary]** **no ip address** *{ip-address} {ip-mask}* EXAMPLE*:* *C5(su)->router* *C5(su)->router>enable* *C5(su)->router#configure* *C5(su)->router(Config)#interface vlan 1* *C5(su)->router(Config-if(Vlan 1))#ip address 10.12.123.1 255.255.255.0* *C5(su)->router(Config-if(Vlan 1))#no ip address 10.12.123.1 255.255.255.0*
VOSS	After creating the VLAN and entering config-if mode within that vlan. **ip address** {*ip_address} {subnet_mask}* EXAMPLE*:* *Switch#configure terminal* *Switch(config)#interface vlan 1* *Switch(config-if)#ip address 10.10.10.1 255.255.255.0* *Switch(config-if)#exit*
BOSS	After creating the VLAN and entering config-if mode within that vlan. **ip address** {*ip_address} {subnet_mask}* EXAMPLE*:*

	Switch#configure terminal *Switch(config)#interface vlan 1* *Switch(config-if)#ip address 10.10.10.1 255.255.255.0* *Switch(config-if)#exit*
Cisco	Following VLAN creation provision IP addressing on VLAN interface **ip address** *ip_address subnet_mask* EXAMPLE*:* *Switch#configure terminal* *Switch(config)# int vlan 1* *Switch(config-if)#ip address 10.12.123.1 255.255.255.0* *Switch(config-if)#end*

Configuring Inter-VLAN Routing

ExtremeXOS	**enable ipforwarding {ipv4 | broadcast} {vlan** vlan_name} EXAMPLE*:* *Enable ipforwarding vlan purple* *Enable ipforwarding vlan black* *Enable ipforwarding vlan all*
EOS	Use this command to disable IP routing on the device. By default, IP routing is enabled when interfaces are configured; they include no shutdown. **ip routing** **no ip routing** Use this command to enable or disable an interface for IP routing: **no shutdown** **shutdown** EXAMPLE*:* *C5(su)->router*

	C5(su)->router>enable *C5(su)->router#configure* *C5(su)->router(Config)#ip routing* *C5(su)->router(Config)#interface vlan 1* *C5(su)->router(Config-if(Vlan 1))#ip address 10.12.123.1 255.255.255.0* *C5(su)->router(Config-if(Vlan 1))#no shutdown*
VOSS	ip routing EXAMPLE*:* *Switch# configure terminal* *Switch(config)# ip routing*
BOSS	ip routing EXAMPLE*:* *Switch# configure terminal* *Switch(config)# ip routing*
Cisco	Enable IP routing ip routing Following VLAN creation provision IP addressing on VLAN interface ip address *ip_address subnet_mask* EXAMPLE*:* *Switch#config t* *Switch(config)# ip routing* *Switch(config)# int vlan 100* *Switch(config-if)#ip address 10.0.0.1 255.255.255.0* *Switch(config-if)#int vlan 200* *Switch(config-if)#ip address 10.20.0.1 255.255.255.0* *Switch(config-if)#end*

Configuring Routing Information Protocol (RIP) Routing

ExtremeXOS	**configure rip add vlan** [vlan_name | **all**] EXAMPLE*:* *Configure rip add vlan purple* *Enable rip*
EOS	**router rip** **no router rip** Use this command to configure the administrative distance for RIP routes. The no form of this command resets RIP administrative distance to the default value of 120. **distance** *{weight}* **no distance** *{weight}* Use this command to allow RIP to receive update packets on an interface. The no form of this command denies the reception of RIP updates. By default, receiving is enabled on all routing interfaces. **receive-interface vlan** *{vlan-id}* **no receive-interface vlan** *{vlan-id}* EXAMPLE*:* *C5(su)->router* *C5(su)->router>enable* *C5(su)->router#configure* *C5(su)->router(Config)#router rip* *C5(su)->router(Config-router)#distance 100* *C5(su)->router(Config-router)#passive-interface vlan 2* *C5(su)->router(Config-if(Vlan 2))#ip rip enable*
VOSS	**router rip enable** **network** {ip_address} EXAMPLE*:*

	Switch# configure terminal *Switch(config)# router rip enable* *Switch(config)# router rip* *Switch(config-rip)# network 10.10.10.10*
BOSS	router rip enable network {ip_address} EXAMPLE*:* *Switch# configure terminal* *Switch(config)# router rip enable* *Switch(config)# router rip* *Switch(config-router)# network 10.10.10.10*
Cisco	router rip network *ip-address* EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#router rip* *Switch(config-router)#network 10.0.0.0* *Switch(config-router)#end*

Configuring Open Shortest Path First (OSPF) Routing

ExtremeXOS	**configure ospf add vlan** [vlan-name | **all**] **area** area-identifier **{passive}** EXAMPLE*:* *Configure ospf add vlan purple area 0.0.0.0* *Enable ospf*
EOS	Use this command to set the OSPF router ID for the device. This IP address must be set manually to run OSPF. The no form of this command removes the router ID for the device. **router id** *{ip-address}* **no router id** **router ospf** *{process-id}* **no router ospf** *{process-id}* **ip ospf areaid** *{area-id}* **no ip ospf areaid** Use this command to enable OSPF on an interface. The no form of this command disables OSPF on an interface. **ip ospf enable** **no ip ospf enable** EXAMPLE*:* *C5(su)->router(Config)#router id 182.127.62.1* *C5(su)->router#conf terminal* *C5(su)->router(Config)#router ospf 100* *C5(su)->router(Config)#interface vlan 1* *C5(su)->router(Config-if(Vlan 1))#ip ospf areaid 0.0.0.0* *C5(su)->router(Config-if(Vlan 1))#ip ospf enable*
VOSS	**router ospf** **enable** **area** *{ip address}*

	network *{ip address}* area *{area-id}* *switch# configure terminal* *switch(config)# router ospf* *switch(config-ospf)# enable* *switch(config-ospf)# area 20.20.20.20* *switch(config-ospf)# network 10.10.10.10 area 20.20.20.20*
BOSS	router ospf enable area *{ip address}* network *{ip address}* area *{area-id}* *switch# configure terminal* *switch(config)# router ospf* *switch(config-router)# enable* *switch(config-router)# area 20.20.20.20* *switch(config-router)# network 10.10.10.10 area 20.20.20.20*
Cisco	router ospf *process-id* network *ip-address wildcard-mask* area *area-id* EXAMPLE*:* *#config t* *(config)# router ospf 100* *(config-route)# network 10.0.0.0 0.0.0.255 area 100* *(config-route)#end*

Configuring Static Routing

ExtremeXOS	**configure iproute add** [ipNetmask | ip_addr mask] gateway **{bfd} {metric} {multicast | multicast-only | unicast | unicast-only} {vlan** egress_vlan} {**vr** vrname} **configure iproute add default** [ipv6Gateway | ipv6ScopedGateway] **{metric}** {**vr** vr_name} **{multicast-only | unicast-only}** EXAMPLE*:* *Config iproute add 10.102.1.0/24 10.2.1.2* EXAMPLE*:* *Config iproute add default 10.2.1.2*
EOS	**ip route** *dest-prefix dest-prefix-mask forwarding-rtr-addr [distance]* **no ip route** *dest-prefix dest-prefix-mask forwarding-rtr-addr* EXAMPLE*:* *C5(su)->router(Config)#ip route 10.102.1.0 255.255.255.0 10.2.1.2* EXAMPLE *Default Route:* *C5(su)->router(Config)#ip route 0.0.0.0 0.0.0.0 10.2.1.2 2*
VOSS	**ip route** {destination_ip_address} {destination_subnet_mask} {next-hop_ip} **weight** {cost} EXAMPLE*:* *Switch#configure terminal* *Switch(config)#ip route 10.1.1.2 255.255.255.0 2.2.2.2 weight 1* EXAMPLE Default*:* *Switch#configure terminal* *Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.2 weight 1*
BOSS	**ip route** {destination_ip_address} {destination_subnet_mask} {next-hop_ip} {cost} EXAMPLE*:* *Switch#configure terminal* *Switch(config)#ip route 10.1.1.2 255.255.255.0 2.2.2.2 1*

	EXAMPLE Default: *Switch#configure terminal* *Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.2 1*
Cisco	**ip route** {*destination prefix}{forwarding router address}* EXAMPLE: *Switch>enable* *Switch#configure terminal* *Switch(config)# ip route 10.102.1.0 255.255.255.0 10.2.1.2* EXAMPLE default: *Switch>enable* *Switch#configure terminal* *Switch(config)# ip route 0.0.0.0 0.0.0.0 10.2.1.2*

Configuring Border Gateway Protocol (BGP) Routing

ExtremeXOS	**configure bgp AS-number** number **configure bgp routerid router** identifier **create bgp neighbor** remoteaddr **remote-AS-number** as-number {**multi-hop**} **enable bgp neighbor** [remoteaddr | **all**] **configure bgp add network {address-family [ipv4-unicast | ipv4-multicast |ipv6-unicast | ipv6-multicast]}** ipaddress/masklength {**network-policy** policy} EXAMPLE: *create vlan loopback* *configure vlan loopback ipa 1.1.1.1/32* *enable loopback-mode vlan loopback* *configure bgp AS-number 65000* *configure bgp routerid 1.1.1.1*

	create bgp neighbor 10.250.1.10 remote-AS-number 65001 *enable bgp neighbor 10.250.1.10* *configure bgp add network 10.249.2.0/24*
EOS	router bgp *{as-number}* no router bgp *{as-number}* interface *{vlan vlan-id | loopback loopback-id | tunnel tunnel-id |* *interface-name}* no interface *{vlan vlan-id | loopback loopback-id | tunnel tunnel-id |interface-name}* bgp address-family *[ipv4 | ipv6] [unicast | multicast | both | bgp-mpls-vpn]* no address-family *{ipv4 | ipv6} {unicast | multicast | both | bgp-mpls-vpn}* EXAMPLE*:* *System(su)->configure* *System(rw-config)->interface loop.0.2* *System(rw-config-intf-loop.0.2)->ip address 1.1.1.1 255.255.255.255* *System(rw-config-intf-loop.0.2)->no shutdown* *System(su-config)->router bgp 65000* *System(su-config-bgp)->bgp router-id 1.1.1.1* *System(su-config-bgp)->neighbor 10.250.1.10 remote-as 65001* Note: not available on C5, so S-Series config is shown
VOSS	router bgp *{as-number}* router bgp *{as-number}* enable network *{ip address/subnet}* router-id *{ip address}* neighbor *{ip address}* enable EXAMPLE*:* *Switch# configure terminal*

	Switch(config)# router bgp 1 *Switch(config)# router bgp 1 enable* *Switch(config)# router bgp* *Switch(router-bgp)# network 20.20.20.0/24* *Switch(router-bgp)# router-id 20.20.20.20* *Switch(router-bgp)# neighbor 30.30.30.30 enable*
BOSS	N/A
Cisco	**router bgp** *as-number* **network** *network-number [***mask** *network-mask] [***route-map** *route-map-name]* **bgp router-id** *ip-address* **neighbor** *neighbor-address* **remote-as** *as-number* **neighbor** *neighbor-address* **description** *text* EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#interface loopback2* *Switch(config-if)# ip address 1.1.1.1 255.255.255.255* *Switch(config-if)#end* *Switch(config)# router bgp 65000* *Switch(config-router)#bgp router-id 1.1.1.1* *Switch(config-router)#neighbor 10.250.1.10 remote-as 65001* *Switch(config-router)#neighbor 10.250.1.10 description example* *Switch(config-router)#end*

Configuring Virtual Router Redundancy Protocol (VRRP)

ExtremeXOS	**create vrrp vlan** [vlan_name | vlan_list] **vrid** [vridval | vrid_list] **configure vrrp vlan** [vlan_name | vlan_list] **vrid** [vridval | vrid_list] **priority** priorityval **enable vrrp** {**vlan** [vlan_name | vlan_list] **vrid** [vridval | vrid_list} EXAMPLE*:* MASTER *configure vlan vlan1 ipaddress 192.168.1.3/24* *create vrrp vlan vlan1 vrid 1* *configure vrrp vlan vlan1 vrid 1 prioirty 255* *configure vrrp vlan vlan1 vrid 1 add 192.168.1.3* *enable vrrp* BACKUP *configure vlan vlan1 ipaddress 192.168.1.5/24* *create vrrp vlan vlan1 vrid 1* *configure vrrp vlan vlan1 vrid 1 prioirty 100* *configure vrrp vlan vlan1 vrid 1 add 192.168.1.3* *enable vrrp*
EOS	**router vrrp** **create vlan** *vlan-id vrid* **address vlan** *vlan-id vrid ip-address owner* **enable vlan** *vlan-id vrid* **Note**: Requires C5 Advanced Routing License. EXAMPLE*:* Master *set vlan create 2* *router*

	enable *configure* *interface vlan 2* *ip address 10.16.128.1 255.255.255.0* *no shutdown* *exit* *interface loopback 1* *ip address 10.16.255.249 255.255.255.248* *no shutdown* *exit* *router vrrp* *create vlan 2 1* *address vlan 2 1 10.16.128.1 1* *enable vlan 2 1* *exit* The "1" at the end of the 'address vlan' command indicates this router owns IP address 10.16.128.1. Specifies a unique Virtual Router ID (VRID) BACKUP *set vlan create 2* *router* *enable* *configure* *interface vlan 2* *ip address 10.16.128.2 255.255.255.0* *no shutdown* *exit*

	interface loopback 1 *ip address 10.16.255.250 255.255.255.248* *no shutdown* *exit* *router vrrp* *create vlan 2 1* *address vlan 2 1 10.16.128.1 0* *enable vlan 2 1* *exit* *The "0" at the end of the 'address vlan' command indicates this router does not own IP address 10.16.128.1*
VOSS	Ip vrrp version *{3|2}* Ip vrrp address *{vrid} {ip address}* Ip vrrp *{vrid}* backup-master enable Ip vrrp *{vrid}* enable EXAMPLE*:* MASTER *Switch# configure terminal* *Switch(Config)# vlan create 3 type port 1* *Switch(Config)# interface vlan 3* *Switch(Config-if)# ip address 30.30.30.1* *Switch(Config-if)# ip vrrp version 2* *Switch(Config-if)# ip vrrp address 30 30.30.30.3* *Switch(Config-if)# ip vrrp 30 backup-master enable* *Switch(Config-if)# ip vrrp 30 enable* BACKUP *Switch# configure terminal*

	Switch(Config)# vlan create 3 type port 1 *Switch(Config)# interface vlan 3* *Switch(Config-if)# ip address 30.30.30.2* *Switch(Config-if)# ip vrrp version 2* *Switch(Config-if)# ip vrrp address 30 30.30.30.3* *Switch(Config-if)# ip vrrp 30 backup-master enable* *Switch(Config-if)# ip vrrp 30 enable*
BOSS	Ip vrrp address *{vrid}{ip address}* Ip vrrp *{vrid}* enable EXAMPLE*:* MASTER *Switch# configure terminal* *Switch(Config)# vlan create 3 type port 1* *Switch(Config)# interface vlan 3* *Switch(Config-if)# ip address 30.30.30.1 255.255.255.0* *Switch(Config-if)# ip vrrp address 30 30.30.30.3* *Switch(Config-if)# ip vrrp 30 enable* BACKUP *Switch# configure terminal* *Switch(Config)# vlan create 3 type port 1* *Switch(Config)# interface vlan 3* *Switch(Config-if)# ip address 30.30.30.2 255.255.255.0* *Switch(Config-if)# ip vrrp address 30 30.30.30.3* *Switch(Config-if)# ip vrrp 30 enable*
Cisco	EXAMPLE*:* MASTER *Switch>enable*

	Switch#configure terminal *Switch(config)#interface gigabitethernet0/1* *Switch(config-if)#ip address 10.16.128.2 255.255.255.0* *Switch(config-if)#vrrp 1 ip 10.16.128.1* *Switch(config-if)#end* BACKUP *Switch>enable* *Switch#configure terminal* *Switch(config)#interface gigabitethernet0/1* *Switch(config-if)#ip address 10.16.128.3 255.255.255.0* *Switch(config-if)#vrrp 1 ip 10.16.128.1* *Switch(config-if)#end*

Configuring Multicast

Configuring PIM-SM

ExtremeXOS	**enable ipmcforwarding** {vlan name} **configure pim {ipv4 | ipv6}** add vlan [vlan-name | **all] {dense | sparse} {passive}** **configure pim {ipv4 | ipv6} crp vlan** vlan_name [none | policy] {priority} **configure pim cbsr {ipv4 | ipv6}** [**{vlan**} vlan_name {priority **[0-254]} | none]** EXAMPLE*:* *create vlan purple* *configure ipforwarding vlan purple* *enable ipmcforwarding vlan purple* *Configure pim add vlan purple sparse* *Configure pim crp vlan purple* *configure pim crp vlan "purple" mgroup* *Configure pim cbsr vlan purple* *Enable pim* *Mgroup (multicast group) policy* *entry anyname {* *if match any { }* *then { nlri 239.255.255.0/24 ;* *}* *}*
EOS	**C5-series** **ip pimsm** **no ip pimsm** EXAMPLE*:* *C5(su)->router*

	C5(su)->router>enable *C5(su)->router#config* *C5(su)->router(Config)# ip pimsm* *C5(su)->router(Config)#interface vlan 10* *C5(su)->router(Config-if(Vlan 10))#ip pimsm enable* *C5(su)->router(Config-if(Vlan 10))#ip pimsm hello-interval 100* S-series ip pim sparse-mode no ip pim sparse-mode ip pim bsr-candidate *interface-address* [priority *priority*] no ip bsr-candidate *interface-address* ip pim rp-candidate *pim-interface-address* {*group-address group-mask* | priority *priority* | group-list *group-list* [priority *priority*]} no ip pim rp-candidate *pim-interface-address* {*group-address group-mask* | group-list *group-list* [priority *priority*]} EXAMPLE*:* *S Chassis(su-config)->interface vlan 1* *S Chassis(su-config-intf-vlan.0.1)->ip pim sparse-mode* *# Global IPv4 PIM Configuration* *ip pim bsr-candidate 1.1.1.1 2 priority 250* *ip pim ssm default* *ip pim rp-candidate 1.1.1.1 2 224.0.0.0 240.0.0.0* *ip pim rp-candidate 1.1.1.1 2 priority 150*
VOSS	ip pim enable ip pim mode sparse EXAMPLE*:* *Switch# configure terminal* *Switch(config)# ip pim enable*

	Switch(config)# ip pim mode sparse
BOSS	**ip pim enable** **ip pim mode sparse** EXAMPLE*:* *Switch# configure terminal* *Switch(config)# ip pim enable* *Switch(config)# ip pim mode sparse*
Cisco	**ip multicast-routing distributed** **ip pim version** [*1* / *2*] **ip pim** { *dense-mode* / *sparse-mode* / *sparse-dense-mode* } **ip pim rp-address** *ip-address* [*access-list-number*] [*override*] **access-list** *access-list-number* { *deny* / *permit* } **source** [*source-wildcard*] EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)# ip multicast-routing distributed* *Switch(config)#ip pim sparse-mode* *Switch(config)#ip pim rp-address 1.1.1.1 2* *Switch(config)#access-list 2 permit 225.2.2.2 0.0.0.0*

Configuring PIM-DM

ExtremeXOS	**enable ipmcforwarding** {vlan name} **configure pim {ipv4 | ipv6}** add vlan [vlan-name | **all] {dense | sparse} {passive}** EXAMPLE*:* *configure pim add vlan purple dense* *enable pim*

EOS	ip pim dense-mode no ip pim dense-mode EXAMPLE: *S Chassis(su-config)->interface vlan 1* *S Chassis(su-config-intf-vlan.0.1)->ip pim dense-mode* Note: Dense-mode is not available on C5-Series.
VOSS	N/A
BOSS	N/A
Cisco	ip multicast-routing distributed ip pim version [*1* / *2*] ip pim { *dense-mode* / *sparse-mode* / *sparse-dense-mode* } ip pim rp-address *ip-address* [*access-list-number*] [*override*] access-list *access-list-number* { *deny* / *permit* } source [*source-wildcard*] EXAMPLE: *Switch>enable* *Switch#configure terminal* *Switch(config)# ip multicast-routing distributed* *Switch(config)#ip pim dense-mode*

Configuring Layer 3 Quality of Service (QoS)

ExtremeXOS	**create qosprofile** [QP2| QP3 | QP4 | QP5 | QP6 | QP7] **disable dot1p examination ports** [port_list | **all**] **configure diffserv examination** code-point code_point {**qosprofile**} qosprofile **enable diffserv examination ports** [port_list | **all**] EXAMPLE*:* *create qosprofile qp5* *configure diffserv examination code-point 32 qp5* *enable diffserv examination ports all*
EOS	**set vlan create** *{vid}* **set vlan name** *{vlan-list} {vlan-name}* **set policy profile** {*profile-index}* [**name** *name*] [**pvid-status** {**enable** | **disable**}][*pvid* **pvid**] [**cos-status** {**enable** | **disable**}] [**cos** *cos*] [**egress-vlans** *egress-vlans*][**forbidden-vlans** *forbidden-vlans*] [**untagged-vlans** *untagged-vlans*][**precedence** *precedence-list*] [**append**] [**clear**] EXAMPLE*:* Create your VLAN: *set vlan create 7* *set vlan name 7 purple* Configure your purple policy profile for tagged frames: *set policy profile 1 name "purple" pvid-status enable pvid 7 cos-status enable cos 4 tagged-vlans 7* Create your CoS to TOS mappings: *set cos state enable* *set cos settings 4 tos-value 184* The CoS setting for CoS-4 applying DSCP value of EF to purple traffic
VOSS	**qos queue-profile** *{1-5}* **apply** **qos level** *{1-6}*

	access-diffserv enable EXAMPLE: *Switch# configure terminal* *Switch(config)# qos queue-profile 1 apply* *Switch(config)# interface vlan 3* *Switch(config-if)# qos queue-profile 1 apply* *Switch(config-if)# exit* *Switch(config)# interface gigabitethernet 1/12* *Switch(config-if)# qos level 3* *Switch(config-if)# access-diffserv enable*
BOSS	qos agent oper-mode enable qos acl-assign port *{port}* acl-type {ip|l2} name *{name}* qos policy *{policy-id}* name *{name}* port *{port}* clfr-type {classifier|Block} clfr-id *{classifier-id}* meter {1-55000} precedence {1-15} EXAMPLE: *Switch# configure terminal* *Switch(config)# qos agent oper-mode enable* *Switch(config)# qos acl-assign port 1/12 acl-type ip name TEST* *Switch(config)# qos policy 100 name TEST port 1/12 clfr-type classifier clfr-id 200 meter 10000 precedence 7*
Cisco	mls qos mls qos vlan-based class-map [match-all |match-any] *class-map-name* match { access-group *acl-index-or-name* | ip dscp*dscp-list* | ip precedence *ip-precedence-list* } class-map [match-all |match-any] *class-map-name* match input-interface*interface-id-list* policy-map *policy-map-name*

	class-map *class-map-name* police *rate-bps burst-byte* [exceed-action { drop |policed-dscp-transmit }] policy-map *policy-map-name* class [*class-map-name* |class-default] trust [cos | dscp | ip-precedence] set { dscp *new-dscp* | ip precedence *new-precedence* } service-policy *policy-map-name* service-policy input *policy-map-name* EXAMPLE*:* *Switch>enable* *Switch#configure terminal* *Switch(config)#mls qos* *Switch(config)#mls qos vlan-based* *Switch(config)#access-list 105 permit ip any any* *Switch(config)#class-map map-105* *Switch(config-cmap)#match access 105* *Switch(config-cmap)#exit* *Switch(config)#policy-map port-map-105* *Switch(config-pmap)#class map-105* *Switch(config-pmap-c)#set dscp 7* *Switch(config-pmap-c)#exit* *Switch(config-pmap)#exit* *Switch(config)#interface vlan 200* *Switch(config-if)#service-policy input port-map-105* *Switch(config-if)#end*

Configuring Layer 3 Security

Configuring DHCP Snooping

ExtremeXOS	*configure trusted-ports [ports|all] trust-for dhcp-server* *configure trusted-servers {vlan} vlan_name add server ip_address trust-for dhcp-server* *enable ip-security dhcp-snooping vlan <VLAN NAME> ports [ALL | <PORT-LIST>] violation-action drop-packet [block-mac | block-port | Block port | snmp-trap]* EXAMPLE: *configure trusted-ports 1 trust-for dhcp-server* *configure trusted-servers vlan purple add server 192.168.10.75 trust-for dhcp-server* *enable ip-security dhcp-snooping vlan "purple" ports all violation-action drop-packet*
EOS	set antispoof dhcp-snooping {enable | disable} *{port-string}* set antispoof dhcp-snooping mac-verification {enable | disable} *{port-string}* set antispoof dhcp-snooping port-mode {trusted | bypass | untrusted} *{port-string}* EXAMPLE: *set antispoof dhcp-snooping enable ge.1.1* *set antispoof dhcp-snooping mac-verification ge.1.2* *set antispoof dhcp-snooping port-mode trusted ge.1.2*
VOSS	Enable globally ip dhcp-snooping enable Set per vlan (in vlan interface) ip dhcp-snooping enable Trust per port (in port interface) ip dhcp-snooping {trusted|untrusted} EXAMPLE: Switch# configure terminal Switch(config)#ip dhcp-snooping Switch# configure terminal Switch(config)# interface gigabit vlan 1

	Switch(config-if)# ip dhcp-snooping enable Switch# configure terminal Switch(config)# interface gigabit 1/1 Switch(config-if)# ip dhcp-snooping trusted
BOSS	Enable globally **ip dhcp-snooping** Set per vlan **ip dhcp-snooping vlan** {vlan} Trust per port (interface-port all) **ip dhcp-snooping port** {port} {**trusted|untrusted**} EXAMPLE*:* *Switch# configure terminal* *Switch(config)#ip dhcp-snooping* *Switch# configure terminal* *Switch(config)# ip dhcp-snooping vlan 1* *Switch# configure terminal* *Switch(config)# interface ethernet all* *Switch(config-if)# ip dhcp-snooping port 1/15 trusted*
Cisco	ip dhcp snooping ip dhcp snooping vlan *vlan-range* ip dhcp snooping information option ip dhcp snooping information option format remote-id [string *ASCII-string* |hostname] ip dhcp snooping information option allow-untrusted ip dhcp snooping vlan *vlan* information option format-type circuit-id [override] string *ASCII-string* ip dhcp snooping trust ip dhcp snooping limit rate *rate* ip dhcp snooping verify mac-address EXAMPLE*:*

	Switch>enable Switch(config)#ip dhcp snooping Switch(config)# ip dhcp snooping vlan 100 Switch(config)#interface gigabitethernet 3/0/1 Switch(config-if)#ip dhcp snooping trust

Setting Gratuitous Address Resolution Protocol (ARP) Protection

ExtremeXOS	**enable iparp gratuitous protect vlan** vlan-name EXAMPLE*:* *enable iparp gratuitous protect vlan purple*
EOS	**ip gratuitous-arp {ignore | reply | request}** **no ip gratuitous-arp** EXAMPLE*:* *(rw-config)->interface vlan 1* *(rw-config-intf-vlan.0.1)->ip gratuitous-arp request*
VOSS	**no ip gratuitous-arp** EXAMPLE*:* *Switch#configure terminal* *Switch(config)#no ip gratuitous-arp*
BOSS	N/A
Cisco	**no ip gratuitous-arp** **Note***:* Available on specific platforms.

Setting Denial of Service (DoS) Protection

ExtremeXOS	**enable dos-protect** **configure dos-protect trusted-ports** [ports [ports | **all**] | add-ports [ports-to-add | **all**] | **delete-ports** [ports-to-delete | **all**]] EXAMPLE*:* *enable dos-protect* *configure dos-protect trusted-ports ports 1-23*
EOS	S-SERIES **hostdos** *{mitigation-type* | **enable** | **icmp-maxlength** *icmp-maxlength}* [**rate** *count* [**per-second** | **per-minute** | **per-hour** | **per-day**]] [**nolog**] **no hostdos** [*mitigation-type*] [**enable** / **disable**] EXAMPLE*:* *S Chassis(rw-config)->hostdos enable* *S Chassis(rw-config)->hostDoS spoof rate 5 per-minute* *S Chassis(rw-config)->hostdos xmasTree nolog* C5-SERIES **set dos-control** [**all** | **sipdip** | **firstfrag** *firstfrag* | **tcpfrag** | **l4port** | **icmp** *icmp* | **smacdmac** | **tcpport** | **udpport** | **tcpflagseq** | **tcpoffset** | **tcpsyn** | **tcpsynfin** |**tcpfinurgpsh** | **icmpv4** *icmpv4* | **icmpv6** *icmpv6* | **icmpfrag**] EXAMPLE*:* *C5(su)->set dos-control all* *C5(su)->set dos-control icmpv4 1024* *C5(su)->clear dos-control all* *C5(su)->clear dos-control icmpv4*
VOSS	N/A
BOSS	N/A
Cisco	N/A

Reference Documentation and Links

Extreme Networks Product Documentation

http://www.extremenetworks.com/support/documentation/

Cisco Documentation

Cisco Configuring Passwords and Privileges

http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.pdf

Cisco Configuring Basic Settings

http://www.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/basic_f.pdf

Reset Catalyst Switches Running Cisco IOS Software

http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2900-xl-series-switches/24328-156.html#reset_ios

Configuring IEEE 802.3ad Link Bundling and Load Balancing

http://www.cisco.com/c/en/us/td/docs/ios/cether/configuration/guide/ce_lnkbndl.html#wp1053903