Nortel Ethernet Routing Switch 8300

Command Reference — NNCLI

NN46200-306 (316810-F Rev 01)

Document status: Standard
Document version: 03.01
Document date: 27 August 2007

Trademarks

Nortel, Nortel Networks, the Nortel Networks logo, the Globemark, are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice.

Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE

SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

1. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

2. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

3. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
6. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

New in this release

The following sections detail what is new in *Nortel Ethernet Routing Switch 8300 Command Reference — NNCLI* (NN462000-306)

Features

The new features in release 4.0 have the following commands:

Layer 2 IGMP snoop querier

- `ip igmp snoop-querier`
- `no ip igmp snoop-querier`
- `ip igmp snoop-querier-addr`
- `no ip igmp snoop-querier`
- `show ip igmp snooping`

Multicast Stream Limitation

- `ip igmp stream-limit`
- `no ip igmp stream-limit`
- `ip igmp stream-limit-group enable max-streams`
- `no ip igmp stream-limit`
- `ip igmp stream-limit-group enable max-streams`
- `no ip igmp stream-limit-group`
- `default ip igmp stream-limit-group`
- `ip igmp stream-limit-max-streams`
- `default ip igmp stream-limit-max-streams`
- `show interfaces vlan igmp`
- `show ip igmp stream-limit`
- `show ip igmp stream-limit`

Network Load Balancing Support

- `vlan nlb-mode`
- `no vlan nlb-mode`
- `show vlan nlb-mode`

Protocol Independent Multicast-Sparse Mode

- `debug ip pim`
- `ip pim`
- `ip pim enable`
- `no ip pim`
- `ip pim interface virtual neighbor`
- `no ip pim interface virtual neighbor`
- `ip pim rp-candidate group rp`
- `no ip pim rp-candidate group rp`
- `ip pim static-rp`
- `no ip pim static-rp`
- `show debug ip pim`
- `show ip pim`
- `show ip pim active-rp`
- `show ip pim bsr`
- `show ip pim interface`
- `show ip pim interface vlan`
- `show ip pim mroute`
- `show ip pim static-rp`

Simple Loop Protection Protocol

- `slpp`
- `Default slpp`
- `no slpp`
- `slpp port`
- `default slpp port`
- `no slpp port`
- `show slpp`

Static source groups

- `ip mroute static-source-group`
- `no ip mroute static-source-group`
- `show ip mroute static-source-group`

Other changes

The following are new or revised commands in release 4.0 that are not associated with the new features:

IP Protocol commands

- `ip irdp`
- `no ip irdp`
- `default ip irdp`
- `no ip irdp multicast`
- `ip irdp vlan multicast`
- `no ip irdp vlan multicast`
- `show ip irdp`

Multicast services commands

In Software Release 4.0, many of the IP IGMP commands that were listed separately in previous releases, are now listed as parameters that are included in the `ip igmp` , `no ip igmp`, and `default ip igmp` commands.

- `ip igmp`
- `no ip igmp`
- `default ip igmp`
- `ip igmp generate-log`
- `no ip igmp generate-log`
- `default ip igmp generate-log`
- `ip igmp generate-trap`
- `no ip igmp generate-trap`
-
- `ip igmp mrdisc`
- `no ip igmp mrdisc`
- `default ip igmp mrdisc`
- `show ip igmp group count`
- `show ip igmp snooping`
- `show ip igmp sys`

Preface

The Nortel* Ethernet Routing Switch 8300 is a flexible and multifunctional Layer 2/Layer 3 switch that supports diverse network architectures and protocols. The Ethernet Routing Switch 8300 provides security and control features such as Extensible Authentication Protocol over LAN (EAPoL), Simple Network Management Protocol, Version 3 (SNMP3), and Secure Shell (SSH). The Ethernet Routing Switch 8300 provides quality of service (QoS) for a high number of attached devices and supports future network requirements for QoS for critical applications, such as Voice over IP (VoIP).

This guide describes the individual NNCLI commands available for the Ethernet Routing Switch 8300 Software Release 4.0. The guide lists each command, together with the complete syntax and a functional description, from the Nortel Networks* Command Line Interface (NNCLI).

Before you begin

This guide is intended for network administrators who have the following background:

- basic knowledge of networks, Ethernet bridging, and IP routing
- familiarity with networking concepts and terminology
- experience with windowing systems or GUIs
- basic knowledge of network topologies

About the NNCLI

This section describes the Nortel Networks Command Line Interface (NNCLI) command modes you use to configure the Ethernet Routing Switch 8300 and the commands you use to access the NNCLI. You can access the NNCLI using the following methods:

- Telnet session
- rlogin
- local console port

NNCLI command modes

The NNCLI has four major command modes, listed in order of increasing privileges:

- User EXEC
- Privileged EXEC
- Global configuration
- Interface configuration

Each mode provides a specific set of commands. The command set of a higher-privilege mode is a superset of a lower-privilege mode. That is, all lower-privilege mode commands are accessible when using a higher-privilege mode.

The command modes are as follows:

- User EXEC mode

  This is the initial mode of access. By default, the User Access Verification Password for this mode is empty, and password checking is disabled. The system administrator can change the password (and password checking enabled) in Global configuration mode. Once the password is changed, it is activated immediately.

- Privileged EXEC mode

  This mode is accessed from the User EXEC mode. When accessing this mode, you are prompted to provide a login name and password. The login name and password combination determines your access level in the Privileged EXEC mode and other higher modes.

- Global configuration mode

  This mode allows you to make changes to the running configuration. If the configuration is saved, these settings survive reboots of the switch.

- Interface configuration mode

  This mode allows you to modify either a logical interface, such as a VLAN, or a physical interface, such as a port/slot.

From either the Global configuration mode or the Interface configuration mode, save all the configuration parameters (both global and interface) to a file. The default name for the configuration parameters file is config.cfg. You can also use alternative filenames.

"NNCLI command modes" (page 43) lists the NNCLI command modes, the prompts for each mode, the abbreviated name for each mode, and how to enter and exit each mode.

NNCLI command modes

Command mode	Prompt	Mode name	Command/mode to enter or exit mode
User EXEC	Passport-8300:5>	exec	Default mode when NNCLI is started **`logout`** to exit
Privileged EXEC	Passport-8300:5#	privExec	**`enable`** to enter from User EXEC mode **`disable`** to exit to User EXEC mode
Global configuration	Passport-8300:5(config)#	config	**`configure`** to enter from Privileged EXEC mode **`exit`** to exit to Privileged EXEC mode
Interface configuration	Passport-8300:5(config-if)#	config-if	**`interface`** to enter from Global configuration mode **`exit`** to exit to Global configuration mode

Note: Prompts are expressed in this table using the format Passport-8300:5; however, prompts returned from your switch typically reflect the specific chassis you use. For example, if you use the 8310 chassis, the prompts use the format Passport-8310:5. Prompts can be customized, also, using the NNCLI command **`snmp-server name <prompt>`**. Refer to *Getting Started (316799-C)* for more information.

Accessing the NNCLI

When you first power up the Ethernet Routing Switch 8300, the default interface is the Ethernet Routing Switch 8300 CLI. To switch from the CLI to the NNCLI, you must change the NNCLI boot flag to **`true`** and save the boot configuration file using the following commands:

```
Passport-8310:5# config boot flags nncli true
Passport-8310:5# save boot
```

You must reboot the switch for this change to take effect. After you reboot the switch, access the NNCLI using Telnet, rlogin, or the local console port. You can log in to the switch using your password and the default privilege password **`nortel`**.

Use the following commands to:

- log in to the software using the default user name and password
- access Global configuration mode

```
Login: xxxxx
Password: xxxxx
Passport-8310:5> enable
Password: nortel
Passport-8310:5# configure terminal
Passport-8310:5(config) #
```

Returning to the CLI

Note: The config.cfg file for the CLI and the config.cfg file for the NNCLI are not compatible. If you decide to change the CLI mode to NNCLI, or the reverse, you must use the config.cfg file for the selected mode.

To switch from the NNCLI to the CLI, enter the following commands:

```
Passport-8310:5(config) # no boot flags nncli
Passport-8310:5(config) # exit
Passport-8310:5(config) # save boot
```

You must reboot the switch for this change to take effect.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **`ping <ip_address>`**, you enter **`ping 192.32.10.12`**
bold body text	Indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, tabs, and menu items.
`bold Courier text`	Indicates command names, options, and text that you must enter. Example: Use the **`dinfo`** command. Example: Enter **`show ip {alerts|routes}`**.

braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **`show ip {alerts|routes}`**, you must enter either **`show ip alerts or show ip routes`**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **`show ip interfaces [-alerts]`**, you can enter either **`show ip interfaces`** or **`show ip interfaces -alerts`**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is **`ethernet/2/1 [ <parameter> <value> ]... ,`** you enter **`ethernet/2/1`** and as many parameter-value pairs as needed.
italic text	Indicates variables in command syntax descriptions. Also indicates new terms and book titles. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **`show at <valid_route>`**, **`valid_route`** is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`

separator (>)	Shows menu paths. Example: **Protocols > IP** identifies the **IP** command on the **Protocols** menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is **`show ip {alerts|routes}`**, you enter either **`show ip alerts`** or **`show ip routes`**, but not both.

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Utility management commands

This chapter describes the NNCLI utility management commands and their parameters.

attribute

Use this command to modify the MS-DOS file attributes.

Syntax

attribute <file> <attributes>

where:

- **file** specifies the MS-DOS file name.
- **attributes** specifies the file attributes as {+|-|A|S|H|R}. The range of values is 1 to 1536 characters.

Command mode

Privileged EXEC mode

boot

Use this command to boot the switch with an image and a configuration file. The command options let you specify the boot source (flash, PCMCIA card, or TFTP server) and file name. If you do not specify a device and file, the NNCLI uses the software and configuration files on the primary boot device that is defined by the Boot Monitor **choice** command.

Note: For the changes made to the Boot Monitor CLI to take effect, you must use the **save** command to save the changed configuration file and then reboot the switch.

Syntax

boot [<file>] [config <value>] [-y]

where:

- **file** is the software image device and file name in the format **[a.b.c.d:]<file>** | **/pcmcia /<file>** | **/flash/<file>**. The file name, including the directory structure, can be up to 1536 characters.
- **config value** is the software configuration device and file name in the format **[a.b.c.d:]<file>** | **/pcmcia/ <file>** | **/flash/ <file>**. The file name, including the directory structure, can be up to 1024 characters.
- **-y** suppresses the confirmation message before the switch reboots. If you omit this parameter, the system prompts you to confirm the action before the switch reboots.

Command mode

Privileged EXEC mode

For more information about this command, see *Getting Started (316799-C)*.

cd

Use this command to change the current file system directory path.

Syntax

cd <dir>

where

dir specifies a directory path name up to 1536 characters.

Command mode

Privileged EXEC mode

chkdisk

This command runs a check of the file system for inconsistencies.

Syntax

chkdsk <device> [repair]

where:

- **device** is the device name, for example /flash | /pcmcia, up to 1536 characters.
- **repair** repairs the errors found.

Command mode

Privileged EXEC mode

clear

Use this command to clear statistics from counters, flush entries from a table, or end a Telnet session.

Syntax

clear

Parameters

This command includes the following options:

clear **followed by:**	
filter statistics <1-512>	Clears filter statistics from the switch counters, where **1-512** is the filter ID.
ip arp vlan <vid>	Clears ARP VLAN entries from the ARP table, where **vid** is the VLAN ID. The valid values are 0 to 255.
ip route vlan <vid>	Clears route entries associated with the specified VLAN, where **vid** is the VLAN ID. The valid values are 0 to 255.
qos policy-stats <1-128>	Clear QoS statistics from the switch counters, where **1-128** is the policy ID.
port-stats [<ports>]	Clears port statistics from the switch counters, where **ports** specifies the ports for which you are entering the command in the form: portlist {slot/port[-slot/port][, ...]}.
telnet <session id>	Ends the specified Telnet session, where **session id** is a number between 0 and 7.

Command mode

Privileged EXEC mode

copy

Use this command to copy a file from one device to another. You can also use a wildcard pattern with this command.

Syntax

`copy <srcfile> <destfile>`

where:

- **`srcfile`** specifies the source device and file name of the file to be copied in one of the following formats:
  - **`[a.b.c.d:] <file>`**
  - **`/pcmcia/ <file>`**
  - **`/flash/ <file>`**

  The range of values is 1 to 1536 characters.
- **`destfile`** specifies the destination device and file name of the file that receives the copied file. The range of values is 1 to 99 characters.

Command mode

Privileged EXEC mode

cp

Use this command to copy a file from one device to another. This command can be used with a wildcard pattern.

Syntax

`cp <srcfile> <destfile>`

where:

- **`srcfile`** specifies the source device and file name of the file to be copied in one of the following formats:
  - **`[a.b.c.d:] <file>`**
  - **`/pcmcia/ <file>`**
  - **`/flash/ <file>`**

  The range of values is 1 to 1536 characters.
- **`destfile`** specifies the destination device and file name of the file that receives the copied file. The range of values is 1 to 99 characters.

Command mode

Privileged EXEC mode

For more information about this command, see *Getting Started (316799-C)*.

date

Use this command to display the current date settings for the switch.

Syntax

date

Command mode

User EXEC mode
Privileged EXEC mode

For more information about this command, see *Getting Started (316799-C)*.

delete

Use this command to remove a file or directory. A wildcard pattern can be used with this command.

> ***Note:*** This command can also be entered as **del**. There is no change in syntax or functionality when using the abbreviated command.

Syntax

delete <file> [-y]

where:

- **file** specifies the device and file name in one of the following formats:
  - **/pcmcia/ <file>**
  - **/flash/ <file>**

  The range of values is 1 to 1536 characters.
- **-y** specifies bypassing the confirmation prompt.

Command mode

Privileged EXEC mode

For more information about this command, see *Getting Started (316799-C)*.

dir

Use this command to list the files in a directory in MS-DOS format. When you execute the **directory** command with no specified device, it displays the contents of all flash devices. When you specify flash or PCMCIA, the **directory** command displays only the contents of that device.

Syntax

directory [<dir>] [-l]

where:

- **dir** specifies either flash or PCMCIA, in the form **/flash** or **/pcmcia**.
- -l displays file details if you specify a path name.

Command mode

Privileged EXEC mode

disable

Use this command to exit the Privileged EXEC command mode and return to the User EXEC command mode.

Syntax

disable

Command mode

Privileged EXEC mode

edit

Use this command to modify the contents of a script file.

Syntax

edit <file>

where

file specifies the file name **/flash**|**/pcmcia** with a value range of 1 to 99.

Command mode

Privileged EXEC mode

enable

Use this command to change from the User EXEC command mode to the Privileged EXEC command mode. If access to the Privileged EXEC command mode is password protected, you must supply a password when executing this command.

Syntax

enable

Command mode

User EXEC mode

Next command mode

Privileged EXEC mode

For more information about this command, see *Getting Started (316799-C)*.

end

Use this command to exit Global configuration mode and return to Privileged EXEC mode. The command is equivalent to pressing Ctrl+Z on the keyboard.

Syntax

`end`

Command mode

Global configuration mode

exit

Use this command from within User EXEC mode or Privileged EXEC mode to end a terminal session and log out of the switch. Use this command from within Interface configuration mode to return to Global configuration mode and from Global configuration mode to return to Privileged EXEC mode.

Syntax

`exit`

Command mode

User EXEC mode
Privileged EXEC
Global configuration
Interface configuration

For more information about this command, see *Getting Started (316799-C)*.

format

This command formats the specified device (flash, or PCMCIA card).

Syntax

`format <device>`

where

`device` specifies the device name (**`/flash`** or **`/pcmcia`**) that you want to format. The valid range is 1 to 1536.

Command mode

Privileged EXEC mode

format-flash

Use this command to format the switch's on-board flash device with an FTL and MS-DOS file system.

Syntax

format-flash

Command mode

Privileged EXEC mode

grep

Use this command to display all lines in a file that have one or more matching strings within the file.

Syntax

grep <string> <file>

where:

- **string** specifies the character string to be matched. The range of values is 0 to 1536 characters.
- **file** specifies the file name in one of the following formats:
  - **/pcmcia/ <file>**
  - **/flash/ <file>**

  The file name, including the directory structure, can be up to 1536 characters

Command mode

Privileged EXEC mode

help

Use this command to display a description of the interactive help system.

Syntax

help

Command mode

User EXEC
Privileged EXEC mode
Global configuration mode
Interface configuration mode

history

Use this command to list the commands that you have entered during the current session.

Syntax

history

Command mode

Privileged EXEC mode

install

Syntax

```
install
```

Command mode

Privileged EXEC mode

logout

Use this command to log out of the current NNCLI, Telnet, or rLogin session from any mode, and return to the main console menu.

Syntax

```
logout
```

Command mode

User EXEC mode
Privileged EXEC mode
Global configuration mode
Interface configuration mode

mkdir

Use this command to create a directory.

Syntax

```
mkdir <dir>
```

where

dir specifies the directory name with a value range of 1 to 99 characters.

Command mode

Privileged EXEC mode

monitor

Use these **monitor** commands to monitor MLT or port statistics.

Syntax

`monitor mlt error collision [ <mlt_id> ]`
`monitor mlt error main [ <mlt_id> ]`
`monitor mlt stats interface main [ <mlt_id> ]`
`monitor mlt stats interface utilization [ <mlt_id> ]`

monitor ports error collision [from <slot/port>]
monitor ports error extended [from <slot/port>]
monitor ports error main [from <slot/port>]
monitor ports stats interface extended [from <slot/port>]
monitor ports stats interface main [from <slot/port>]
monitor ports stats interface utilization [from <slot/port>]
monitor ports stats rmon [from <slot/port>]
monitor ports stats stp [from <slot/port>]

Command mode

Privileged EXEC mode

monitor-stats

Use this command to configure the duration and interval of the **monitor** commands.

Syntax

monitor-stats

Parameters

This command includes the following options:

monitor-stats **followed by:**	
duration <integer>	Sets the length of the monitor period. To clear the display, type Ctrl/L. • **integer** is an integer value with a range of 1 to 1800 seconds. The default is 300 seconds.
interval <integer>	Sets the frequency of the update interval. To clear the display, type Ctrl/L. • **integer** is an integer value with a range of 1 to 600 seconds. The default is 5 seconds.

Command mode

Global configuration mode

more

Use this command to display the contents of a file one page at a time.

Syntax

more <file> [type]

where:

- **file** Specifies the device and file name in one of the following formats:
  - **[a.b.c.d:] <file>**
  - **/pcmcia/ <file>**
  - **/flash/ <file>**

  The range of values is 1 to 1536 characters.
- **type** specifies the file type, either ASCII or Binary. This is an optional parameter.

Command mode

Privileged EXEC mode

mv

Use this command to move or rename a file or directory. This command can be used with a wildcard pattern. You cannot use the **mv** command to move a file between two devices. Use the **cp** or the **copy** command instead.

Syntax

mv <old_filename> <new_filename>

where:

- **old_filename** specifies the old device and file name in one of the following formats:
  - **/pcmcia/ <file>**
  - **/flash/ <file>**

  The range of values is 1 to 1536 characters.
- **new_filename** specifies the new file name. The range of values is 1 to 99 characters.

Command mode

Privileged EXEC mode

pcmcia-stop

This command enables you to terminate access to the PCMCIA card.

Syntax

pcmcia-stop

Command mode

Privileged EXEC mode

peer

Use this command to access the standby CPU with telnet or rlogin. This command can make changes to the standby CPU without reconnecting to the console port on that module.

Syntax

peer <operation>

where

operation specifies the type of session access. The options are **telnet** or **rlogin**.

Note: You must set an rlogin access policy on the standby CPU before you can use the rlogin peer command to access the standby from the master CPU. To set an access policy on the standby CPU, connect a terminal to the Console port on the standby CPU.

Command mode

Privileged EXEC mode

ping

Use this command to test the network connection to another network device. The **ping** command sends an Internet Control Message Protocol (ICMP) packet or echo message from the switch to the target device. If the device receives the packet, it sends a ping reply. When the switch receives the reply, it displays a message indicating that the specified IP address is alive. If no reply is received, a message indicates that the address is not responding.

Syntax

ping <ipaddr>

where

ipaddr is the IP address of the other network device.

Parameters

This command includes the following options:

ping <ipaddr> **followed by:**	
[datasize <value>]	Specifies the size of the ping data. The range of **value** is 16 to 4076 bytes.
[count <value>]	Specifies the number of times to ping. The range of **value** is 1 to 9999, with a default of 1.
[-s]	Specifies a continuous ping (with an interval of -I).
[-I <value>]	Specifies the interval between transmissions in seconds. The range of **value** is 1 to 60.
[-t <value>]	Specifies the no-answer timeout value in seconds. The range of **value** is 1 to 120.
[-d]	Sets ping debug mode. In debug mode, the ping reply includes additional information about the device pinged.

Command mode

Privileged EXEC mode

pwd

Use this command to print the current working directory path in the file system.

Syntax

pwd

Command mode

Privileged EXEC mode

reload

Use this command to reset the switch. When you reset the switch, the most recently saved configuration file is used to reload the system parameters.

Syntax

reload [-y]

where **-y** skips the information prompt. If you omit this option, the system prompts you to confirm the action before the switch performs the reload.

Command mode

Privileged EXEC mode

rename

Use this command to move or rename a file or directory. This command can be used with a wildcard pattern.

Syntax

rename <old> <new>

where:

- **old** specifies the old device and file name in one of the following formats:
  - **/pcmcia/ <file>**
  - **/flash/ <file>**

  The range of values is 1 to 1536 characters.
- **new** specifies the new device and file name.

  The range of values is 1 to 99 characters

Command mode

Privileged EXEC mode

rlogin

Use this command from Privileged EXEC mode to allow the login of a remote device.

Syntax

rlogin <ipaddr>

where

ipaddr specifies the IP address of the remote device in the format a.b.c.d.

Command mode

Privileged EXEC mode

rlogin-sessions

Use this command from Global configuration mode to specify the number of rlogin sessions.

Syntax

rlogin-sessions <session>

where

sessions specifies the number of rlogin sessions. The valid values are 0 to 8.

Command mode

Global configuration mode

rsh

Use this command to execute a shell command on a remote device.

Syntax

rsh <ipaddr> -l <value> <cmd>

where:

- **ipaddr** specifies the IP address of the remote device in the format a.b.c.d.
- **value** specifies the user login name. The range of values is a string of 0 to 1536 characters.
- **cmd** specifies the command to execute on the remote host. The range of values is a string of 0 to 1536 characters.

Command mode

Privileged EXEC mode

save

Use this command to save the running configuration to a selected file.

Syntax

save <savetype> [file <value>] [standby <value>] [backup <value>]

where:

- **savetype** specifies the type of file to save; options are **config, bootconfig, log**, and **trace**.
- **file <value>** specifies the file name in one of the following formats:
  - **[a.b.c.d:] <file>**
  - **/pcmcia/ <file>**
  - **/flash/ <file>**

  The file name, including the directory structure, can be up to 99 characters.
- **standby <value>** saves the specified file name to the standby CPU.
- **backup <value>** saves the specified file name and identifies the file as a backup file.

Command mode

Privileged EXEC mode

show running-config

Use this command to display the running system information.

Syntax

```
show running-config
```

Command mode

Privileged EXEC mode

source

Use this command to merge a configuration script file into the running configuration without having to reboot the switch.

Syntax

```
source <file>
```

where:

- **file** specifies the device and file name of the new configuration file in one of the following formats:
  - **[a.b.c.d:] <file>**
  - **/pcmcia/ <file>**
  - **/flash/ <file>**

  The range of values is 1 to 1536 characters.

Parameters

This command includes the following options:

source <file> **followed by:**	
[debug]	Provides a debug script output.
[stop]	Stops the script when it finds an error in the file.
[syntax]	Verifies the script's syntax.

Command mode

Privileged EXEC mode

sys-action

This command resets system functions.

Syntax

```
sys-action
```

Parameters

This command includes the following options:

sys-action **followed by:**	
cpuswitchover	Resets the switch to change over to the backup CPU.
resetconsole	Reinitializes the hardware Universal Asynchronous Receiver/Transmitter (UART) drivers. Use this command only if the console connection is hung.
resetcounters	Resets all the statistics counters in the switch to zero.

Command mode

Privileged EXEC mode

telnet

Use this command from Privileged EXEC mode to set up a Telnet session to a remote device, for example, to the standby CPU.

Syntax

```
telnet [ <ipaddr> ]
```

where

ipaddr is an optional parameter that specifies the IP address {a.b.c.d} of the remote device.

Command mode

Privileged EXEC mode

telnet-access

Use this command from Global configuration mode to set the number of seconds to wait for a Telnet login before closing the connection or to change the allowable number of inbound Telnet sessions.

Syntax

```
telnet-access {login-timeout <seconds> |sessions
<sessions> }
```

where:

- **seconds** is the number of seconds to wait for a Telnet login before closing the connection. The valid range is 30 to 65535 seconds.

- **sessions** is the number of inbound Telnet sessions that you can have. The valid range is 0 to 8 sessions.

Command mode

Global configuration mode

test

Use this command to perform a loopback test or to stop a currently running loopback test.

Syntax

```
test {loopback <slot/port> |stop}
```

where

slot/port specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.

Command mode

Privileged EXEC mode

test

Use this command to set all interfaces or the specified interface(s) in testing mode.

Syntax

```
test [port <slot/port> ]
```

where

slot/port specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.

Command mode

Interface configuration mode

trace

Use this command to display the status of the switch at any given time.

Syntax

```
trace
```

Parameters

This command includes the following options:

trace **followed by:**	
clear	Clears the trace file.
filter	Filters trace messages.
grep	Performs a comparison of trace messages.
level <modid> [<level>]	Displays the trace level on a software module for the specified module ID when the optional level parameter is omitted. The optional level parameter specifies trace levels. • 0 = Disabled • 1 = Very terse • 2 = Terse • 3 = Verbose • 4 = Very verbose
modid-list	Displays the module ID numbers which can be traced.
off	Disables tracing on a module.
route-policy	Traces a route policy.
screen [<setting>]	Enables or disables displaying the trace file. The setting value is either on or off.
slot	Specifies the line card slot number, from 1 to 10.

Command mode

Privileged EXEC mode

trace auto-enable

Use this command to configure the switch to automatically enable a trace in the event CPU utilization reaches a pre-defined value.

Syntax

```
trace auto-enable
```

Parameters

This command includes the following parameters:

trace auto-enable **followed by:**	
add-module <modid> <level>	Adds a module to be traced by the trace auto-enable feature. • **modid** identifies the module that you want to add. For example, 3 = Port Manager, 20 = Topology Discovery. The valid range is 0 to 66. For a list of valid module IDs, enter **trace level ?**. • **level** identifies the level of detail you want in the trace. For example, 0 = Disabled, 1 = Very Terse. The valid range is 0 to 7.
auto-trace <enable|disable>	Enables or disables auto-trace. The default value is disable.
high-percentage <percent>	Specifies the CPU utilization percentage above which auto trace must be enabled. • **percent** is a value from 60 to 100. The default is 90.
high-track-duration <seconds>	Specifies the time in seconds to monitor CPU utilization before triggering a trace. • **seconds** is a value from 3 to 10. The default is 5.
low-percentage <percent>	Specifies the CPU utilization percentage below which auto-trace should be disabled. • **percent** is a value from 50 to 90. The default is 75.

trace auto-enable **followed by:**	
low-track-duration <seconds>	Specifies the time, in seconds, to monitor CPU utilization before disabling the trace. • **seconds** is a value from 3 to 10. The default is 5.
remove-module <modid>	Removes a module from automatic tracing. • **modid** identifies the module for which you want to disable auto-trace. For example, 3 = Port Manager, 20 = Topology Discovery. The valid range is 0 to 66. For a list of valid module IDs, enter **trace level ?**.

Note: The enabling or disabling of auto-trace is not saved to the configuration file. When the Ethernet Routing Switch 8300 reboots, auto-trace functionality is disabled.

Command mode

Privileged EXEC mode

traceroute

Use this command to trace the route to a remote host. *traceroute* is a valuable tool for troubleshooting because it shows all the routes that are used or indicates that the remote network cannot be reached.

Syntax

traceroute <ipaddr> [<datasize>] [-m <value>] [-p <value>] [-q <value>] [-w <value>] [-v]

where:

- **ipaddr** is the IP address {a.b.c.d} of the remote host.
- **datasize** is the size of the probe packet (1 to 1464).
- **-m <value>** is maximum time-to-live (TTL) value (1 to 255).
- **-p <value>** is the base UDP port number (0 to 65535).
- **-q <value>** is the number of probes per TTL (1 to 255).
- **-w <value>** is the wait time per probe (1 to 255).
- **-v** is the verbose mode (showing all).

Command mode

Privileged EXEC mode

write memory

Use this command to save the running configuration to memory

Syntax

```
write memory
```

Command mode

Privileged EXEC mode

Bootconfig commands

This chapter describes NNCLI boot configuration commands and their parameters.

Bootconfig Command
"no bootconfig flags factorydefaults" (page 87)
"bootconfig flags ftpd" (page 88)
"no bootconfig flags ftpd" (page 88)
"bootconfig flags info" (page 88)
"bootconfig flags logging" (page 88)
"no bootconfig flags logging" (page 89)
"bootconfig flags nncli" (page 89)
"no bootconfig flags nncli" (page 89)
"bootconfig flags reboot" (page 89)
"no bootconfig flags reboot" (page 90)
"bootconfig flags rlogind" (page 90)
"no bootconfig flags rlogind" (page 90)
"bootconfig flags savetostandby" (page 90)
"no bootconfig flags savetostandby" (page 90)
"bootconfig flags telnetd" (page 91)
"bootconfig flags telnetd" (page 91)
"no bootconfig flags telnetd" (page 91)
"bootconfig flags tftpd" (page 91)
"no bootconfig flags tftpd" (page 91)
"bootconfig flags trace-logging" (page 91)
"no bootconfig flags trace-logging" (page 92)
"bootconfig flags verify-config" (page 92)
"no bootconfig flags verify-config" (page 92)
"bootconfig flags wdt" (page 92)
"no bootconfig flags wdt" (page 93)
"bootconfig host ftp-debug" (page 93)
"no bootconfig host ftp-debug" (page 93)
"bootconfig host password" (page 93)
"bootconfig host password" (page 93)
"bootconfig host tftp-debug" (page 94)
"no bootconfig host tftp-debug" (page 94)
"bootconfig host tftp-hash" (page 94)
"no bootconfig host tftp-hash" (page 94)
"bootconfig host tftp-rexmit" (page 95)
"bootconfig host tftp-timeout" (page 95)

Bootconfig Command
"bootconfig host user" (page 95)
"bootconfig master" (page 96)
"bootconfig master" (page 96)
"bootconfig net autonegotiate" (page 96)
"bootconfig net autonegotiate" (page 96)
"no bootconfig net autonegotiate" (page 96)
"bootconfig net bootp" (page 97)
"no bootconfig net bootp" (page 97)
"bootconfig net fullduplex" (page 97)
"no bootconfig net fullduplex" (page 98)
"bootconfig net ip" (page 98)
"bootconfig net restart" (page 99)
"boot net route" (page 100)
"bootconfig net speed" (page 100)
"bootconfig net tftp" (page 101)
"bootconfig sio" (page 102)
"bootconfig sio baud" (page 103)
"bootconfig sio 8databits" (page 103)
"no bootconfig sio 8databits" (page 103)
"bootconfig sio disable" (page 104)
"bootconfig sio enable" (page 104)
"bootconfig sio info" (page 104)
"bootconfig sio mode" (page 104)
"bootconfig sio mtu" (page 105)
"bootconfig sio my-ip" (page 105)
"bootconfig sio peer-ip" (page 106)
"bootconfig sio pppfile" (page 106)
"bootconfig sio restart" (page 107)
"bootconfig sio slip-compression" (page 107)
"no bootconfig sio slip-compression" (page 107)
"bootconfig sio slip-rx-compression" (page 108)
"no bootconfig sio slip-rx-compression" (page 108)
"show bootconfig" (page 108)
"show bootconfig choice" (page 109)
"show bootconfig cli" (page 109)

Bootconfig Command
"show bootconfig config" (page 109)
"show bootconfig flags" (page 110)
"show bootconfig host" (page 110)
"show bootconfig info" (page 110)
"show bootconfig master" (page 110)
"show bootconfig net" (page 110)
"show bootconfig sio" (page 111)
"show bootconfig tz" (page 111)

boot choice license-file

This command loads the license file to the chassis.

Syntax

boot choice <boot choice> license-file <file>

Parameters

This command includes the following parameters:

bootfollowed by:	
choice<boot choice>	Specifies the order in which the specified boot path is accessed when the switch is rebooted: primary, secondary, or tertiary.
license-file <file>	The source can be Flash memory, a PCMCIA card, or a remote TFTP server. • /flash/<file_name> • /pcmcia/<file_name> • <a.b.c.d.>:<file_name>

Command mode

Global configuration mode

bootconfig bootp

Use this command to set or clear the bootp CLI configuration commands.

Syntax

bootconfig bootp

Parameters

This command includes the following options:

bootconfig bootp **followed by:**	
image-name <name> [<slot>]	Set or clear the bootp CLI configuration commands. • **name** is the bootfile to set or clear. If the name is set as default, then the configuration will be cleared. • **slot** is slot number to use for the bootfile. Acceptable values range from 1 to 10.

Command mode

Global configuration mode

bootconfig choice config-file

Use this command to select runtime and boot configuration file choices or change the order in which the boot sources (flash and PCMCIA card) are accessed.

Syntax

bootconfig choice <boot-choice> config-file <file>

Parameters

This command includes the following options:

bootconfig choice **followed by:**	
<boot-choice>	Specifies the order in which the selected boot device is accessed when you reboot the switch. The options are: **primary, secondary,** and **tertiary**. The default order is to access the PCMCIA card first, and then the onboard flash.
config-file <file>	Specifies the boot configuration device and file name. The range of values is up to 256 characters including the path.

Command mode

Global configuration mode

bootconfig choice image-file

Use this command to select runtime and boot image file choices or change the order in which the boot sources (flash and PCMCIA card) are accessed.

Syntax

```
bootconfig choice <boot-choice> image-file <file>
[config-file <file> ]
```

Parameters

This command includes the following options:

bootconfig choice **followed by:**	
<boot-choice>	Specifies the order in which the selected boot device is accessed when you reboot the switch. The options are: **primary, secondary,** and **tertiary**. The default order is to access the PCMCIA card first, and then the onboard flash.
image-file <file>	Specifies the boot image device and file name. The range of values is up to 256 characters including the path.
[config-file <file>]	Specifies the boot configuration device and file name. The range of values is up to 256 characters including the path.

Command mode

Global configuration mode

bootconfig cli more

Use this command to set the output display for the Command Line Interface (CLI) to one line at a time.

Syntax

```
bootconfig cli more
```

Command mode

Global configuration mode

no bootconfig cli more

Use this command to set the output display for the Boot Monitor Command Line Interface (CLI) to continuous scrolling.

Syntax

```
no bootconfig cli more
```

Command mode

Global configuration mode

bootconfig cli prompt

Use this command to change the Boot Monitor prompt for the Command Line Interface (CLI) to the defined string.

Syntax

```
bootconfig cli prompt <value>
```

where

value specifies the prompt text. The range of values is an ASCII string of 1 to 32 characters.

Note: Enclose the string in quotation marks if it has spaces between characters.

Command mode

Global configuration mode

bootconfig cli rlogin-sessions

Use this command to specify the allowable number of inbound remote login sessions to the Boot Monitor Command Line Interface (CLI).

Syntax

```
bootconfig cli rlogin-sessions <value>
```

where

<value> specifies the allowable number of remote login sessions. The range of values is 0 to 8. The default is 8.

Command mode

Global configuration mode

bootconfig cli screenlines

Use this command to specify the number of lines in the output display for the Boot Monitor Command Line Interface (CLI).

Syntax

```
bootconfig cli screenlines <value>
```

where

<value> specifies the number of lines in the output display. The range of values is 1 to 64. The default is 23.

Command mode

Global configuration mode

bootconfig cli telnet-sessions

Use this command to specify the allowable number of inbound telnet sessions to the Boot Monitor Command Line Interface (CLI).

Syntax

```
bootconfig cli telnet-sessions <value>
```

where

<value> specifies the allowable number of telnet sessions. The range of values is 0 to 8. The default is 8.

Command mode

Global configuration mode

bootconfig cli timeout

Use this command to specify the idle timeout period before automatic logout for Command Line Interface (CLI) sessions.

Syntax

```
bootconfig cli timeout <seconds>
```

where

<seconds> specifies the timeout period in seconds. The range of values is 0 to 65536.

Command mode

Global configuration mode

bootconfig delay

Use this command to set the number of seconds a standby CPU should wait (delay) before trying to become the master CPU for booting the switch. This command applies only during a cold start and does not apply to a failover start.

Syntax

bootconfig delay <seconds>

where

<seconds> specifies the number of seconds of delay. The default range is 0-255 seconds.

Command mode

Global configuration mode

bootconfig flags

Use this command to set system flags. You enable or disable access services by setting flags. Changes to certain flags (factorydefaults, ftpd, tftpd, wdt) take effect only after you save changes to the boot configuration file and reset the switch.

Syntax

bootconfig flags

Parameters

This command includes the following options:

bootconfig flags **followed by:**	
autoboot	Sets the switch to automatically run the run-time image after being reset. Setting to no autoboot is useful for some debugging tasks. The default is **autoboot**.
block-snmp	Blocks access to the SNMP protocol. The default is no blocking.
daylight-saving-time	Enables Daylight Saving Time on the switch. The default is disabled.
debug-config	Enables run-time debugging of the configuration file. The default is no run-time debugging.
debugmode	Stops switch in debug mode following a fatal error. Debug mode provides information equivalent to the **trace** commands. A list of options is displayed that allows you to select a software module to debug. The default is no **debugmode**.

bootconfig flags **followed by:**	
factorydefaults	Sets the runtime switch configuration to factory default settings. The default is to reset.
ftpd	Enables FTP server on the switch. To enable FTP, make sure the **no bootconfig flags tftpd** command is set. The default is no FTP.
jumboframe	Enables jumbo frames. The default is no jumbo frames.
logging	Enables system logging to a file on the PCMCIA card. The default is system logging.
nncli	Enables NNCLI services on a switch. ***Note:*** Ethernet Routing Switch Command Line Interface (CLI) services are provided when NNCLI is disabled.
reboot	Enables the automatic reboot on a fatal error. The default is to reboot. This command is equivalent to the **debugmode** command.
rlogind	Enables the rlogin/rsh server. The default is disabled.
savetostandby	Saves the config/bootconfig setup to a standby CPU, if one is available. The default is disabled.
sshd	Enables the secure shell (SSH) daemon. the default is disabled.
telnetd	Enables the Telnet server. The default is disabled.
tftpd	Enables the TFTP server. The default is disabled.
trace-logging	Enables system tracing to a file on the PCMCIA card. The default is disabled.

bootconfig flags **followed by:**	
verify-config	Enables syntax checking of the configuration file and prevents execution of the file if an error is found. The factory default configuration file is loaded instead. The default is enabled.
wdt	Enables the hardware watchdog timer, which monitors a hardware circuit. The watchdog timer reboots the switch based on software errors. The default is enabled.

Command mode

Global configuration mode

no bootconfig flags

Use this command to set system flags. You enable or disable access services by setting flags. Changes to certain flags (factorydefaults, ftpd, tftpd, wdt) take effect only after you save changes to the boot configuration file and reset the switch.

Syntax

```
no bootconfig flags
```

Parameters

This command includes the following options:

no bootconfig flags **followed by:**	
autoboot	Sets the switch to automatically stop at the monitor prompt after being reset. Setting to no autoboot is useful for some debugging tasks. The default is **autoboot**.
block-snmp	Unblocks access to the SNMP protocol. To use this command, disable SSH secure mode first.
daylight-saving-time	Disables Daylight Saving Time on the switch.

no bootconfig flags **followed by:**	
debugmode	Automatically reboots the switch following a fatal error. The default is **no debugmode**.
debug-config	Disables run-time debugging of the configuration file.
factorydefaults	Disables reset of the switch configuration to factory default settings.
ftpd	Disables FTP server on the switch.
jumboframe	Enables jumbo frames. The default is no jumbo frames.
logging	Disables system logging to a file on the PCMCIA card.
nncli	Disables NNCLI services on a switch. ***Note:*** Ethernet Routing Switch Command Line Interface (CLI) services are provided when NNCLI is disabled.
reboot	Disables automatic reboot on fatal errors.
rlogind	Disables the rlogin/rsh server.
sshd	Enables the SSH daemon. The default is disabled.
savetostandby	Disables saving the config/bootconfig setup to a standby CPU, even if one is available.
telnetd	Disables the Telnet server.
tftpd	Disables the TFTP server.

no bootconfig flags **followed by:**	
trace-logging	Disables system tracing to a file on the PCMCIA card.
verify-config	Disables syntax checking of the configuration file. Execution of the file occurs even if an error is found.
wdt	Disables the hardware watchdog timer, which monitors a hardware circuit. The watchdog timer reboots the switch based on software errors.

Command mode

Global configuration mode

bootconfig flags autoboot

Use this command to set the switch to automatically run the run-time image after being reset. Setting to **no autoboot** is useful for some debugging tasks. The default is **autoboot**.

Syntax

bootconfig flags autoboot

Command mode

Global configuration mode

no bootconfig flags autoboot

Use this command to set the switch to automatically stop at the monitor prompt after being reset. Setting to **no autoboot** is useful for some debugging tasks. The default is **autoboot**.

Syntax

no bootconfig flags autoboot

Command mode

Global configuration mode

bootconfig flags block-snmp

Use this command to block switch access to the SNMP protocol. The default is no blocking.

Syntax

bootconfig flags block-snmp

Command mode

Global configuration mode

no bootconfig flags block-snmp

Use this command to allow switch access to the SNMP protocol. To use this command, disable Secure Shell (SSH) secure mode first. The default is no blocking.

Syntax

```
no bootconfig flags block-snmp
```

Command mode

Global configuration mode

bootconfig flags daylight-saving-time

Use this command to enable Daylight Savings Time on the switch. The default is disabled.

Syntax

```
bootconfig flags daylight-saving-time
```

Command mode

Global configuration mode

no bootconfig flags daylight-saving-time

Use this command to disable Daylight Savings Time on the switch. The default is disabled

Syntax

```
no bootconfig flags daylight-saving-time
```

Command mode

Global configuration mode

bootconfig flags debug-config

Use this command to enable run-time debugging of the configuration file. The default is no run-time debugging.

Syntax

```
bootconfig flags debug-config
```

Command mode

Global configuration mode

no bootconfig flags debug-config

Use this command to disable run-time debugging of the configuration file. The default is no run-time debugging.

Syntax

```
no bootconfig flags debug-config
```

Command mode

Global configuration mode

bootconfig flags debugmode

Use this command to stop the switch in debug mode following a fatal error. Debug mode provides information equivalent to the **trace** commands. A list of options is displayed that allows you to select a software module to debug. The default is no debug mode.

Syntax

```
bootconfig flags debugmode
```

Command mode

Global configuration mode

no bootconfig flags debugmode

Use this command to automatically reboot the switch following a fatal error. The default is no debug mode.

Syntax

```
no bootconfig flags debugmode
```

Command mode

Global configuration mode

bootconfig flags factorydefaults

Use this command to reset the runtime switch configuration to factory default settings. Changes to the factorydefaults flag take effect only after you save changes to the boot configuration file and reset the switch. The default is to reset.

Syntax

```
bootconfig flags factorydefaults
```

Command mode

Global configuration mode

no bootconfig flags factorydefaults

Use this command to disable reset of the switch boot configuration to factory default settings. Changes to the factorydefaults flag take effect only after you save changes to the boot configuration file and reset the switch. The default is to reset.

Syntax

```
no bootconfig flags factorydefaults
```

Command mode

Global configuration mode

bootconfig flags ftpd

Use this command to enable the FTP (File Transfer Protocol) server on the switch. To enable FTP, ensure that the **no bootconfig flags tftpd** command is set. Changes to the FTP flag take effect only after you save changes to the boot configuration file and reset the switch. The default is no FTP.

Syntax

```
bootconfig flags ftpd
```

Command mode

Global configuration mode

no bootconfig flags ftpd

Use this command to disable the FTP (File Transfer Protocol) server on the switch. Changes to the FTP flag take effect only after you save changes to the boot configuration file and reset the switch. The default is no FTP.

Syntax

```
no bootconfig flags ftpd
```

Command mode

Global configuration mode

bootconfig flags info

Use this command to display information about the current boot configuration flag settings.

```
bootconfig flags info
```

Command mode

Global configuration mode

bootconfig flags logging

Use this command to enable system logging to a file on the PCMCIA card. The default is system logging.

Syntax

```
bootconfig flags logging
```

Command mode

Global configuration mode

no bootconfig flags logging

Use this command to disable system logging to a file on the PCMCIA card. The default is system logging.

Syntax

```
no bootconfig flags logging
```

Command mode

Global configuration mode

bootconfig flags nncli

Use this command to enable NNCLI services on the switch.

Note: Ethernet Routing Switch Command Line Interface (CLI) services are provided when NNCLI is disabled.

Syntax

```
bootconfig flags nncli
```

Command mode

Global configuration mode

no bootconfig flags nncli

Use this command to disable NNCLI services on the switch.

Note: Ethernet Routing Switch Command Line Interface (CLI) services are provided when NNCLI is disabled.

Syntax

```
no bootconfig flags nncli
```

Command mode

Global configuration mode

bootconfig flags reboot

Use this command to enable the automatic reboot on a fatal error. The default is to reboot.

Syntax

```
bootconfig flags reboot
```

Command mode

Global configuration mode

no bootconfig flags reboot

Use this command to disable the automatic reboot on a fatal error. The default is to reboot.

Syntax

```
no bootconfig flags reboot
```

Command mode

Global configuration mode

bootconfig flags rlogind

Use this command to enable the rlogin/rsh server. The default is disabled.

Syntax

```
bootconfig flags rlogind
```

Command mode

Global configuration mode

no bootconfig flags rlogind

Use this command to disable the rlogin/rsh server. The default is disabled.

Syntax

```
no bootconfig flags rlogind
```

Command mode

Global configuration mode

bootconfig flags savetostandby

Use this command to save the config/bootconfig setup to a standby CPU, if one is available. The default is disabled.

Syntax

```
bootconfig flags savetostandby
```

Command mode

Global configuration mode

no bootconfig flags savetostandby

Use this command to disable saving the config/bootconfig setup to a standby CPU, even if one is available. The default is disabled.

Syntax

```
no bootconfig flags savetostandby
```

Command mode

Global configuration mode

bootconfig flags telnetd

Use this command to enable the Telnet server. The default is disabled.

Syntax

```
bootconfig flags telnetd
```

Command mode

Global configuration mode

no bootconfig flags telnetd

Use this command to disable the Telnet server. The default is disabled.

Syntax

```
no bootconfig flags telnetd
```

Command mode

Global configuration mode

bootconfig flags tftpd

Use this command to enable the TFTP (Trivial File Transfer Protocol) server. To enable TFTP, ensure that the **`no bootconfig flags ftpd`** command is set. Changes to the TFTP flag take effect only after you save changes to the boot configuration file and reset the switch. The default is no TFTP.

Syntax

```
bootconfig flags tftpd
```

Command mode

no bootconfig flags tftpd

Use this command to disable the TFTP (Trivial File Transfer Protocol) server. Changes to the TFTP flag take effect only after you save changes to the boot configuration file and reset the switch. The default is no TFTP.

Syntax

```
no bootconfig flags tftpd
```

Command mode

Global configuration mode

bootconfig flags trace-logging

Use this command to enable system tracing to a file on the PCMCIA card. The default is disabled.

Syntax

```
bootconfig flags trace-logging
```

Command mode

Global configuration mode

no bootconfig flags trace-logging

Use this command to disable system tracing to a file on the PCMCIA card. The default is disabled.

Syntax

```
no bootconfig flags trace-logging
```

Command mode

Global configuration mode

bootconfig flags verify-config

Use this command to enable syntax checking of the configuration file and prevent execution of the file, if an error is found. The factory default configuration file is loaded instead. The default is disabled.

Syntax

```
bootconfig flags verify-config
```

Command mode

Global configuration mode

no bootconfig flags verify-config

Use this command to disable syntax checking of the configuration file. Execution of the file occurs, even if an error is found. The default is disabled.

Syntax

```
no bootconfig flags verify-config
```

Command mode

Global configuration mode

bootconfig flags wdt

Use this command to enable the watchdog timer, which monitors a hardware circuit. The watchdog timer reboots the switch based on software errors. Changes to the wdt flag take effect only after you save changes to the boot configuration file and reset the switch. The default is enabled.

Syntax

```
bootconfig flags wdt
```

Command mode

Global configuration mode

no bootconfig flags wdt

Use this command to disable the watchdog timer, which monitors a hardware circuit. The watchdog timer reboots the switch based on software errors. Changes to the wdt flag take effect only after you save changes to the boot configuration file and reset the switch. The default is enabled.

Syntax

```
no bootconfig flags wdt
```

Command mode

Global configuration mode

bootconfig host ftp-debug

Use this command to enable the debug mode for FTP/FTPd (File Transfer Protocol) transfers with the remote host login. If you enable debug mode, debug messages are displayed on the management console screen. The default is disabled.

Syntax

```
bootconfig host ftp-debug
```

Command mode

Global configuration mode

no bootconfig host ftp-debug

Use this command to disable the debug mode for FTP/FTPd (File Transfer Protocol) transfers with the remote host login. If you disable the debug mode, debug messages are not displayed on the management console screen. The default is disabled.

Syntax

```
no bootconfig host ftp-debug
```

Command mode

Global configuration mode

bootconfig host password

Use this command to set the password for FTP (File Transfer Protocol) transfers with the remote host. When this password is set, a login with the password is required to perform FTP transfers with the remote host.

Note: This password must match the password for the FTP server, or FTP operation fails.

Syntax

```
bootconfig host password <value>
```

where

value specifies the password. The range of values is a string of up to 16 characters.

Command mode

Global configuration mode

bootconfig host tftp-debug

Use this command to enable the debug mode for TFTP (Trivial File Transfer Protocol) transfers with the remote host. If you enable the debug mode, debug messages are displayed on the management console screen. The default is disabled.

Syntax

```
bootconfig host tftp-debug
```

Command mode

Global configuration mode

no bootconfig host tftp-debug

Use this command to disable the debug mode for TFTP (Trivial File Transfer Protocol) transfers with the remote host. If you disable the debug mode, debug messages are not displayed on the management console screen. The default is disabled.

Syntax

```
no bootconfig host tftp-debug
```

Command mode

Global configuration mode

bootconfig host tftp-hash

Use this command to enable TFTP (Trivial File Transfer Protocol) hash bucket display for the remote host. The default is disabled.

Syntax

```
bootconfig host tftp-hash
```

Command mode

Global configuration mode

no bootconfig host tftp-hash

Use this command to disable TFTP (Trivial File Transfer Protocol) hash bucket display for the remote host. The default is disabled.

Syntax

```
no bootconfig host tftp-hash
```

Command mode

Global configuration mode

bootconfig host tftp-rexmit

Use this command to set the TFTP (Trivial File Transfer Protocol) retransmission timeout for remote host.

Syntax

```
bootconfig host tftp-rexmit <seconds>
```

where

seconds specifies the retransmission timeout in seconds. The range of values is 1 to 2147483647.

Command mode

Global configuration mode

bootconfig host tftp-timeout

Use this command to set the TFTP (Trivial File Transfer Protocol) timeout for the remote host.

Syntax

```
bootconfig host tftp-timeout <seconds>
```

where

seconds specifies the timeout in seconds. The range of values is 1 to 2147483647.

Command mode

Global configuration mode

bootconfig host user

Use this command to set the remote host user login name.

Syntax

```
bootconfig host <value>
```

where

value specifies the remote user login name. The range of values is a string of up to 16 characters.

Command mode

Global configuration mode

bootconfig master

Use this command to specify which CPU becomes master when the switch is turned on. The master CPU performs a loopback test to test the switch fabric.

Syntax

bootconfig master <cpu-slot>

where

<cpu-slot><cpu-slot> specifies the module position for the master CPU. The options are slot 5 or slot 6. The default is slot 5.

Command mode

Global configuration mode

bootconfig net autonegotiate

Use this command to enable autonegotiation for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The defaults are:

- **mgmt** - enabled
- **cpu2cpu** - disabled

Syntax

bootconfig net <cpu-net-port> autonegotiate

where

<cpu-net-port> specifies the CPU network port. The options are **mgmt**, **cpu2cpu**.

Command mode

Global configuration mode

no bootconfig net autonegotiate

Use this command to disable autonegotiation for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The defaults are:

- **mgmt** - enabled
- **cpu2cpu** - disabled

Syntax

no bootconfig net <cpu-net-port> autonegotiate

where

<cpu-net-port> specifies the CPU network port. The options are: **mgmt, cpu2cpu**.

Command mode

Global configuration mode

bootconfig net bootp

Use this command to enable the Bootstrap Protocol (Bootp) for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The default is enabled for all specified port types.

Syntax

bootconfig net <cpu-net-port> bootp

where

<cpu-net-port> specifies the CPU network port. The options are **mgmt**, **cpu2cpu**.

Command mode

Global configuration mode

no bootconfig net bootp

Use this command to disable the Bootstrap Protocol (Bootp) for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The default is enabled for all specified port types.

Syntax

no bootconfig net <cpu-net-port> bootp

where

<cpu-net-port> specifies the CPU network port. The options are: **mgmt, cpu2cpu**.

Command mode

Global configuration mode

bootconfig net fullduplex

Use this command to enable the full-duplex mode for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The defaults are:

- **mgmt** - disabled
- **cpu2cpu** - enabled

Note: Use the **bootconfig net mgmt ip <ipaddr> <mask>** command to assign an IP address to the switch.

Syntax

bootconfig net <cpu-net-port> fullduplex

where

<cpu-net-port> specifies the CPU network port. The options are **mgmt**, **cpu2cpu**.

Command mode

Global configuration mode

no bootconfig net fullduplex

Use this command to disable the full-duplex mode for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port. The defaults are:

- **mgmt** - disabled
- **cpu2cpu** - enabled

Syntax

no bootconfig net <cpu-net-port> fullduplex

where

<cpu-net-port> specifies the CPU network ports. The options are: **mgmt, cpu2cpu**.

Command mode

Global configuration mode

bootconfig net ip

Use this command to assign an IP address and network mask to the specified CPU network port device. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

Note: Use the **bootconfig net mgmt ip <ipaddr> <mask>** command to assign an IP address to the switch.

Syntax

bootconfig net <cpu-net-port> ip <ipaddr> <mask> <cpu-slot value>

Parameters

This command includes the following options:

bootconfig net <cpu-net-port> ip **followed by:**	
<cpu-net-port>	Specifies the CPU network port. The options are: **mgmt, cpu2cpu**.
<ipaddr> <mask>	Assigns an IP address or mask for the specified port. The options are: • **a.b.c.d/x** • **a.b.c.d/x.x.x.x** • **default** (The default is 0.0.0.0.)
<cpu-slot value>	Specifies the slot position of the 8393SF module. The options are slot 5 or slot 6. If you do not specify a slot number for the IP address, the IP address is assigned to the currently active management module.

Command mode

Global configuration mode

bootconfig net restart

Use this command to restart the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

> ***Note:*** Use the **bootconfig net mgmt ip <ipaddr> <mask>** command to assign an IP address to the switch.

Syntax

bootconfig net <cpu-net-port> restart

where

<cpu-net-port> specifies the CPU network port. The options are **mgmt**, **cpu2cpu**.

Command mode

Global configuration mode

boot net route

Use this command to set a route for the specified CPU network port. The three network port types are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

> ***Note:*** Use the **`bootconfig net mgmt ip <ipaddr> <mask>`** command to assign an IP address to the switch.

Syntax

`boot net <cpu-net-port> route [add|del|net] <netaddr> <gateway>`

Parameters

This command includes the following options:

`bootconfig net <cpu-net-port> route` **followed by:**	
`<cpu-net-port>`	Specifies the CPU network port. The options are: **`mgmt, cpu2cpu`**.
`[add|del|net]`	Performs the selected action on the specified port: • Adds the specified route for the selected port. • Deletes the specified route for the selected port. • Changes the specified route for the selected port to a network route.
`<netaddr>`	Specifies the IP address of the destination network for the selected port.
`<gateway>`	Specifies the IP address of the gateway for the selected port.

Command mode

Global configuration mode

bootconfig net speed

Use this command to set the connection speed for the specified CPU network port. The three network ports are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

Note: Use the **bootconfig net mgmt ip <ipaddr> <mask>** command to assign an IP address to the switch.

Syntax

bootconfig net <cpu-net-port> speed

Parameters

This command includes the following options:

bootconfig net <cpu-net-port> speed **followed by:**	
<cpu-net-port>	Specifies the CPU network port. The options are: **mgmt, cpu2cpu**.
<10|100>	Sets the connection speed to 10 Mb/s or 100 Mb/s. The defaults are: • **mgmt** - 10 Mb/s • **cpu2cpu** - 100 Mb/s

Command mode

Global configuration mode

bootconfig net tftp

Use this command to specify a TFTP (Trivial File Transfer Protocol) server for the CPU network port. The three network ports are the management port, the CPU port, and the PCMCIA card, if it is acting as a network port.

Note: Use the **bootconfig net mgmt ip <ipaddr> <mask>** command to assign an IP address to the switch.

Syntax

bootconfig net <cpu-net-port> tftp <ipaddr>

Parameters

This command includes the following options:

bootconfig net <cpu-net-port> tftp **followed by:**	
<cpu-net-port>	Specifies the CPU network port. The options are: **mgmt, cpu2cpu**.
<ipaddr>	Specifies the IP address of the TFTP server in the format a.b.c.d.

Command mode

Global configuration mode

bootconfig sio

Use this command to configure the CPU serial input/output (sio) port devices.

Syntax

bootconfig sio [8databits <true|false>] [baud <rate>] [restart]

Parameters

This command includes the following options:

bootconfig sio <cpu-sio-port> **followed by:**	
[8databits <true|false>]	Specifies the data bits per byte that the software interprets. The options are: • **true** (8 data bits per byte) • **false** (7 data bits per byte) The default is **false**.
[baud <rate>]	Specifies the baud rate for the selected port. The default is **9600**.
[restart]	Shuts down and reinitializes the specified CPU serial port.

Command mode

Global configuration mode

bootconfig sio 8databits

Use this command to specify that the software interprets eight data bits per byte for the selected CPU serial input/output (sio) port devices. The default is seven data bits per byte.

Syntax

```
bootconfig sio 8databits
```

Command mode

Global configuration mode

no bootconfig sio 8databits

Use this command to specify seven data bits per byte for the software to interpret for the CPU serial input/output (sio) port.

Syntax

```
no bootconfig sio 8databits
```

Command mode

Global configuration mode

bootconfig sio baud

Use this command to specify the baud rate for the selected CPU serial input/output (sio) port.

Syntax

```
bootconfig sio baud <rate>
```

Parameters

This command includes the following options:

`bootconfig sio <cpu-sio-port> baud` **followed by:**	
`<rate>`	Specifies the baud rate for the port. The default is 9600.

Command mode

Global configuration mode

bootconfig sio disable

Use this command to disable the selected CPU serial input/output (sio) port.

Syntax

```
bootconfig sio disable
```

Command mode

Global configuration mode

bootconfig sio enable

Use this command to enable the selected CPU serial input/output (sio) port.

Syntax

```
bootconfig sio enable
```

Command mode

Global configuration mode

bootconfig sio info

Use this command to display configuration information about the specified CPU serial input/output (sio) port.

Syntax

```
bootconfig sio info
```

Command mode

Global configuration mode

bootconfig sio mode

Use this command to specify the communication mode the selected CPU serial input/output (sio) port device.

Syntax

```
bootconfig sio mode <ascii|slip|ppp>
```

Parameters

This command includes the following options:

bootconfig sio <cpu-sio-port> mode **followed by:**	
<ascii|slip|ppp>	Specifies the communication mode for the serial port. The default is **ascii**. To configure the Console port, set the mode to **ascii**. If you are configuring the Modem port, you can set the port to use the same SLIP or PPP communication mode as the modem.

Command mode

Global configuration mode

bootconfig sio mtu

Use this command to specify the size of the maximum transmission unit (mtu) for a point-to-point link with the selected CPU serial input/output (sio) port device.

Syntax

bootconfig sio mtu <bytes>

Parameters

This command includes the following options:

bootconfig sio <cpu-sio-port> mtu **followed by:**	
<bytes>	Specifies the mtu size in bytes. The range of values is 0 to 2048. The default is **0**.

Command mode

Global configuration mode

bootconfig sio my-ip

Use this command to specify the near-end IP address on a point-to-point link with the selected CPU serial input/output (sio) port device.

Syntax

```
bootconfig sio my-ip <ipaddr>
```

Parameters

This command includes the following options:

bootconfig sio <cpu-sio-port> my-ip **followed by:**	
<ipaddr>	Specifies the near-end IP address on a point-to-point link. The default is 0.0.0.0.

Command mode

Global configuration mode

bootconfig sio peer-ip

Use this command to specify the peer IP address on a point-to-point link with the selected CPU serial input/output (sio) port device.

Syntax

```
bootconfig sio peer-ip <ipaddr>
```

Parameters

This command includes the following options:

bootconfig sio <cpu-sio-port> peer-ip **followed by:**	
<ipaddr>	Specifies the peer IP address on a point-to-point link. The default is 0.0.0.0.

Command mode

Global configuration mode

bootconfig sio pppfile

Use this command to specify which file to use for PPP initialization parameters for the selected CPU serial input/output (sio) port.

Syntax

```
bootconfig sio pppfile <file>
```

Parameters

This command includes the following options:

bootconfig sio <cpu-sio-port> pppfile **followed by:**	
<file>	Specifies which file to use for PPP initialization parameters. The options are: • **a.b.c.d: <file>** • **/pcmcia/ <file>** • **/flash/ <file>**

Command mode

Global configuration mode

bootconfig sio restart

Use this command to shut down and reinitialize the selected CPU serial input/output (sio) port.

Syntax

```
bootconfig sio restart
```

Command mode

Global configuration mode

bootconfig sio slip-compression

Use this command to enable TCP/IP header compression for the selected CPU serial input/output (sio) port. The default is disabled.

Syntax

```
bootconfig sio slip-compression
```

Command mode

Global configuration mode

no bootconfig sio slip-compression

Use this command to disable TCP/IP header compression for the selected CPU serial input/output (sio) port. The default is disabled.

Syntax

```
no bootconfig sio slip-compression
```

Command mode

Global configuration mode

bootconfig sio slip-rx-compression

Use this command to enable TCP/IP header compression on the receive packet for the selected CPU serial input/output (sio) port. The default is disabled.

Syntax

```
bootconfig sio slip-rx-compression
```

Command mode

Global configuration mode

no bootconfig sio slip-rx-compression

Use this command to disable TCP/IP header compression on the receive packet for the selected CPU serial input/output (sio) port. The default is disabled.

Syntax

```
no bootconfig sio slip-rx-compression
```

Command mode

Global configuration mode

show bootconfig

Use this command to display the current configuration of the Boot Monitor and the Boot Monitor CLI.

Syntax

```
show bootconfig
```

Parameters

This command includes the following options:

`show bootconfig` **followed by:**	
`bootp`	
`choice`	Displays the current boot configuration choices.
`cli`	Displays the current Boot Monitor CLI configuration.

show bootconfig **followed by:**	
config	Displays the current Boot Monitor configuration.
flags	Displays the current flag settings for the switch.
host	Displays the current host configuration.
info	Displays information about the switch boot image.
master	Displays the slot where the Master CPU resides and the settings for the **delay** and **multicast** commands.
net	Displays the current configuration of the CPU network ports.
sio	Displays the current configuration of the CPU serial ports.
tz	Displays the switch's current time zone settings.

Command mode

Privileged EXEC mode

show bootconfig choice

Use this command to display the current boot configuration choices.

Syntax

show bootconfig choice

Command mode

Privileged EXEC mode

show bootconfig cli

Use this command to display the current configuration of the Boot Monitor CLI.

Syntax

show bootconfig cli

Command mode

Privileged EXEC mode

show bootconfig config

Use this command to display the current configuration of the Boot Monitor.

Syntax

```
show bootconfig config
```

Command mode

Privileged EXEC mode

show bootconfig flags

Use this command to display the current flag settings for the switch.

Syntax

```
show bootconfig flags
```

Command mode

Privileged EXEC mode

show bootconfig host

Use this command to display the current configuration of the host.

Syntax

```
show bootconfig host
```

Command mode

Privileged EXEC mode

show bootconfig info

Use this command to display information about the switch boot image.

Syntax

```
show bootconfig info
```

Command mode

Privileged EXEC mode

show bootconfig master

Use this command to display the slot where the Master CPU resides and to display the settings for the **`bootconfig delay`** and **`bootconfig multicast`** commands.

Syntax

```
show bootconfig master
```

Command mode

Privileged EXEC mode

show bootconfig net

Use this command to display the current configuration of the CPU network ports.

Syntax

```
show bootconfig net
```

Command mode

Privileged EXEC mode

show bootconfig sio

Use this command to display the current configuration of the CPU serial ports.

Syntax

```
show bootconfig sio
```

Command mode

Privileged EXEC mode

show bootconfig tz

Use this command to display the switch's current time zone settings.

Syntax

```
show bootconfig tz
```

Command mode

Privileged EXEC mode

System management commands

This chapter describes the NNCLI system management commands and their parameters.

System Management Command
"portlock" (page 124)
"prompt" (page 124)
"rlogin-sessions" (page 124)
"screenlines" (page 125)
"show autotopology" (page 125)
"show basic config" (page 125)
"show link-flap-detect" (page 126)
"show logging config" (page 126)
"show logging file" (page 126)
"show log filter" (page 127)
"show slot" (page 127)
"show sys hash-calc mltindex ip dest-mac dest-ip src-mac src-ip src-port mlt" (page 128)
"show sys hash-calc mltindex non-ip dest-mac src-mac src-port mlt" (page 128)
"show sys hash-calc mltindex ip-mcast source group vlan-id src-port mlt" (page 129)
"show sys hash-calc mltindex ip-mcast source group vlan-id src-port mlt" (page 129)
"show sys-info" (page 131)
"show sys perf" (page 131)
"show sys sw" (page 132)
"shutdown" (page 132)
"no shutdown" (page 132)
"sys-action cpuswitchover" (page 132)
"sys-action resetconsole" (page 133)
"sys-action resetcounters" (page 133)
"udpsrc-by-vip" (page 133)
"no udpsrc-by-vip" (page 133)

auto-recover-delay

Use this command to configure the auto recovery delay timer for ports.

Syntax

```
auto-recover-delay<5-3600>
```

where

`<5-3600>` is the auto recovery delay time in seconds. The default is 30.

Command mode

Global configuration mode

default auto-recover-delay

Use this command to set the auto recovery delay timer to default values.

Syntax

```
default auto-recover-delay
```

Command mode

Global configuration mode

no auto-recover-delay

Use this command set the auto recovery delay timer to default values.

Syntax

```
no auto-recovery-delay
```

Command mode

Global configuration mode

autotopology

Use this command to turn the topology feature on. The topology feature generates topology packets used by network management software. When this feature is off, the topology table is not generated. The default is on.

Syntax

```
autotopology
```

Command mode

Global configuration mode

no autotopology

Use this command to turn the topology feature off. The topology feature generates topology packets used by network management software. When this feature is off, the topology table is not generated. The default is on.

Syntax

```
no autotopology
```

Command mode

Global configuration mode

banner

Use this command to add lines of text to the NNCLI login banner.

Syntax

banner <string>

where

string specifies the lines of text. The range of values is an ASCII string of 1 to 1024 characters.

Note: Enclose the string in quotation marks if it has spaces between characters.

Parameters

This command includes the following options:

banner **followed by:**	
custom	Enables the use of the custom banner as defined by `banner` <*banner*>.
motd [displaymotd | <*motd*>]	Enables the display of a Message of the Day (MoTD) following the user login. The MoTD is from 1- 1536 characters.
static	Enables the default Nortel banner.
<*banner*>	Enables the user of a custom banner defined by the user. The length is from 0- 80 characters.

Command mode

Global configuration mode

no banner

Use this command to disable the display of a banner following the user login.

Syntax

no banner <motd> [displaymotd]

where

<motd> specifies a message from 1- 1536 characters.

clock set

Use this command to set the calendar time in the form of hour, minute, second, month, day, and year. You set the time zone using the **bootconfig tz** command at the Global configuration level.

Syntax

clock set <MMddyyyyhhmmss>

where

<MMddyyyyhhmmss> sets the calendar time in the format month, day, year, hour, minutes, seconds.

Note that you must be logged in as rwa to use this command.

Command mode

Global configuration mode

clock-sync-time

Use this command to configure the time interval between synchronizing the real-time and system clocks.

Syntax

clock-sync-time <minutes>

where

minutes specifies the time interval between synchronizations. The range of values is 15 to 3600 minutes.

Command mode

Global configuration mode

enable

Use this command to change the current command mode from Privileged EXEC to Global Config, or, if you execute this command in Global Config mode, to change the password for the enable command.

Syntax

enable

In Global configuration mode, the syntax is:

enable <password>

where

password string length is from 1-32 characters.

Command mode

Global configuration mode

link-flap-detect

Use this command to configure the control of link state changes.

Syntax

link-flap-detect

Parameters

This command includes the following parameters:

link-flap-detect **followed by:**	
auto-port-down	Enables automatic disabling of the port if the link-flap threshold is exceeded. The default is enable.
frequency <frequency>	Sets the number of changes that are allowed during the time specified by the interval command. The frequency range is 1–9999. The default is 10.
interval <interval>	Sets the link-flap-detect interval in seconds. The interval range is 2–600. The default is 60.
send-trap	Enables trap sending to force the port out of service. The default is enable.

Command mode

Global configuration mode

no link-flap-detect auto-port-down

Use this command to disable the automatic disabling of port.

Syntax

```
no link-flap-detect auto-port-down
```

Command mode

Global configuration mode

no link-flap-detect send-trap

Use this command to disable sending traps.

Syntax

```
no link-flap-detect send-trap
```

command mode

Global configuration mode

load-module

Use this command to dynamically load modules.

Syntax

```
load-module {<AES>|<3DES>|<DES>}
```

Parameters

This command includes the following options:

load-module **followed by:**	
AES> filename	Sets the module ID to AES.
<*3DES*> filename	Sets the module ID to 3 DES.
<*DES*> filename	Sets the module ID to DES

Command mode

Global configuration mode

logging

Use this command to configure and display the log files for the switch. When you save the **bootconfig flags logging** command in the configuration file, the log entries are written to the **/pcmcia/syslog.txt** file. If the logging flag is not set to true, the entries are stored in memory.

Syntax

```
logging [clear] [filter <string> ] [level <level>]
[logToPCMCIA] [screen <true/false>] [transferFile
<hostID> [ <add-ip>|<filename>|<remove-IP> ]] [write]
```

Parameters

This command includes the following options:

logging **followed by:**	
[clear]	Erases log file entries.
[filter <string>]	Specifies a string to match in the log file.

logging **followed by:**	
[level <level>]	Shows and sets the logging level. level is one of the following values: 0 = Information; all messages are recorded. 1 = Warning; only warning and more serious messages are recorded. 2 = Error; only error and more serious messages are recorded. 3 = Manufacturing; this parameter is not available for customer use. 4 = Fatal; only fatal messages are recorded.
logToPCMCIA	Starts logging to PCMCIA media.
screen <true|false>	Enables (true) or disables (false) screen logging.
[transferFile <hostID> [<add-IP>|<filename> |<remove-IP>]]	Sets the remote host you wish to log, where: • add-IP and remove-IP specify the IP address. • filename is a string from 1- 256.
[write]	Writes an entry to the log file.

Command mode

Global configuration mode

loginprompt

Use this command to change the CLI login prompt.

Syntax

loginprompt <string>

where

<string> specifies the text for the new CLI login prompt. The range of values is an ASCII string of 1 to 1536 characters.

Note: Enclose the string in quotation marks if it has spaces between characters.

Command mode

Privileged EXEC mode

no loginprompt

Use this command to disable the default login banner.

Syntax

```
no loginprompt
```

Command mode

Privileged EXEC mode

mgmt-virtual-ip

Use this command to create a virtual management address for the Ethernet Routing Switch 8300. Although each CPU can have its own unique physical IP address, they share a common virtual address. This is helpful when the master CPU fails and the standby CPU comes up. If the virtual IP address is defined, the switch still responds to this address, even when using the backup CPU.

Syntax

```
mgmt-virtual-ip <ipaddr> <mask>
```

where

<ipaddr> <mask> specifies the IP address and mask that you assign to the virtual management port.

Note: Ensure that the virtual IP address is on the same IP subnet as the CPU physical IP address(es).

Command mode

Global configuration mode

no mgmt-virtual-ip

Use this command to remove/delete the virtual management IP address.

Syntax

```
no mgmt-virtual-ip <ipaddr> <mask>
```

where

<ipaddr> <mask> specifies the IP address and mask assigned to the virtual management port.

Command mode

Global configuration mode

monitor-stats

Use this command to configure and manage the monitor duration (refresh rate).

Syntax

monitor-stats [duration <integer>] [interval <integer>]

Parameters

This command includes the following options:

monitor-stats **followed by:**	
[duration <integer>]	Changes the monitoring time duration (refresh rate) for the **monitor** commands. **duration <integer>** specifies the time duration in seconds. The range of values is 1 to 1800. The default is 300.
[interval <integer>]	Changes the monitoring time interval between screen updates set by the **monitor** commands. **interval <integer>** specifies the time duration in seconds. The range of values is 1 to 600. The default is 5.

Command mode

Global configuration mode

more

Use this command to set the display output to scroll one page at a time.

Syntax

more

Command mode

Privileged EXEC mode

no more

Use this command to set the display output to continuous scrolling.

Syntax

```
no more
```

Command mode

Privileged EXEC mode

msg-control

Use this command to enable system message control and suppress duplicate error messages.

Syntax

```
msg-control
```

Command mode

Global configuration mode

no msg-control

Use this command to disable the system message control.

Syntax

```
no msg-control
```

Command mode

Global configuration mode

mtu

This command is not valid in the Ethernet Routing Switch 8300 since Jumbo Frames are not supported in Release 2.2.

passwordprompt

Use this command to change the NNCLI password prompt.

Syntax

```
passwordprompt <string>
```

where

`<string>` specifies the text for the CLI password prompt. The range of values is an ASCII string of 1 to 1536 characters.

Note: Enclose the string in quotation marks if it has spaces between characters.

Command mode

Privileged EXEC mode

no passwordprompt

Use this command to disable changing the NNCLI password prompt.

Syntax

no passwordprompt

Command mode

Privileged EXEC mode

portlock

Use this command to globally turn port locking on or off. To specify the ports to be locked, use the **ethernet <ports> lock** command.

This command enables port locking globally so you can enable or disable per-port locking. Locking a port or ports prevents other users from changing port parameters or modifying port action. Locked ports cannot be modified in any way until the port is first unlocked.

Syntax

portlock <on|off>

Command mode

Global configuration mode

prompt

Use this command to set the root-level prompt.

Syntax

prompt <prompt>

where

<prompt> specifies the text for the root-level prompt. The range of values is an ASCII string of 1 to 255 characters. The default prompt is *Passport-8310*.

Command mode

Privileged EXEC mode

rlogin-sessions

Use this command to set the allowable number of inbound rlogin/rsh sessions.

Syntax

rlogin-sessions <nsessions>

where

<nsessions> specifies the number of sessions. The range of values is 0 to 8. The default is 8.

Command mode

Global configuration mode

screenlines

Use this command to set the number of lines in the output display of the terminal screen.

Syntax

screenlines <nlines>

where

<nlines> specifies the number of lines. The range of values is 8 to 64.

Command mode

Privileged EXEC mode

show autotopology

Use this command to display the topology table. The topology table shows the information that is sent to Optivity network management software for creating network displays.

Syntax

show autotopology nmm-table

Command mode

Privileged EXEC mode

show basic config

Use this command to display information for the auto-recover-delay.

Syntax

show basic config

Command mode

Privileged EXEC mode

show interfaces GigabitEthernet interface

This command displays the MTU values for all ports on the chassis.

Syntax

show interfaces GigabitEthernet interface [portlist]

Command mode

User Exec mode

show link-flap-detect

Use this command to display the link-flap-detect settings.

Syntax

```
show link-flap-detect
```

Command mode

Privileged EXEC mode

show logging config

Use this command to display the level of information being entered in the log. The levels range from information (INFO), where all messages are entered, to FATAL, where only fatal errors are recorded. The manufacturing (MFG) level is for manufacturing purposes only and not available for customer use.

Syntax

```
show logging config
```

Command mode

Privileged EXEC mode

show logging file

Use this command to display the selected log file.

Syntax

```
show logging file [category] [CPU] [name-of-file]
[save-to-file] [severity] [tail]
```

Parameters

This command includes the following options:

`show logging file` **followed by:**	
`[category <string> ]`	Specifies the category of log file information to display for the `show logging` command. The range of characters is 0 to 100.
`[CPU <integer> ]`	Specifies the CPU number for which to display log file information.The range of values is 0 to 25.
`[name-of-file <string> ]`	Specifies the file for which to display log information. The range of characters is 1 to 99.

show logging file **followed by:**	
[save-to-file <string>]	Specifies the file to save log file information to. The range of characters is 1 to 99.
[severity <string>]	Specifies the severity level for which to display log information. The range of characters is 0 to 25.
[tail]	Specifies displaying the log file in reverse order, with the most recent information first.

Command mode

Privileged EXEC mode

show log filter

Use this command to display the log filter configuration.

Syntax

```
show log filter
```

Command mode

Privileged EXEC mode

show running-config

Use this command to display information about the current switch configuration.

Syntax

```
show running-config
```

Command mode

Privileged EXEC mode

show slot

Use this command to display the administrative status of the module.

Syntax

```
show slot <slot-number>
```

where

<slot-number> specifies the slot number in the chassis. The range of values is 1 to 10.

Note: Slots are numbered from top to bottom in Ethernet Routing Switch 8300 switches.

Command mode

Privileged EXEC mode

show sys hash-calc mltindex ip dest-mac dest-ip src-mac src-ip src-port mlt

Use this command to calculate unicast IP traffic distribution.

Syntax

```
show sys hash-calc mltindex ip dest-mac
<value>dest-ip <value>src-mac<value>src-ip<value>src-
port,value>mlt<value>
```

Parameters

This command includes the following parameters

show sys hash-calc mltindex ip **followed by:**	
dest-mac < value>	Specifies the destination MAC address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00:0x00}.
dest-ip< value>	Specifies the destination IP address {a.b.c.d}
src-mac<value>	Specifies the source MAC address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00:0x00}.
src-ip<value>	Specifies the source IPaddress {a.b.c.d}.
src-port <value>	Specifies the ingress port in the format {slot/port}.
mlt<value>	Specifies the MLT ID. Value is an integer in the range of 1 to 31.

Command mode

Global configuration mode

show sys hash-calc mltindex non-ip dest-mac src-mac src-port mlt

Use this command to calculate unicast non-IP distribution.

Syntax

```
show sys hash-calc mltindex non-ip dest_mac
<value>src-mac<value>src-port,value>mlt<value>
```

Parameters

This command includes the following parameters.

show sys hash-calc mltindex non-ip **followed by:**	
dest-mac < value>	Specifies the destination MAC address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00}.
src-mac<value>	Specifies the source MAC address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00}.
src-port <value>	Specifies the ingress port in the format {slot/port}.
mlt<value>	Specifies the MLT ID. Value is an integer in the range of 1 to 31.

Commande mode

Global configuration mode

show sys hash-calc mltindex ip-mcast source group vlan-id src-port mlt

Use this command to calculate multicast traffic distribution.

Syntax

```
show sys hash-calc mltindex ip-mcast source
<value>group<value>vlan-id<value>src-
port,value>mlt<value>
```

Parameters

This command includes the following parameters:

show sys hash-calc mltindex ip-mcast **followed by:**	
source < value>	Specifies the multicast source address {a.b.c.d}.
group<value>	Specifies the multicast source address {a.b.c.d}.

show sys hash-calc mltindex ip-mcast **followed by:**	
vlan-id<value>	Specifies the VLAN ID. Value is an integer from 1 to 4000. The egress VLAN ID is used for IP-Mcast hash.
src-port <value>	Specifies the ingress port in the format {slot/port}.
mlt<value>	Specifies the MLT ID. Value is an integer in the range of 1 to 31.

Command mode

Global configuration mode

show sys hash-calc mltindex non-ip-mcast dest-mac vlan-id src-port mlt

Use this command to calculate non-IP multicast traffic distribution.

Syntax

```
show sys hash-calc mltindex non-ip-mcast dest-
mac<value>vlan-id<value>src-port,value>mlt<value>
```

Parameters

This command includes the following parameters:

show sys hash-calc mltindex non-ip-mcast **followed by:**	
dest-mac< value>	Specifies the destination mac address in hexadecimal {0x00:0x00:0x00:0x00:0x00:0x00}.
vlan-id<value>	Specifies the VLAN ID. Value is an integer from 1 to 4000. The egress VLAN ID is used for IP-Mcast hash.
src-port <value>	Specifies the ingress port in the format {slot/port}.
mlt<value>	Specifies the MLT ID. Value is an integer in the range of 1 to 31.

Command mode

Global configuration mode

show sys-info

Use this command to display the system status and technical information about the configuration of switch hardware components.

This command displays general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, and topology status.

Syntax

```
show sys-info [card] [asic] [mda]
```

Parameters

This command includes the following options:

show sys-info **followed by:**	
[card]	Displays information about all the installed modules.
[asic]	Displays information about the ASICS installed on each module.
[mda]	Displays information about installed MDAs.

Command mode

Privileged EXEC mode

show sys perf

Use this command to display system performance information, such as CPU and switch fabric utilization and NVRAM size and use. The information is updated once per second, so it is no more than one second from real time.

Syntax

```
show sys perf
```

Command mode

Privileged EXEC mode

show sys sw

Use this command to display the version of software running on the switch, the last update of that software, and the Boot Config Table. The Boot Config Table lists the current system settings and flags.

Syntax

```
show sys sw
```

Command mode

Privileged EXEC mode

shutdown

Use this command to configure shutdown policies for a module.

Syntax

```
shutdown <slots>
```

where

<slots> specifies the applicable slot number in the chassis. The range of values is 1 to 10.

Note: Slots are numbered from top to bottom in Ethernet Routing Switch 8300 switches.

Command mode

Global configuration mode

no shutdown

Use this command to enable the administrative status of the module.

Syntax

```
no shutdown <slots>
```

Command mode

Global configuration mode

sys-action cpuswitchover

Use this command to reset the switch to changeover to the backup CPU.

Syntax

```
sys-action cpuswitchover
```

Command mode

Privileged EXEC mode

sys-action resetconsole

Use this command to reinitializes the hardware UART drivers. Use this command only if the console or modem connection is hung.

Syntax

```
sys-action resetconsole
```

Command mode

Privileged EXEC mode

sys-action resetcounters

Use this command to reset all the statistics counters in the switch to zero.

Syntax

```
sys-action resetcounters
```

Command mode

Privileged EXEC mode

udpsrc-by-vip

Use this command to enable the flag that directs the IP header to have the same source address as the management virtual IP address for self-generated User Datagram Protocol (UDP) packets.

Syntax

```
udpsrc-by-vip
```

Command mode

Global configuration mode

no udpsrc-by-vip

Use this command to disable the flag that directs the IP header to have the same source address as the management virtual IP address for self-generated User Datagram Protocol (UDP) packets.

Syntax

```
no udpsrc-by-vip
```

Command mode

Global configuration mode

SNMP commands

This chapter describes NNCLI SNMP commands and their parameters.

snmp-server authentication-trap

Use this command to specify that you want to send authentication failure traps of SNMP transmission.

Syntax

```
snmp-server authentication-trap
```

Command mode

Global configuration mode

no snmp-server authentication-trap

Use this command to specify that you do not want to send authentication failure traps of SNMP transmission.

Syntax

```
no snmp-server authentication-trap
```

Command mode

Global configuration mode

snmp-server bootstrap

Use this command to provide a configuration for switch access.

Syntax

```
snmp-server bootstrap
```

Parameters

This command includes the following options:

`snmp-server bootstrap` **followed by:**	
`min-secure`	Provides the minimum security configuration for switch access.
`semi-secure`	Provides restricted view access to the switch.
`very-secure`	Does not provide any configuration to users; users must configure the switch by themselves.

Command mode

Global configuration mode

snmp-server community

Use this command to create and configure an SNMPv1/v2 community on the switch. SNMP community strings are required for access to the switch using Device Manager or other SNMP-based management software.

Syntax

```
snmp-server community
```

Parameters

This command includes the following options:

snmp-server community **followed by:**	
<comm Idx>	A unique SNMP community index value. The range is 1-32 characters.
<name>	The community string input for the community table that represents a configuration. The range is 1-255 characters.
<security>	Maps the community string to the security name in VACM Group Member Table. The range is 1-32.

Command mode

Global configuration mode

snmp-server community name

Use this command to change the name of an SNMP community by changing the name of an entry in the SNMP community table.

Syntax

```
snmp-server community name <comm Idx> <new-name>
```

Parameters

This command includes the following options:

snmp-server community name **followed by:**	
<comm Idx>	Specifies a unique SNMP community index value. The range is 1-32 characters.
<new-name>	Specifies the new name for the entry in the community table.

Command mode

Global configuration mode

snmp-server community security

Use this command to change the security name of an SNMP community by changing the security name of an entry in the SNMP community table.

Syntax

```
snmp-server community security <comm Idx> <security>
```

Parameters

This command includes the following options:

snmp-server community security **followed by:**	
<comm Idx>	Specifies a unique SNMP community index value. The range is 1-32 characters.
<security>	Maps the community string to the security name in VACM Group Member Table.

Command mode

Global configuration mode

no snmp-server community

Use this command to delete an SNMP community on the switch by deleting an entry in the SNMP community table.

Syntax

```
no snmp-server community <comm Idx>
```

where

<comm Idx> specifies a unique SNMP community index value. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

snmp-server contact

Use this command to set the SNMP contact information for the switch.

Syntax

```
snmp-server contact <contact>
```

where

<contact> specifies the contact information text. The range of values is an ASCII string from 0 to 255 characters (for example a phone extension or email address). Strings with spaces must be enclosed in quotes (e.g., "John Smith").

Command mode

Global configuration mode

snmp-server group

Use this command to create new access for a group in the VACM table.

Syntax

snmp-server group <group name> <prefix> <model> <level>

where:

- **group name** specifies the group access name. The range is 1 to 32 characters.
- **prefix** is not supported in the current release of the Ethernet Routing Switch 8300; however, because it is part of the index for the table, it must be configured. When you configure prefix, enter " " to indicate an empty string. The range is 0 to 32 characters.
- **model** is the valid options are usm, snmpv1, and snmpv2c.
- **level** is the minimum level of security required to gain the access rights allowed by this conceptual row. The valid options are authPriv, authNoPriv, or noAuthNoPriv.

Parameters

This command includes the following option:

snmp-server group **followed by:**	
view <group name> <prefix> <model> <level> [read <value>] [write <value>]	Assigns a MIB view for the specified group. • **read value** indicates that you want the group to have read access to the specified value (that is, MIB view). • **write value** indicates that you want the group to have write access to the specified value (that is, MIB view).

Command mode

Global configuration mode

no snmp-server group

Use this command to delete group access from the v3 VACM table.

Syntax

```
no snmp-server group <group name> <prefix> <model>
<level>
```

where:

- **group name** specifies the group access name. The range is 1 to 32 characters.
- **prefix** is not supported in the current release of the Ethernet Routing Switch 8300; however, because it is part of the index for the table, it must be configured. When you configure prefix, enter " " to indicate an empty string. The range is 0 to 32 characters.
- **model** is the valid options are usm, snmpv1, and snmpv2c.
- **level** is the minimum level of security required to gain the access rights allowed by this conceptual row. The valid options are authPriv, authNoPriv, or noAuthNoPriv.

Command mode

Global configuration mode

snmp-server host

Use this command to set an SNMP trap receiver.

Syntax

```
snmp-server host <ipaddr> <v1|v2c> <commstr>
```

Parameters

This command includes the following options:

snmp-server host **followed by:**	
<ipaddr>	Specifies the IP address of the trap receiver.
<v1|v2c>	Specifies SNMP version 1 or SNMP version 2.
<commstr>	Specifies the input community string from 1 to 20 characters.

Command mode

Global configuration mode

no snmp-server host

Use this command to delete the SNMP trap receiver.

Syntax

```
no snmp-server host <ipaddr>
```

where

`<ipaddr>` specifies the IP address of the trap receiver.

Command mode

Global configuration mode

show snmp-server

Use this command to display the current SNMP settings.

Syntax

```
show snmp-server
```

Command mode

Privileged EXEC mode
Global configuration mode
Interface configuration mode

snmp-server location

Use this command to set the location information for the switch.

Syntax

```
snmp-server location <location>
```

where

`<location>` specifies the location information. The range of a values is an ASCII string from 0 to 255 characters (for example, Finance).

Command mode

Global configuration mode

snmp-server member

Use this command to create a new group member on the Ethernet Routing Switch 8300.

Syntax

```
snmp-server member <user name> <model> [<group name>]
```

where:

- **user name** specifies the name of the user group. The range is 1 to 32 characters.
- **model** specifies the message processing model to use when generating an SNMP message. The valid options are usm, snmpv1, and snmpv2c.
- **group name** assigns the user to the group for data access. The range is 1 to 32 characters.

Parameters

This command uses the following option:

snmp-server member **followed by:**	
name <user name> <model> <group name>	Changes the group name for the v3 VACM table.

Command mode

Global configuration mode

no snmp-server member

Use this command to delete a user group from the v3 VACM table.

Syntax

no snmp-server member <user name> <model>

where:

- **user name** specifies the name of the user group. The range is 1 to 32 characters.
- **model** specifies the message processing model to use when generating an SNMP message. The valid options are usm, snmpv1, and snmpv2c.

Command mode

Global configuration mode

snmp-server name

Use this command to set the root-level prompt name for the switch.

Syntax

snmp-server name <prompt>

where

<prompt> specifies the text of the root-level prompt name for the SNMP server. The range of values is an ASCII string from 0 to 255 characters (for example, LabSC7 or Closet4).

Command mode

Global configuration mode

snmp-server user

Use this command to create a new user in the USM table on the Ethernet Routing Switch 8300:

snmp-server user <UserName> [<auth protocol>] [auth <password>] [priv <password>]

where:

- **UserName** specifies the SNMPv3 user name. The name is used as an index to the table. The range is 1 to 32 characters.
- **auth protocol** specifies an authentication protocol. If no value is entered, the entry has no authentication capability. The protocol choices are MD5 and SHA.
- **auth <password>** specifies an authentication password. If no value is entered, the entry has no authentication capability. The range is 1 to 32 characters.
- **priv <password>** assigns a privacy password. If no value is entered, the entry has no privacy capability. The range is 1 to 32 characters. You must set authentication before you can set the privacy option.

Parameters

This command uses the following options:

snmp-server user **followed by:**	
auth <user name> old-password <value> new-password <value>	Changes the authentication password for an existing user.
priv <user name> old-password <value> new-password <value>	Changes privacy password for an existing user.

Command mode

Global configuration mode

no snmp-server user

Use this command to delete a user from the v3 VACM table.

Syntax

```
no snmp-server user <user name>
```

where

user name specifies the user's security name that is an index to the table. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

snmp-server view

Use this command to create a new entry for the MIB View table on the Ethernet Routing Switch 8300:

Syntax

```
snmp-server view <View Name> <subtree oid> [mask <value> ]
[type <value> ]
```

where:

- **View Name** represents an SNMP access view. The range is 1 to 32 characters.
- **subtree oid** is the prefix that defines the set of MIB objects accessible by this SNMP entity. The range is 1 to 32 characters.
- **mask <value>** specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.
- **type <include|exclude>** determines whether access to a mib object is granted or denied.

Parameters

This command includes the following options:

snmp-server view **followed by:**	
mask <View Name> <subtree oid> <new-mask>	Changes the view mask for an entry in the MIB-view table.
type <View Name> <subtree oid> <new-type>	Changes the type for an entry in the MIB-view table.

Command mode

Global configuration mode

no snmp-server view

Use this command to delete an entry for the MIB view table.

Syntax

no snmp-server view <view name> <subtree oid>

where:

- **view name** specifies the group name of the user. The range of values is 1 to 32 characters.
- **subtree oid** specifies the object identifier prefix that defines the set of MIB objects accessible by this SNMP entity. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

Ethernet port commands

This chapter describes NNCLI Ethernet port commands and their parameters.

Ethernet port command
"tx-queue" (page 160)
"no tx-queue" (page 161)
"unknown-mac-discard" (page 162)
"no unknown-mac-discard" (page 163)
"test loopback" (page 163)
"untagged-frames-discard" (page 164)
"no untagged-frames-discard" (page 164)

action

Use this command to perform port-specific actions such as flush table entries.

Syntax

```
action <port | none | flushMacFdb |flushALL|
clearLoopDetectAlarm>
```

Parameters

This command includes the following parameters:

action **followed by:**	
port	Specifies the port.
none	Specifies none.
flushMacFdb	Flushes MAC forwarding table for port.
flushALL	Flushes all tables.
clearLoopDetectAlarm	Clears loop detect alarm.

Command mode

Interface configuration mode

auto-negotiate

Use this command to enable autonegotiation (adjusting between 10 Mb/s and 100 Mb/s and half- or full-duplex) on selected ports.

Syntax

```
auto-negotiate [port <port list>]
```

where

`port list` specifies the applicable ports in port list form: {`slot/port [-slot/port] [, ...]`}

Command mode

Interface configuration mode

no auto-negotiate

Use this command to disable autonegotiation on selected ports.

Syntax

```
no auto-negotiate [port <port list>]
```

where

`port list` specifies the applicable ports in port list form: {`slot/port [-slot/port] [, ...]`}

Command mode

Interface configuration mode

auto-recover-port

Use this command to enable auto recovery on ports.

Syntax

```
auto-recover-port [port <portlist>] [enable]
```

Parameters

This command includes the following options:

`auto-recover-port` **followed by:**	
`[port <portlist> ]`	Specifies the applicable ports in port list form: {`slot/port [-slot/port] [, ...]`}.
`[enable]`	Enables auto recovery. The default is disabled.

Command mode

Interface configuration mode

default auto-recover-port

Use this command to set auto recovery on ports to default values.

Syntax

```
default auto-recover-port [port <portlist>] [enable]
```

Parameters

This command includes the following options:

default auto-recover-port **followed by;**	
[port <portlist>]	Specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.
[enable]	Disables auto recovery. The default is disabled.

Command mode

Interface configuration mode

no auto-recover-port

Use this command to remove auto recovery on ports.

Syntax

```
no auto-recover-port [port <portlist>] [enable]
```

Parameters

This command includes the following options:

no auto-recover-port **followed by:**	
[port <portlist>]	Specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.
[enable]	Disables auto recovery. The default is disabled.

Command mode

Interface configuration mode

bcast-mcast-rate-limit

Use this command to enable broadcast and multicast rate limit on the ports.

Syntax

```
bcast-mcast-rate-limit <value> [port <port list>]
```

Parameters

This command includes the following parameters:

bcast-mcast-rate-limit **followed by:**	
<value>	Value is the broadcast-rate-limit with a range of 1 to 100.
[port <port list>]	Specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.

Command mode

Interface configuration mode

cp-limit

Use this command to enable Control Packet rate Limit (CP-Limit).

Syntax

```
cp-limit [port <port list> ]
```

where

port list specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}

Command mode

Interface configuration mode

no cp-limit

Use this command to disable Control Packet rate Limit (CP-Limit).

Syntax

```
no cp-limit [port <portlist> ]
```

where

port list specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}

Note: After a CP-Limit is disabled on a port, it can only be re-enabled by disabling and re-enabling the port with command:

```
shutdown [port <ports>]
```

Command mode

Interface configuration mode

default-vlan-id

Use this command to define the default Virtual LAN (VLAN) identification on selected ports.

Note: The default switch configuration includes a port-based VLAN that includes all the ports in the system. This VLAN has a VID of 1 and is referred to as the Default VLAN. This VLAN is special in the sense that it cannot be deleted from the system, and that it is statically bound to the Default STG.

You should not confuse that Default VLAN with this default-vlan-id parameter. The purpose of this parameter is to place an incoming data packet into a user-defined (default) VLAN if the packet is expected to be carrying a VLAN ID and this value cannot be determined by the switch.

Syntax

```
default-vlan-id [port <ports> ] <vid>
```

Parameters

This command includes the following options:

default-vlan-id **followed by:**	
[port <ports>]	Specifies the applicable ports in port list form: **{slot/port [-slot/port] [, ...]}**.
<vid>	Specifies the VLAN ID The range of values is 1 to 2000

Command mode

Interface configuration mode

duplex

Use this command to set the operating mode of the selected port to half-duplex or full-duplex when autonegotiation is disabled.

Syntax

```
duplex [port <ports> ] <half|full>
```

Parameters

This command includes the following options:

duplex **followed by:**	
[port <ports>]	Specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.
half	Sets the operating mode of the specified port to half-duplex when autonegotiation is disabled. The default is half-duplex.
full	Sets the operating mode of the specified port to full-duplex when autonegotiation is disabled. The default is half-duplex.

Command mode

Interface configuration mode

eapol

Use this command to configure EAPoL on a specific port.

Syntax

```
eapol [guest-vlan<vid> [port <portlist> ] [init]
[max-request <1....10>]
[quiet-interval <1...65535] [re-authenticate]
[re-authentication <enable|disable>]
[re-authentication-period <1...2147483647>]
[server-timeout <1...65535>]
[supplicant-timeout <1...65535>]
[traffic-control <in|in-out>] [transmit-interval
<1...65535>]
```

Parameters

This command includes the following options:

eapol **followed by:**	
guest-vlan <vid>	Specifies the ID of the guest VLAN.
init	Reinitializes EAPoL authentication on this port.
max-request <1...10>	Sets the maximum number of times to retry sending packets to the Supplicant. The default is 2.

eapol **followed by:**	
port <portlist>	Enter the port or ports you want to configure for EAPoL, and use the convention {slot/port[-slot/port][,...]}. ***Note:*** If you omit this parameter, the system uses the port number specified when you entered the **interface** command.
quiet-interval <1...65535>	Sets the time interval (in seconds) between authentication failure and the start of a new authentication. The default is 60.
re-authenticate	Re-authenticates the Supplicant connected to this port immediately. ***Note:*** Before you can reauthenticate the Supplicant connected to this port, you must first enable reauthentication **re-authentication <enable|disable>**
re-authentication <enable|disable>	When enabled, re-authenticates an existing Supplicant at the time interval specified in **re-authentication-period <1...2147483647>** The default is disable.
re-authentication-period <1...2147483647>	Sets the time interval (in seconds) between successive re-authentications **re-authentication <enable|disable>**. The default is 3600 (1 hour).
server-timeout <1...65535>	Sets the time (in seconds) to wait for a response from the RADIUS server. The default is 30.

eapol **followed by:**	
status <auto|unauthorized|authorized>	Sets the authentication status for this port. The default is ***authorized***. • *auto* - port authorization depends on the results of the EAPoL authentication by the RADIUS server. • *unauthorized* - port is always unauthorized. • *authorized* - port is always authorized.
supplicant-timeout <1...65535>	Sets the time (in seconds) to wait for a response from a Supplicant for all EAP packets except EAP Request/Identity packets. The default is 30.
traffic-control <in|in-out>	Sets the desired level of traffic control for a port. • **in** - Blocks incoming traffic when EAP authentication fails. • in-out - Blocks incoming and outgoing traffic when EAP authentication fails.
transmit-interval <1...65535>	Sets the time (in seconds) to wait for a response from a Supplicant for EAP Request/Identity packets. The default is 30.

Command mode

Interface configuration mode

no eapol

Use this command to disable eapol globally on the switch.

Syntax

```
no eapol [port <port list>]
```

where

port list specifies the applicable ports in port list form: {**slot/port [-slot/port] [, ...]**}

Command mode

Interface configuration mode

encapsulation

Use this command to enable encapsulation on selected ports.

Syntax

```
encapsulation [port <port list> ]
```

where

port list specifies the applicable ports in port list form: {**slot/port [-slot/port] [, ...]**}

Command mode

Interface configuration mode

no encapsulation

Use this command to disable encapsulation on selected ports.

Syntax

```
no encapsulation [port <port list> ]
```

where

port list specifies the applicable ports in port list form: {**slot/port [-slot/port] [, ...]**}

Command mode

Interface configuration mode

linktrap

Use this command to enable the link up/down trap of a specific port.

Syntax

```
linktrap [port <port list> ]
```

where

port list specifies the applicable ports in port list form: {**slot/port [-slot/port] [, ...]**}

Command mode

Interface configuration mode

no linktrap

Use this command to disable the link up/down trap of a specific port.

Syntax

linktrap [port <port list>]

where

port list specifies the applicable ports in port list form: {**slot/port [-slot/port] [, ...]**}

Command mode

Interface configuration mode

lock

Use this command to lock the selected port or ports for exclusive use if the portlock feature is globally enabled by the **portlock <on|off>** command.

Syntax

lock [port <port list>]

where

[port <port list>] is an optional parameter that specifies the applicable ports in port list form: {**slot/port [-slot/port] [, ...]**}.

Command mode

Interface configuration mode

no lock

Use this command to unlock the selected port or ports from exclusive use if the portlock feature is globally enabled by the **portlock <on|off>** command.

Syntax

no lock [port <port list>]

where

[port <port list>] is an optional parameter that specifies the applicable ports in port list form: {**slot/port [-slot/port] [, ...]**}.

Command mode

Interface configuration mode

name

Use this command to assign a name to the selected ports.

Syntax

```
name [port <ports> ] <name>
```

Parameters

This command includes the following parameters:

name **followed by:**	
[port <ports>]	Specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.
<name>	Specifies the name of the port. The range of values is a string of 0 to 20 characters.

Command mode

Interface configuration mode

shutdown

Use this command to disable the interface on selected ports.

Syntax

```
shutdown [port <ports> ]
```

where

[port <port list>] is an optional parameter that specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.

Command mode

Interface configuration mode

For more information about configuring port interfaces, see *Configuring IP Routing and Multicast Operations using the NNCLI and CLI (316800-B)* and *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI (316805-C)*

no shutdown

Use this command to enable the interface on selected ports.

Syntax

```
no shutdown [port <ports> ]
```

where

[port <port list>] is an optional parameter that specifies the applicable ports in port list form: {**slot/port [-slot/port] [, ...]**}.

Command mode

Interface configuration mode

spanning-tree stp

Configures the ports in a specified Spanning Tree Group (STG). This command can also display current settings for the port spanning tree group.

Syntax

spanning-tree [port <ports>] stp <sid>

Parameters

This command includes the following parameters:

spanning-tree [port <ports>] stp **followed by:**	
<sid>	Specify a spanning tree group ID from 1 to 64.
change-detection	Enable or Disable the topology change detection for the specified spanning tree.
cost **<value>**	Sets the contribution of this port to the path cost. The IEEE 802.1D standard recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN. • **value:** Specify a value from 1 to 65535.
faststart	When enabled on a port with no other bridges, Spanning Tree FastStart brings the port up more quickly following switch initialization or a spanning tree change. The port goes through the normal listening and learning states before the forwarding state, but the hold times for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default).

spanning-tree [port <ports>] stp **followed by:**	
priority <value>	Sets this port's priority. • **value:** Specify a value from 0 to 65535.
[port <portlist>]	**portlist:** Defines the list of ports for this STG. Use the format: {slot/port[-slot/port][,...]}.

Note: Ports must have tagging enabled in order to belong to multiple spanning tree groups.

Command mode

Interface configuration mode

no spanning-tree stp

Disables the ports in a specified Spanning Tree Group (STG).

Syntax

```
no spanning-tree [port <ports>] stp <sid>
```

Command mode

Interface configuration mode

tx-queue

Use this command to configure transmit queue parameters for the specified ethernet port or ports.

Syntax

```
tx-queue [port <ports>] <queue-id>
```

where:

- **ports** specify the ports in the portlist form {slot/port[-slot/port][, ...]}.
- **queue-id** is the queue ID, which represents a priority with a value range of 0 (lowest) to 7 (highest).

Parameters

This command includes the following options:

tx-queue [port <ports>] <queue-id> **followed by:**	
tx <enable|disable>	Enables or disables the transmit queue feature.
size <size>	Specifies the number of traffic descriptors. One descriptor can hold one packet. **size** range is 16 to 384.
scheduler <strict-priority|DWRR1|DWRR0>	Specifies one of the following scheduling group names: • strictPriority has the highest priority. • dwrr1 is a Deficit Weighted Round-Robin servicing technique with a medium level of priority. • dwrr0 is a Deficit Weighted Round-Robin servicing technique with the lowest priority.
weight <weight>	Specifies the relative portion of bandwidth assigned to this queue compared to other queues. The relative weight uses a Deficit Weighted Round-Robin (DWRR) servicing technique. **weight** range is 1 to 256.
shaper <enable|disable>	Enables or disables the shaper feature.
rate <in mbps>	Maximum shaper rate in mbps. **in mbps** has a value range of 1 to 10000.
burst-size <in kilobps>	Shaper burst size in kilo bytes. **in kilobps** has a value range of 4 to 16000.

Command mode

Interface fastethernet mode

no tx-queue

Disables transmit queue parameters for the specified ethernet port or ports.

Syntax

```
no tx-queue [port <ports> ] <queue-id>
```

where:

- **ports** specify the ports in the portlist form {**slot/port[-slot/port][, ...]**}.
- **queue-id** is the queue ID, which represents a priority with a value range of 0 (lowest) to 7 (highest).

Command mode

Interface configuration mode

unknown-mac-discard

Use this command to configure the unknown-mac-discard option on selected ports.

Syntax

```
unknown-mac-discard [port <ports> ] [activation] [add-
allow-mac <0x00:0x00:0x00:0x00:0x00:0x00>] [autolearn
] [autolearn-mode <one-shot|continuous>] [lock-
autolearn-mac] [violation-downport] [violation-logging]
[violation-sendAuthentificationTrap]
```

Parameters

This command includes the following options:

unknown-mac-discard [port <ports>] **followed by:**	
activation	Sets unknown MAC discard.
add-allow-mac <0x00:0x00:0x00:0x00:0x00:0x00>	Sets the add allow mac address of this port.
autolearn	Sets autolearn on this port.
autolearn-mode <one-shot|continuous>	Sets the autolearn mode.
lock-autolearn-mac <enable|disable>	Sets the lock autolearn MAC address of this port.
port <ports>	Specifies the port numbers which are to be changed
violation-downport	Sets violation down port action of this port.
violation-logging	Sets violation logging action of this port.
violation-sendAuthentificationTrap	Sets violation send authentication action of this port.

Command mode

Interface configuration mode

no unknown-mac-discard

Use this command to disable the unknown-mac-discard option on selected ports.

Syntax

```
no unknown-mac-discard [port <ports> ] [activation]
[autolearn ] [autolearn-mode <one-shot|continuous>]
[lock-autolearn-mac] [max-mac-count <max MAC count> ]
[remove-allow-mac <mac> ] [violation-downport] [viola-
tion-logging] [violation-sendAuthentificationTrap]
```

Parameters

This command includes the following options:

`no unknown-mac-discard [port <ports> ]` **followed by:**	
`activation`	Sets unknown MAC discard.
`autolearn`	Sets autolearn on this port.
`autolearn-mode <one-shot|continuous>`	Sets the autolearn mode.
`lock-autolearn-mac <enable|disable>`	Sets the lock autolearn MAC address of this port.
`max-mac-count <max MAC count>`	Sets the maximum number of MAC addresses allowed on this port.
`remove-allow-mac <mac>`	Removes allow MAC address from this port.
violation-downport	Sets violation down port action of this port.
violation-logging	Sets violation logging action of this port.
violation- sendAuthentificationTrap	Sets violation send authentication action of this port.

Command mode

Interface configuration mode

test loopback

Enables loopback test on specified ports.

Syntax

```
test loopback <ports>
```

where

ports specify the ports in the portlist form {*slot/port*[-*slot/port*][, ...]}.

Command mode

Interface configuration mode

test stop

Disables loopback test on specified ports.

Syntax

```
test stop <ports>
```

where

ports specify the ports in the portlist form {*slot/port*[-*slot/port*][, ...]}.

Command mode

Interface configuration mode

untagged-frames-discard

Use this command to enable the discard untagged frames option on selected ports.

Syntax

```
untagged-frames-discard [port <ports>] <enable|disable>
```

Parameters

This command includes the following parameter:

untagged-frames-discard **followed by:**	
[port <ports>]	Specifies the applicable ports in port list form: **{slot/port [-slot/port] [, ...]}**.

Command mode

Interface configuration mode

no untagged-frames-discard

Use this command to disable the discard untagged frames option on selected ports.

Syntax

no untagged-frames-discard [port <ports>] <enable|disable>

Parameters

This command includes the following parameter:

no untagged-frames-discard **followed by:**	
[port <ports>]	Specifies the applicable ports in port list form: **{slot/port [-slot/port] [, ...]}**.

Command mode

Interface configuration mode

custom autonegotiation advertisements

Configuration: new command available at the interface level

- For <10/100> interface fast auto-negotiation-advertisements <slot/port>
- For <10/100/1000> interface fast auto-negotiation-advertisements <slot/port>

Show command:

- For <10/100> show interface fast 2/1
- For <10/100/1000> show interface giga 3/1

Security commands

This chapter describes NNCLI security commands and their parameters.

Security Commands
"access-policy disable" (page 169)
"access-policy enable" (page 169)
"access-policy info" (page 169)
"access-policy policy" (page 169)
"access-policy policy" (page 171)
"access-policy policy create" (page 172)
"access-policy policy info" (page 174)
"no access-policy policy" (page 176)
"no nsna" (page 177)
"no nsna enable" (page 177)
"no nsna nsnas" (page 177)
"no nsna phone-signature" (page 178)
"no nsna vlan" (page 178)
"nsna" (page 181)
"nsna enable" (page 182)
"nsna nsnas" (page 182)
"nsna phone-signature" (page 183)
"nsna vlan color" (page 183)
"radius-server info" (page 187)
"no radius-server" (page 178)
"radius" (page 184)
"radius clear-stat" (page 187)
"radius info" (page 187)
"radius-server info" (page 187)
"show access-policy" (page 187)

Security Commands
"show nsna" (page 188)
"show nsna client" (page 188)
"show nsna nsnas" (page 188)
"show nsna interface" (page 189)
"show nsna phone-signature" (page 189)
"show nsna vlan" (page 189)
"show radius" (page 189)
"show radius-server" (page 190)
"show syslog" (page 190)
"show syslog host" (page 190)
"snmp-server authentication-trap" (page 190)
"snmp-server contact" (page 191)
"snmp-server group" (page 191)
"snmp-server group info" (page 192)
"snmp-server group match" (page 192)
"snmp-server group view" (page 193)
"no snmp-server group" (page 179)
"snmp-server host" (page 194)
"snmp-server host" (page 195)
"no snmp-server group" (page 179)
"snmp-server info" (page 195)
"snmp-server location" (page 195)
"snmp-server member" (page 196)
"snmp-server member info" (page 196)
"snmp-server member name" (page 197)
"no snmp-server member" (page 197)
"snmp-server name" (page 198)
"snmp-server user" (page 198)
"snmp-server user auth" (page 199)
"snmp-server user info" (page 200)
"snmp-server user priv" (page 200)
"no snmp-server view" (page 180)
"no snmp-server view" (page 180)
"snmp-server view info" (page 202)
"snmp-server view mask" (page 202)

Security Commands
"snmp-server view type" (page 203)
"syslog host" (page 204)
"syslog host" (page 204)
"syslog host" (page 205)
"syslog host create" (page 206)
"syslog host severity" (page 207)
"no syslog host" (page 181)

access-policy disable

Use this command to globally disable the IP access policy feature on the switch so that no policies on the switch are applied. The default is disabled.

Syntax

```
access-policy disable
```

Command mode

Global configuration mode

access-policy enable

Use this command to globally enable the IP access policy feature on the switch. The default is disabled.

Syntax

```
access-policy enable
```

Command mode

Global configuration mode

access-policy info

Use this command to display the global access policy settings.

Syntax

```
access-policy info
```

Command mode

Global configuration mode

access-policy policy

Use this command to modify an IP access policy with a specific access policy ID. Sets access level policies.

Syntax

```
access-policy policy <vid>
```

```
[name <name> ]
[<enable|disable>]
[mode <allow|deny>]
[precedence <value> ]
[network <ip/mask> ]
[host <ip> ]
[username <name> ]
[accesslevel <string> ]
```

where

<vid> specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535

Parameters

This command includes the following options:

access-policy policy <vid> **followed by:**	
[accesslevel <string>]	Specifies an access level for a policy. The options are: **{ro | rw | rwa}** or **{read-only| read-write|read-write-all}**.
create	Creates a new access policy. See "access-policy policy create" (page 172) for the full parameters under this command.
ftp <http/rlogin/ssh>	Enables FTP
http <rlogin/ssh>	Enables HTTP.
[host <ip>]	Specifies the access policy for the trusted host address. Applies only for remote login and remote shell execution.
[name <name>]	Specifies a name for the access policy. The range of values is a string of 0 to 15 characters.
[<enable|disable>]	Enables or disables the specified access policy.
[mode <allow|deny>]	Specifies the access policy mode. The options are: **allow** or **deny**.
[precedence <value>]	Specifies the access policy precedence. Precedence determines which policy to use if multiple policies apply. **<value>** specifies the precedence level. The range of values is 1 to 128, with the lowest number having the highest precedence.

access-policy policy <vid> **followed by:**	
[network <ip/mask>]	Specifies stations affected by the access policy using the network IP address and subnet mask. • **ip** specifies the IP address **{a.b.c.d}** of the host used to authenticate the user. The login must be the specified user at the specified host for access. If you specify an IP address and subnet mask, that location is either allowed or denied access, depending on the **mode** setting. The options are: **{a.b.c.d/x | a.b.c.d/x.x.x.x | default}**. • **default** specifies that everyone on the network is either allowed or denied access, as defined by the **mode** setting.
rlogin <ssh>	Enables rlogin.
snmp-group <name 1-32>	Adds an SNMP-v3 group under this access policy.
snmp-v3	Enables SNMP-V3.
ssh	Enables SSH.
telnet <ftp/http/rlogin/ssh/tftp>	Enables Telnet.
tftp <ftp/http/rlogin/ssh>	Enables TFTP.
[username <name>]	Specifies the trusted host user name for the trusted host with the specified policy. Applies only to rlogin access

Command mode

Global configuration mode

access-policy policy

Use this command to specify access level policies for different methods of access.

Syntax

```
access-policy policy <vid>
[ftp <enable|disable>]
[http <enable|disable>]
[rlogin <enable|disable>]
[snmp <enable|disable>]
[telnet <enable|disable>]
[tftp <enable|disable>]
```

Parameters

This command includes the following options:

`access-policy policy <vid>` **followed by:**	
`<vid>`	Specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535
`[ftp <enable|disable>]`	Enables or disables access to ftp network communication protocols for the specified policy.
`[http <enable|disable>]`	Enables or disables access to http network communication protocols for the specified policy.
`[rlogin <enable|disable>]`	Enables or disables access to rlogin network communication protocols for the specified policy.
`[snmp-group WORD <1-32>]`	Adds an SNMP-V3 group under the specific access policy. • `WORD <1-32>` is the name the SNMP-V3 group.
`[snmpv3 <enable|disable>]`	Enables or disables SNMP-V3.
`[ssh <enable|disable>]`	Enables of disables SSH.
`[telnet <enable|disable>]`	Enables or disables access to telnet network communication protocols for the specified policy.
`[tftp <enable|disable>]`	Enables or disables access to tftp network communication protocols for the specified policy.

Command mode

Global configuration mode

access-policy policy create

Use this command to create an IP access policy with a specified access policy ID. This command sets accesslevel policies.

Syntax

```
access-policy policy <vid> create
[name <name> ]
[<enable|disable>]
[mode <allow|deny>]
[precedence <value> ]
[network <ip/mask> ]
[host <ip> ]
[username <name> ]
[accesslevel <string> ]
```

Parameters

This command includes the following options:

`access-policy policy <vid> create` **followed by:**	
`<vid>`	Specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535
`[name <name> ]`	Specifies a name for the access policy. The range of values is a string of 0 to 15 characters.
`[<enable|disable>]`	Enables or disables the specified access policy.
`[mode <allow|deny>]`	Specifies the access policy mode. The options are: **`allow`** or **`deny`**.
`[precedence <value> ]`	Specifies the access policy precedence. Precedence determines which policy to use if multiple policies apply. **`<value>`** specifies the precedence level. The range of values is 1 to 128, with the lowest number having the highest precedence.
`[network <ip/mask> ]`	Specifies stations affected by the access policy using the network IP address and subnet mask. • **`ip`** specifies the IP address **`{a.b.c.d}`** of the host used to authenticate the user. The login must be the specified user at the specified host for access. If you specify an IP address and subnet mask, that location is either allowed or denied access, depending on the **`mode`** setting.

access-policy policy <vid> create **followed by:**	
	The options are: **{a.b.c.d/x| a.b.c.d/x.x.x.x| default}**. • **default** specifies that everyone on the network is either allowed or denied access, as defined by the **mode** setting.
[host <ip>]	Specifies the access policy for the trusted host address. Applies only for remote login and remote shell execution.
[username <name>]	Specifies the trusted host user name for the trusted host with the specified policy. Applies only to rlogin access
[accesslevel <string>]	Specifies an access level for a policy. The options are: {ro | rw | rwa} or {read-only| read-write | read-write-all}.

Command mode

Global configuration mode

access-policy policy info

Use this command to create an IP access policy with a specified access policy ID. Sets accesslevel policies.

Syntax

access-policy policy <vid> info

where

<vid> specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535.

Command mode

Global configuration mode

eapol default-guest-vlan

This command enables the EAPOL default guest VLAN.

Syntax

eapol default-guest-vlan <vid>

Command mode

Global configuration mode.

eapol guest-vlan

This command enables the EAPOL guest VLAN.

Syntax

```
eapol guest-vlan
```

Command mode

Global configuration mode.

eapol allow-non-eap mac-max

This command sets the maximum number of non-EAP clients.

Syntax

```
eapol allow-non-eap mac-max {<1-8>}
```

Command mode

Global configuration mode.

eapol non-eap-mac add

This command adds a non-EAP MAC Address to the allow list.

Syntax

```
eapol non-eap-mac add {<mac-add>}
```

no eapol guest-vlan

This command disables guest-vlan.

Syntax

```
no eapol guest-vlan
```

Command mode

This command is in the Interface configuration mode.

eapol guest-vlan-id

This command sets the guest-vlan at port level

Syntax

```
n
```

Command mode

This command is in the Interface configuration mode.

eapol multihost

This command enables EAPOL multihost.

Syntax

```
eapol multihost
```

eapol guest-vlan

This command enables guest-vlan

Syntax

```
eapol guest-vlan
```

Command mode

This command is in the Interface Config mode.

eapol multihost mac-max

This command sets the maximum number of EAP clients. The default is 1.

Syntax

```
eapol multihost mac-max {<1-8>}
```

eapol allow-non-eap

This command allows non-EAP clients.

Syntax

```
eapol allow-non-eap
```

no access-policy policy

Use this command to delete access policies for a specific policy ID.

Syntax

```
no access-policy policy <pid>
```

where

<pid> specifies the access policy ID number assigned when the policy was created. The range of values is 1 to 65535.

Command mode

Global configuration mode

For more information about access policies, see *Configuring and Managing Security using the NNCLI and CLI (316804-C)*.

no eapol allow-non-eap

This command disallows non-EAP clients.

Syntax

```
no eapol allow-non-eap
```

no eapol guest-vlan

This command disables the EAPOL guest VLAN.

Syntax

```
no eapol guest-vlan
```

Command mode

This command is in the Global Config mode.

no eapol multihost

This command disables EAPOL multihost.

Syntax

```
no eapol multihost
```

no eapol non-eap-mac

This command removes a non-EAP MAC Address from the allow list.

Syntax

```
np eapol non-eap-mac {<mac-add>}
```

no nsna

Use this command to remove an NSNA port.

Syntax

```
no nsna
```

Command mode

Ethernet Interface configuration mode

no nsna enable

Use this command to disable NSNA.

Syntax

```
no nsna enable
```

Command mode

Global configuration mode

no nsna nsnas

Use this command to remove the NSNAS 4050 subnet.

Syntax

```
no nsna nsnas <ipaddr/mask>
```

where

<ipaddr/mask> is the NSNAS 4050 IP address and network mask (a.b.c.d/<0-32>).

Command mode

Global configuration mode

no nsna phone-signature

Use this command to remove NSNA phone signatures.

Syntax

```
no nsna phone-signature <LINE>
```

where

<LINE> is the phone signature string (for example: Nortel-i2007-A).

no nsna vlan

Use this command to remove an NSNA VLAN.

Syntax

```
no nsna vlan <vid>
```

where

<vid> is the VLAN ID in the range 1-4000.

Command mode

Global configuration mode

no radius

Use this command to remove CLI commands from accounting requests for Remote Access Dial-in User Services (RADIUS).

Syntax

```
no radius acct-include-cli-commands
```

Command mode

Global configuration mode

no radius-server

Use this command to disable the IP address for Remote Access Dial-in User Services (RADIUS) on the server.

Syntax

```
no radius-server <ipaddr>
```

where

<ipaddr> specifies the IP address for RADIUS on the server.

Command mode

Global configuration mode

For more information about RADIUS operations, see *Configuring and Managing Security using the NNCLI and CLI (316804-C)*.

no snmp-server group

Use this command to delete view-based access for a Signaling Network Management Protocol (SNMP) group.

Syntax

```
no snmp-server group
<group name>
<prefix>
<model>
<level>
```

Parameters

This command includes the following options:

no snmp-server group **followed by:**	
<group name>	Creates the new group access with this group name. The range of values is 1 to 32 characters.
<prefix>	Assigns a context prefix. The range of values is 1 to 32 characters.
<model>	Assigns the authentication checking to communicate to the switch. The options are: **usm, snmpv1,** and **snmpv2c**.
<level>	Specifies the minimum level of security required to gain access rights allowed by this conceptual row.

Command mode

Global configuration mode

no snmp-server host

Use this command to delete the Signaling Network Management Protocol (SNMP) trap receiver.

Syntax

```
no snmp-server host <ipaddr>
```

where

<ipaddr> specifies the IP address of the trap receiver.

Command mode

Global configuration mode

no snmp-server user

Use this command to delete a Signaling Network Management Protocol (SNMP) user in the User Security Model (USM) table and v3 VACM table on the switch.

Syntax

```
no snmp-server user <user name>
```

where

<user name> specifies the user's security name that is an index to the table. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

no snmp-server v1v2 community

Use this command to set the switch to check the v1v2 community string against the login access level.

Syntax

```
no snmp-server v1v2 community
```

Command mode

Global configuration mode

no snmp-server view

Use this command to delete the Management Information Base (MIB) view for the Signaling Network Management Protocol (SNMP) on the switch.

Syntax

```
no snmp-server view <view name> <subtree oid>
```

Parameters

This command includes the following options:

no snmp-server user view **followed by:**	
<view name>	Specifies the group name of the user. The range of values is 1 to 32 characters.
<subtree oid>	Specifies the object identifier prefix that defines the set of MIB objects accessible by this SNMP entity. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

no syslog host

Use this command to delete a syslog host.

Syntax

```
no syslog host <id>
```

where

<id> specifies the syslog host ID. The range of values is 1 to 10.

Command mode

Global configuration mode

nsna

Use this command to configure NSNA on ports.

Syntax

```
nsna
```

Parameters

This command uses the following parameters:

nsna **folowed by:**	
disable	Enables/disables the Nortel SNA state of the port.
dynamic [voip-vlans <value>]	Sets the Nortel SNAS 4050 dynamic port configuration, where <value> is the VoIP VLAN IDs (vlan-id[-vlan-id][,...]).

nsna **folowed by:**	
info	Shows the current Nortel SNA settings for the port.
uplink uplink-vlans	Defines the Nortel SNAS 4050 uplink VLAN list, where <value> is the Nortel SNA VLAN IDs (vlan-id[-vlan-id][,...]).

Command mode

Interface fastethernet or gigabitethernet mode

nsna enable

Use this command to enable NSNA.

Syntax

```
nsna enable
```

Note: You must enable SSH before you enable Nortel SNA globally. The command to enable Nortel SNA fails if you do not enable SSH.

Command mode

Global configuration mode

nsna nsnas

Use this command to configure the Nortel SNA 4050 subnet.

Syntax

```
nsna nsnas <ipaddr/mask>
```

where

<ipaddr/mask> is the Nortel SNAS 4050 pVIP address and network mask (a.b.c.d/<0-32> | a.b.c.d/x.x.x.x | default).

Parameters

This command includes the following parameters:

nsna nsnas <ipaddr/mask> **followed by:**	
port <value>	Defines the TCP port number for the Switch to Nortel SNAS 4050 Communication Protocol (SSCP) server. Values are in the range 1024–65535. The default setting is 5000.

Command mode

Global configuration mode

nsna phone-signature

Use this command to specify IP phone signatures for the NSNA solution.

Syntax

nsna phone-signature <LINE>

where

<LINE> is the phone signature string (for example: Nortel-i2007-A).

Command mode

Global configuration mode

nsna uplink vlans

Use this command to add the uplink port to the NSNA VLANs. You must have the uplink filter configured before you add the uplink port to the VLANs.

Syntax

nsna uplink vlans <vidlist>

where

<vidlist> is the NSNA uplink VLAN IDs, entered using the convention {vlan-id[-vlan-id][,...]}.

Command mode

Interface fastethernet or gigabitethernet mode

nsna vlan color

Use this command to configure the NSNA VLANs.

Syntax

nsna vlan <vid> color <red|yellow|green|voip>

where

<vid> is the VLAN ID in the range 2–4000.
<red|yellow|green|voip> is the color of the VLAN.

Parameters

This command includes the following parameters:

nsna vlan <vid> color <red|yellow|green|voip> **followed by:**	
filter <filter-id>	Sets the NSNA filter ID. Values are in the range 1–1024. ***Note:*** This parameter is not allowed for configuration of a VoIP VLAN. VoIP filters are part of the Red/Yellow filters.
yellow-submask <ipaddr/mask>	Sets the Yellow VLAN subnet IP and mask (a.b.c.d/<0-32>) ***Note:*** This parameter is only allowed for configuration of the Yellow VLAN. The Yellow subnet is the Remediation server IP address/subnet.

Command mode

Global configuration mode

radius

Use this command to configure Remote Access Dial-in User Services (RADIUS) on the switch. This command can also display global RADIUS settings.

Syntax

```
radius
[<enable|disable>]
[attribute-value <value> ]
[maxserver <INT> ]
[acct-enable|acct-disable]
[acct-attribute-value <value> ]
```

Parameters

This command includes the following options:

radius **followed by:**	
[<enable|disable>]	Enables or disables the RADIUS authentication feature.

radius **followed by:**	
[attribute-value <value>]	Specific to RADIUS authentication. Specifies the vendor-specific attribute value of the Access-Priority attribute to match the type value set in the dictionary file on the RADIUS server. Nortel recommends the default setting of 192 for Ethernet Routing Switch 8300 Series switches. The range of values is 192 to 240.
[maxserver <INT>]	Specific to RADIUS authentication. Specifies the maximum number of servers allowed for the switch. The range of values is 1 to 10.
[acct-enable | acct-disable]	Enables or disables RADIUS accounting globally. RADIUS accounting cannot be enabled unless a valid server is configured. The default is **acct-disable**.
[acct-attribute-value <value>]	Specific to RADIUS accounting. Sets the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server. <value> must be different from the access-priority attribute value configured for authentication. The range of values is 192 to 240. The default value is 193.

radius

radius **followed by:**	
[access-priority-attribute <value>]	Specifies the value for Access-Priority attributes. The range of values is 192 to 240 and the default is 192.
acct	Enables radius accounting.

radius followed by:	
[acct-attribute-value <value>]	Specific to RADIUS accounting. Sets the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server. <value> must be different from the access-priority attribute value configured for authentication. The range of values is 192 to 240. The default value is 193.
[acct-include-cli-commands]	Includes CLI commands in RADIUS accounting updates.
[authentication]	Enables RADIUS authentication for CLI login.
<cr>	Enables RADIUS.
[clear-stat]	Clears RADIUS statistics.
[cli-commands-attribute<value>]	Specifies the integer value for the CLI-Commands attribute. The range of values is 192 to 240 and the default is 195.
[cli-profile]	Enables RADIUS CLI profiling. The default is disabled.
[command-access-attribute<value>]	Specifies the integer value for the Command-Access attribute. The range is 192 to 240 and the default is 194.
[maxserver <INT>]	Specific to RADIUS authentication. Specifies the maximum number of servers allowed for the switch. The range of values is 1 to 10 and the default is 10.
[acct-enable| acct-disable]	Enables or disables RADIUS accounting globally. RADIUS accounting cannot be enabled unless a valid server is configured. The default is acct-disable.
[acct-attribute-value <value>]	Specific to RADIUS accounting. Sets the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server.

radius **followed by:**	
	<value> must be different from the access-priority attribute value configured for authentication. The range of values is 192 to 240. The default value is 193.

Command mode

Global configuration mode

radius clear-stat

Use this command to clear statistics from the server for the Remote Access Dial-in User Services (RADIUS) on the switch.

Syntax

```
radius clear-stat
```

Command mode

Global configuration mode

radius info

Use this command to display global settings for the Remote Access Dial-in User Services (RADIUS) on the switch.

Syntax

```
radius info
```

Command mode

Global configuration mode

radius-server info

Use this command to display a list of all servers configured for Remote Access Dial-in User Services (RADIUS) on the switch.

Syntax

```
radius-server info
```

Command mode

Global configuration mode

show access-policy

Use this command to display the global access policy settings. If you specify a policy name, the settings for the policy are displayed.

Syntax

```
show access-policy [ <polname> ]
```

where

[<polname>] is an optional parameter that specifies the name of the access policy. The range is 0 to 15 characters.

Command mode

Privileged EXEC mode

show nsna

Use this command to view information on the state of NSNA on the switch.

Syntax

```
show nsna
```

Command mode

Privileged EXEC mode

show nsna client

Use this command to view information on NSNA clients that are currently connected to the switch.

Syntax

```
show nsna client [interface <interface-type>] | [<interface-id>] | [mac-address <H.H.H>]
```

where

<interface-type> is the port type (for example, FastEthernet)
<interface-id> is the slot/port number entered as {slot/port[-slot/port][,...]}
<H.H.H> is the MAC address of the host.

show nsna nsnas

Use this command to view information related to the Nortel SNAS 4050 subnet.

Syntax

```
show nsna nsnas <ipaddr/mask>
```

where

<ipaddr/mask> is the Nortel SNAS 4050 IP address and network mask (a.b.c.d/<0-32>).

Command mode

Privileged EXEC mode

show nsna interface

Use this command to view information related to the NSNA ports.

Syntax

```
show nsna interface [<interface-type>] [<interface-id>]
```

where

<interface-type> is the port type (for example, FastEthernet)
<interface-id> is the slot/port number entered as {slot/port[-slot/port][,...]}

Command mode

Privileged EXEC mode:

show nsna phone-signature

Use this command to view configure NSNA phone signatures.

Syntax

```
show nsna phone-signature <LINE>
```

where

<LINE> is the phone signature string (for example: Nortel-i2007-A).The <LINE> parameter can contain an asterisk (*) at the end of the string to indicate that all signatures that start with the specified string aredisplayed. For example, if you enter Nort* as the LINE parameter, output displays any signatures that start with the string Nort.

Command mode

Privileged EXEC mode

show nsna vlan

Use this command to view information related to the NSNA VLANs.

Syntax

```
show nsna vlan <vid>
```

where

<vid> is the VLAN ID in the range 1-4000.

show radius

Use this command to display the global status of Remote Access Dial-in User Services (RADIUS) information.

Syntax

```
show radius
```

Command mode

Privileged EXEC mode

show radius-server

Use this command to display current Remote Access Dial-in User Services (RADIUS) server configurations and statistics.

Syntax

```
show radius-server
```

Command mode

Privileged EXEC mode

show syslog

Use this command to display system log information for the entire system.

Syntax

```
show syslog
```

Command mode

Privileged EXEC mode

show syslog host

Use this command to display system log information for a specified host.

Syntax

```
show syslog host <id>
```

where

`<id>` specifies the host ID number.

Command mode

Privileged EXEC mode

snmp-server authentication-trap

Use this command to specify whether or not to send authentication failure traps of the Signaling Network Management Protocol (SNMP) transmission.

Syntax

```
snmp-server authentication-trap <enable|disable>
```

Parameters

This command includes the following options:

snmp-server authentication-trap **followed by:**	
enable	Enables sending authentication failure traps of the SNMP transmission.
disable	Disables sending authentication failure traps of the SNMP transmission.

Command mode

Global configuration mode

snmp-server contact

Use this command to set the contact information for the Signaling Network Management Protocol (SNMP) server.

Syntax

```
snmp-server contact <contact>
```

where

<contact> specifies the contact information.
The range of values is an ASCII string from 1 to 1024 characters (for example, a phone extension or e-mail address).

Command mode

Global configuration mode

snmp-server group

Use this command to configure view-based access for a Signaling Network Management Protocol (SNMP) group.

Syntax

```
snmp-server group
<group name>
<prefix>
<model>
<level> [match <value> ]
```

Parameters

This command includes the following options:

snmp-server group **followed by:**	
<group name>	Creates the new group access with this group name. The range of values is 1 to 32 characters.
<prefix>	Assigns a context prefix. The range of values is 1 to 32 characters.
<model>	Assigns the authentication checking to communicate to the switch. The options are **usm, snmpv1**, and **snmpv2c**.
<level>	Assigns the minimum level of security required to gain access rights allowed by this conceptual row.
[match <value>]	Specifies the context match. The options are **exact** and **prefix**. • **exact** specifies that all rows in which the context name exactly matches the context prefix are selected. • **prefix** specifies that all rows in which the starting octet of the context name exactly matches the context prefix are selected.

Command mode

Global configuration mode

snmp-server group info

Use this command to display current level parameter settings and next level directories for a Signaling Network Management Protocol (SNMP) group.

Syntax

snmp-server group info

Command mode

Global configuration mode

snmp-server group match

Use this command to change the group access context match in the v3 VACM table for a Signaling Network Management Protocol (SNMP) group.

Syntax

```
snmp-server group match
<group name>
<prefix>
<model>
<level> [match <value> ]
```

Parameters

This command includes the following options:

snmp-server group match **followed by:**	
<group name>	Creates the new group access with this group name. The range of values is 1 to 32 characters.
<prefix>	Assigns a context prefix. The range of values is 1 to 32 characters.
<model>	Assigns the authentication checking to communicate to the switch. The options are: **usm**, **snmpv1**, and **snmpv2c**.
<level>	Assigns the minimum level of security required to gain access rights allowed by this conceptual row.
[match <value>]	Specifies the context match. The options are **exact** and **prefix**. • **exact** specifies that all rows in which the context name exactly matches the context prefix are selected. • **prefix** specifies that all rows in which the starting octet of the context name exactly matches the context prefix are selected.

Command mode

Global configuration mode

snmp-server group view

Use this command to change the group access view name match in the v3 VACM table for a Signaling Network Management Protocol (SNMP) group.

Syntax

```
snmp-server group view
<group name>
<prefix>
<model>
<level>
[read <value> ]
[write <value> ]
```

Parameters

This command includes the following options:

snmp-server group view **followed by:**	
<group name>	Creates the new group access with this group name. The range of values is 1 to 32 characters.
<prefix>	Assigns a context prefix. The range of values is 1 to 32 characters.
<model>	Assigns the authentication checking to communicate to the switch. The options are: **usm, snmpv1,** and **snmpv2c**.
<level>	Specifies the minimum level of security required to gain access rights allowed by this conceptual row.
[read <value>]	
[write <value>]	

Command mode

Global configuration mode

snmp-server host

Use this command to create a server host for Signaling Network Management Protocol (SNMP) transmission.

Syntax

```
snmp-server host
```

Command mode

Global configuration mode

snmp-server host

Use this command to set a trap receiver for the Signaling Network Management Protocol (SNMP) transmission.

Syntax

```
snmp-server host
<ipaddr>
<v1|v2c>
<commstr>
```

Parameters

This command includes the following options:

snmp-server host **followed by:**	
`<ipaddr>`	Specifies the IP address of the trap receiver.
`<v1|v2c>`	Specifies the SNMP version. The options are: **v1** (version 1) or **v2c** (version 2).
`<commstr>`	Specifies the input community string of 1 to 1024 characters.

Command mode

Global configuration mode

snmp-server info

Use this command to display the current Signaling Network Management Protocol (SNMP) parameter settings.

Syntax

```
snmp-server info
```

Command mode

Global configuration mode

snmp-server location

Use this command to set the location information for the Signaling Network Management Protocol (SNMP) server.

Syntax

```
snmp-server location <location>
```

where

<location> specifies the SNMP location information. The range of values is an ASCII string from 1 to 1024 characters (for example, Finance).

Command mode

Global configuration mode

snmp-server member

Use this command to create a new Signaling Network Management Protocol (SNMP) group member with this user name.

Syntax

```
snmp-server member
<user name>
<model>
[ <group name> ]
```

This command includes the following options:

snmp-server member **followed by:**	
<user name>	Assigns a user name to the SNMP member. The range of values is 1 to 32 characters.
<model>	Specifies the message processing model to use when generating an SNMP message. The options are: **usm, snmpv1,** and **snmpv2c**.
[<group name>]	Assigns the SNMP member to a SNMP group for data access. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

snmp-server member info

Use this command to display current level parameter settings and next level directories for Signaling Network Management Protocol (SNMP) group members.

Syntax

```
snmp-server member info
```

Command mode

Global configuration mode

snmp-server member name

Use this command to change a Signaling Network Management Protocol (SNMP) group member name for the v3 VACM table.

Syntax

```
snmp-server member name
<user name>
<model>
<group name>
```

Parameters

This command includes the following options:

snmp-server member name **followed by:**	
<user name>	Assigns a user name to the SNMP member. The range of values is 1 to 32 characters.
<model>	Specifies the message processing model to use when generating an SNMP message. The options are: **usm, snmpv1,** and **snmpv2c**.
<group name>	Assigns the SNMP member to a SNMP group for data access. The range of values is 1 to 32 characters.

Command mode

Global configuration mode

no snmp-server member

Use this command to delete a Signaling Network Management Protocol (SNMP) group member from the v3 VACM table.

Syntax

```
no snmp-server member
```

Parameters

This command includes the following options:

no snmp-server member **followed by:**	
<user name>	Specifies the user name of the SNMP member. The range of values is 1 to 32 characters.
<model>	Specifies the message processing model to use when generating an SNMP message. The options are: usm, snmpv1, and snmpv2c.

Command mode

Global configuration mode

snmp-server name

Use this command to set the box or root level prompt name for the Signaling Network Management Protocol (SNMP) server.

Syntax

```
snmp-server name <prompt>
```

where

<prompt> specifies the root level prompt name for the SNMP server. The range of values is an ASCII string from 1 to 1024 characters (for example, LabSC7 or Closet4).

Command mode

Global configuration mode

snmp-server user

Use this command to create a new Signaling Network Management Protocol (SNMP) user in the User Security Model (USM) table on the switch.

Syntax

```
snmp-server user
<user name>
[ <auth protocol> ]
[auth <password> ]
[priv <password> ]
```

Parameters

This command includes the following options:

snmp-server user **followed by:**	
<user name>	Specifies a security name for the new SNMP user entry. The security name is an index to the table. The range is 1 to 32 characters.
[<auth protocol>]	Specifies an authentication protocol. If no value is entered, the entry has no authentication capability. The protocol choices are: **MD5** and **SHA**.
[auth <password>]	Specifies an authentication password. If no value is entered, the entry has no authentication capability. The range of values is 1 to 32 characters.
[priv <password>]	Specifies a privacy password. If no value is entered, the entry has no privacy capability. The range is 1 to 32 characters. ***Note:*** You must set authentication before you can set the privacy option.

Command mode

Global configuration mode

snmp-server user auth

Use this command to change the authentication password for a Signaling Network Management Protocol (SNMP) user on the switch.

Syntax

```
snmp-server user auth
<user name>
old-pass <value>
new-pass <value>
```

Parameters

This command includes the following options:

snmp-server user auth **followed by:**	
<user name>	Specifies the security name of the user whose authentication password is being changed. The security name is an index to the table. The range is 1 to 32 characters.
new-pass <value>	Specifies the new password.
old-pass <value>	Specifies the old password.

Command mode

Global configuration mode

snmp-server user info

Use this command to display current level parameter settings and next level directories for a Signaling Network Management Protocol (SNMP) user.

Syntax

```
snmp-server user info
```

Command mode

Global configuration mode

snmp-server user priv

Use this command to change the privacy password for a Signaling Network Management Protocol (SNMP) user on the switch.

Syntax

```
snmp-server user priv
<user name>
old-pass <value>
new-pass <value>
```

Parameters

This command includes the following options:

snmp-server user priv **followed by:**	
<user name>	Specifies the security name of the user whose privacy password is being changed. The security name is an index to the table. The range of values is 1 to 32 characters.
new-pass <value>	Specifies the new password.
old-pass <value>	Specifies the old password.

Command mode

Global configuration mode

snmp-server view

Use this command to configure the Management Information Base (MIB) view for the Signaling Network Management Protocol (SNMP) on the switch.

Syntax

```
snmp-server view
<view name>
<subtree oid> [mask <value> ]
[type <value> ]
```

Parameters

This command includes the following options:

snmp-server view **followed by:**	
<view name>	Specifies the group name of the user whose privacy password is being changed. The security name is an index to the table. The range of values is 1 to 32 characters.
<subtree oid>	Specifies the object identifier prefix that defines the set of MIB objects accessible by this SNMP entity. The range of values is 1 to 32 characters.

snmp-server view **followed by:**	
[mask <value>]	Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.
[type <value>]	Specifies whether access to a MIB object is granted or denied. The options are: • **included** (granted) • **excluded** (denied)

Command mode

Global configuration mode

snmp-server view info

Use this command to display the current level parameter settings and next level directories for the Management Information Base (MIB) view of the Signaling Network Management Protocol (SNMP) on the switch.

Syntax

```
snmp-server view info
```

Command mode

Global configuration mode

snmp-server view mask

Use this command to change the view mask for an entry in the Management Information Base (MIB) View table for the Signaling Network Management Protocol (SNMP) on the switch.

Syntax

```
snmp-server view mask
<view name>
<subtree oid>
<new-mask>
```

Parameters

<This command includes the following options:

snmp-server view mask **followed by:**	
<view name>	Specifies the group name of the user whose privacy password is being changed. The security name is an index to the table. The range of values is 1 to 32 characters.
<subtree oid>	Specifies the object identifier prefix that defines the set of MIB objects accessible by this SNMP entity. The range of values is 1 to 32 characters.
<new-mask>	Specifies the new bit mask used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.

Command mode

Global configuration mode

snmp-server view type

Use this command to change the type for an entry in the Management Information Base (MIB) View table for the Signaling Network Management Protocol (SNMP) on the switch.

Syntax

```
snmp-server view type
<view name>
<subtree oid>
<new-type>
```

Parameters

This command includes the following options:

snmp-server view type **followed by:**	
<view name>	Specifies the group name of the user whose privacy password is being changed. The security name is an index to the table. The range of values is 1 to 32 characters.

snmp-server view type **followed by:**	
<subtree oid>	Specifies the object identifier prefix that defines the set of MIB objects accessible by this SNMP entity. The range of values is 1 to 32 characters.
<new-type>	Specifies the new view type used.

Command mode

Global configuration mode

syslog host

Use this command to configure a host location for the system log information (syslog) host.

Syntax

```
syslog host <id>
[address <ipaddr> ]
[udp-port <port> ]
[facility <facility> ]
[<enable|disable>]
```

Parameters

This command includes the following options:

syslog host <id> **followed by:**	
<id>	Specifies the syslog host ID. The range of values is 1 to 10.
[address <ipaddr>]	Specifies the IP address of the UNIX system syslog host.
[udp-port <port>]	Specifies the UNIX system syslog host port number on which to send syslog messages to the syslog host. The range of values is 514 to 530.
[facility <facility>]	Specifies the UNIX system syslog host facility. The range of values is **LOCAL0** to **LOCAL7**.
[<enable|disable>]	Enables or disables sending syslog messages on the switch.

Command mode

Global configuration mode

syslog host

Use this command to specify the severity of syslog messages that require the messages to be sent to specified modules.

Syntax

```
syslog host <id>
[mapinfo <level> ]
[mapwarning <level> ]
[maperror <level> ]
[mapfatal <level> ]
```

Parameters

This command includes the following options:

syslog host <id> **followed by:**	
<id>	Specifies the syslog host ID. The range of values is 1 to 10.
[mapinfo <level>]	Specifies the severity level of syslog messages that require the messages to be sent to specified modules. The options are: **{emergency|alert|critical|error|warning|notice|info|debug}.**
[mapwarning <level>]	Specifies the severity level of syslog messages that require the messages to be sent to specified modules. The options are: **{emergency|alert|critical|error|warning|notice|info|debug}.**

syslog host <id> **followed by:**	
[maperror <level>]	Specifies the severity level of syslog messages that require the messages to be sent to specified modules. The options are: {emergency|alert|critical|error|warning|notice|info|debug}.
[mapfatal <level>]	Specifies the severity level of syslog messages that require the messages to be sent to specified modules. The options are: {emergency|alert|critical|error|warning|notice|info|debug}.

Command mode

Global configuration mode

syslog host create

Use this command to create a system log information (syslog) host and configure a host location.

Syntax

```
syslog host <id> create
[<enable|disable>]
[address <ipaddr> ]
[facility <facility> ]
[udp-port <port> ]
```

Parameters

This command includes the following options:

syslog host <id> create **followed by:**	
<id>	Specifies the syslog host ID. The range of values is 1 to 10.
[<enable|disable>]	Enables or disables the syslog host.
[address <ipaddr>]	Specifies the IP address of the UNIX system syslog host.

syslog host <id> create **followed by:**	
[facility <facility>]	Specifies the UNIX system syslog host facility. The range of values is **LOCAL0** to **LOCAL7**.
[udp-port <port>]	Specifies the UNIX system syslog host port number on which to send syslog messages to the syslog host. The range of values is 514 to 530.

Command mode

Global configuration mode

syslog host severity

Use this command to specify the severity level of system log information (syslog) messages sent for the specified modules.

Syntax

```
syslog host <id> severity
<info|warning|error|fatal>
[<info|warning|error|fatal>]
[<info|warning|error|fatal>]
[<info|warning|error|fatal>]
```

Parameters

This command includes the following options:

syslog host <id> severity **followed by:**	
<id>	Specifies the syslog host ID. The range of values is 1 to 10.
<info|warning| error|fatal>	Specifies the severity levels of syslog messages sent for the specified modules. The options are: {info|warning|error|fatal}.
[<info|warning| error|fatal>]	Specifies the severity levels of syslog messages sent for the specified modules. The options are: {info|warning|error|fatal}.

syslog host <id> severity **followed by:**	
[<info|warning|error|fatal>]	Specifies the severity levels of syslog messages sent for the specified modules. The options are: {info|warning|error|fatal}.
<info|warning|error|fatal>]	Specifies the severity levels of syslog messages sent for the specified modules. The options are: {info|warning|error|fatal}.

Command mode

Global configuration mode

show eapol

This command displays the global settings updated to provide guest vlan and eap-mac-max information.

Syntax

```
show eapo
```

Command mode

Privileged Exec mode

show eapol

This command displays the guest VLAN and multihost configurations.

Syntax

```
show eapol
```

Command mode

Privileged Exec mode

IP protocol commands

This chapter describes NNCLI IP protocol commands and their parameters.

IP Protocol Commands
"no ip forward-protocol udp" (page 223)
"ip forward-protocol udp portfwdlist" (page 224)
"no ip forward-protocol udp portfwdlist" (page 224)
"no ip forward-protocol udp porffwdlist" (page 225)
"ip forward-protocol udp" (page 225)
"no ip forward-protocol udp" (page 226)
"ip icmp-unreach-msg" (page 226)
"no ip icmp-unreach-msg" (page 227)
"ip irdp enable" (page 227)
"no ip irdp enable" (page 227)
"ip irdp" (page 227)
"no ip irdp" (page 228)
"default ip irdp" (page 228)
"no ip irdp multicast" (page 229)
"ip irdp vlan multicast" (page 229)
"no ip irdp vlan multicast" (page 229)
"ip more-specific-non-local-route enable" (page 229)
"no ip more-specific-non-local-route enable" (page 230)
"ip ospf" (page 230)
"ip ospf spf-run" (page 232)
"ip prefix-list" (page 232)
"no ip prefix-list" (page 233)
"ip routing" (page 233)
"no ip routing" (page 233)
"ip rip" (page 234)
"ip route" (page 238)
"no ip route" (page 239)
"ip route preference protocol" (page 239)
"lldp" (page 240)
"default lldp" (page 241)
"lldp port status" (page 241)
"no lldp port" (page 241)
"default lldp port" (page 242)
"lldp tx-tlv" (page 242)
"lldp port status" (page 242)

IP Protocol Commands
"no lldp status" (page 242)
"default lldp port" (page 243)
"lldp tx-tlv" (page 243)
"no lldp tx-tlv" (page 243)
"default lldp tx-tlv" (page 244)
"lldp tx-tlv dot1" (page 244)
"no lldp tx-tlv dot1" (page 244)
"default lldp tx-tlv dot1" (page 245)
"lldp tx-tlv dot3" (page 245)
"default lldp tx-tlv dot1" (page 245)
"lldp tx-tlv dot3" (page 245)
"no lldp tx-tlv dot3" (page 245)
"default lldp tx-tlv dot3" (page 246)
"lldp tx-tlv med" (page 246)
"no lldp tx-tlv med" (page 246)
"default lldp tx-tlv med" (page 247)
"lldp location-identification civic-address " (page 247)
"manualtrigger ip rip interface vlan" (page 248)
"network" (page 248)
"no network" (page 249)
"network" (page 249)
"network area" (page 249)
"redistribute enable" (page 250)
"redistribute source" (page 250)
"route-map " (page 251)
"route-map " (page 252)
"no route-map " (page 254)
"router ospf " (page 254)
"router ospf enable" (page 254)
"no router ospf enable" (page 254)
"router rip" (page 255)
"router rip enable" (page 255)
"no router rip enable" (page 255)
"router-id" (page 255)
"show interface loopback" (page 259)

IP Protocol Commands
"show ip arp" (page 259)
"show ip dhcp-relay fwd-path" (page 260)
"show ip dhcp-relay counters" (page 260)
"show ip forward-protocol udp" (page 260)
"show ip forward-protocol udp portfwdlist" (page 260)
"show ip forward-protocol udp interface" (page 261)
"show ip global" (page 261)
"show ip irdp" (page 261)
"show ip irdp interface" (page 262)
"show ip irdp interface vlan" (page 262)
"show ip interface" (page 261)
"Showing OSPF general configuration information" (page 262)
"Showing OSPF router acceptance parameter information" (page 262)
"Showing OSPF area information" (page 262)
"Showing OSPF external lsas information" (page 263)
"Showing OSPF interface authentication information" (page 263)
"Showing OSPF default-metric information" (page 264)
"Showing OSPF host-route information" (page 264)
"Showing OSPF interface statistics information" (page 264)
"Showing OSPF authentication information" (page 265)
"Showing OSPF timers information" (page 265)
"Showing OSPF interface information" (page 265)
"Showing OSPF lsdb information" (page 266)
"Showing OSPF neighbours information" (page 266)
"Showing OSPF redistribute information" (page 267)
"Showing OSPF statistics information" (page 267)
"Showing OSPF interface timers information" (page 267)
"show ip prefix-list" (page 268)
"show ip rip" (page 268)
"show ip rip interface" (page 268)
"show ip rip interface" (page 268)
"show ip route" (page 269)
"show ip route preference" (page 270)

IP Protocol Commands
"show route-map " (page 269)
"show ip route preference" (page 270)
"show ip route " (page 270)
"show ip static-route" (page 270)
"show ip tcp" (page 271)
"show lldp" (page 271)
"show lldp neighbor" (page 273)
"show ports stats dhcp-relay " (page 274)
"show slpp" (page 274)
"show vlan nlb-mode" (page 274)
"slpp" (page 256)
"no slpp" (page 257)
"slpp port" (page 257)
"no slpp port" (page 258)
"timer basic" (page 274)
"timers basic holddown" (page 276)
"trap enable" (page 276)
"vlan nlb-mode" (page 277)
"no vlan nlb-mode" (page 277)

accept adv-rtr

This command configures OSPF acceptance:

Syntax

```
accept adv-rtr <ipaddr>
```

Where:

- <ipaddr> is router ID.

Parameters

This command includes the following parameters:

accept adv-rtr followed by:	
	Accept ospf router.
<ipaddr> enable	Enable OSPF accept on particular router. <ipaddr> is router ID.

accept adv-rtr followed by:	
<ipaddr> metric-type [type1|type2|any]	Set OSPF accept on particular router with particular metric type. <ipaddr> is router ID. [type1|type2|any] is metric type.
<ipaddr> route-policy WORD<0-64>	Set OSPF accept on particular router with particular routing policy. <ipaddr> is router ID. WORD<0-64> is policy name.

To set OSPF acceptance to a default condition, precede the command with the word **default**.

Example:

```
default accept adv-rtr <ipaddr>
```

To cancel or delete OSPF acceptance, precede the command with the word **no**.

Example:

```
no accept adv-rtr <ipaddr>
```

Command mode

Router Configuration mode.

area

This command creates and configures an OSPF area:

Syntax

```
area <ipaddr>
```

Where:

- <ipaddr> is area ID.

Parameters

This command includes the following options:

area followed by:	
<ipaddr> import [external|noexternal|nssa]	Set particular area as stub or nssa or normal area. <ipaddr> is area ID. [external|noexternal|nssa] is area type.

area **followed by:**	
1.1.1.1 import-summaries enable	Enable import-summaries on particular area.
1.1.1.1 stub-metric <0-16777215>	Set stub-metric on particular area. <0-16777215> is stub metric value.
range <ipaddr> <ipaddr/x | ipaddr/x.x.x.x | default> [summary-link|nssa-extlink] [advertise-metric <0-65535>|advertise-mode [summarize|suppress|no-summarize]]	Creates an OSPF area range with the specified IP address and advertising mode. <ipaddr> is area ID. <ipaddr/x | ipaddr/x.x.x.x | default> is ip range. [summary-link|nssa-extlink] is lsa type. <0-65535> is metric value. [summarize|suppress|no-summarize] is advertise.
virtual-interface <ipaddr> <ipaddr>	Creates a virtual interface area identifier. <ipaddr> is area ID. <ipaddr> is router ID.
virtual-interface message-digest-key <ipaddr> <ipaddr> <1-255> md5-key WORD<1-16>	Adds an md5 key to the virtual interface. At most, two md5 keys can be configured to an interface. Multiple md5 key configurations are used for md5 transitions without bringing down an interface. <ipaddr> is area ID. <ipaddr> is virtual-interface ID. <1-255> is key ID. WORD<1-16> is md5 key.

To set an OSPF area configuration to a default condition, precede the command with the word **default**.

Example:

```
default area <ipaddr>
```

To cancel or delete an OSPF area configuration, precede the command with the word **no**.

Example:

```
no area <ipaddr>
```

Command mode

Router Configuration mode.

as-boundary-router enable

This command enables OSPF Autonomous System boundary router:

Syntax

```
as-boundary-router enable
```

To set OSPF Autonomous System boundary router to a default condition, use the following command:

```
default as-boundary-router enable
```

To cancel or delete OSPF Autonomous System boundary router, use the following command:

```
no as-boundary-router enable
```

Command mode

Router Configuration mode.

auto-vlink enable

This command enables OSPF auto-vlink:

Syntax

```
auto-vlink enable
```

To set OSPF auto-vlink to a default condition, use the following command:

```
default auto-vlink enable
```

To cancel or delete OSPF auto-vlink, use the following command:

```
no auto-vlink enable
```

Command mode

Router Configuration mode.

default-metric

This command allows you to set the value of the default metric to apply to routes imported into the RIP domain.

Syntax

```
default-metric <metric>
```

where

metric is an integer value with a range of 0 to 15. The default is 8.

This is the metric used for routes not learned through RIP if a route policy does not specify a metric for a particular protocol, such as OSPF.

> ***Note:*** You cannot assign a value of 0 to the default import metric. Entering the command **default-metric 0** deconfigures this parameter and restores the default value of 8.

Command mode

Router Configuration mode

default default-metric

The default import metric is the metric used for routes not learned through RIP if a route policy does not specify a metric for a particular protocol, such as OSPF. This command allows you to return the default import metric to its default value of 8.

Syntax

```
default default-metric
```

or

```
default-metric 0
```

Command mode

Router Configuration mode

default timer basic

This command allows you to return global timer parameters to their default values, use the following command:

Syntax

```
default timer basic
```

Parameter

This command includes the following parametes:

`default timer basic` **followed by:**	
`holddown`	Resets the RIP holddown timer to its default value of 120 seconds on all the interfaces. The value of the holddown timer is the length of time (in seconds) that RIP will continue to advertise a network after determining that it is unreachable.
`timeout`	Resets the RIP timeout timer to its default value on all the interfaces. The default value is set indirectly by the global update time parameter. By default, the timeout timer is set at 6 times the update timer, in accordance with the RFC specification. With a default global update parameter setting of 30 seconds, the default timeout interval is 180 seconds.
`update`	Resets the RIP update timer to its default value of 30 seconds. The value of the update timer is the time interval (in seconds) between regular RIP updates.

Command mode

Router Configuration mode

host-route

This command configures OSPF host-route parameters:

Syntax

host-route <ipaddr>

Where:

- <ipaddr> is IP address.

Parameters

This command includes the following parameters:

host-route followed by:	
area <ipaddr>	<ipaddr> is the area id.
<ipaddr> metric <0-65535>	Creates an OSPF host route for the IP address and sets the metric (cost) for the host route. <ipaddr> is ip address <0-65535> is metric value

To set an OSPF host-route parameters to a default condition, use the following command:

default host-route <ipaddr>

To cancel or delete an OSPF host-route parameters, use the following command:

no host-route <ipaddr>

Command mode

Router Configuration mode.

interface loopback

The commands to configure CLIP are in the loopback interface configuration mode. This command allows you to access the loopback interface configuration mode.

Syntax

interface loopback <id>

where

<id> is an integer you assign to identify the CLIP interface. The range is 1 to 32.

Note: You can configure a maximum of 32 CLIP interfaces on each device.

Command mode

Loopback interface configuration mode

ip address

This command allows you to create a CLIP interface in loopback interface configuration mode.

Syntax

```
ip address [id <id> ]
```

where

`<id>` is an integer you assign to identify the CLIP interface. The range is 1 to 32.

Parameter

This command includes the following parameters:

`ip address` **followed by:**	
`<ipaddr>`	The IP address of the CLIP interface.
`<net mask>`	The subnet mask of the CLIP interface.

Command mode

Interface configuration mode

no ip address

This command allows you to delete a CLIP interface.

Syntax

```
no ip address
```

Command mode

Interface configuration mode

ip alternative-route

Use this command to enable alternative routing in the Ethernet Routing Switch 8300. The alternative route feature allows fast convergence to an alternative route in those cases when the primary route is unavailable. By default, alternative routing is enabled in the Ethernet Routing Switch 8300, thus allowing re-routing to an alternative link.

Syntax

```
ip alternative-route
```

Command mode

Global configuration mode

no ip alternative-route

Use this command to disable alternative routing in the Ethernet Routing Switch 8300.

Syntax

```
no ip alternative-route
```

Command mode

Global configuration mode

ip arp

Use this command to add a static entry to the Address Resolution Protocol (ARP) table on the Ethernet Routing Switch 8300.

Syntax

```
ip arp
multicast-mac-flooding <enable | disable>
timeout <value>
<ipaddr> <macaddr> <slot/port> <vid>
```

Parameters

This command includes the following parameters:

ip arp **followed by:**	
multicast-mac-flooding <*enable* | *disable*>	Enables or disables multicast MAC flooding.
timeout <*value*>	Sets the ARP entries lifetime aging period. Valid values here range from 1-32767 minutes.
<*ipaddr*> <*macaddr*> <*slot/port*> <*vid*>	Adds a static ARP entry to the specified IP address, MAC address, slot/port, or VLAN ID. ***Note:*** An IP address must be assigned to a VLAN before a static ARP entry can be associated with it.

Command mode

Interface configuration mode

no ip arp

Use this command to delete an ARP entry at the port level.

Syntax

```
no ip arp <ipaddr>
```

where

`<ipaddr>` specifies the IP address in dotted decimal notation {a.b.c.d.}.

Command mode

Interface configuration mode

ip arp proxy

Use this command to enable proxy ARP on a VLAN.

Syntax

```
ip arp proxy
```

Command mode

Interface VLAN mode

no ip arp proxy

Use this command to disable proxy ARP on a VLAN.

Syntax

```
no ip arp proxy
```

Command mode

Interface VLAN mode

ip arp response

Use this command to enable ARP response.

Syntax

```
ip arp response
```

Command mode

Interface VLAN mode

no ip arp response

Use this command to disable ARP response

Syntax

no ip arp response

Command mode

Interface VLAN mode

ip default-ttl

Use this command to set the default time-to-live (ttl) value for a routed packet.

Syntax

```
ip default-ttl <seconds>
```

where

<seconds> specifies the maximum number of seconds between 1 and 255 before a packet is discarded. The default value of 255 is inserted in the ttl field whenever one is not supplied.

Command mode

Global configuration mode

ip dhcp-relay broadcast

Use this command to enable dhcp-relay broadcasting.

Syntax

```
ip dhcp-relay broadcast <enable|disable>
```

Command mode

Interface VLAN mode

ip dhcp-relay

Use this command to enable dhcp-relay.

Syntax

```
ip dhcp-relay <enable|disable>
```

Command mode

Interface VLAN mode

ip dhcp-relay max-hop

Use this command to specify the value for the dhcp-relay max-hop.

Syntax

```
ip dhcp-relay max-hop <max-hop>
```

Command mode

Interface VLAN mode

ip dhcp-relay min-sec

Use this command to specify the minutes and seconds of dhcp-relay.

Syntax

```
ip dhcp-relay min-sec <min-sec>
```

Command mode

Interface VLAN mode

ip dhcp-relay mode

Use this command to specify the dhcp-relay mode.

Syntax

```
config interface vlan ip dhcp-relay mode
<bootp|dhcp|bootp_dhcp>
```

Command mode

Interface VLAN mode

ip forward-protocol udp

A UDP forwarding protocol specifies which port to watch for incoming UDP broadcasts, as well as the protocol name for that port.

Use this command to create a UDP forwarding protocol.

Syntax

```
ip forward-protocol udp <updport> <protoname>
```

where:

- **updport** is an integer value with a range of 1 to 65535.
- **protoname** is a string length {1..15}.

Command mode

Global configuration mode

no ip forward-protocol udp

This command allows you to delete a UDP protocol, use the following command in **Global Config** mode:

Syntax

```
no ip forward-protocol udp <updport>
```

where

updport specifies the port protocol to delete.

Command mode

Global configuration mode

ip forward-protocol udp portfwdlist

A UDP forwarding policy is a list of one or more UDP protocols that are assigned a forwarding IP address. Each forwarding policy also has a unique name and number. You can repeat this command to add additional UDP protocols to an existing policy, to add another forwarding IP address for an existing UDP protocol, or to update the policy name.

Use this command to create a UDP forwarding policy.

Syntax

ip forward-protocol udp portfwdlist <listid> <updport> <ipaddr> [<name>]

where:

- **listid** is an integer value from 1 to 1000. This provides a unique identifier for the UDP forwarding policy.
- **updport** is an integer value with a range of 1 to 65535. This port must have a defined UDP protocol.
- **ipaddr** is the forwarding destination. You can enter either a specific server IP address, or an IP limited broadcast in dotted-decimal notation {a.b.c.d}.
- **name** is a string length {1..15} used to describe the forwarding policy. If no value is entered when creating a new UDP forwarding policy, they system generates a name automatically.

Command mode

Global configuration mode

no ip forward-protocol udp portfwdlist

Use this command to delete an entire UDP forwarding policy.

Syntax

no ip forward-protocol udp portfwdlist <listid>

where

listid specifies the UDP forwarding policy ID to delete.

Command mode

Global configuration mode

no ip forward-protocol udp porffwdlist

This command allows you to remove a UDP protocol from an existing UDP forwarding policy.

Syntax

no ip forward-protocol udp portfwdlist <listid> <updport> <ipaddr>

where:

- **listid** specifies the UDP forwarding policy ID to delete.
- **updport** specifies the port protocol to remove.
- **ipaddr** is the forwarding destination for this port protocol. You can enter either a specific server IP address, or an IP limited broadcast in dotted-decimal notation {a.b.c.d}.

Command mode

Global configuration mode

ip forward-protocol udp

Use this command to apply a UDP forwarding policy, to set the broadcast mask, and to set maximum TTL value for this interface.

Syntax

ip forward-protocol udp [vlan <vlan>]

where

vlan is an optional integer with a range of 1 to 4000, specifying a particular VLAN on this interface to apply the specified settings.

This command includes the following parameters:

ip forward-protocol udp [vlan] **followed by:**	
portfwdlist <listid>	Apply the specified UDP forwarding policy to this interface, and (optionally) set the broadcast mask for this interface and the maximum TTL value. • **listid** is an integer with a range of 1 to 1000.

ip forward-protocol udp [vlan] **followed by:**	
broadcastmask <mask>	Set the broadcast mask for this interface, and (optionally) set the maximum TTL value. • **mask** is the subnet mask in A.B.C.D format.
maxttl <maxttl>	Set the maximum TTL value for this interface. • **maxttl** is an integer value with a range of 1 to 16. The default value is 4.

Command mode

Interface configuration mode

no ip forward-protocol udp

Use this command to remove UDP forwarding policies from an interface.

Syntax

no ip forward-protocol udp [vlan <vlan>] [portfwdlist <listid>] [broadcastmask <mask>]

where:

- **vlan** specifies a particular VLAN to remove the UDP forwarding policy from.
- **listid** specifies the UDP forwarding policy ID to remove.
- **mask** specifies the subnet mask to remove.

If no optional parameters are included with this command, then all UDP forwarding policies are removed from the interface being configured.

Command mode

Interface configuration mode

ip icmp-unreach-msg

Use this command to enable the Internet Control Message Protocol (ICMP) unreachable message. When enabled, this command allows the generation of ICMP net unreachable messages if the destination network is not reachable from this switch. These messages assist in determining if the routing switch is reachable over the network.

Syntax

```
ip icmp-unreach-msg
```

Command mode

Global configuration mode

no ip icmp-unreach-msg

Use this command to disable the ICMP unreachable message.

Syntax

```
no ip icmp-unreach-msg
```

Command mode

Global configuration mode

ip irdp enable

By default, router discovery is disabled. Use this command to enable router discovery.

Syntax

```
ip irdp enable
```

Command mode

Global configuration mode

no ip irdp enable

Use this command to disable router discovery.

Syntax

```
no ip irdp enable
```

Command mode

Global configuration mode

ip irdp

Enabling router discovery

By default, router discovery is disabled. Use this command to enable router discovery.

Syntax

```
ip irdp
```

Command mode

Global configuration mode

Configuring router discovery on VLANs

Use this command to configure router discovery on VLANs.

Syntax

```
ip irdp
```

Parameters

This command includes the following parameters:

ip irdp **followed by:**	
address <A.B.C.D>	Specifies the route discovery advertisement address.
holdtime <value>	Specifies the holdtime for router advertisements.
maxadvertinterval <value>	Specifies the Maximum Advertisement interval for router advertisements.
minadvertinterval <value>	Specifies the Minimum Advertisement interval for router advertisements.
multicast	Enables router discovery by setting the advertise flag to true.
preference <value>	Specifies the preference level for router advertisement.

Command mode

Interface VLAN mode

no ip irdp

Use this command to disable router discovery.

Syntax

```
no ip irdp
```

Command mode

Global configuration mode

default ip irdp

Use this command to set the router discovery to default values.

Syntax

```
default ip irdp
```

Command mode

Global configuration mode

no ip irdp multicast

Use this command to disable router discovery on VLANs.

Syntax

```
no ip irdp multicast
```

Command mode

Interface VLAN mode

ip irdp vlan multicast

Use this command to enable router discovery on a selected VLAN.

Syntax

```
ip irdp vlan <vid> multicast
```

where

<vid> is the ID of the selected VLAN.

Command mode

Interface VLAN mode

no ip irdp vlan multicast

Use this command toe disable router discovery on a specific VLAN.

Syntax

```
no ip irdp vlan <vid> multicast
```

where

<vid> is the ID of the selected VLAN.

Command mode

Interface VLAN mode

ip more-specific-non-local-route enable

This command enables static routes to networks that are not directly connected. When enabled, this command allows a more specific non-local route to go into the routing table. The default is disabled.

Syntax

```
ip more-specific-non-local-route enable
```

Command mode

Global configuration mode

no ip more-specific-non-local-route enable

This command allows you to disable that feature that permits a more specific non-local route to go into the routing table.

Syntax

```
no ip more-specific-non-local-route enable
```

Command mode

Global configuration mode

ip ospf

This command configures OSPF on an interface:

Syntax

```
ip ospf
```

Parameters

This command includes the following options:

ip ospf followed by:	
`advertise-when-down enable`	The network on this interface is advertised as up, even if no ports in the VLAN are active
`area<ipaddr>`	Set the vlan interface in a particular area. <ipaddr> is area ID.
`authentication-key WORD<0-8>`	Set the authentication key for the VLAN. WORD<0-8> is simple authentication key.
`authentication-type [message-digest|none|simple]`	Set the OSPF authentication type for the VLAN. [message-digest|none|simple] is authentication type.
`authentication-key WORD<0-2147483647>`	Set the OSPF dead interval for the VLAN. The dead interval is the number of seconds the switch's OSPF neighbors should wait before assuming that this OSPF router is down. PT_LONG<0-2147483647> is dead-interval value
`enable`	Enables OSPF on the VLAN.
`hello-interval <1-65535>`	Set the OSPF hello interval for the VLAN. The hello interval is the number of seconds between hello packets sent on this VLAN. <1-65535> is hello-interval value
`interface-type [broadcast|passive]`	Set the interface type, default is broadcast. A passive interface will not form neigborship with other routers. [broadcast|passive] is interface type.

ip ospf followed by:	
message-digest-key <1-255>md5-key WORD<0-16>	Set the authentication message-digest-key for the VLAN. <1-255> is message-digest-key ID WORD<0-16> is md5 key
metric <1-65535>	Set the OSPF metric for the VLAN. The switch advertises the metric in router link advertisements. <1-65535> is metric value
primary-md5-key <1-255>	Set primary message-digest-key. <1-255> is message-digest-key ID
priority <0-255>	Set the OSPF priority for the VLAN during the election process for the designated router. The VLAN with the highest priority number is the best candidate for the designated router. If the priority is 0, the VLAN cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. <0-255> is priority value
retransmit-interval <0-3600>	Set the retransmit interval for the virtual interface. The retransmit interval is the number of seconds between link-state advertisement retransmissions. <0-3600> is retransmit interval value
transit-delay <0-3600>	Sets the transmit delay for the virtual interface. The transmit delay is the estimated number of seconds it takes to transmit a link-state update over the interface. <0-3600> is transit delay value
vlan<1-4094>	Set ospf configuration on paticular vlan. <1-4094> is the vlan ID.

To configure OSPF parameters on an interface to a default condition, use the following command:

```
default ip ospf
```

To cancel or delete OSPF configuration parameters on an interface, use the following command:

```
no ip ospf
```

Command mode

Interface configuration mode

ip ospf spf-run

This command forces an OSPF SPF run:

Syntax

ip ospf spf-run

Command mode

User Exec mode

ip prefix-list

The prefix list is a list of networks used by route policies to define an action. You can create one or more IP prefix lists and apply that list to any IP route policy.

When you configure the ge (mask length from) field to be less than the le (mask length to) field, it can also be used as a range.

This command allows you to configure a prefix list.

Syntax

ip prefix-list <prefix-list name>

where

prefix-list name is a string length {1..64} that indicates the name of the prefix list

Parameter

This command includes the following parameters:

ip prefix-list <prefix-list name> **followed by:**	
<ipaddr/mask> [ge <value>] [le <value>]	Adds a prefix entry to the prefix list. Creates the prefix list if it does not already exist. • **ipaddr/mask {a.b.c.d/x|a.b.c.d/x.x.x.x|default}** is the IP address and network mask. • **ge <value>** is the lower bound of the mask length, where **value** is an integer value with a range of 0 to 32. The default is the mask length. • **le <value>** is the higher bound of the mask length, where **value** is an integer value with a range of 0 to 32. The default is the mask length.

ip prefix-list <prefix-list name> followed by:	
	Note: Lower bound and higher bound mask lengths together can define a range of networks
name <name>	Renames the prefix list specified in the command. • **name** is a string length {1..64}.

Command mode

Global configuration mode

no ip prefix-list

This command allows you to delete a prefix list.

Syntax

no ip prefix-list <prefix-list name>

Command mode

Global configuration mode

ip routing

Use this command to enable IP routing on the Ethernet Routing Switch 8300. By default, IP routing is enabled.

Syntax

ip routing

Command mode

Global configuration mode

no ip routing

Use this command to disable IP routing on the Ethernet Routing Switch 8300.

Syntax

no ip routing

Command mode

Global configuration mode

ip rip

Use this command to configure RIP on a specified VLAN interface.

Syntax

```
ip rip
```

Parameter

This command includes the following parameters:

ip rip **followed by:**	
advertise-when-down <enable|disable>	If enabled, the network on this interface will be advertised as up, even if the VLAN is down. The default is disabled. When you configure a VLAN without any link and enable advertise-when-down, it will not advertise your route until the VLAN is active. Then the route is advertised even when the link is down. To disable advertising based on link status, disable this parameter.
auto-summary <enable|disable>	Enables or disables automatic route aggregation on the interface. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a network of a different class. The default is disabled. Routes with different metrics can be aggregated. RIP uses the out metric associated with the first route found in the routing table that is to be aggregated.
cost <cost>	Sets the RIP cost for this interface. • **cost** is an integer value with a range of 1 to 15. The default value is 1.
default-listen <enable|disable>	Configures whether or not the interface will listen for RIP updates for the default route learned through RIP. The default is disabled.
default-supply <enable|disable>	Configures whether or not the interface will send RIP advertisements for the default route, if one exists in the routing table. The default is disabled.

ip rip **followed by:**	
domain <domain>	Specifies the value inserted into the Routing Domain field of all RIP packets sent on this interface. • **domain** is an integer value with a range of 0 to 65535. The default is 0.
holddown <seconds>	Sets the RIP holddown timer for the interface. The value of the holddown timer is the length of time (in seconds) that RIP will continue to advertise a network after determining that it is unreachable. • **seconds** is an integer value with a range of 0 to 360. The default value is set by the global holddown parameter, which has a default of 120 seconds. The interface timer setting overrides the global parameter. However, if you subsequently reset the global parameter, the global setting then overrides the interface timer setting.
in-policy <policy name>	Sets the RIP policy for inbound filtering on the interface. The in-policy determines which routes will be learned on the interface. • **policy name** is a string length {0..64}. To delete the policy, enter an empty string.
listen <enable|disable>	Configures whether or not the interface will listen for RIP routes. The default is enabled.

ip rip **followed by:**	
out-policy <policy name>	Sets the RIP policy for outbound filtering on the interface. The out-policy determines which routes will be advertised from the routing table on the interface. • **policy name** is a string length {0..64}. To delete the policy, enter an empty string.
poison <enable|disable>	Sets whether or not RIP routes on the interface learned from a neighbor are advertised back to the neighbor. • If disabled, split horizon is invoked, and IP routes learned from an immediate neighbor are not advertised back to the neighbor. • If enabled, the RIP updates sent to a neighbor from which a route is learned are "poisoned" with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. The default is disabled.
receive version <version>	Indicates which version of RIP updates the router will accept for this interface. The options for **version** are: • **rip1** — RIP version 1 (complies with RFC 1058). • **rip2** — RIP version 2 (complies with RFC 2453). • **rip1orrip2** — both versions of RIP. The default is **rip1orrip2**.

ip rip **followed by:**	
send version <version>	Indicates which version of RIP updates the router sends on this interface. The options for **version** are: • **notsend** — no updates are sent. • **rip1** — RIP version 1 (complies with RFC 1058; updates are broadcast). • **rip1comp** — compatible with RIP version 1 (RIP version 2 updates are broadcast using RFC 1058 route subsumption rules). • **rip2** — RIP version 2 (complies with RFC 2453; updates are multicast). The default is **rip1comp**.
supply <enable|disable>	Enables or disables the interface to supply RIP updates.
timeout <seconds>	Sets the RIP timeout interval for the interface. • **seconds** is an integer value with a range of 15 to 259200. The default value is set indirectly by the global update time parameter. By default, the timeout timer is set at 6 times the update timer, in accordance with the RFC specification. With a default global update timer setting of 30 seconds, the default timeout interval is 180 seconds. Configure the timeout parameter on the interface only if you want to break the relationship with the update timer. For example, if you have set the global update parameter to a very short interval in order to minimize the problem of fast convergence, the associated default timeout may be too short. In this case, configure the timeout interval manually.

ip rip **followed by:**	
	The interface timer setting overrides the global parameter. However, if you subsequently reset the global parameter, the global setting then overrides the interface timer setting. The timeout interval must be greater than the global update time parameter.
triggered <enable|disable>	Enables or disables automatic triggered updates for RIP on this interface. The default is disabled.

Command mode

Interface configuration mode

ip route

Use this command to create a new static route. You create static routes in order to route traffic from the Ethernet Routing Switch 8300 to other devices in the network, like an Ethernet Routing Switch 8600.

Syntax

```
ip route [route] [mask] [next-hop] [cost] preference
<value> <enable | disable]
<weight>
```

Parameters

This command includes the following parameters:

ip route *<ipaddr/mask>* **followed by:**	
[route] [mask] [next-hop] [cost]	Adds a static or default route to the switch. *route/mask* is the IP address and mask for the route's destination. *next-hop* <*value*> is the IP address of the next hop router; the next router at which packets must arrive on this route. *cost* <*value*> is the metric of the route. Valid values here are from 1-65535.

ip route ***<ipaddr/mask>*** **followed by:**	
preference <value>	*preference* <*value*> specifies the route preference value assigned to the routes. Valid values range from 1-255, with a default of 1.
<enable|disable>	Enables or disables the route.
<weight>	Specifies the route weight. Valid values range from 1-255.

Command mode

Global configuration mode

no ip route

Use this command to delete a static route.

Syntax

```
no ip route [route] [mask] [next-hop <value> ]
```

Parameters

This command includes the following parameters:

no ip route **followed by:**	
[route] [mask] [next-hop]	Deletes a static or default route to the switch. route/mask is the IP address and mask for the route's destination. next-hop <*value*> is the IP address of the next hop router; the next router at which packets must arrive on this route.

Command mode

Global configuration mode

ip route preference protocol

Use this command to configure route preferences by protocol.

Syntax

```
ip route preference protocol {static|rip} <value>
```

where **value** is an integer value with a range of 0 to 255, indicating the preference. The value of 0 is reserved for local routes. If two protocols have the same configured value, the default value is used to break the tie. The default preference values are:

- local routes = 0
- static routes = 5
- RIP routes = 100

This command includes the following options

ip route preference protocol {static|rip}<value>	
ospf-intra	Specifies the protocol type OSPF-intra.
ospf-inter	Specifies the protocol type OSPF-inter.
ospf-extern1	Specifies the protocol type OSPF-extern1.
ospf-extern2	Specifies the protocol type OSPF-extern2.

Command mode

Global configuration mode

lldp

Use this command to set the LLDP transmission parameters.

Syntax

```
lldp [tx-interval <5-32768>] [tx-hold-multiplier <2-10>]
[reinit-delay <1-10>] [tx-delay <1-8192>] [med-fast-start
<1-10>]
```

Parameter

This command includes the following parameters:

lldp **followed by**	
tx-interval <5-32768>	sets the global interval between successive transmission cycles (default value is 30)
tx-hold-multiplier <2-10>	sets the multiplier for the tx-interval used to compute the Time To Live value for the TTL TLV (default value is 4)
reinit-delay <1-10>	sets the delay for the reinitialization attempt if the adminStatus is disabled (default value is 2)

lldp **followed by**	
tx-delay <1-8192>	sets the minimum delay between successive LLDP frame transmissions (default value is 2)
med-fast-start <1-10>	sets the MED Fast Start repeat count value (default value is 3)

Command mode

Global configuration mode

default lldp

Use this command to set the LLDP transmission parameters to their default values. If no parameters are specified, the default lldp sets all parameters to their default parameters.

Syntax

```
default lldp [tx-interval ] [tx-hold-multiplier ]
[reinit-delay] [tx-delay] [med-fast-start]
```

Command mode

Global configuration mode

lldp port status

Use this command to set the LLDPU transmit and receive status on the ports.

rxonly: enables LLDPU receive only.

txAndRx: enables LLDPU transmit and receive.

txOnly: enables LLDPU transmit only. (default value is txAndRx)

Syntax

lldp port <portlist> status {rxOnly | txAndRx | txOnly}

Command mode

Interface configuration mode

no lldp port

Use this command to disable LLDP features on the port,

Syntax

```
no lldp port <portlist> [status]
```

Command mode

Interface configuration mode

default lldp port

This command sets the LLDP port parameters to their default values.

Syntax

```
default lldp port <portlist> [status]
```

Command mode

Interface configuration mode

lldp tx-tlv

This command sets the optional Management TLVs to be included in the transmitted LLDPDUs.

Syntax

```
lldp [port <portlist>] tx-tlv [port-desc] [sys-name]
[sys-desc] [sys-cap] [local-mgmt-addr]
```

Command mode

Interface configuration mode

lldp port status

This command sets the LLDPU transmit and receive status on the ports.

rxonly: enables LLDPU receive only.

txAndRx: enables LLDPU transmit and receive.

txOnly: enables LLDPU transmit only. (default value is txAndRx)

Syntax

```
lldp port <portlist> status {rxOnly | txAndRx | txOnly}
```

Command mode

Interface configuration mode

no lldp status

This command disables the LLDP features on the port.

Syntax

```
no lldp [status]
```

Command mode

Interface configuration mode

default lldp port

This command sets the LLDP port parameters to their default values.

Syntax

```
default lldp port <portlist> [status]
```

Command mode

Interface configuration mode

lldp tx-tlv

This command set the optional Management TLVs to be included in the transmitted LLDPDUs.

Syntax

```
lldp [port <portlist> tx-tlv [port-desc] [sys-name]
[sys-desc] [sys-cap] [local-mgmt-addr]
```

Parameters

This command includes the following parameters:

`lldp [port <portlist> tx-tlv` **followed by**	
`port-desc`	port description TLV (default value is false: not included)
`sys-name`	system name TLV (default value is false: not included)
`sys-desc`	system description TLV (default value is false: not included)
`sys-cap`	system capabilities TLV (default value is false: not included)
`local-mgmt-addr`	local management address TLV (default value is false: not included)

Command mode

Interface configuration mode

no lldp tx-tlv

This command specifies the optional Management TLVs not to include in the transmitted LLDPDUs

Syntax

```
no lldp [port <portlist> tx-tlv [port-desc] [sys-name]
[sys-desc] [sys-cap] [local-mgmt-addr]
```

Command mode

Interface configuration mode

default lldp tx-tlv

This command sets the LLDP Management TLVs to their default values,

Syntax

```
default lldp [port <portlist> tx-tlv [port-desc] [sys-name]
[sys-desc] [sys-cap] [local-mgmt-addr]
```

Command mode

Interface configuration mode

lldp tx-tlv dot1

This command sets the optional IEEE 802.1 organizationally-specifc TLVs to be included in the transmitted LLDPDUs

Syntax

```
lldp [port <portlist> tx-tlv dot1 [port-vlan-id] [vlan-name]
[port-protocol-vlan-id] [protocol-identity {EAP | LLDP | STP}
]
```

Parameters

This command includes the following parameters:

`lldp [port <portlist> tx-tlv dot1]` **followed by**	
`port-vlan-id`	Port VLAN ID TLV (default value is false: not included)
`vlan-name`	VLAN Name TLV (default value is none)
`port-protocol-vlan-id`	Port and Protocol VLAN ID TLV (default value is none)
`protocol-identity {EAP | LLDP | STP}`	Protocol Identity TLV (default value is none)

Command mode

Interface configuration mode

no lldp tx-tlv dot1

This command specifies the optional IEEE 802.1 TLVs to exclude in the transmitted LLDPDUs.

Syntax

```
no lldp [port <portlist>] tx-tlv dot1 [port-vlan-id]
[vlan-name] [port-protocol-vlan-id] [protocol-identity { EAP
| LLDP | STP } ]
```

Command mode

Interface configuration mode

default lldp tx-tlv dot1

This command resets the optional IEEE 802.1 organizationally-specifc TLVs to their default values.

Syntax

```
default lldp [port <portlist> ] tx-tlv dot1 [port-vlan-id]
[vlan-name ] [port-protocol-vlan-id] [protocol-identity {EAP
| LLDP | STP} ]
```

Command mode

Interface configuration mode

lldp tx-tlv dot3

This command specifies the optional IEEE 802.3 organizationally-specifc TLVs to be included in the transmitted LLDPDUs.

Syntax

```
lldp [port <portlist> ] tx-tlv dot3 [mac-phy-config-status]
[mdi-power-support] [link-aggregation][maximum-frame-size]
```

Parameters

This command includes the following parameters:

`lldp [port <portlist>] tx-tlv dot3` **followed by**	
`mac-phy-config-status`	MAC/Phy Configuration/Status TLV (default value is false: not included)
`mdi-power-support`	Power Via MDI TLV (default value is false: not included)
`link-aggregation`	Link Aggregation TLV (default value is false: not included)
`maximum-frame-size`	Maximum Frame Size TLV (default value is false: not included)

Command mode

Interface configuration mode

no lldp tx-tlv dot3

This command specifies the optional IEEE 802.3 TLVs not to include in the transmitted LLDPDUs.

Syntax

```
no lldp [port <portlist> ] tx-tlv dot3 [mac-phy-
config-status] [mdi-power-support] [link-aggregation]
[maximum-frame-size]
```

Command mode

Interface configuration mode

default lldp tx-tlv dot3

This command sets the optional IEEE 802.3 organizationally-specifc TLVs to their default values.

Syntax

```
default lldp [port <portlist> ] tx-tlv dot3 [mac-phy-
config-status] [mdi-power-support] [link-aggregation]
[maximum-frame-size]
```

Command mode

Interface configuration mode

lldp tx-tlv med

This command specifies the optional organizationally-specific TLVs for use by MED devices to be included in the transmitted LLDPDUs.

Syntax

```
lldp [port <portlist> ] tx-tlv med [capabilities]
[network-policy] [location] [extendedPSE]
```

Parameters

This command includes the following parameters:

`lldp [port <portlist>] tx-tlv med` **followed by**	
`capabilities`	Enables MED capabilities TLV (default value is false: not included).
`extendedPSE`	Enables extended PSE TLV (default value is false: not included).
`location`	Enables location Identification TLV (default value is false: not included).
`network-policy`	Enables Network Policy TLV (default value is false: not included).

Command mode

Interface configuration mode

no lldp tx-tlv med

This command specifies the optional Management TLVs not to include in the transmitted LLDPDUs.

Syntax

```
no lldp [port <portlist> ] tx-tlv med [capabilites]
[extendedPSE] [location] [network-policy]
```

Command mode

Interface configuration mode

default lldp tx-tlv med

This command sets the optional organizationally-specifc TLVs for MED devices to their default values.

Syntax

```
default lldp [port <portlist> ] tx-tlv med [capabilities]
[extendedPSE] [location] [network-policy]
```

Command mode

Interface configuration mode

lldp location-identification civic-address

This command specifies LLDP civic address parameters. Note: The maximum total size for the civic-address TLV is 256 bytes. If this TLV is any larger, the 8300 Series switch does not transmit it.

Syntax

```
lldp location-identification civic-address [country-code]
[additional-code] [additional-information] [apartment]
[block] [building] [city] [city-district ] [county]
[floor] [house-number] [house-number-suffix] [landmark]
[leading-street-direction] [name] [p.o.box] [place-type]
[postal-community-name] [postal/zip-code] [room-number]
[state] [street] [street-suffix] [trailing-street-suffix]
```

Command mode

Interface configuration mode

Parameters

This command includes the following parameters:

`lldp location-identification civic-address` **followed by**	
`country-code`	Country code value
`additional-code`	Additional code
`additional-information`	Additional location information
`apartment`	Unit (apartment, suite)
`block`	Neighborhood, block

lldp location-identification civic-address followed by	
building	Building (structure)
city	City, township, shi (JP)
city-district	City division, city district, ward
county	County, parish, gun (JP), district (IN)
floor	Floor
house-number	House number
house-number-suffix	House number suffix
landmark	Landmark or vanity address
leading-street-direction	Leading street direction
name	Residence and office occupant
pobox	Post office box
place-type	Office
postal-community-name	Postal community name
zip-code	Zip code
room-number	Room number
state	National subdivisions (state, canton, region)
street	Street
street-suffix	Street suffix
trailing-street-suffix	Trailing street suffix

manualtrigger ip rip interface vlan

Use this command to execute a manually triggered RIP update on a specified VLAN interface.

Syntax

manualtrigger ip rip interface vlan <vid>

where

vid is the VLAN ID.

Command mode

User EXEC mode

network

In addition to being enabled globally on the switch, RIP must be enabled separately on each participating interface.

This command enables RIP on an interface.

Syntax

network <ipaddr>

where

ipaddr indicates the IP address of the interface.

Command mode

Router Configuration mode

no network

Use this command to disable RIP on an interface.

Syntax

no network <ipaddr>

where

ipaddr indicates the IP address of the interface.

Command mode

Router Configuration mode

network

This command enables OSPF on an interface:

Syntax

network <ipaddr>

where:

- <ipaddr> is the interface network ip address.

To set OSPF on an interface to a default condition, use the following command:

default network <ipaddr>

To cancel or delete OSPF on an interface, use the following command:

no network <ipaddr>

Command mode

Router Config mode.

network area

This command sets an OSPF interface on a particular OSPF area:

Syntax

```
network <ipaddr> area <ipaddr>
```

where:

- <ipaddr> is interface network ip address.
- <ipaddr> is the area ID.

To set an OSPF interface on a particular OSPF area to a default condition, use the following command:

```
default network <ipaddr> area <ipaddr>
```

To cancel or delete an OSPF interface on a particular OSPF area, use the following command:

```
no network <ipaddr> area <ipaddr>
```

Command mode

Router Configuration mode.

redistribute enable

This command enables OSPF redistribution:

Syntax

```
redistribute enable
```

To set OSPF redistribution to a default condition, use the following command:

```
default redistribute enable
```

To cancel or delete OSPF redistribution, use the following command:

```
no redistribute enable
```

Command mode

Router Configuration mode.

redistribute source

This command creates OSPF redistribution from particular source, metric and type:

Syntax

```
redistribute source [direct|rip|static] [enable|metric
<0-65535>| metric-type [type1|type2|any]|route-policy
WORD<0-64>| subnets [allow|supress]]
```

where:

- [direct|rip|static] is source type

- <0-65535> is metric value
- [type1|type2|any] is metric type
- WORD<0-64> is policy name
- [allow|supress] is subnet redistribute type

To set OSPF redistribution from particular source, metric and type to a default condition, use the following command:

```
default redistribute source [direct|rip|static]
[enable|metric <0-65535>| metric-type
[type1|type2|any]|route-policy WORD<0-64>| subnets
[allow|supress]]
```

To cancel or delete OSPF redistribution from particular source, metric and type,use the following command:

```
no redistribute source [direct|rip|static] [enable|metric
<0-65535>| metric-type [type1|type2|any]|route-policy
WORD<0-64>| subnets [allow|supress]]
```

Command mode

Router Configuration mode.

route-map

This command allows you to create a route policy and specify the action to be taken when a route policy is selected for a specific route.

Syntax

route-map <policy name>

where

policy name is a string length {0..64}indicating the name you assigned to the policy

The **route-map <policy name>** command includes the following parameters.

route-map <policy name> **followed by:**	
<seq number>	Specifies the sequence number. The range is 1 to 65535.
permit [<seq number>]	Allows the route.
deny [<seq number>]	Denies the route.

Command mode

Global configuration mode

route-map

This command allows you to enable and configure a route policy.

Syntax

route-map <policy name> <seq number>

where:

- **policy name** is a string length {0..64} indicating the name assigned to the policy
- **seq number** indicates the sequence number. The range is 1 to 65535.

  Note: You must enable a route policy before you can configure its match and set parameters.

Parameter

This command includes the following parameters.

route-map <policy name> <seq number> **followed by:**	
enable	Enables the route policy with the policy name and sequence number specified in the command.
match [interface <prefix-list>] [metric <metric>] [network <prefix-list>] [next-hop <prefix-list>] [protocol <protocol name>] [route-source <prefix-list>]	If configured, the switch matches the specified criterion: • **interface <prefix-list>** — matches the IP address of the received interface against the contents of the specified prefix list, where **prefix-list** is a string length {0..1027}. Applicable to RIP only. • **metric <metric>**— matches the metric of the incoming advertisement or existing route against the specified value, where **metric** is an integer value with a range of 0 to 65535. If 0, then this field is ignored. The default is 0. • **network <prefix-list>** — matches the destination network against the contents of the specified prefix list, where **prefix-list** is a string length {0..1027}.

route-map <policy name> <seq number> **followed by:**	
	• **next-hop <prefix-list>** — matches the next hop IP address of the route against the contents of the specified prefix list, where **prefix-list** is a string length {0..1027}. • **protocol <protocol name>** — matches the protocol through which the route is learned, where **protocol name {any|xxx}** is a string length {0..40} and **xxx** is **local|rip|static** or any combination separated by | (vertical line). Used for RIP announce policies only. • **route-source <prefix-list>** — matches the source IP address for RIP routes against the contents of the specified prefix list, where **prefix-list** is a string length {0..1027}. This field is ignored for all other route types.
name <policy name>	Renames a policy once it has been created. This command changes the name field for all sequence numbers under the given policy. • **policy name** is a string length {0..64}.
set [injectlist <prefix-list>] [ip-preference <pref-value>] [mask <ipaddr>]	If configured, the switch sets the specified parameter: • **injectlist <prefix-list>** — replaces the destination network of the route that matches this policy with the contents of the specified prefix list, where **prefix-list** is a string length {0..1027}. • **ip-preference <pref-value>** — specifies the route preference value to be assigned to the route that matches this policy, where **pref-value** is an integer value with a range of 0 to 255. If 0, the global preference value is used. The default is 0. Used for accept policies only. • **mask <ipaddr>** — sets the mask of the route that matches this policy, where **ipaddr** is a valid contiguous IP mask. Used for RIP accept policies only.

Command mode

Global configuration mode

no route-map

This command allows to delete a route policy.

Syntax

```
no route-map <policy name> <seq number>
```

where:

- **policy name** is a string length {0..64} indicating the name assigned to the policy
- **seq number** indicates the sequence number. The range is 1 to 65535.

Command mode

Global configuration mode

router ospf

This command allows you to enter Router Config mode for OSPF. Once in Router Config mode, you can configure OSPF global parameters:

Syntax

```
router ospf
```

Command mode

Global configuration mode

router ospf enable

This command enables OSPF globally on the switch

Syntax

```
router ospf enable
```

To disable OSPF globally on the switch, use the following command:

```
no router ospf enable
```

Command mode

Global configuration mode

no router ospf enable

This command disables OSPF globally on the switch

Syntax

```
no router ospf enable
```

Command mode

Global configuration mode

router rip

This command allows you to enter Router Config mode for RIP. Once in Router Config mode, you can configure the RIP global timer and default metric parameters:

Syntax

```
router rip
```

Command mode

Global configuration mode

router rip enable

This command enables RIP globally on the switch.

Syntax

router rip enable

Command mode

Global configuration mode

no router rip enable

This command disables RIP globally on the switch.

Syntax

```
no router rip enable
```

Command mode

Global configuration mode

router-id

This command sets the OSPF router ID:

Syntax

```
router-id <ipaddr>
```

where:

- <ipaddr> is the router ID.

To set OSPF router ID to a default condition, use the following command:

```
default router-id <ipaddr>
```

To cancel or delete OSPF router ID, use the following command:

```
no router-id <ipaddr>
```

Command mode

Router Configuration mode

slpp

This command is used to configure Simple Loop Protection Protocol (SLPP).

Syntax

```
slpp
```

Parameters

This command includes the following parameters:

Parameter	Description
`operation`	Enables the SLPP operation.
`ethertype <1-65535|0x1-0xffff>`	Specifies the SLPP PDU ether type. Enter a value from 1 to 65535 in hexadecimal (0x8104) or decimal (33028) format. The default is 0x8104.
`tx-interval <500-5000>`	Sets the SLPP packet transmit interval. The range is 500 to 5000 ms, and the default is 500 ms.
`vid <1-4000>`	Adds VLANs to a SLPP transmission list. Enter a vlan id from 1-4000.

Command mode

Global configuration mode

Default slpp

Use this command to set the SLPP parameters to default.

Syntax

```
default slpp
```

Parameters

Parameter	Description
`operation`	Sets the SLPP operation to default: disable.

Parameter	Description
`ethertype`	Sets the SLPP PDU ether type to default: 0x8104.
`tx-interval`	Sets the SLPP packet transmit interval to default: 500 ms.

Command mode

Global configuration mode

no slpp

Use this command to disable SLPP parameters.

Syntax

```
no slpp
```

Parameters

This command includes the following parameters:

Parameter	Description
`<cr>`	Indicates a carriage return.
`operation`	Disables the SLPP operation.
`vid <1-4000>`	Deletes VLANs from a SLPP transmission list. Enter a VLAN ID from 1-4000.

Command mode

Global configuration mode

slpp port

Use this command to configure SLPP on a port.

Syntax

```
slpp port [port <portlist>] [packet-rx ] [packet-rx-threshold]
```

where

`<portlist>` is the slot/port.

Parameters

This command includes the following parameters:

Parameter	Description
packet-rx	Enables SLPP packet reception on the listed ports.
packet-rx-threshold	Specifies the SLPP reception threshold on the ports. Enter a value from 1-500.

Command mode

Interface fastethernet or gigabitethernet mode

default slpp port

Use this command to set the SLPP parameters on a port to default.

Syntax

default slpp [port<portlist>] [packet-rx] [packet-rx-threshold]

where

portlist is the slot/port.

Parameters

This command includes the following parameters:

Parameter	Description
packet-rx	Sets the SLPP operation on the listed port or ports to default:disable
packet-rx-threshold	Sets the SLPP PDU reception threshold on the ports to default: 1.

Command mode

Interface fastethernet or gigabitethernet mode

no slpp port

Use this command to cancel the configuration of SLPP parameters.

Syntax

```
no slpp [port <portlist>] [packet-rx]
```

where

`<portlist>` is the slot/port.

Parameters

This command includes the following parameter:

Parameter	Description
`packet-rx`	Disables SLPP packet reception on the listed ports

Command mode

Interface fastethernet or gigabitethernet mode

show interface loopback

This command allows you to view the CLIP interfaces, enter the following command in any mode:

Syntax

```
show interface loopback
```

show ip arp

Use this command to display the Address Resolution Protocol (ARP) table.

Syntax

```
show ip arp [ip <ipaddr> ] [-s <value> ]
```

Parameters

This command includes the following options:

`show ip arp` **followed by:**	
`[<ipaddress>]`	Specifies the selected net IP address for the table.
[-s <*value*>] `[-s<value>]`	Specifies the selected subnet in the format: {a.b.c.d/x | a.b.c.d/x.x.x.x | default}

Command mode

Interface configuration mode

show ip dhcp-relay fwd-path

This command display the dhcp-relay forward path

Syntax

```
show ip dhcp-relay fwd-path
```

Command mode

Privileged EXEC mode

show ip dhcp-relay counters

This command displays the ip dhcp-relay counters.

Syntax

```
show ip dhcp-relay counters
```

Command mode

Privileged EXEC mode

show ip forward-protocol udp

This command allows you to view the existing UDP forwarding protocol.

Syntax

```
show ip forward-protocol udp
```

Command mode

User EXEC mode

show ip forward-protocol udp portfwdlist

This command allows you to display a list of all UDP forwarding policies.

Syntax

```
show ip forward-protocol udp portfwdlist [ <listid> ]
```

where

listid is the specific UDP forwarding policy number. Allowable values range from 1 to 1000. If a **listid** is specified, then the system only shows protocols and forwarding addresses for that UDP forwarding policy. If no **listid** is specified, then the system shows all UDP forwarding policies.

Command mode

User EXEC mode

show ip forward-protocol udp interface

This command allows you to display all UDP forwarding policies applied to this interface, together with settings and general usage statistics for each forwarding policy:

Syntax

```
show ip forward-protocol udp interface
```

Parameter

This command includes the following parameters:

ip forward-protocol udp interface **followed by:**	
[vlan <vlan>]	Display the UDP forwarding policy applied to an existing VLAN. If no VLAN ID number is provided, applied policies to all interfaces are shown. • **vlan** is a specific vlan ID number. Allowable values range from 1 to 4000.

show ip global

Use this command to display the global IP configuration settings.

Syntax

```
show ip global
```

Command mode

Interface configuration mode

show ip interface

Use this command to display the IP interfaces on the switch.

Syntax

```
show ip interface
```

Command mode

User EXEC mode

show ip irdp

Use this command to view the router discovery status.

Syntax

```
show ip irdp
```

Command mode

User EXEC mode

show ip irdp interface

Use this command to view the router discovery status on ports.

Syntax

```
show ip irdp interface {fastethernet|gigabitethernet}
```

Command mode

User EXEC mode

show ip irdp interface vlan

Use this command to view the router discovery status on VLANs.

Syntax

```
show ip irdp interface vlan [<vid>]
```

where

[<vid>}] is the ID of the selected VLAM. It is an integer in the range of 1 to 4000.

Command mode

User EXEC mode

show ip ospf

This command displays information about the OSPF general configuration:

Syntax

```
show ip ospf
```

Command mode

User EXEC mode

show ip ospf accept

This command displays information about the OSPF router acceptance parameter configuration:

Syntax

```
show ip ospf accept
```

Command mode

User EXEC mode

show ip ospf area

This command displays information about the OSPF area configuration:

Syntax

```
show ip ospf area
```

Parameters

This command includes the following parameters:

show ip ospf area followed by:	
`<cr>`	Display ospf area information. <cr> is carriage return.
`<ipaddr>`	Display ospf area information with area ID. <ipaddr> is area ID.
`area-range`	Display ospf area range information
`area-range <ipaddr>`	Display ospf area range information with area ID. <ipaddr> is area ID.

Command mode

User EXEC mode

show ip ospf ase

This command displays information about the OSPF external lsas configuration:

Syntax

```
show ip ospf ase
```

Parameters

This command includes the following parameters:

show ip ospf ase followed by:	
`<cr>`	Display ospf external lsas information. <cr> is carriage return.
`metric-type<1-2>`	Display ospf external lsas metric-type information. <1-2> is metric type 1 or type 2.

Command mode

User EXEC mode

show ip ospf authentication interface

This command displays information about the OSPF interface authentication configuration:

Syntax

```
show ip ospf authentication interface
```

Parameters

This command includes the following parameters:

show ip ospf authentication interface followed by	
`<cr>`	Display ospf authentication on interface. <cr> is carriage return.
`vlan`	Display ospf authentication on vlan interface.
`vlan <1-4094>`	Display ospf authentication on particular vlan interface. <1-4094> is the vlan ID.

Command mode

User EXEC mode

show ip ospf default-metric

This command displays information about the OSPF default-metric configuration:

Syntax

```
show ip ospf default-metric
```

Command mode

User EXEC mode

show ip ospf host-route

This command displays information about the OSPF host-route configuration:

Syntax

```
show ip ospf host-route
```

Command mode

User EXEC mode

show ip ospf ifstats

This command displays information about the OSPF interface statistics:

Syntax

```
show ip ospf ifstats [detail|mismatch|<ipaddr>]
```

where:

- *detail* is shown more detail information

- *mismatch* is shown mismatch information
- *<ipaddr>* is interface ip address

Command mode

User EXEC mode

show ip ospf int-auth

This command displays information about the OSPF authentication configuration:

Syntax

```
show ip ospf int-auth
```

Command mode

User EXEC mode

show ip ospf int-timers

This command displays information about the OSPF timers configuration:

Syntax

```
show ip ospf int-timers
```

Command mode

User EXEC mode

show ip ospf interface

This command displays information about the OSPF interface configuration:

Syntax

```
show ip ospf interface
```

Parameters

This command includes the following parameters:

show ip ospf interface followed by	
`<cr>`	Display ospf interface information. <cr> is carriage return.
`vlan`	Display ospf vlan interface information.
`vlan <1-4094>`	Display ospf information on particular vlan interface. <1-4094> is the vlan ID.

Command mode

User EXEC mode

show ip ospf lsdb

This command displays information about the OSPF lsdb configuration:

Syntax

```
show ip ospf lsdb
```

Parameters

This command includes the following parameters:

show ip ospf isdb followed by	
`<cr>`	Display ospf lsdb info information. <cr> is carriage return.
`adv-rtr <ipaddr>`	Display ospf lsdb information on particular advertisement router. <ipaddr> is router ID.
`adv-rtr <ipaddr> detail`	Display ospf detail lsdb information on particular advertisement router. <ipaddr> is router ID.
`area <ipaddr>`	Display ospf lsdb information on particular area. <ipaddr> is area ID.
`detail`	Display ospf detail lsdb information.
lsa-type `lsa-type <0-7>`	Display particular type of ospf lsdb information. <0-7> is for typ1 to type 7.
`lsid <ipaddr>`	Display ospf lsdb infomation with a particular lsid. <ipaddr> is lsa ID.

Command mode

User EXEC mode

show ip ospf neighbours interface

This command displays information about OSPF neighbours:

Syntax

```
show ip ospf neighbours interface
```

Parameters

This command includes the following parameters:

show ip ospf interface followed by	
`<cr>`	Display all ospf neighbours. <cr> is carriage return.

show ip ospf interface followed by	
`vlan`	Display all ospf neighbours on a vlan interface.
`vlan <1-4094>`	Display all ospf neighbours on a particular vlan interface. <1-4094> is the vlan ID.

Command mode

User EXEC mode

show ip ospf redistribute

This command displays information about the OSPF redistribute configuration:

Syntax

```
show ip ospf redistribute
```

Command mode

User EXEC mode

show ip ospf stats

This command displays information about the OSPF statistics:

Syntax

```
show ip ospf stats
```

Command mode

User EXEC mode

show ip ospf timer interface

This command displays information about OSPF interface timers:

Syntax

```
show ip ospf timer interface
```

Parameters

This command includes the following parameters:

show ip ospf timer interface followed by	
`<cr>`	Display ospf timers information on an interface. <cr> is carriage return.

show ip ospf timer interface followed by	
`vlan`	Display ospf timers information on a vlan interface.
`vlan <1-4094>`	Display ospf timers information on a particular vlan interface. <1-4094> is the vlan ID.

Command mode

User EXEC mode

show ip prefix-list

This command allows you to view prefix list information:

Syntax

```
show ip prefix-list
```

Command mode

User EXEC mode

show ip rip

Use this command to display information about the RIP global configuration on the switch.

Syntax

```
show ip rip
```

Command mode

Global or Interface configuration mode

show ip rip interface

Use this command to display information about a specific RIP interface or all RIP interfaces on the switch.

Syntax

```
show ip rip interface [vlan <vid> ]
```

where

`vid` is the interface VLAN ID.

Command mode

Global or Interface configuration mode

show ip route

Use this command to display the existing IP route table for the switch or for a specific net or subnet.

Syntax

```
show ip route [ <ipaddr> ] [-s <value> ] [alternative]
```

Parameters

This command includes the following options:

show ip route **followed by:**	
`[-s<value>]`	Specifies a subnet in the format: {a.b.c.d x.x.x.x}.
`[alternative]`	Displays alternative routes.
`<iipaddr>`	Specifies the selected net IP address: (1.2. = 1.2.0.0) {a.b.c.d}.

Command mode

Interface configuration mode

show ip routing

Use this command to display the status of IP routing on the switch.

Syntax

```
show ip routing
```

Command mode

Interface configuration mode

show route-map

This command allows you to view a route policy, enter the following command in **User EXEC** mode:

Syntax

```
show route-map [ <policy name> <seq number>][detail]
```

where:

- **`policy name`** is a string length {0..64} indicating the name assigned to the policy
- **`seq number`** indicates the sequence number. The range is 1 to 65535.

Command mode

User EXEC mode

show ip route

This command allows you to view the route table,

Syntax

```
show ip route [ <ip address> ] [-s <value> ] [alternative]
```

where:

- **<ip address>** is the specific net (1.2. = 1.2.0.0) {a.b.c.d}.
- **-s <value>** is the specific subnet {**a.b.c.d/x**|**a.b.c.d/x.x.x.x**|**default**}.
- **alternative** specifies the alternative-route you wish to display.

Command mode

User EXEC mode

show ip route preference

This command allows you to view route preferences.

Syntax

```
show ip route preference
```

Command mode

User EXEC mode

show ip static-route

Use this command to display the existing IP static routes for the switch or for a specific net or subnet.

Syntax

```
show ip static-route
[ <ip address> ]
[-s <value> ]
```

Parameters

This command includes the following options:

show ip static-route **followed by:**	
[*ip* <*ipaddr*>]	Specifies the selected net IP address: (1.2. = 1.2.0.0) {a.b.c.d}.
[-s <*value*>]	Specifies the selected subnet in the format: {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.

Command mode

Interface configuration mode

show ip tcp

Use this command to view the current TCP switch connections.

Syntax

```
show ip tcp
<info-connections>
<statistics-global>
<properties-global>
```

Parameters

This command includes the following options:

show ip tcp **followed by:**	
`<info-connections>`	Displays TCP connection table information.
`<statistics-global>`	Displays TCP global statistics.
`<properties-global>`	Displays TCP global statistics.

Command mode

Interface configuration mode

show lldp

This command displays the LLDP parameters for the local system.

Syntax

```
show lldp
```

Parameters

This command includes the following parameters:

show lldp **followed by:**	
interface [FastEthernet | GigabitEthernet] <portlist>	Displays LLDP port parameters.
local-sys-data {dot1 | dot3 | med |detail}	Displays the organizationally-specific TLV properties on the local switch: • dot1: displays the 802.1 TLV properties • dot3: displays the 802.3 TLV properties • med: displays the MED TLV properties • detail: displays all organizationally specific TLV properties To display the properties of the optional management TLVs, include only the local-sys-data parameter in the command.
mgmt-sys	Displays the local management system data.
pdu-tlv-size	Displays the different TLV sizes and the number of TLVs in an LLDPDU.
[rx-stats] [FastEthernet | GigabitEthernet] <portlist>	Displays the LLDP receive statistics for ports on the local system.
stats	Displays the LLDP table statistics for the remote system.
[tx-stats] [FastEthernet | GigabitEthernet] <portlist>	Displays the LLDP transmit statistics for ports on the local system.
tx-tlv {dot1 | dot3 | med | [FastEthernet | GigabitEthernet] <portlist> }	Displays which TLVs are transmitted from the local switch in LLDPDUs: • dot1: displays status for 802.1 TLVs • dot3: displays status for 802.3 TLVs • med: displays status for MED TLVs • [FastEthernet | GigabitEthernet] [portlist] • displays the status for management TLVs for specific ports. To display the transmission status of the optional management TLVs for all ports, include only the tx-tlv parameter in the command.

Command mode

User EXEC mode

show lldp neighbor

This command displays the LLDP parameters for the neighbor system.

Syntax

```
show lldp neighbor
```

Parameters

This command includes the following parameters:

show lldp **followed by:**	
[neighbor [FastEthernet | GigabitEthernet] <portlist>]	Displays the learned LLDP neighbors by port.
neighbor { dot1 [vnlan-names | protocol-id] } | [dot3] | { med [capabilities] [network-policy] [location] [extended-power] } | { [FastEthernet | GigabitEthernet] <portlist>}	Displays the neighbor TLVs: • dot1: displays 802.1 TLVs: — vlan-names: VLAN Name TLV — protocol-id: Protocol Identity TLV • dot3: displays 802.3 TLVs • med: displays MED TLVs: — capabilities: Capabilities TLV — network-policy: Network Policy Discovery TLV — location: Location Identification TLV — extended-power: Extended Power-via-MDI TL • [FastEthernet | GigabitEthernet] <portlist> : displays neighbor TLVs for the specified port

Command mode

User EXEC mode

show lldp neighbor-mgmt-addr

Use this command to display the LLDP neighbor management address.

Syntax

```
show lldp neighbor-mgmt-addr
```

Parameters

This command includes the following parameters.

show lldp neighbor-mgmt-addr **followed by:**	
<cr>	Indicates a carriage return.
[FastEthernet | GigabitEthernet]	Specifies the learned LLDP neighbors by type of port.
<portlist>	Displays the learned LLDP neighbors by port.

Command mode

Privileged EXEC mode

show slpp

Use this command to display SLPP information.

Syntax

```
show slpp
```

Command mode

Privileged EXEC mode

show ports stats dhcp-relay

Use this command to display port statistics for dhcp-relay.

Syntax

```
show ports stats dhcp-relay broadcast [ <ports> ]
```

Command mode

Privileged EXEC mode

show vlan nlb-mode

Use this command to display the NLBS mode.

Syntax

```
show vlan nlb-mode
```

Command mode

Privileged EXEC mode

timer basic

Use this command to set the global update, holddown, and timeout timers.

Syntax

```
timer basic
```

Parameter

This command includes the following options:

timer basic **followed by:**	
holddown <seconds>	Sets the RIP holddown timer. The value of the holddown timer is the length of time (in seconds) that RIP will continue to advertise a network after determining that it is unreachable. • **seconds** is an integer value with a range of 0 to 360. The default is 120 seconds. The global **holddown** parameter sets the value of the holddown timer for the VLAN interfaces, but you can override the value for a specific interface.
timeout <seconds>	Sets the RIP timeout interval. • **seconds** is an integer value with a range of 15 to 259200. The default value is set indirectly by the global update time parameter. By default, the timeout timer is set at 6 times the update timer, in accordance with the RFC specification. With a default global update parameter setting of 30 seconds, the default timeout interval is 180 seconds. The default global timeout setting changes when the global update time parameter is changed. Configure the timeout parameter only if you want to break the relationship with the update timer. For example, if you have set the global update parameter to a very short interval in order to minimize the problem of fast convergence, the associated default timeout may be too short. In this case, configure the timeout interval manually.

timer basic **followed by:**	
	The global **timeout** parameter sets the value of the timeout timer for the VLAN interfaces, but you can override the value for a specific interface .
update <seconds>	Sets the RIP update timer. The value of the update timer is the time interval (in seconds) between regular RIP updates. • **seconds** is an integer value with a range of 1 to 2147483647. The default is 30 seconds. The global **updatetime** parameter sets the update timer for the VLAN interfaces. The **updatetime** value must be less than the timeout interval.

Command mode

Router Configuration mode

timers basic holddown

This command sets the OSPF holddown timer value:

Syntax

```
timers basic holddown <0-60>
```

where:

- <0-60> is holddown timer value in seconds.

To set OSPF holddown timer value to a default value, use the following command in Router Config mode:

```
default timers basic holddown
```

Command mode

Router Configuration mode.

trap enable

This command enables OSPF traps:

Syntax

```
trap enable
```

To set OSPF trap to a default condition, use the following command in Router Config mode:

```
default trap enable
```

To disable OSPF traps, use the following command in Router Config mode:

```
no trap enable
```

Command mode

Router Configuration mode

vlan nlb-mode

Use this command to configure network load balancing (NLBS) on a specific VLAN.

Syntax

```
vlan nlb-mode <vid> <igmp-mcast|multicast|unicast>
```

where

<vid> is the VLAN ID from 1 to 4000.
<disable|igmp-mcast|multicast|unicast> specifies the mode of the NLBS feature. NLBS must be in the disable mode, which is the default mode, before you can choose one of the other three modes.

Command mode

Global configuration mode

no vlan nlb-mode

Use this command to configure NLSB in disable mode.

Syntax

```
no vlan nlb-mode <vid>
```

where

<vid> is the VLAN ID from 1 to 4000.

Command mode

Global configuration mode

Layer 2 and 3 operations commands

This chapter describes NNCLI layer 2 and layer 3 operations commands and their parameters.

Layer 2 Operations Commands
"show mlt stats" (page 290)
"show spanning-tree" (page 291)
"show spanning-tree config" (page 291)
"show interface vlan" (page 291)
"show vlan autolearn-mac" (page 292)
"show vlan vid basic" (page 292)
"show vlan vid fdb-filter" (page 293)
"show vlan vid fdb-static" (page 293)
"show interfaces vlan ip" (page 294)
"show vlan manual-edit-mac" (page 294)
"show vlan members" (page 294)
"show vlan static-mcastmac" (page 294)
"spanning-tree stp" (page 295)
"spanning-tree stp add-ports" (page 296)
"spanning-tree stp create" (page 297)
"telnet-access" (page 298)
"spanning-tree stp remove-ports" (page 297)
"no spanning-tree" (page 298)
"vlan action" (page 299)
"vlan add-mlt" (page 299)
"vlan members" (page 300)
"vlan qos-level" (page 301)
"no vlan" (page 301)
"vlan create type port" (page 302)
"vlan create type protocol-ApltkEther2Snap" (page 302)
"vlan create type protocol-decEther2" (page 303)
"vlan create type protocol-decOtherEther2" (page 304)
"vlan create type protocol-ipEther2" (page 305)
"vlan create type protocol-ipv6Ether2" (page 305)
"vlan create type protocol-ipx802.2" (page 306)
"vlan create type protocol-ipx802.3" (page 307)
"vlan create type protocol-ipxEther2" (page 308)
"vlan create type protocol-ipxSnap" (page 308)
"vlan create type protocol-Netbios" (page 309)
"vlan create type protocol-RarpEther2" (page 310)

Layer 2 Operations Commands

bcast-mcast-rate-limit enable

This command enables rate limiting on a port.

Syntax

```
bcast-mcast-rate-limit {port <portlist>}<percent value>
enable
```

where

`port <portlist>` is the list of ports, on which you enable rate limiting.

Parameters

This command includes the following parameters:

Parameter	Description
`<percent value>`	Specifies the rate limit to use, expressed as a percentage. The value can be from 1-100.

Command mode

Interface configuration mode

ist

This command configures an IST MLT from an existing MLT.

Syntax

```
ist [ip <A,B,C,D> ] [vlan <1-4000>]
```

Parameter

This command includes the following parameters:

Parameter	Description
`ip <A,B,C,D>`	Specifies the peer IP address for the IST.
`vlan <1-4000>`	Specifies a VLAN ID for the IST.

Command mode

MLT Interface Configuration mode

no ist

This command clears the IST configuration.

Syntax

```
no ist [ip]
```

where

`[ip]` specifies the peer IP address for the IST.

Command mode

MLT Interface Configuration mode

ist enable

This command enables the IST MLT.

Syntax

```
ist enable
```

Command mode

MLT Interface Configuration mode

no ist enable

This command disables the IST.

Syntax

```
no ist enable
```

Command mode

MLT Interface Configuration mode

no mlt encapsulation dot1q

This command removes encapsulation from a link aggregation group.

Syntax

```
no mlt <mid> encapsulation dot1q
```

Parameters

This command includes the following parameters:

Parameter	Description
`<mid>`	Specify a link aggregation group number from 1 to 31.

Command mode

Global configuration mode

no mlt name

This command removes a link aggregation group name.

Syntax

```
no mlt <mid> name
```

Parameters

This command includes the following parameters:

Parameter	Description
`<mid>`	Specify a link aggregation group number from 1 to 31.

Command mode

Global configuration mode

interface mlt

This command enters the MLT Interface Configuration command mode.

Syntax

```
interface mlt <1-31>
```

Parameters

This command includes the following parameters:

Parameter	Description
`mlt<1-31>`	Specifies the ID of the MLT to configure.

Command mode

Global configuration mode

smlt

This command creates an SMLT from an existing MLT.

Syntax

```
smlt <1-31>
```

Parameters

This command includes the following parameters:

Parameter	Description
`smlt<1-31>`	Specifies the SMLT ID.

Command mode

MLT Interface Configuration mode

no smlt

This command deletes the SMLT.

Syntax

```
no smlt <1-31>
```

Command mode

MLT Interface Configuration mode

smlt

This command configures an interface as a single-port SMLT.

Syntax

```
smlt <1-512>
```

Parameters

This command includes the following parameters:

Parameter	Description
`smlt <1-512>`	Specifies the ID for the single-port SMLT

Command mode

Interface Configuration mode

no smlt

This command deletes the single-port SMLT.

Syntax

```
no smlt
```

Command mode

Interface Configuration mode

mlt members

Use this command to add members to the MultiLink Trunking (MLT) on the switch.

Syntax

```
mlt <mid> member <slot/ports>
```

Parameter

This command includes the following options:

`mlt <mid> member` **followed by:**	
`<mid>`	Specifies the MLT ID. The range of values is 1 to 31.
`<slots/ports>`	Specifies the applicable members in member list form: `{ slot/port [- slot/port ] [, ...] }`.

Command mode

Global configuration mode

mlt add-vlan

Use this command to add an existing VLAN to the MultiLink Trunking (MLT) on the switch.

Syntax

mlt <mid> add-vlan <vid>

Parameter

This command includes the following options:

mlt <mid> add-vlan **followed by:**	
<mid>	Specifies the MLT ID. The range of values is 1 to 31.
<vid>	Specifies the VLAN ID. The default range of values is 1 to 4000.

Command mode

Global configuration mode

mlt name

Use this command to name the MultiLink Trunk (MLT) on the switch. .

Syntax

mlt <mid> name <string>

Parameters

This command includes the following parameters:

mlt <mid> name <string> **followed by:**	
<mid>	Specifies the MLT ID. The range of values is 1 to 31.
<string>	Specifies the name of the MLT. The range of values is 0 to 20 alphanumeric characters.

Command mode

Global configuration mode

no mlt members

Use this command to remove members from the MultiLink Trunking (MLT) on the switch.

Syntax

no mlt <mid> member <slot/ports>

Parameter

This command includes the following options:

`no mlt <mid> member` **followed by:**	
`<mid>`	Specifies the MLT ID. The range of values is 1 to 31.
`<ports>`	Specifies the applicable members in member list form: `{ slot/port [- slot/port ] [, ...] }`.

Command mode

Global configuration mode

mlt remove-vlan

Use this command to remove a VLAN from the MultiLink Trunking (MLT) on the switch.

Syntax

`mlt <mid> remove-vlan <vid>`

Parameter

This command includes the following options:

`mlt <mid> remove-vlan` **followed by:**	
`<mid>`	Specifies the MLT ID. The range of values is 1 to 31.
`<vid>`	Specifies the VLAN ID. The default range of values is 1 to 4000.

Command mode

Global configuration mode

mlt create

Use this command to create the specified MultiLink Trunking (MLT) on the switch.

Syntax

`mlt <mid> create`

where

<mid> specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

mlt encapsulation

Use this command to set tagging for the specified MultiLink Trunking (MLT) on the switch.

Syntax

```
mlt <mid> encapsulation dot1q
```

where

<mid> specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

no mlt encapsulation

Use this command to removes tagging for the specified MultiLink Trunking (MLT) on the switch.

Syntax

```
no mlt <mid> encapsulation dot1q
```

where

<mid> specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

no mlt

Use this command to delete the specified MultiLink Trunking (MLT) on the switch.

Syntax

```
no mlt <mid>
```

where

<mid> specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

show mlt

Use this command to display information about MultiLink Trunking (MLT) operation on the switch or the status of a specified MLT.

Syntax

```
show mlt [ <mid> ]
```

where

`[ <mid> ]` is an optional parameter that specifies the MLT ID. The range of values is 1 to 31.

Command mode

Privileged EXEC mode

show mlt error

Use this command to display information about the types of Ethernet errors sent and received by all configured MultiLink Trunks (MLTs) or for the specified MLT.

Syntax

```
show mlt error [ <mid> ]
```

where

`[ <mid> ]` is an optional parameter that specifies the MLT ID. The range of values is 1 to 31.

Command mode

Privileged EXEC mode

show mlt error collision

Use this command to display the number and type of Ethernet collision errors for all configured MultiLink Trunks (MLTs) or for the specified MLT.

Syntax

```
show mlt error collision [ <mid> ]
```

where

`[ <mid> ]` is an optional parameter that specifies the MLT ID. The range of values is 1 to 31.

Command mode

Privileged EXEC mode

show smlt

This command shows the SMLT and single-port SMLT configurations on the switch.

Syntax

```
show smlt <mlt | fastethernet>
```

Parameters

This command includes the following parameters:

Parameter	Description
`mlt`	Displays only the MLT-based SMLTs.
`fastethernet`	Displays only the port-based SMLTs.

show ist

This command shows the IST configuration on the switch.

Syntax

```
show ist
```

Command mode

User Exec mode

show ist stat

This command shows the IST statistics for the switch.

Syntax

```
show ist stat
```

Command mode

User Exec mode

show mlt stats

Use this command to display statistics about MultiLink Trunking (MLT) operation on the switch or statistics for a specified MLT.

Syntax

```
show mlt stats [ <mid> ]
```

where

`[ <mid> ]` is an optional parameter that specifies the MLT ID. The range of values is 1 to 31.

Command mode

Privileged EXEC mode

show spanning-tree

Use this command to display spanning-tree group information about the specified ports or port.

Syntax

```
show spanning-tree [port <ports>]
```

where

`[port <ports> ]` specifies the applicable ports in port list form: `{ slot/port [- slot/port ] [, ...]}`.

Command mode

Privileged EXEC mode

show spanning-tree config

Use this command to display configuration and status information for a spanning-tree group.

Syntax

```
show spanning-tree config [<sid>]
```

where

`<sid>` specifies the spanning tree group ID. The range of values is 1 to 64.

Command mode

Privileged EXEC mode

show interface vlan

Use this command to display protocol, configuration, and parameter information for all Virtual LANs (VLANs) on the switch or for a specified or VLAN.

Syntax

```
show interface vlan [<vid>]
```

where

`[ <vid> ]` is an optional parameter that specifies the VLAN ID. The default range of values is 1 to 2000, unless the flag vid-max4k is set, and it becomes 4000.

Command mode

Privileged EXEC mode

show vlan advance

Use this command to display protocol, configuration, and parameter information all Virtual LANs (VLAN) for a specified VLAN.

Syntax

```
show vlan vid <vid> advance
```

where

`<vid>` specifies the VLAN ID. The default range of values is 1 to 2000, unless the flag vid-max4k is set, and it becomes 4000.

Command mode

Global configuration mode

show ip arp interface

Use this command to display Address Resolution Protocol (ARP) configurations for all Virtual LANs (VLANs) on the switch or for a specified VLAN.

Syntax

```
show ip arp interface[ <vid> ]
```

where

`[ <vid> ]` is an optional parameter that specifies the VLAN ID. The default range of values is 1 to 2000, unless the flag vid-max4k is set, and it becomes 4000.

Command mode

Privileged EXEC mode

show vlan autolearn-mac

Use this command to display the Mac addresses that were autolearned for the switch.

Syntax

```
show vlan autolearn-mac
```

Command mode

Global configuration mode

show vlan vid basic

Use this command to display the basic Mac addresses for the switch.

Syntax

```
show vlan [vid <vid>] basic
```

where

[vid <vid>] specifies the VLAN ID. The range of values is 1 to 4000.

Command mode

Global configuration mode

show vlan vid fdb-entry

Use this command to display forwarding database information for the specified Virtual LAN (VLAN).

Syntax

```
show vlan vid <vid> fdb-entry
```

where

<vid> specifies the VLAN ID. The range of values is 1 to 4000.

Command mode

Global configuration mode

show vlan vid fdb-filter

Use this command to display the forwarding database filters for the specified Virtual LAN (VLAN).

Syntax

```
show vlan vid <vid> fdb-filter
```

where

<vid> specifies the VLAN ID. The range of values is 1 to 4000.

Command mode

Global configuration mode

show vlan vid fdb-static

Use this command to display the forwarding database MAC addresses that have been manually (statically) configured by the user. This is used in situations where the device does not actively advertise its address. For example, a device that does not participate in ARP.

Syntax

```
show vlan vid <vid> fdb-static
```

where

<vid> specifies the VLAN ID. The range of values is 1 to 4000.

Command mode

Global configuration mode

show interfaces vlan ip

Use this command to display the Internet Protocol (IP) address configuration for all Virtual LANs (VLANs) on the switch or for a specified VLAN.

Syntax

```
show interfaces vlan ip [ <vid> ]
```

where

<vid> specifies the VLAN ID. The range of values is 1 to 4000.

Command mode

Privileged EXEC mode

show vlan manual-edit-mac

Use this command to display the manually entered Media Access Control (MAC) addresses and their associated ports.

Syntax

```
show vlan manual-edit-mac
```

Command mode

Interface VLAN mode

show vlan members

Use this command to display Virtual LAN (VLAN) information for a specified port or ports.

Syntax

```
show vlan [vid <vid> ] members
```

where

<vid> specifies the VLAN ID. The range of values is 1 to 4000.

Command mode

Global configuration mode

show vlan static-mcastmac

Use this command to display the Layer 2 multicast Media Access Control (MAC) filters for any Virtual LANs (VLANs) on the switch or for a specified VLAN.

Syntax

```
show vlan [vid <vid> ] static-mcastmac
```

where

`[ vid <vid>]` specifies the VLAN ID.
The range of values is 1 to 4000.

Command mode

Privileged EXEC mode

spanning-tree stp

Use this command to set general Spanning Tree environment variables.

Syntax

```
spanning-tree stp <sid>
[forward-delay <timeval> ]
[group-stp <enable|disable> ]
[hello-interval <timeval> ]
[max-age <timeval> ]
[priority <number> ]
[trap-stp <enable|disable> ]
```

Parameters

This command includes the following options:

`spanning-tree stp <sid>` **followed by:**	
`<sid>`	Specifies the STG ID. The range of values is 1 to 64.
`[forward-delay <timeval> ]`	Specifies the bridge forward delay time in 1/100 seconds. The range of values is 400 to 3000. The default is 1500 (15 seconds).
`[group-stp <enable|disable>]`	Enables or disables the spanning tree protocol on the specified STG. The default is enable.
`[hello-interval <timeval> ]`	Specifies the bridge hello time in 1/100 seconds. The range of values is 100 to 1000. The default is 200 (2 seconds).

spanning-tree stp <sid> followed by:	
[max-age <timeval>]	Specifies the bridge maximum age time in 1/100 seconds. The range of values is 600 to 4000. The default is 2000 (20 seconds).
[priority <number>]	Specifies the bridge priority number of the specified port. The range of values is 0 to 65535. The default is 32768.
[trap-stp <enable|disable>]	Enables or disables the spanning tree protocol trap for the specified STG. The default is enable.

Command mode

Global configuration mode

spanning-tree stp add-ports

Use this command to add ports to a Spanning Tree Group (STG).

Syntax

```
spanning-tree stp <sid> add-ports <value>
```

Parameters

This command includes the following options:

spanning-tree stp <sid> add-ports followed by:	
<sid>	Specifies the STG ID. The range of values is 1 to 64.
<value>	Specifies the applicable ports in port list form: { slot/port [- slot/port] [, ...]}.

Command mode

Global configuration mode

spanning-tree stp create

Use this command to create a new Spanning Tree Group (STG).

Syntax

```
spanning-tree stp <sid> create
[ <ports> ] [vlan <value> ]
```

Parameters

This command includes the following options:

spanning-tree stp <sid> create followed by:	
`<sid>`	Specifies the STG ID. The range of values is 1 to 64.
`[ <ports> ]`	Specifies the applicable ports in port list form: `{ slot/port [- slot/port ][, ...]}`.
`[vlan <value> ]`	Specifies the VLAN ID. ***Note:*** If a VLAN spans multiple switches, it must be within the same STG across all switches.

Command mode

Global configuration mode

spanning-tree stp remove-ports

Use this command to remove ports from a Spanning Tree Group (STG).

Syntax

```
spanning-tree stp <sid> remove-ports <value>
```

Parameters

This command includes the following parameters:

spanning-tree stp <sid> remove-ports **followed by:**	
<sid>	Specifies the Spanning Tree group ID. The range of values is 1 to 64.
<value>	Specifies the applicable ports in port list form: { slot/port [- slot/port][, ...]}.

Command mode

Global configuration mode

no spanning-tree

Use this command to delete the specified Spanning Tree Group (STG).

Syntax

```
no spanning-tree <sid>
```

where

<sid> specifies the spanning tree group ID. The range of values is 1 to 64.

Command mode

Global configuration mode

telnet-access

Use this command to define parameters for the telnet login environment.

Syntax

```
telnet-access <login-timeout> <sessions>
```

Parameters

This command includes the following parameters:

telnet-access **followed by:**	
login-timeout	Specifies the login timeout. The range is 30 to 65535. The default is 900 seconds.
sessions	Specifies number of sessions. The range is 0 to 8. The default is 8.

Command mode

Global configuration mode

vlan action

Use this command to flush dynamically learned entries from a table.

Syntax

```
vlan action <vid>
<none | flush | MacFdb | flushArp | flushIp | all >
```

Parameters

This command includes the following parameters:

vlan action <vid> followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
none	Specifies no table is flushed.
flush MacFdb	Specifies flushing of MacFdb table.
flushArp	Specifies flushing of Arp table.
flushIp	Specifies flushing of the IP table.
all	Specifies flushing of all tables.

Command mode

Global configuration mode

vlan add-mlt

Use this command to add MultiLink Trunking (MLT) to a Virtual LAN (VLAN).

Syntax

```
vlan add-mlt <vid> <mid>
```

Parameters

This command includes the following parameters:

vlan <vid> add-mlt **followed by:**	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<mid>	Specifies the MLT ID. The range of values is 1 to 31.

Command mode

Global configuration mode

vlan members

Use this command to add one or more ports to an existing Virtual LAN (VLAN).

Syntax

vlan members <add|remove> <vid> <ports> [<member value>]

Parameters

This command includes the following parameters:

vlan members **followed by:**	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<ports>	Specifies the applicable ports in port list form **{ slot/port [- slot/port][, ...]}**
[<member value>]	Specifies the port member type. The options are: • **portmember** (always a member), • **static** (always a member), or • **notallowed** (never a member).
<add | remove>	Add or remove a port from the VLAN.

Command mode

Global configuration mode

vlan name

Use this command to change the name of a Virtual LAN (VLAN).

Syntax

```
vlan name <vid> <vname>
```

Parameters

This command includes the following parameters:

vlan name **followed by:**	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<vname>	Specifies the VLAN name. The range of values is a string of 0 to 20 characters. The default VLAN name is VLAN <vid>.

Command mode

Global configuration mode

vlan qos-level

Use this command to set a Quality of Service (QoS) level for the specified Virtual LAN (VLAN).

Syntax

```
vlan qos-level <vid> <integer>
```

Parameters

This command includes the following parameters:

vlan qos-level **followed by:**	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<integer>	Specifies the QoS level. The range of values is 0 to 7. Level 7 is reserved and cannot be set.

Command mode

Global configuration mode

no vlan

Use this command to delete a Virtual LAN (VLAN).

Syntax

```
no vlan <vid>
```

where

`<vid>` specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

vlan create type port

Use this command to create a port-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type port <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

`vlan create <vid> type port` **followed by:**	
`<vid>`	Specifies the VLAN ID. The default range of values is 1 to 2000.
`[name <value> ]`	Specifies the name of the VLAN. The range of values is 0 to 20 characters. The default name is VLAN <vid>.
`<sid>`	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
`[color <value> ]`	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ApltkEther2Snap

Use this command to create an ApltkEther2Snap protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
```

```
type protocol-ApltkEther2Snap <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-ApltkEther2Snap followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-decEther2

Use this command to create a decEther2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-decEther2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-decEther2 followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.

vlan create <vid> type protocol-decEther2 followed by:	
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-decOtherEther2

Use this command to create a decOtherEther2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-decOtherEther2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-decOtherEther2 followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipEther2

Use this command to create an ipEther2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-ipEther2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

`vlan create <vid> type protocol-ipEther2` **followed by:**	
`<vid>`	Specifies the VLAN ID. The default range of values is 1 to 2000.The default name is VLAN <vid>.
`[name <value> ]`	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
`<sid>`	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
`[color <value> ]`	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipv6Ether2

Use this command to create an ipv6Ether2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-ipv6Ether2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-ipv6Ether2 **followed by:**	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipx802.2

Use this command to create an ipx802.2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-ipx802.2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type ipx802.2 **followed by:**	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.

vlan create <vid> type ipx802.2 **followed by:**	
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipx802.3

Use this command to create an ipx802.3 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-ipx802.3 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type ipx802.3 **followed by:**	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipxEther2

Use this command to create an ipxEther2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-ipxEther2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-ipxEther2 followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-ipxSnap

Use this command to create an ipxSnap protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-ipxSnap <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-ipxSnap **followed by:**	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-Netbios

Use this command to create a Netbios protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-Netbios <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-Netbios **followed by:**	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-RarpEther2

Use this command to create a RarpEther2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-RarpEther2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-RarpEther2 followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN.The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-sna802.2

Use this command to create a sna802.2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-sna802.2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-sna802.2 followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-snaEther2

Use this command to create a snaEther2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-snaEther2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-snaEther2 followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN.The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-Userdef

Use this command to create a Userdef protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-Userdef <sid> <pid>
[color <value> ] [encap <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-Userdef followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
<pid>	Specifies a user-defined protocol not included in the list.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).
[encap <value>]	Specifies the frame encapsulation method.The values are ethernet-ii, llc,and snap. The default is all encapsulation types.

Command mode

Global configuration mode

vlan create type protocol-vinesEther2

Use this command to create a vinesEther2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-vinesEther2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-vinesEther2 followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan create type protocol-xnsEther2

Use this command to create a xnsEther2 protocol-based Virtual LAN (VLAN).

Syntax

```
vlan create <vid> [name <value> ]
type protocol-xnsEther2 <sid>
[color <value> ]
```

Parameters

This command includes the following parameters:

vlan create <vid> type protocol-xnsEther2 followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000. The default name is VLAN <vid>.
[name <value>]	Specifies the name of the VLAN. The range of values is 0 to 20 characters.

vlan create <vid> type protocol-xnsEther2 followed by:	
<sid>	Specifies the spanning tree group ID. The range of values is 1 to 64 characters.
[color <value>]	Specifies the color of the VLAN. The range of values is 0 to 32. System software uses the color attribute to display the VLAN. The default color is 0 (white).

Command mode

Global configuration mode

vlan fdb-entry aging-time

Use this command to set the forwarding database aging timer for a Virtual LAN (VLAN).

Syntax

vlan fdb-entry <vid> aging-time <seconds>

Parameters

This command includes the following parameters:

vlan fdb-entry <vid> aging-time <seconds> followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<seconds>	Specifies the timeout period in seconds. The range of values is 10 to 1000000. The default is 300.

Command mode

Global configuration mode

vlan fdb-entry flush

Use this command to flush the forwarding database for a Virtual LAN (VLAN).

Syntax

vlan fdb-entry <vid> flush

where

<vid> specifies the VLAN ID. The default range of values is 1 to 2000, unless the flag vid-max4k is set, and it becomes 4000.

Command mode

Global configuration mode

vlan fdb-entry qos-level

Use this command to specify the parameters for the forwarding database and set the QoS Level of a Virtual LAN (VLAN). To set the QoS level, the entry must be in the forwarding database (FDB).

Syntax

```
vlan fdb-entry <vid> qos-level <mac> <0...7>
```

Parameters

This command includes the following parameters:

vlan fdb-entry <vid> qos-level followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<mac>	Specifies the MAC address.
<0...7>	Specifies the QoS level. The range of values is 0 to 7. Level 7 is reserved and cannot be set.

Command mode

Global configuration mode

vlan fdb-entry sync

Use this command to synchronize the forwarding database of the switch with the forwarding database of the other aggregation switch.

Syntax

```
vlan fdb-entry <vid> sync
```

where

<vid> specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

vlan fdb-filter add

Use this command to create a filter that can be applied to an entry in the Forwarding Database (FDB).

Syntax

```
vlan fdb-filter <vid> add <mac> <port value> drop
<none|srcOnly|dstonly|Both> qos <level>
```

Parameters

This command includes the following parameters:

vlan fdb-filter <vid> add followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<mac>	Specifies the MAC address.
<port value>	Specifies the applicable ports in port list form: **{slot/port [-slot/port][, ...]}**.
action	none srcOnly dstOnly Both

Command mode

Global configuration mode

no vlan fdb-filter

Use this command to remove Virtual LAN (VLAN) filter members.

Syntax

```
no vlan fdb-filter <vid> <mac>
```

Parameters

This command includes the following parameters:

no vlan fdb-filter followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<mac>	Specifies the MAC address.

Command mode

Global configuration mode

vlan fdb-static add

Use this command to add a static member to a Virtual LAN (VLAN) bridge.

Syntax

```
vlan fdb-static <vid> add
<mac> <port value> [ <qos value> ]
```

Parameters

This command includes the following parameters:

vlan fdb-static <vid> add followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<mac>	Specifies the multicast MAC address.
<port value>	Specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.
Operational parameter: [<qos value>]	Specifies the Quality of Service level. The QoS level range is 0 to 7. Level 7 is reserved. The default is 1.

Command mode

Global configuration mode

no vlan fdb-static

Use this command to remove Virtual LAN (VLAN) static members.

Syntax

```
no vlan fdb-static <vid> <mac>
```

Parameters

This command includes the following parameters:

no vlan fdb-static followed by:	
<vid>	Specifies the VLAN ID. The default range of values is 1 to 2000.
<mac>	Specifies the MAC address.

Command mode

Global configuration mode

vlan static-mcastmac add

Use this command to add static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

```
vlan static-mcastmac <vid> add <mac>
[mlt <mid>] [ports <ports>]
```

where

<vid> specifies the VLAN ID. The default range of values is 1 to 2000.

Parameters

This command includes the following parameters:

vlan static-mcastmac <vid> add followed by:	
<mac>	Specifies the MAC address.
[mlt <mid>]	Specifies the MultiLink Trunking ID. The range is 1 to 31.
[ports <ports>]	Specifies the port(s) to receive the multicast flooding.

Command mode

Global configuration mode

For more information about configuring VLAN, see *Configuring IP Multicast Routing Protocols*.

vlan static-mcastmac add-mlt

Use this command to add MultiLink Trunking (MLT) to static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

```
vlan static-mcastmac <vid> add-mlt <mid>
```

where

<vid> specifies the VLAN ID. The default range of values is 1 to 2000.
<mid> specifies the multilink trunk identifier. The default range of values is 1 to 31.

Parameters

This command includes the following parameters:

vlan static-mcastmac <vid> add-mlt <mid> followed by:	
<mid>	Specifies the MultiLink Trunking ID. The range is 1 to 31.
<mac>	Specifies the MAC address.

Command mode

Global configuration mode

vlan static-mcastmac remove-mlt

Use this command to delete MultiLink Trunking (MLT) to static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

```
vlan static-mcastmac <vid> remove-mlt
ports <ports/slots> <mac>
```

where

<vid> specifies the VLAN ID. The default range of values is 1 to 2000.

Parameters

This command includes the following parameters:

vlan static-mcastmac <vid> remove-mlt followed by:	
<mid>	Specifies the MultiLink Trunking ID. The range is 1 to 31.
<mac>	Specifies the MAC address.

Command mode

Global configuration mode

vlan static-mcastmac add-ports

Use this command to add ports to static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

```
vlan static-mcastmac <vid> add-ports <ports> <mac>
```

where

<vid> specifies the VLAN ID. The default range of values is 1 to 2000.

Parameters

This command includes the following parameters:

vlan static-mcastmac <vid> add-ports **followed by:**	
<ports>	Specifies the applicable ports in port list form: {slot/port [-slot/port][,...]}.
<mac>	Specifies the MAC address.

Command mode

Global configuration mode

vlan static-mcastmac remove

Use this command to remove MAC-to-VLAN static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

```
vlan static-mcastmac <vid> remove <mid> <mac>
```

where

<vid> specifies the VLAN ID. The default range of values is 1 to 2000.

Parameters

This command includes the following parameters:

vlan static-mcastmac <vid> remove **followed by:**	
<mid>	Specifies the MultiLink Trunking ID. The range is 1 to 31.
<mac>	Specifies the MAC address.

Command mode

Global configuration mode

For more information about configuring VLAN, see *Configuring IP Multicast Routing Protocols*.

vlan static-mcastmac remove-mlt

Use this command to remove MultiLink Trunking (MLT) from static multicast Media Access Control (MAC) entries for a Virtual LAN (VLAN).

Syntax

```
vlan static-mcastmac <vid> remove-mlt <mid> <mac>
```

where

`<vid>` specifies the VLAN ID. The default range of values is 1 to 2000.

Parameters

This command includes the following parameters:

`vlan static-mcastmac <vid> remove-mlt` **followed by:**	
`<mid>`	Specifies the MultiLink Trunking ID. The range is 1 to 31.
`<mac>`	Specifies the MAC address.

Command mode

Global configuration mode

vlan static-mcastmac remove-ports

Use this command to delete ports from the Layer 2 multicast Media Access Control (MAC) entries on a Virtual LAN (VLAN).

Syntax

```
no vlan static-mcastmac <vid> remove-ports <mid> <mac>
```

where

`<vid>` specifies the VLAN ID. The default range of values is 1 to 2000.

Parameters

This command includes the following parameters:

`vlan static-mcastmac <vid> remove-ports` **followed by:**	
`<mid>`	Specifies the MultiLink Trunking ID.
`<mac>`	Specifies the MAC address.

Command mode

Global configuration mode

no vlan static-mcastmac

Use this command to delete Layer 2 multicast Media Access Control (MAC) entries on a Virtual LAN (VLAN).

Syntax

```
no vlan static-mcastmac <vid> mac <mac>
```

where

`<vid>` specifies the VLAN ID. The default range of values is 1 to 2000.

`<mac>` specifies the MAC address.

Command mode

Global configuration mode

Layer 3 Operations Commands

interface vlan

Use this command to interface with a Virtual LAN (VLAN).

Syntax

```
interface vlan <vid>
```

where

`<vid>` specifies the VLAN ID. The default range of values is 1 to 2000.

Command mode

Global configuration mode

ip address

Use this command to assign an IP address and subnet mask to a Virtual LAN (VLAN).

Syntax

```
ip address <ipaddr mask>
```

Parameters

This command includes the following parameters:

ip address followed by:	
`<ipaddr>`	Specifies the IP address.
`<mask>`	Specifies the subnet mask `{a.b.c.d}`.

Command mode

Interface configuration mode

no ip address

Use this command to delete the specified IP address of a Virtual LAN (VLAN).

Syntax

```
no ip address <ipaddr>
```

where

`<ipaddr>` specifies the IP address of the VLAN.

Command mode

Interface configuration mode

For more information about configuring VLAN, see *Nortel Ethernet Routing Switch 8300 Configuration — VLANs, Spanning Tree, and Static Link Aggregation using the NNCLI (NN46200-504)*.

ip arp proxy

Use this command to enable a proxy Address Resolution Protocol (ARP) on a Virtual LAN (VLAN). A proxy ARP on a VLAN allows a router to answer a local ARP request for a remote destination.

Syntax

```
ip arp proxy
```

Command mode

Interface configuration mode

no ip arp proxy

Use this command to disable a proxy Address Resolution Protocol (ARP) on a Virtual LAN (VLAN).

Syntax

```
no ip arp proxy
```

Command mode

Interface configuration mode

ip arp response

Use this command to enable Address Resolution Protocol (ARP) responses on a Virtual LAN.

Syntax

```
ip arp response
```

Command mode

Interface configuration mode

no ip arp response

Use this command to disable Address Resolution Protocol (ARP) responses on a Virtual LAN.

Syntax

```
no ip arp response
```

Command mode

Interface configuration mode

Route filters commands

This chapter describes NNCLI route filters commands and their parameters.

filter acl ip

Use this command to create a new IP ACL.

Syntax

filter acl <acl-id> ip [acl-name <value>] [act-id <value>]

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **act-id <value>** specifies the ACT ID (from 1 to 2) for this ACL entry.

  Note: ACLs can be of either type. Access Control Entities (ACEs) can match packets classified as 'ip' (ip header and below) or 'non-ip' (ethernet header).

Parameter

This command includes the following options:

filter acl <acl-id> ip <act-id> **followed by:**	
acl-name <value>	A descriptive name that identifies this ACL. If you do not assign a name, the system automatically assigns one.
act-id	Identifies the access control template (ACT) bound to this interface. act-id - the range is 1 to 2. If you do not assign a ACT, the system automatically uses act-id 1 ***Note:*** The rules in the ACL specified in AclIdList must be a subset of the values defined in the ACT entry.

Command mode

Global configuration mode

filter acl non-ip

Use this command to create a new non-IP ACL.

Syntax

filter acl <acl-id> non-ip <acl-name> <act-id>

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **<act-id>** specifies the ACT ID (from 1 to 2) for this ACL entry.

Note: ACLs can be of either type. Access Control Entities (ACEs) can match packets classified as 'ip' (ip header and below) or 'non-ip' (ethernet header).

Parameter

This command includes the following options:

filter acl <acl-id> non-ip <act-id> **followed by:**	
acl-name <value>	A descriptive name that identifies this ACL. If you do not assign a name, the system automatically assigns one.
act-id	Identifies the access control template (ACT) bound to this interface. act-id - the range is 1 to 2. If you do not assign a ACT, the system automatically uses act-id 1 ***Note:*** The rules in the ACL specified in AclIdList must be a subset of the values defined in the ACT entry.

Command mode

Global configuration mode

filter acl action

Use this command to create and configure an ACE.

Syntax

```
filter acl <acl-id> action <ace-id> <mode> [trust-dscp
<value>] [remark-dscp <value>] [remark-user-priority
<value>] [police <value> <ace-name>] [precedence <value>]
[traffic-type <value>]
```

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **<ace-id>** is a unique identifier (from 1 to 256) for this ACE entry.
- **<mode>** specifies the operating mode associated with this ACE. Enter one of the following modes to determine what action the ACE takes when it matches a packet:
  - — **inactive**—no affect on traffic
  - — **permit**—permits traffic

— **deny**—denies traffic

— **redirect**—redirects traffic

— **fwd2cpu**—forwards to the central processing unit (CPU

The default setting is **deny**.

Parameter

This command includes the following options:

filter acl <acl-id> action <ace-id> <mode> **followed by:**	
trust-dscp <enable|disable>	Specifies trust dscp.
remark-dscp <value>	Causes DSCP to re-mark non-standard traffic classes so it uses a local per hop behavior (PHB). The range is 0 to 63. **<value>** is one of the following choices: disable phbcs0 phbcs1 phbaf11 phbaf12 phbaf13 phbcs2 phbaf21 phbaf22 phbaf23 phbcs3 phbaf31 phbaf32 phbaf33 phbcs4 phbaf41 phbaf42 phbaf43 phbcs5 phbef phbcs6 phbcs7 The default setting is **disable**.

filter acl <acl-id> action <ace-id> <mode> **followed by:**	
remark-user-priority <value>	Sets the User Priority as described by Layer 2 standards: 802.1Q, 802.1p. **value** is one of the following choices: • ignore | zero | one | ... | seven • 0 ... 7 The default setting is **ignore**.
police <value>	**police <value>** sets the desired policing profile identifier in the range from 0 to 128. When policing is not desired, set to disable (0).
<ace-name>	**<ace-name>** is a string that names the ACE. The range is 0 to 255. If you do not assign a name, the system automatically assigns one.
next-hop <ipaddr>	**<next-hop>** is an IP address {a.b.c.d}. This value redirects matching IP traffic to the next hop, as specified by this IP address.
precedence <0 to 255>	**precedence** sets the order for when each ACE is applied within an ACL. This value is in the range from 0 to 255, and the default is 0. An ACL can contain multiple ACEs that match a packet. The lower the value that you assign to an ACE increases its order of precedence. For example, the highest precedence that you can assign to an ACE is 0, and the lowest precedence (256) is reserved for the default ACE.
traffic-type <value>	**<traffic-type>** <value> can be:

filter acl <acl-id> action <ace-id> <mode> **followed by:**	
	{all | bridged | routed | tagged | tagged-bridged | tagged-routed | untagged | untagged-bridged | untagged-routed}. • **all** - matches both bridged and routed packets. • **bridged** - matches bridged packets. • **routed** - matches IPv4 unicast routed packets. • tagged • untagged • tagged-bridged • tagged-routed • untagged-bridged • untagged-routed The default setting is **all**. This value indicates the type of packets that the ACE is set to match.

Command mode

Global configuration mode

no filter acl

Use this command to delete an ACL or an ACE.

Syntax

no filter acl <acl-id> [<ace-id>]

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **<ace-id>** is a unique identifier (from 1 to 256) for this ACE entry.

Command mode

Global configuration mode

filter acl ethernet

Use this command to configure an ACE's Ethernet values.

Syntax

```
filter acl <acl-id> ethernet <ace-id> src-mac <value>
<ace-op> <src-mac> dst-mac <value> <ace-op> <dst-mac>
ether-type <value> anyvlan vlan-id <value> user-priority
<value>
```

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **<ace-id>** is a unique identifier (from 1 to 256) for this ACE entry.

Parameter

This command includes the following options:

filter acl <acl-id> ethernet <ace-id> **followed by:**	
src-mac <value> <ace-op> <src-mac>	Specifies the MAC source address to match {a:b:c:d}. **<ace-op>** specifies the logical operator: **{any|eq|ne|le|ge|range|mask}**. The default is **any**. **<src-mac>** sets the mask or higher address for MAC source address, when ace-op is set to mask or range.
dst-mac <value> <ace-op> <dst-mac>	Specifies the MAC source address to match {a:b:c:d:e:f}. **<ace-op>** specifies the logical operator: **{any | eq | ne | le | ge | range | mask}**. The default is **any**. **<dst-mac>** sets the mask or higher address for MAC destination address, when ace-op is set to mask or range.

filter acl <acl-id> ethernet <ace-id> **followed by:**	
ether-type <value>	Specifies the EtherType value from the Ethernet header. • ip • arp • rarp • appleTalk • decLat • ipv6 • any (outside valid range) The default is **any**.
vlan-id <value>	Specifies the Vlan-ID to match. This value is in the range of 1 - 2000. If the flag vid-max4k is set the range is 1 to 4000. The default is 0.
user-priority <value>	Sets the Priority bits (3-bit value) from the 802.1Q/p. **<value>** is one of the following choices: • 0...7 • 0x0...0x07 • ignore|zero|one|two|three|four|five|six|seven The default setting is **ignore**.

Command mode

Global configuration mode

filter acl ip-hdr

Use this command to configure an ACE's IP values.

Syntax

```
filter acl <acl-id> ip <ace-id> [src-ip <value> <ace-op>
<src-ip>] [dst-ip <value> <ace-op> <dst-ip>] [dscp <value>
<ace-op> <dscp>] ipfragment <value>
```

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **<ace-id>** is a unique identifier (from 1 to 256) for this ACE entry.

  Note: ACLs can be of either type. The Access Control Entities (ACEs) can match packets classified as 'ip' (ip header and below) or 'non-ip' (ethernet header).

Parameter

This command includes the following options:

filter acl <acl-id> ip-hdr <ace-id> **followed by:**	
src-ip <value> <ace-op> <src-ip>	Specifies the IP source address to match **{a.b.c.d} from the IP header**. **<ace-op>** specifies the logical operator: **{any|eq|ne|le|ge|range|mask}**. The default is **any**. **<src-ip>** sets the mask or higher address for the IP source address, when: **ace-op** is set to mask or range.
dst-ip <value> <ace-op> <dst-ip>	Specifies the IP destination address to match from the IP header. **<ace-op>** specifies the logical operator: **{any|eq|ne|le|ge|range|mask}**. The default is **any**. **<dst-ip>** sets the mask or higher address for the IP destination address, when: **ace-op** is set to mask or range.

filter acl <acl-id> ip-hdr <ace-id> **followed by:**	
dscp <value> <ace-op> <dscp>	Causes DSCP to re-mark non-standard traffic classes so it uses a local per hop behavior (PHB). **<value>** is one of the following choices: disable phbcs0 phbcs1 phbaf11 phbaf12 phbaf13 phbcs2 phbaf21 phbaf22 phbaf23 phbcs3 phbaf31 phbaf32 phbaf33 phbcs4 phbaf41 phbaf42 phbaf43 phbcs5 phbef phbcs6 phbcs7 The default setting is **disable**. **<ace-op>** specifies the logical operator: **any** | **eq** | **ne** | **le** | **ge** | **range** | **mask** The default is **any**. **<dscp>** sets the mask or higher address for the DSCP value, when: **ace-op** is set to mask or range.
i **pfragment<value>**	Set the match option for IP fragmented packets. The value is one of the following: • any = any packet • fragments = IP fragemented packets only • non-fragments = non-IP fragmented packets only The default is any.

filter acl <acl-id> ip-hdr <ace-id> **followed by:**	
	Note: This option must be set whenever a match on an L4 field is required. This field will be automatically set to either 'non-fragments' or 'any' whenever an L4 field is set or unset.

Command mode

Global configuration mode

filter acl port

Use this command to configure an ACE's port values.

Syntax

```
filter acl <acl-id> port <ace-id>
src-port <value> <ace-op> <src-port>
dst-port <value> <ace-op> <dst-port>
```

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **<ace-id>** is a unique identifier (from 1 to 256) for this ACE entry.

Parameter

This command includes the following options:

filter acl <acl-id> port <ace-id> **followed by:**	
src-port <value> <ace-op> <src-port>	Specifies the TCP or UDP source port to match.**<value>** is one of the following choices: • 0...65535 • 0x0...0xffff **<ace-op>** specifies the logical operator: **{any|eq|ne|le|ge|range|mask}**. The default is **any**.

filter acl <acl-id> port <ace-id> **followed by:**	
	<src-port> sets the TCP or UDP source port, when: **ace-op** is set to mask or range.
dst-port <value> <ace-op> <dst-port>	Specifies the TCP or UDP destination port to match. **<value>** is one of the following choices: • 0...65535 • 0x0...0xffff • any|bgp|bootpstrap|bootpd-dhcp|dns|echo|ftpcontrol|ftpdata|hdot323|http|rip|rtp|rtcp|ssh|telnet|tftp **<ace-op>** specifies the logical operator: **{any|eq|ne|le|ge|range|mask}**. The default is **any**. **<dst-port>** sets the mask or higher address for the TCP or UDP destination port, when: **ace-op** is set to mask or range.

Command mode

Global configuration mode

filter acl protocol

Use this command to configure an ACE's protocol values.

Syntax

filter acl <acl-id> protocol <ace-id> <ip-protocol> <ace-op> <ip-protocol>

where:

- <acl-id> is a unique identifier (from 1 to 512) for this ACL entry.
- <ace-id> is a unique identifier (from 1 to 256) for this ACE entry.
- <ip-protocol> is the protocol name:

Parameter

This command includes the following options:

filter acl <acl-id> protocol <ace-id> <ip-protocol> **followed by:**	
<ace-op> <ip-protocol>	<ace-op> specifies the logical operator: {any|eq|ne|le|ge|range|mask}. The default is any. <ip-protocol> sets the protocol, when: ace-op is set to mask or range.

Command mode

Global configuration mode

filter acl debug

Use this command to debug an ACE.

Syntax

filter acl <acl-id> debug <ace-id> match-count <value> mirror <value>

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **<ace-id>** is a unique identifier (from 1 to 255) for this ACE entry.

Parameter

This command includes the following options:

filter acl <acl-id> debug <ace-id> **followed by:**	
match-count <value>	Counts the packets and octets of matching traffic from all ports where the list is active. <value> is one of the following choices: • **disable** - Set this mode when counters are not required. This is the default. • **bytes-pkts** - Set this mode when the count of octets is accurately required.

filter acl <acl-id> debug <ace-id> **followed by:**	
	• **kbytes-pkts** - Set this mode when the octets count is desired in kilobytes. ***Note:*** There is potential for an overflow of the octet counter. For example, consider an interface with a forwarding rate of 17 million 64-byte pkts per second. If the statistics are accumulated from 10 such interfaces in a 64-bit counter, the counter could overflow in approximately a year.
mirror <value>	Mirrors matching packets. <value> is {enable | disable}. The default is disable.

Command mode

Global configuration mode

filter acg

Use this command to configure an Access Control Group (ACG), which may contain one each of ACL type ip and ACL type non-ip.

Syntax

filter acg <acg-id> <acl-id> <acg-name>

where

<acg-id> is a unique identifier (from 1 to 1024) for this ACG entry.

Parameter

This command includes the following options:

filter acg <acg-id> **followed by:**	
<acl-id>	<acl-id> is a unique identifier (from 1 to 512) for this ACG entry.
<acg-name>	<acg-name> is a descriptive name that identifies this ACG. If you do not assign a name, the system automatically assigns one.

Command mode

Global configuration mode

filter acg modify

Use this command to modify an ACG's acl-id-list.

Syntax

```
filter acg <acg-id> modify <acl-id> <acg-name>
```

where:

- <acg-id> is a unique identifier (from 1 to 1024) for this ACG entry
- <acl-id> is a unique identifier (from 1 to 512) for this ACG entry.

Parameter

This command includes the following options:

`filter acg <acg-id> modify` **followed by:**	
`<acl-id>`	Specifies a unique identifier (from 1 to 512) for this ACL entry.
`<acg-name>`	A descriptive name that identifies this ACG.

Command mode

Global configuration mode

no filter acg

Use this command to delete an ACG.

Syntax

```
no filter acg <acg-id>
```

where

`<acg-id>` is a unique identifier (from 1 to 1024) for this ACG entry.

Command mode

Global configuration mode

filter act ethernet

Use this command to create an Ethernet ACT.

Syntax

```
filter act <act-id> ethernet <acl-type> src-mask <value>
dst-mask <value> ether-type <value> vlan-mask <value> name
<value>
```

where:

- <act-id> is a unique identifier (from 1 to 2) for this ACT.
- <acl-type> specifies the type of ACL: IP or non-IP. ACLs can be of either type because access control entities (ACEs) can match packets as 'ip' or 'non-ip'.

Parameter

This command includes the following options:

`filter act <act-id> ethernet <acl-type>` **followed by:**	
`act-id`	Identifies the access control template (ACT) bound to this interface. The range is 1 to 2. ***Note 1:*** The rules in the ACL specified in AclIdList must be a subset of the values defined in the ACT entry. ***Note 2:*** Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
`src-mask <value>`	Specifies a mask for the source MAC address. This mask is used by the ACEs that are members of the ACLs using this ACT. ***Note 1:*** A MAC address with all zeros indicates this value is not desired in the match criteria. ***Note 2:*** Partial masking is not supported. Masks must be defined as either all 0's or all 1's.

filter act <act-id> ethernet <acl-type> **followed by:**	
dst-mask <value>	Specifies a mask for the destination MAC address. This mask is used by the ACEs that are members of the ACLs using this ACT. ***Note 1:*** A MAC address with all zeros indicates this value is not desired in the match criteria. ***Note 2:*** Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
ether-type <value>	Specifies a mask for the Ether type value to match. The range for this value is from 0 to 65535. ***Note 1:*** An Ether type of zero indicates this value is not desired in the match criteria. ***Note 2:*** Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
vlan-mask <value>	Specifies a mask for the VLAN tag information to match. This mask is for the first byte in 802.1Q/802.1p tagged frames that encode the VLAN ID in 12 bits. The range is 1 to 2. ***Note 1:*** A value of zero indicates the VLAN Tag information is not desired in the match criteria. ***Note 2:*** Partial masking is not supported. Masks must be defined as either all 0's or all 1's.

filter act <act-id> ethernet <acl-type> **followed by:**	
name <value>	A descriptive name that identifies this ACT. If you do not assign a name, the system automatically assigns one. The range is 0 to 255. ***Note:*** Partial masking is not supported. Masks must be defined as either all 0's or all 1's.

Command mode

Global configuration mode

filter act ip-hdr

Use this command to configure an IP ACT.

Syntax

```
filter act <act-id> ip-hdr src-mask <value> dst-mask <value>
protocol <value> tos <value> src-port <value> dst-port
<value> tcp-flags <value> icmp <value>
```

where

<act-id> is a unique identifier (from 1 to 2) for this ACT.

Parameter

This command includes the following options:

filter act <act-id> ip-hdr **followed by:**	
src-mask <value>	src-mask - <value> is one of the following: • 0.0.0.0 • 255.255.255.255 Specifies a mask for the source IP address.

filter act <act-id> ip-hdr **followed by:**	
	Note 1: An IP address with all zeros indicates this value is not desired in the match criteria. ***Note 2:*** Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
dst-mask <value>	Specifies a mask for the destination IP address. dst-mask - <value> is one of the following: • 0.0.0.0 • 255.255.255.255 ***Note 1:*** A destination IP address with all zeros indicates this value is not desired in the match criteria. ***Note 2:*** Partial masking is not supported. Masks must be defined as either all 0's or all 1's.
protocol <value>	Specifies a mask for the protocol value in the IP header to match. <value> can be one of: • 0...255 • 0x0...0xff. ***Note:*** A value of zero indicates this value is not desired in the match criteria.

filter act <act-id> ip-hdr **followed by:**	
tos <value>	Specifies a mask for the TOS byte (DSCP value) in the IP header to match. DSCP is encoded in the 6 most significant bits of the ToS byte (see RFC 2474). <value> can be one of: • 0...255 • 0x0...0xff. ***Note:*** A value of zero indicates this value is not desired in the match criteria.
src-port <value>	Specifies a mask for the source TCP/UDP port in TCP/UDP header to match. <value> can be one of: • 0...65535 • 0x0...0xffff. ***Note:*** A value of zero indicates this value is not desired in the match criteria.
dst-port <value>	Specifies a mask for the destination TCP/UDP port in TCP/UDP header to match. <value> can be one of: • 0...65535 • 0x0...0xffff. ***Note:*** A value of zero indicates this value is not desired in the match criteria.

filter act <act-id> ip-hdr **followed by:**	
tcp-flags <value>	Specifies a mask for the 6 bits in the TCP flags value in the TCP header to match. <value> can be one of: • 0...63 • 0x0...0x3f. ***Note:*** A value of zero indicates this value is not desired in the match criteria.
icmp <value>	Specifies a mask for the ICMP message Type and Code to match. The 8-bit Type value is encoded in the MSB and the 8-bit Code value is encoded in the LSB. <value> can be one of: • 0...65535 • 0x0...0xffff. ***Note:*** A value of zero indicates this value is not desired in the match criteria.

Command mode

Global configuration mode

no filter act

Use this command to delete an ACT.

Syntax

```
no filter act <act-id> <acl-type>
```

where:

- <act-id> is a unique identifier (from 1 to 2) for the ACT entry.
- <acl-type> is either ip or non-ip.

Command mode

Global configuration mode

show filter acg

Use this command to display the list of ACGs configured on the switch.

Syntax

```
show filter acg [<acg-id>]
```

where

`<acg-id>` is a unique identifier (from 1 to 1024) for this ACG entry.

Command mode

Global configuration mode

show filter acl action

Use this command to display the list of ACLs and their related ACE actions.

Syntax

```
show filter acl action [<acl-id>] [<ace-id>]
```

where:

- `<acl-id>` is a unique identifier (from 1 to 512) for this ACL entry.
- `<ace-id>` is a unique identifier (from 1 to 256) for this ACE entry.

Command mode

Global configuration mode

show filter acl ethernet

Use this command to display information about the Ethernet ACEs.

Syntax

```
show filter acl ethernet [<acl-id>] [<ace-id>]
```

where:

- `<acl-id>` is a unique identifier (from 1 to 512) for this ACL entry.
- `<ace-id>` is a unique identifier (from 1 to 256) for this ACE entry.

Command mode

Global configuration mode

show filter acl ip

Use this command to display information about the IP ACEs.

Syntax

```
show filter acl ip [<acl-id>] [<ace-id>]
```

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **<ace-id>** is a unique identifier (from 1 to 256) for this ACE entry.

Command mode

Global configuration mode

show filter acl port

Use this command to display information about the ACEs port.

Syntax

```
show filter acl port [<acl-di>] [<ace-id>]
```

<acl-id> is a unique identifier (from 1 to 512) for this ACL entry.
<ace-id> is a unique identifier (from 1 to 256) for this ACE entry.

Command mode

Global configuration mode

show filter acl statistics

Use this command to display the ACE statistics.

Syntax

```
show filter acl statistics [<acl-id>] [<ace-id>]
```

where:

- **<acl-id>** is a unique identifier (from 1 to 512) for this ACL entry.
- **<ace-id>** is a unique identifier (from 1 to 256) for this ACE entry.

Command mode

Global configuration mode

show filter act ethernet

Use this command to display information about the Ethernet ACTs.

Syntax

```
show filter act ethernet [<acl-id>]
```

where

<acl-id> is a unique identifier (from 1 to 512) for this ACL entry.

Command mode

Global configuration mode

show filter act ip

Use this command to display information about the IP ACTs.

Syntax

```
show filter act ip [<acl-id>]
```

where

<acl-id> is a unique identifier (from 1 to 512) for this ACL entry.

Command mode

Global configuration mode

Test and diagnostic commands

This chapter describes NNCLI test and diagnostic commands and their parameters.

Test and Diagnostic Commands
"no rmon event" (page 361)
"rmon history" (page 361)
"no rmon history" (page 362)
"rmon memsize" (page 362)
"rmon stats" (page 363)
"no rmon stats" (page 363)
"rmon trap-option" (page 364)
"rmon trap-option" (page 364)
"rmon util-method" (page 364)
"show port-mirroring" (page 365)
"show interface fast-ethernet or gigabit-Ethernet" (page 365)
"show interface statistics" (page 366)
"show rmon" (page 367)
"show spanning-tree config" (page 368)
"show spanning-tree port" (page 368)
"show sys-info" (page 368)
"show test" (page 369)
"show trace file" (page 369)
"show trace level" (page 370)
"test" (page 370)
"trace auto-enable" (page 371)
"trace auto-enable add-module" (page 372)
"trace auto-enable auto-trace" (page 373)
"trace auto-enable remove-module" (page 373)
"trace clear" (page 374)
"trace filter" (page 374)
"trace grep" (page 374)
"trace level" (page 375)
"trace off" (page 375)
"trace route-policy" (page 375)
"trace screen" (page 376)
"traceroute" (page 376)
"vct test" (page 377)

clear port-stats

Use this command to clear port statistics from the switch counters.

Syntax

```
clear port-stats [ <portlist> ]
```

where

`[ <portlist> ]` is an optional parameter that specifies the ports to be cleared in the port list form: `{slot/ port[-slot/port][, ...]}`.

Command mode

Privileged EXEC mode

clear telnet

Use this command to end a Telnet session.

Syntax

```
clear telnet <session id>
```

where

`<session id>` specifies the ID number of the Telnet session. The range of values is 0 to 7.

Command mode

Privileged EXEC mode

monitor mlt error collision

Use this command to monitor the number and type of Ethernet collision errors for all Multilink Trunks (MLT) or for a specified MLT. Sample interval and duration are set by the monitor command in Global configuration mode.

Syntax

```
monitor mlt error collision [ <mid> ]
```

where

`[<mid>]` is an optional parameter that specifies the ID number of the MLT. The range is 1 to 31.

Command mode

Privileged EXEC mode

monitor mlt error main

Use this command to monitor basic information about the number of different types of Ethernet errors for all Multilink Trunks (MLT) or for a specified MLT.

Syntax

```
monitor mlt error main
[ <mid> ]
```

where

[<mid>] is an optional parameter that specifies the ID number of the MLT.

Command mode

Privileged EXEC mode

monitor mlt stats interface main

Use this command to monitor interface statistics for all Multilink Trunking (MLT) or a specified MLT.

Syntax

```
monitor mlt stats interface main [ <mid> ]
```

where

[<mid>] is an optional parameter that specifies the ID number of the MLT.

Command mode

Privileged EXEC mode

monitor mlt stats interface utilization

Use this command to monitor interface utilization statistics for all Multilink Trunking (MLT) or for a specified MLT.

Syntax

```
monitor mlt stats interface utilization [ <mid> ]
```

where

[<mid>] is an optional parameter that specifies the ID number of the MLT.

Command mode

Privileged EXEC mode

monitor ports error collision

Use this command to monitor the number and type of Ethernet collision errors for all ports or for specified ports.

Syntax

```
monitor ports error collision
```

```
[ <ports> ]
[from <value> ]
```

Parameters

This command includes the following options:

monitor ports error collision **followed by:**	
[<ports>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.
[from <value>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.

Command mode

Privileged EXEC mode

monitor ports error extended

Use this command to monitor additional information about Ethernet errors for all ports or for specified ports.

Syntax

```
monitor ports error extended
[ <ports> ]
[from <value> ]
```

Parameters

This command includes the following options:

monitor ports error extended **followed by:**	
[<ports>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.
[from <value>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.

Command mode

Privileged EXEC mode

monitor ports error main

Use this command to monitor basic information about the number of different types of Ethernet errors for all ports or for specified ports.

Syntax

```
monitor ports error main[ <ports> ]
[from <value> ]
```

Parameters

This command includes the following options:

monitor ports error main **followed by:**	
[<ports>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port][, ...]}.
[from <value>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port][, ...]}.

Command mode

Privileged EXEC mode

monitor ports stats interface extended

Use this command to monitor extended port interface statistics for all ports or for specified ports.

Syntax

```
monitor ports stats interface extended
[ <ports> ]
[from <value> ]
```

Parameters

This command includes the following options:

monitor ports stats interface extended **followed by:**	
[<ports>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.
[from <value>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.

Command mode

Privileged EXEC mode

monitor ports stats interface main

Use this command to monitor basic port interface statistics for all ports or for specified ports.

Syntax

```
monitor ports stats interface main
[ <ports> ]
[from <value> ]
```

Parameters

This command includes the following options:

monitor ports stats interface main **followed by:**	
[<ports>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.
[from <value>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.

Command mode

Privileged EXEC mode

monitor ports stats interface utilization

Use this command to monitor port interface utilization statistics for all ports or for specified ports.

Syntax

```
monitor ports stats interface utilization
[ <ports> ]
[from <value> ]
```

Parameters

This command includes the following options:

monitor ports stats interface utilization **followed by:**	
[<ports>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.
[from <value>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.

Command mode

Privileged EXEC mode

monitor ports stats rmon

Use this command to monitor Remote Network Monitoring (RMON) statistics for all ports or for specified ports.

Syntax

```
monitor ports stats rmon [ <ports> ] [from <value> ]
```

Note: RMON must be enabled on the port or ports to be monitored.

Parameters

This command includes the following options:

monitor ports stats rmon **followed by:**	
[<ports>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.
[from <value>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port] [, ...]}.

Command mode

Privileged EXEC mode

monitor ports stats stp

Use this command to monitor Spanning Tree Protocol (STP) statistics for all ports or for specified ports.

Syntax

```
monitor ports stats stp
[ <ports> ]
[from <value> ]
```

Parameters

This command includes the following options:

monitor ports stats stp **followed by:**	
[<ports>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port][, ...]}.
[from <value>]	Specifies the port(s) to be monitored in the port list form: {slot/port [-slot/port][, ...]}.

Command mode

Privileged EXEC mode

port-mirroring

Use this command to create a new entry in the port mirroring table for a specified port. Also use this command to specify the mirroring mode. You can configure up to 10 mirroring ports and one mirroring monitor port.

> ***Note:*** Nortel recommends that you disable port mirroring when not in use to reduce the load on the switch.

Syntax

```
port-mirroring <id> <enable|disable> mirror-port
<slot/port> monitor-port <port> mode <tx|rx|both>
```

Parameters

This command includes the following options:

port-mirroring **followed by:**	
<id>	Specifies the port mirroring ID. The range is 1 to 383.
<tx>[<enable|disable>]	Creates a new port mirroring table entry. • **tx** mirrors transmit packets. • **enable** enables the mirror-port. • **disable** disables the the mirror-port.
<rx> **port <value>** **port <value>** **[{enable} {disable}]**	Creates a new port mirroring table entry. • **rx** mirrors receive packets • **port <value>** is the monitor port. • **port <value>** is the mirror-port • **enable** enables the mirror-port. • **disable** disables the the mirror-port.
<both> **[{enable} {disable}]**	Creates a new port mirroring table entry. • **both** mirrors both transmit and receive packets. • **enable** enables the mirror-port. • **disable** disables the the mirror-port.
[mode] <tx|rx|both>	Specifies the mirroring port mode. • **tx** mirrors transmit packets. • **rx** mirrors receive packets. • **both** mirrors both transmit and receive packets.
<enable>	Enables a mirroring port already created in the mirror-by-port table.
<disable>	Disables a mirroring port already created in the mirror-by-port table.
[monitor-port <port>]	Specifies the mirrored port.
[mirror-port <port>]	Specifies the mirroring port.

Note: Nortel Networks recommend that you disable port mirroring when not in use to reduce the load on the switch.

Command mode

Global configuration mode

no port-mirroring

Use this command to delete an entry in the port mirroring table.

Syntax

```
no port-mirroring <id>
```

where

`<id>` specifies the port mirroring ID. The range is 1 to 383.

Command mode

Global configuration mode

rmon alarm

Use this command to create an alarm interface for the Remote Monitoring (RMON) functions on the switch.

Syntax

```
rmon alarm <1-65535> <WORD> <1-3600> {absolute|delta}
rising-threshold <-32768-65535> ] falling-threshold
<-32768-65535> ] [owner <value> ]
```

Parameters

This command includes the following options:

`rmon alarm` **followed by:**	
`<1-65535>`	Specifies the alarm interface index number. The range of values is 1 to 65535.
`<WORD>`	Specifies the alarm name. The name is case sensitive and its range of values is a string of 1 to 1536 characters.
`<1-3600>`	Specifies the sample interval. The range of values is 1 to 3600.
`{absolute|delta}`	Specifies the sample type. The options are: `absolute` and `delta`.

rmon alarm **followed by:**	
rising-threshold <-32768-65535>	Specifies the rising threshold. The range of values is -32768 to 65535.
[<1-65535>]	Specifies the rising event number.
falling-threshold <-32768-65535>	Specifies the falling threshold. The range of values is -32768 to 65535.
[<1-65535>]	Specifies the falling event number.
[owner <value>]	Specifies the name of the owner. The range of values is a string of 1 to 48 characters.

Command mode

Global configuration mode

no rmon alarm

Use this command to delete the specified Remote Monitoring (RMON) alarm.

Syntax

```
no rmon alarm [ <1-65535> ]
```

where

[<1-65535>] is an optional parameter that specifies the alarm index number. The range of values is 1 to 65535.

Command mode

Global configuration mode

rmon event

Use this command to create a Remote Monitoring (RMON) event on the switch.

Syntax

```
rmon event <1-65535> trap_src <value> trap_dest <value>
[log-type <value> ] [description <LINE> ] [community
<value> ] [owner <LINE> ]
```

Parameters

This command includes the following options:

rmon event **followed by:**	
<1-65535>	Specifies the event index number. The range of values is 1 to 65535.
trap_src <value>	Specifies the trap source IP address.
trap_dest <value>	Specifies the trap destination IP address.
[log-type <value>]	Specifies the event type. The options are: none, log, snmp-trap, or log-and-trap.
[description <LINE>]	Specifies the event description. The range of values is a string of 0 to 127 characters.
[community <value>]	Specifies the event community. The range of values is a string of 0 to 127 characters.
[owner <LINE>]	Specifies the owner. The range of values is a string of 1 to 48 characters.

Command mode

Global configuration mode

no rmon event

Use this command to delete the specified Remote Monitoring (RMON) event.

Syntax

```
no rmon event [ <1-65535> ]
```

where

[<1-65535>] is an optional parameter that specifies the event index number. The range of values is 1 to 65535.

Command mode

Global configuration mode

rmon history

Use this command to create a history control interface for Remote Monitoring (RMON) functions on the switch.

Syntax

```
rmon history <1-65535> <ports> [buckets <value> ]
[intv <value> ] [owner <LINE> ]
```

Parameters

This command includes the following options:

rmon history **followed by:**	
<1-65535>	Specifies the index number of the history control interface. The range of values is 1 to 65535.
<ports>	Specifies the port(s) in the port list form: {slot/port [-slot/port][, ...]}.
[buckets <value>]	Specifies the number of buckets requested. The range of values is 1 to 350. The default is - 50.
[intv <value>]	Specifies the time interval in seconds over which the data is sampled for each bucket. The range of values is 1 to 3600. The default is - 1800.
[owner <LINE>]	Specifies the name of the owner. The range of values is a string of 1 to 48 characters. The default is cli.

Command mode

Global configuration mode

no rmon history

Use this command to delete the specified history control interface for the Remote Monitoring (RMON) functions on the switch.

Syntax

```
no rmon history [ <1-65535> ]
```

where

[<1-65535>] is an optional parameter that specifies the index number for the history control interface. The range of values is 1 to 65535.

rmon memsize

Use this command to specify the amount of Random Access Memory (RAM) in bytes to allocate for the Remote Monitoring (RMON) functions on the switch.

Syntax

```
rmon memsize <memsize>
```

where

`<memsize>` specifies the memory size in bytes. The range of values is 250000 to 4000000.

Command mode

Global configuration mode

rmon stats

Use this command to create an ether-stats control interface for the Remote Monitoring (RMON) functions on the switch.

Syntax

```
rmon stats <1-65535> <ports> [owner <value> ]
```

Parameters

This command includes the following options:

rmon stats **followed by:**	
`<1-65535>`	Specifies the index number of the ether-stats control interface. The range of values is 1 to 65535.
`<ports>`	Specifies the port(s) in the port list form: `{slot/port [-slot/port] [, ...]}`.
`[owner <value> ]`	Specifies the name of the owner. The range of values is a string of 1 to 48 characters.

Command mode

Global configuration mode

no rmon stats

Use this command to delete the specified ether-stats control interface for the Remote Monitoring (RMON) functions on the switch.

Syntax

```
no rmon stats [ <1-65535> ]
```

where

`1-65535` is an optional parameter that specifies the index number for the ether-stats control interface. The range of values is 1 to 65535.

Command mode

Global configuration mode

rmon trap-option

Use this command to specify whether the Remote Monitoring (RMON) traps are sent to the owner or all trap recipients.

Syntax

```
rmon trap-option {toOwner|toAll}
```

Parameters

This command includes the following options:

`rmon trap-option` **followed by:**	
`toOwner`	Specifies to send RMON traps to the owner.
`toAll`	Specifies to send RMON traps to all trap recipients.

Command mode

Global configuration mode

rmon util-method

Use this command to specify whether port utilization is calculated in half or full duplex for the Remote Monitoring (RMON) functions on the switch.

Syntax

```
rmon util-method {half|full}
```

Parameters

This command includes the following options:

`rmon util-method` **followed by:**	
`half`	Specifies that port utilization is calculated in half duplex.
`full`	Specifies that port utilization is calculated in full duplex.

Command mode

Global configuration mode

show port-mirroring

Use this command to display information about mirrored ports on the switch.

Syntax

```
show port-mirroring
```

Command mode

Privileged EXEC mode

show interface fast-ethernet or gigabit-Ethernet

Use this command to display information about the ports on the switch.

Syntax

```
show interface <fast-ethernet|gigabit-Ethernet>
```

where

ports is an optional parameter that specifies the applicable ports in port list form: **{ slot/port [- slot/port][, ...]}**.

Parameters

This command includes the following options:

show interface <fastEthernet|gigabitEthernet> **followed by:**	
all [<ports>] **[by <value>]**	Displays general information about all ports or about specified ports. **[by <value>]** displays group information by ID number or by each feature {default ID}
config [<ports>]	Displays general configuration information about all ports or about specified ports.
cp-limit	Displays the port packet cp-limit commands.

show interface <fastEthernet|gigabitEthernet> **followed by:**	
eapol [<ports>]	Displays Extensible Authorization Protocol (EAP) information about all ports or about specified ports. There are 5 options: • auth-diags • auth-stats • config • oper-stats • session-stats
error [<ports>]	Displays general error information about all ports or about specified ports.
igmp [<ports>]	Displays Internet Group Management Protocol (IGMP) information about all ports or about specified ports.
interface [<ports>]	Displays information about the physical interface for all ports or for specified ports.
name [<ports>]	Displays general information, including the name or names for all ports or for specified ports.
qos [<ports/slots>]	Displays Quality of Service (QoS) information about all ports or about specified ports.
tx-queue [<ports>]	Displays the transmit queue for all ports or for specified ports.
unknown-mac-discard [<ports>]	Displays settings for the unknown MAC discard feature for all ports or for specified ports.

Command mode

Privileged EXEC mode

show interface statistics

Use this command to display statistics for the specified port or for all ports.

Syntax

```
show interface <fastEthernet|gigabitEthernet> statistics
```

where

`[<portlist>]` is an optional parameter that specifies the port(s) in port list form: `{ slot/port [- slot/port ][, ...]}`.

Parameters

This command includes the following options:

`show interface <fastEthernet|gigabitEthernet> statistics` **followed by:**	
`rmon [ <portlist> ]`	Displays remote monitoring statistics about all ports or about specified ports.
`stg [ <portlist> ]`	Displays statistics about spanning tree groups for all ports or for specified ports.

Command mode

Privileged EXEC mode

show rmon

Use this command to display various Remote Monitoring (RMON) settings.

Syntax

`show rmon`

Parameters

This command includes the following options:

`show rmon` **followed by:**	
`info`	Displays the status and general configuration of RMON on the switch.
`alarm`	Displays the RMON Alarm table entries.
`event`	Displays the RMON event table entries.
`history`	Displays the RMON history control table entries.
`log`	Displays the RMON log table entries.
`stats`	Displays the RMON statistics table entries.

Command mode

Privileged EXEC mode

show spanning-tree config

Use this command to display the Spanning-Tree Group (STG) status and configuration for the specified STG.

Syntax

show spanning-tree config [<sid>]

where

<sid> is an optional parameter that specifies the STG ID. The range of values is 1 to 64.

Command mode

Privileged EXEC mode

For more information about system tools, see *Configuring VLANs, Spanning Tree, and MultiLink Trunking using the NNCLI*.

show spanning-tree port

Use this command to display the Spanning-Tree Group (STG) information about all ports or about specified ports.

Syntax

show spanning-tree port [<portlist>]

where

[<portlist>] is an optional parameter that specifies the applicable ports in the port list form: **{ slot/port [- slot/port] [, ...]}**.

Command mode

Privileged EXEC mode

show sys-info

Use this command to display system information about status, hardware, software, and operation of the switch. The information available from the **show sys-info** command includes general information about the system (such as location), hardware (chassis, power supplies, fans, and modules), system errors, boot configuration, software versions, memory, port information (locking status, configurations, names, interface status), OSPF (area, interface, neighbors), and log and trace files.

Syntax

show sys-info [asic] [card] [mda]

Parameters

This command includes the following options:

show sys-info **followed by:**	
asic	Displays detailed information about the Application Specific Integrated Circuit (ASIC) trays in the switch.
card	Displays detailed information about the cards in the switch.
mda	Displays detailed information about the Media Dependent Adapters (MDAs) in the switch.

Command mode

Privileged EXEC mode

show test

Use this command to display test results for the switch.

Syntax

```
show test [artable] [fabric] [loopback [ <portlist> ]]
```

Parameters

This command includes the following options:

show test **followed by:**	
loopback [<portlist>]	Displays the results of the latest loopback test for the switch or for the specified port or ports.

Command mode

Privileged EXEC mode

show trace file

Use this command to display the trace message file when tracing is enabled.

Syntax

```
show trace file [tail]
```

where

`[tail]` is an optional parameter that displays the log file in reverse order with the most recent information first.

Command mode

Privileged EXEC mode

show trace level

Use this command to display trace information for the switch.

Syntax

```
show trace level
```

Command mode

Privileged EXEC mode

test

Use this command to perform a loopback test. The test and show test commands allow you to test an Ethernet Routing Switch 8300 while the switch is operating and show the test results. The tests do not interfere with normal bridging and routing activities in the switch, but they do occupy the CPU.

Syntax

```
test [loopback <port/slot>] [stop loopback <port/slot>]
```

Parameters

This command includes the following options:

`test` **followed by:**	
`loopback <port/slot> [ <int|ext> ]`	Places the specified ports into internal or external loopback mode. • `portlist` specifies one or more ports, shown as `{ slot/port [- slot/port ] [,...]}`. • `int|ext` is a string between 1 and 1536.
`stop loopback <port/slot>`	Stops the current loopback test. `ports` specifies one or more ports, shown as `{ slot/port [- slot/port ] [,...]}`.

Note: To test a port in loopback mode, put the port into the testing state using the command **`state [port <ports>] test`**. After the test is complete, return the port to its normal mode using the command **`state [port <ports>] enable`**.

Command mode

Privileged EXEC mode

trace auto-enable

Use this command to configure the switch to automatically enable a trace in the event that CPU usage reaches a pre-defined value.

Syntax

```
trace auto-enable [high-percentage <percent>]
[high-track-duration <seconds> ]
[low-percentage <percent> ]
[low-track-duration <seconds> ]
```

Parameters

This command includes the following optional parameters:

`trace auto-enable` **followed by:**	
`[high-percentage <percent> ]`	Specifies the percentage of CPU utilization above which auto trace is started. The range of values is 60 to 100. The default is 90.
`[high-track-duration <seconds> ]`	Specifies the time in seconds to monitor CPU utilization before triggering a trace. The range of values is 3 to 10. The default is 5.
`[low-percentage <percent> ]`	Specifies the percentage of CPU utilization below which auto-trace is stopped. The range of values is 50 to 90. The default is 75.
`[low-track-duration <seconds> ]`	Specifies the time in seconds to monitor CPU utilization before disabling the trace. The range of values is 3 to 10. The default is 5.

Note: The enabling or disabling of auto-trace is not saved to the configuration file. When the switch re-boots, auto-trace functionality is disabled.

Command mode

Privileged EXEC mode

trace auto-enable add-module

Use this command to add a software module to the automatic trace configuration.

Syntax

`trace auto-enable add-module <modid> <level>`

Parameters

This command includes the following parameters:

`trace auto-enable add-module` **followed by:**	
`<modid>`	Specifies the module to be traced. The range is 0 to 66. For example, 3 = Port Manager, 20 = Topology Discovery. For a complete list of module IDs, enter: **`trace auto-enable add-module ?`**.
`<level>`	Specifies the level of detail for the trace. The options are: • 0 = Disabled • 1 = Very terse • 2 = Terse • 3 = Verbose • 4 = Very verbose

Note: The enabling or disabling of auto-trace is not saved to the configuration file. When the switch re-boots, auto-trace functionality is disabled.

Command mode

Privileged EXEC mode

trace auto-enable auto-trace

Use this command to configure the switch to automatically enable a trace in the event that CPU usage reaches a pre-defined value.

Syntax

```
trace auto-enable auto-trace <enable|disable>
```

Parameters

This command includes the following parameters:

trace auto-enable auto-trace **followed by:**	
enable	Enables auto-trace. The default is disable.
disable	Disables auto-trace. The default is disable.

Note: The enabling or disabling of auto-trace is not saved to the configuration file. When the switch re-boots, auto-trace functionality is disabled.

Command mode

Privileged EXEC mode

trace auto-enable remove-module

Use this command to remove a module from the automatic trace configuration.

Syntax

```
trace auto-enable remove-module <modid> <level>
```

Parameters

This command includes the following parameters:

trace auto-enable remove-module **followed by:**	
<modid>	Specifies the module for disabling of auto-trace. For example, 3 = Port Manager, 20 = Topology Discovery. For a complete list of module IDs, enter: **trace auto-enable add-module ?**.
<level>	Specifies the level of the trace. The options are: • 0 = Disabled

`trace auto-enable remove-module` **followed by:**	
	• 1 = Very terse • 2 = Terse • 3 = Verbose • 4 = Very verbose

Note: The enabling or disabling of auto-trace is not saved to the configuration file. When the switch re-boots, auto-trace functionality is disabled.

Command mode

Privileged EXEC mode

trace clear

Use this command to clear the trace file.

Syntax

`trace clear`

Command mode

Privileged EXEC mode

trace filter

Use this command to filter trace messages.

Syntax

`trace filter`

Command mode

Privileged EXEC mode

trace grep

Use this command to search and extract information from a text string.

Syntax

`trace grep`

Command mode

Privileged EXEC mode

trace level

Use this command to specify the trace level for a software module with the specified module ID. Use `?` to see a list of ID numbers.

Syntax

```
trace level [ <modid> ] [ <level> ]
```

Parameters

This command includes the following options:

`trace level` **followed by:**	
`[ <modid> ]`	Specifies the module to be traced. For example, 3 = Port Manager, 20 = Topology Discovery. For a complete list of module IDs, enter: `trace auto-enable add-module ?`.
`[ <level> ]`	Specifies the level of detail for the trace. The options are: • 0 = Disabled • 1 = Very terse • 2 = Terse • 3 = Verbose • 4 = Very verbose

Command mode

Privileged EXEC mode

trace off

Use this command to disable tracing on a module.

Syntax

```
trace off
```

Command mode

Privileged EXEC mode

trace route-policy

Use this command to trace a route policy.

Syntax

```
trace route-policy
```

Command mode

Privileged EXEC mode

trace screen

Use this command to display the trace on the screen.

Syntax

```
trace screen [ <setting> ]
```

where

[<setting>] is an optional parameter that specifies whether the trace is displayed on the screen. The options are: **on** or **off**.

Command mode

Privileged EXEC mode

traceroute

Use this command to trace the route to a remote host. It is a valuable tool for troubleshooting because it shows all the routes that are used or indicates that the remote network cannot be reached.

Syntax

```
traceroute <ipaddr> [ <datasize> ] [-m <value> ]
[-p <value> ] [-q <value> ] [-w <value> ] [-v]
```

Parameters

This command includes the following options:

traceroute **followed by:**	
<ipaddr>	Specifies the IP address of the remote host.
[<datasize>]	Specifies the size of the probe packet. The range of values is 1 to 1464.
[-m <value>]	Specifies the maximum time-to-live (TTL) value. The range of values is 1 to 255.
[-p <value>]	Specifies the base UDP port number. The range of values is 0 to 65535

traceroute **followed by:**	
[-q <value>]	Specifies the number of probes per TTL. The range of values is 1 to 255.
[-w <value>]	Specifies the wait time per probe. The range of values is 1 to 255.
[-v]	Specifies the verbose mode for displaying extensive trace information.

Command mode

Privileged EXEC mode

vct test

Use this command to configure and enable the Virtual Cable Tester (VCT).

Note: The following message will appear:

```
WARNING: VCT test will impact the traffic flow.  Do
you want to continue y/n?
```

Syntax

vct test <ports>

where

<ports> specifies the port(s) in port list form:
{ slot/port [- slot/port] [, ...] }.

Command mode

Global Configuration mode

Multicast services commands

This chapter describes NNCLI multicast services commands and their parameters.

Multicast Services Command
"debug ip pim" (page 381)
"interface vlan" (page 382)
"ip igmp " (page 383)
"no ip igmp" (page 386)
"default ip igmp" (page 387)
"ip igmp generate-log" (page 389)
"no ip igmp generate-log" (page 390)
"default ip igmp generate-log" (page 390)
"ip igmp generate-trap" (page 390)
"no ip igmp generate-trap" (page 390)
"default ip igmp generate-trap" (page 390)
"ip igmp immediate-leave-mode" (page 382)
"default ip igmp immediate-leave-mode" (page 383)
"ip igmp mrdisc" (page 391)
"no ip igmp mrdisc " (page 391)
"default ip igmp mrdisc" (page 392)
"ip igmp snoop-querier" (page 392)
"no ip igmp snoop-querier" (page 392)
"ip igmp snoop-querier-addr" (page 392)
"no ip igmp snoop-querier-addr" (page 393)
"ip igmp stream-limit" (page 393)
"no ip igmp stream-limit" (page 393)
"ip igmp stream-limit-group enable max-streams" (page 394)
"no ip igmp stream-limit-group " (page 394)

Multicast Services Command
"default ip igmp stream-limit-group" (page 394)
"ip igmp stream-limit-max-streams" (page 394)
"default ip igmp stream-limit-max-streams" (page 395)
"ip mroute static-source-group " (page 395)
"no ip mroute static-source-group" (page 395)
"ip pim" (page 396)
"ip pim enable" (page 399)
"no ip pim " (page 400)
"ip pim interface virtual neighbor " (page 400)
"ip pim rp-candidate group rp" (page 401)
"no ip pim rp-candidate group rp" (page 401)
"ip pim static-rp" (page 402)
"no ip pim static-rp " (page 403)
"show debug ip pim" (page 403)
"show interfaces vlan igmp" (page 403)
"show ip igmp" (page 403)
"show ip igmp access" (page 404)
"show ip igmp cache" (page 404)
"show ip igmp group" (page 405)
"show ip igmp group " (page 405)
"show ip igmp interface" (page 406)
"show ip igmp mrdisc" (page 406)
"show ip igmp router-alert" (page 406)
"show ip igmp sender" (page 406)
"show ip igmp snooping" (page 407)
"show ip igmp snoop-trace" (page 407)
"show ip igmp static" (page 408)
"show ip igmp stream-limit " (page 408)
"show ip igmp sys" (page 408)
"show ip mroute static-source-group" (page 408)
"show ip pim" (page 409)
"show ip pim active-rp" (page 409)
"show ip pim bsr" (page 409)
"show ip pim interface" (page 409)
"show ip pim interface vlan" (page 410)

Multicast Services Command
"show ip pim mroute" (page 410)
"show ip pim neighbor" (page 410)
"show ip pim rp-candidate" (page 410)
"show ip pim virtual-neighbor" (page 411)

debug ip pim

Use this command to configure PIM-SM protocol traces for troubleshooting.

Syntax

```
debug ip pim
```

Parameters

This command includes the following parameters:

debug ip pim **followed by:**	
assert / no debug ip pim assert	Allows you to set the switch to display the assert debug traces
bstrap /no debug ip pim bstrap	Allows you to set the switch to display bootstrap debug traces.
group<ipaddress>	Allows you to set the switch to display debug traces from a specific group ip-address.
hello / no debug ip pim hello	Allows you to set the switch to display hello debug traces.
joinprune /no debug ip pim joinprune	Allows you to set the switch to display join/prune debug traces.
pimdbgtrace /no debug ip pim pimdbgtrace	Allows you to set the switch to display PIM-SM debug traces.
pimdbglog /no debug ip pim pimdbglog	Allows you to control whether the switch logs debug traces.
register /no debug ip pim register	Allows you to set the switch to display register debug traces.

debug ip pim **followed by:**	
regstop /no ip debug ip pim regstop	Allows you to set the switch to display register stop debug traces.
rp-adv / no debug ip pim rp-adv	Allows you to set the switch to display rp advertisement debug traces.
send-trace /no debug ip pim send-trace	Allows you to set the switch to display send debug traces.
rcv-dbg-trace /no debug ip pim rcv-dbg-trace	Allows you to set the switch to display received debug traces.
source<ipaddress>	Allows you to set the switch to display debug traces from a specific source ip-address.

Command mode

Global configuration mode

interface vlan

Use this command to access the interface on a Virtual LAN (VLAN).

Syntax

interface vlan <vid>

where

vid is a VLAN ID from 1 to 4000. (Note that 1 to 2000 is the default, while 1 to 4000 is valid when the *vid-max4k* flag is set to true).

Command mode

Interface configuration mode

ip igmp immediate-leave-mode

Use this command to set the immediate leave mode.

Syntax

ip igmp immediate-leave-mode <multiple-user|one-user mode>

where

<multiple-user|one-user mode> specifies the immediate leave mode as multiple user or one user.

Command mode

Global configuration mode

default ip igmp immediate-leave-mode

Use this command to set the immediate leave mode to the default setting.

Syntax

```
default ip igmp immediate-leave-mode
```

Command mode

Global configuration mode

ip igmp

Use this command to configure IGMP on a VLAN.

Syntax

```
ip igmp
```

Parameters

This command includes the following parameters:

ip igmp **followed by;**	
access-list WORD <1-64> <HostAddress> <MaskAddress> <deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both>	Sets the IP multicast access group list parameters. • <1-64> is an IP prefix-list entry name in a 1 to 64 character string. • <deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both> indicates the action you want for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.
immediate-leave	Enables IGMP immediate-leave mode on the interface. The default is enabled.
immediate-leave-members {slot/port [-slot/port][, ...]}	If you enable immediate-leave, this parameter configures IGMP immediate-leave members. The default is added.

ip igmp **followed by;**	
last-member-query-interval	Configures the IGMP last member query interval (in 1/10 seconds). .
mrouter {slot/port [-slot/port][, ...]}	Adds multicast router ports. ***Note:*** When IGMP join or multicast data ingress to an Ethernet Routing Switch 8300 snoop VLAN port, they are only forwarded upstream via the querier port. You can use this parameter to create your own mrouter ports statically. After you create static mrouter ports, join and data are also forwarded to these static mrouter ports.
proxy	Enables the proxy option for the VLAN. ***Note:*** When IGMP report messages come from different clients, all of these messages are sent to the querier. If you enable IGMP proxy snoop, then only one report message is sent to the querier for that group. As a result, this parameter allows you to suppress control messages going to the CPU.
query-interval	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN. ***Note:*** In the case of IGMP snoop, be sure that the query-interval is configured the same as the multicast router (IGMP querier).
query-max-response <0-255>	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface.

ip igmp **followed by;**	
robust-value	Allows tuning for the expected packet loss on a network. ***Note:*** In the case of IGMP snoop, be sure that the robustval parameter is configured the same as the multicast router (IGMP querier).
router-alert	Enables the router alert feature. When enabled, this parameter instructs the router to drop packets without the router-alert flag in the IP header. ***Note:*** To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use. • IGMPv1 - Disable • IGMPv2 - Enable • IGMPv3 - Enable (not supported in the Ethernet Routing Switch 8300)
snooping	Enables the snooping option for the VLAN. ***Note:*** When multicast data enters a Layer 2 VLAN, data packets are flooded to all ports in that VLAN. If you enable IGMP snoop on the VLAN, these packets are only forwarded to the ports on which IGMP joins have been received. In other words, data packets are forwarded only on multicast client ports.

ip igmp **followed by;**	
static-group <groupAddress> port {slot/port[-slot/port][,...]} <static|blocked>	Configures IGMP static members on a VLAN. The Ethernet Routing Switch 8300 allows you to configure static receivers, or members, for given multicast groups on specific VLANs using the VLAN IP address. Static receivers allow multicast traffic to be sent for the configured groups on the VLAN without IGMP receivers having to be attached to this VLAN.
version <1|2>	Specifies the version of IGMP as IGMPv1 or IGMPv2. The default is IGMPv2.

Command mode

Interface VLAN mode

no ip igmp

Use the following command to disable IGMP features on a VLAN.

Syntax

```
no ip igmp
```

Parameters

This command includes the following parameters:

no ip igmp **followed by:**	
access-list <grpAddr> WORD <1-64>	Deletes the selected multicast access group.
immediate-leave	Disables IGMP fast-leave mode on the interface.
immediate-leave-members {slot/port [-slot/port][, ...]}	If you disable fast-leave, this parameter disables IGMP fast-leave members.
mrouter {slot/port [-slot/port][, ...]}	Deletes specific multicast router ports.
proxy	Disables the proxy option for the VLAN.
router-alert	Disables the router alert feature.

no ip igmp **followed by:**	
snooping	Disables the snooping option for the VLAN.
static-group <groupAddress>	Configures IGMP static members on a VLAN.

Command mode

Interface VLAN mode

default ip igmp

Use this command to set the IGMP parameters to the default values

Syntax

default ip igmp

Parameters

This command includes the following parameters:

default ip igmp **followed by;**	
access-list WORD<1-64> <HostAddress> <MaskAddress> <deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both>	Sets the IP multicast access group list parameters to default values. • **<1-64>** is an IP prefix-list entry name in a 1 to 64 character string. • **<deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both>** indicates the action you want for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.
immediate-leave	Enables IGMP immediate-leave mode on the interface. The default is enabled.
immediate-leave-members {slot/port [-slot/port][, ...]}	If you enable immediate-leave, this parameter configures IGMP immediate-leave members. The default is added.

default ip igmp **followed by;**	
last-member-query-interval	Configures the IGMP last member query interval (in 1/10 seconds).
proxy	Enables the proxy option for the VLAN. ***Note:*** When IGMP report messages come from different clients, all of these messages are sent to the querier. If you enable IGMP proxy snoop, then only one report message is sent to the querier for that group. As a result, this parameter allows you to suppress control messages going to the CPU.
query-interval	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN. ***Note:*** In the case of IGMP snoop, be sure that the query-interval is configured the same as the multicast router (IGMP querier).
query-max-response <0-255>	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface.
robust-value	Allows tuning for the expected packet loss on a network. ***Note:*** In the case of IGMP snoop, be sure that the robustval parameter is configured the same as the multicast router (IGMP querier).

default ip igmp **followed by;**	
router-alert	Enables the router alert feature. When enabled, this parameter instructs the router to drop packets without the router-alert flag in the IP header. ***Note:*** To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use. • IGMPv1 - Disable • IGMPv2 - Enable • IGMPv3 - Enable (not supported in the Ethernet Routing Switch 8300)
snooping	Enables the snooping option for the VLAN. ***Note:*** When multicast data enters a Layer 2 VLAN, data packets are flooded to all ports in that VLAN. If you enable IGMP snoop on the VLAN, these packets are only forwarded to the ports on which IGMP joins have been received. In other words, data packets are forwarded only on multicast client ports.
default ip igmp version	Sets IGMP to the default version. The default is IGMPv2.

Command mode

Interface VLAN mode

ip igmp generate-log

Use this command to configure on IGMP generate log.

Syntax

```
ip igmp generate-log
```

Command mode

Global configuration mode

no ip igmp generate-log

Use this command to disable an IGMP generate log.

Syntax

```
no ip igmp generate-log
```

Command mode

Global configuration mode

default ip igmp generate-log

Use this command to set an IGMP generate log to default values.

Syntax

```
default ip igmp generate-log
```

Command mode

Global configuration mode

ip igmp generate-trap

Use this command to configure an IGMP generate trap.

Syntax

```
ip igmp generate-trap
```

Command mode

Global configuration mode

no ip igmp generate-trap

Use this command to disable an IGMP generate log.

Syntax

```
no ip igmp generate-trap
```

Command mode

Global configuration mode

default ip igmp generate-trap

Use this command to set an IGMP generate log to default values.

Syntax

```
default ip igmp generate-trap
```

Command mode

Global configuration mode

ip igmp mrdisc

Use this command to configure multicast router discovery parameters on a VLAN.

Syntax

```
ip igmp mrdisc
```

Parameters

This command uses the following parameters:

ip igmp mrdisc **followed by:**	
<cr>	Enables multicast router discovery parameters on a VLAN. • <cr> is a carriage return.
maxadvertinterval <value>	Specifies the maximum interval in seconds between successive advertisements.
maxinitadvertinterva<value>	Specifies the maximum advertisement interval in seconds between successive initial advertisements.
maxinitadvertisements <value>	Specifies the maximum advertisements after initialisation.
minadvertinterval <value>	Specifies the minimum interval in seconds between successive advertisements.
neighdeadinterval <value>	Specifies the maximum time in seconds allowed before a neighbor is declared dead.

Command mode

Interface VLAN mode

no ip igmp mrdisc

Use this command to disable multicast router discovery on a VLAN.

Syntax

```
no ip igmp mrdisc
```

Command mode

Interface VLAN mode

default ip igmp mrdisc

Use this command to set the default values for multicast router discovery on a VLAN.

Syntax

```
default ip igmp mrdisc
```

Command mode

Interface VLAN mode

ip igmp snoop-querier

Use this command to enable IGMP snoop querier.

Syntax

```
ip igmp snoop-querier
```

Command mode

Interface VLAN mode

no ip igmp snoop-querier

Use this command to disable IGMP snoop querier.

Syntax

```
no ip igmp snoop-querier
```

Command mode

Interface VLAN mode

ip igmp snoop-querier-addr

Use this command to configure the source IP address used in the query message.

Syntax

```
ip igmp snoop-querier-addr<ipaddr>
```

where

`<ipaddr>` is the source IP address used in the query message.

Command mode

Interface VLAN mode

no ip igmp snoop-querier-addr

Use this command to return the source IP address to the default value, 0.0.0.0.

Syntax

```
no ip igmp snoop-querier-addr
```

Command mode

Interface VLAN mode

ip igmp stream-limit

Use this command to configure multicast stream limitation on a VLAN.

Syntax

```
ip igmp stream-limit
```

Parameters

This command includes the following parameters:

ip igmp stream-limit **followed by:**	
<cr>	Enables mulitcast stream limitation on a VLAN. • <cr> is carriage return.
stream-limit-max-streams <value>	Sets the maximum number of streams allowed on an interface. • <value> is an integer in a range from 0 to 65535 and the default is 4.

Command mode

Interface VLAN mode

no ip igmp stream-limit

Use this command to disable multicast stream limitation an a VLAN.

Syntax

```
no ip igmp stream-limit
```

Command mode

Interface VLAN mode

ip igmp stream-limit-group enable max-streams

Use this command to enable the multicast stream limit group and set the mximum streams.

Syntax

```
ip igmp stream-limit-group <ports> enable max-streams <value>
```

where

<ports> is a port list in the format {slot/port [..slot/port]}. These are the member ports of the multicast stream limit group.

<value> sets the maximum number of streams allowed on an interface. The range is from 0 to 65535, and the default is 4.

Command mode

Interface VLAN mode

no ip igmp stream-limit-group

Use this command to disable a multicast stream limit member.

Syntax

```
no ip igmp stream-limit-group <ports>
```

where

<ports> is a port list in the format {slot/port [..slot/port]}. These are the member ports of the multicast stream limit group.

Command mode

Interface VLAN mode

default ip igmp stream-limit-group

Use this command to set a multicast stream limit group parameters to the default values.

Syntax

```
default ip igmp stream-limit-group <ports>
```

where

<ports> is a port list in the format {slot/port [..slot/port]}. These are the member ports of the multicast stream limit group.

ip igmp stream-limit-max-streams

Use this command to configure the stream limitation maximum streams.

Syntax

```
ip igmp stream-limit-max-streams <0-65535>
```

where

`<0-65535>` is the value of the maximum streams.

Command mode

Interface VLAN mode

default ip igmp stream-limit-max-streams

Use this command to set the stream imitation maximum streams to the default values.

Syntax

```
default ip igmp stream-limit-max-streams
```

Command mode

Interface VLAN mode

ip mroute static-source-group

Use this command to add a static source-group entry to the PIM multicast routing table.

Syntax

```
ip mroute static-source-group <A.B.C.D> <A.B.C.D/0-32>
```

where

`<A.B.C.D>` is the multicast source address for this static source-group entry. How you configure the source address depends on the protocol you are using and in what mode.

`<A.B.C.D/0-32>` is the subnet mask of the source for this static source-group entry.

Command mode

Global configuration mode

no ip mroute static-source-group

Use this command to remove a static source-group entry from the PIM multicast routing table.

Syntax

```
no ip mroute static-source-group <A.B.C.D> <A.B.C.D/0-32>
```

where

`<A.B.C.D>` is the multicast source address for this static source-group entry. How you configure the source address depends on the protocol you are using and in what mode.

`<A.B.C.D/0-32>` is the subnet mask of the source for this static source-group entry.

ip pim

Use this command to:

- configure PIM-SM globally.
- configure PIM-SM on a VLAN

Configuring PIM-SM globally

Use this command to configure PIM-SM globally on a switch.

Syntax

ip pim

Parameters

This command includes the following parameters:

ip pim **followed by:**	
bootstrap-period<integer>	Specifies the interval (in seconds) that the elected BSR waits between originating bootstrap messages. • **integer** is an integer in the range of 5–32757. The default is 60.
rp-c-adv-timeout<integer>	Specifies how often (in seconds) that routers configured as candidate RPs send C-RP advertisement messages. When this timer expires, the C-RP sends an advertisement message to the elected BSR. • **integer** is an integer in the range of 5–26214. The default is 60.
disc-data-timeout <integer>	Specifies how long (in seconds) to discard data until the Join is received from the RP. An ipmc discard record is created after a register packet is sent, until the the timer expires or when a Join is received. • **integer** is an integer in the range of 5–65535. The default is 60.

ip pim **followed by:**	
activity-chk-interval <15|30|210>	Specifies how often (in seconds) to check traffic activity for a multicast group. The lower the value, the more often the switch checks the activity. • The default is 210. **Notes:** • Before you can change the activity-chk-interval, you must disable PIM-SM globally. • Nortel recommends an activity check interval of 30 seconds. • Nortel recommends that you set the activity check interval to 210 seconds for systems that have a large number (200+) of S,G streams. • When one of the timer activity-chk-interval or fwd-cache-timeout is configured with a nondefault value, the other cannot be configured.
join-prune-interval <integer>	Specifies how long to wait (in seconds) before the PIM-SM router sends out the next join/prune message to its upstream neighbors. • **integer** is an integer in the range of 1–18724. The default is 60.
fwd-cache-timeout<integer>	Configures the forward cache timeout globally. The default is 210 • **integer**is an integer in the range 10–86400. The default is 210

ip pim **followed by:**	
register-suppression-timeout <integer>	Sets the PIM-SM register suppression timeout. The default is 60. • **integer** is an integer in the range 6–65535. The default is 60
unicast-route-change-timeout <integer>	Sets the PIM-SM unicast route change timeout. • **integer** is an integer in the range 2–65535. The default is 5.

Command mode

Global configuration mode

Configuring PIM-SM on a VLAN

Use this command to configure PIM-SM on a VLAN.

Syntax

ip pim

Parameters

This command includes the following parameters:

ip pim **followed by:**	
bsr-candidate preference <integer>	Enables the BSR candidate. • **integer** is an integer with a range of 0 to 255. The default is -1, which indicates that the current interface is not a Candidate BSR
enable	Enables PIM on a particular VLAN.

ip pim **followed by:**	
interface-type <active|passive>	Sets the interface type on a particular VLAN. • **active** allows PIM-SM control traffic to be transmitted and received. • **passive**passive prevents PIM-SM control traffic from being transmitted or received, thereby reducing the load on a system. This feature is useful when a high number of PIM-SM interfaces exist and are connected to end users, not to other switches.
join-prune-interval<seconds>	Specifies how long to wait (in seconds) before the PIM-SM switch sends out the next join/prune message to its upstream neighbors. The range is 1 to 18724 seconds and the default is 60 seconds.
query-interval<seconds>	Sets the hello interval to a particular VLAN. The range is 0 to 18724 seconds and the default is 30 seconds.

Command mode
Interface VLAN mode

ip pim enable

You can use this command to:

- enable Protocol Independent Multicast-Sparse Mode (PIM-SM) globally.
- enable PIM-SM on a selected VLAN

  When you enable PIM-SM on a selected VLAN, you must also enable it globally.

Enabling PIM-SM globally

You can use this command to enable PIM globally on the switch

Syntax
ip pim enable

Command mode
Global configuration mode

Enabling PIM-SM on a VLAN

You can use this command to enable PIM on a VLAN.

Syntax

```
ip pim enable
```

no ip pim

Use this command to:

- disable PIM-SM globally.
- disable PIM-SM on a VLAN

Disabling PIM-SM globally

You can use this command to disable PIM globally on the switch

Syntax

```
no ip pim
```

Command mode

Global configuration mode

Disabling PIM-SM on a VLAN

You can use this command to disable PIM on a VLAN.

Syntax

```
no ip pim
```

Command mode

Interface VLAN mode

ip pim interface virtual neighbor

Use this command to enable a virtual neighbor. A virtual neighbor is a PIM-SM neighbor IP address on the Ethernet Routing Switch 8300 neighbor table. A virtual neighbor is typically used where the next-hop for a static route cannot run PIM-SM, such as the virtual VRRP address on an adjacent device.

Syntax

```
ip pim interface <ipaddr> virtual-neighbor <ipaddr>
```

where

<ipaddr> is the IP address of the interface.
<ipaddr> is the IP address of the virtual neighbor.

Command mode

Global configuration mode

no ip pim interface virtual neighbor

Use this command to disable a virtual neighbor.

Syntax

```
no ip pim interface <ipaddr> virtual-neighbor
```

where

<ipaddr> is the IP address of the interface.

ip pim rp-candidate group rp

Use this command to add a rendezvous point (RP) in the RP set.

Syntax

```
ip pim rp-candidate group<ipaddr> <mask> rp <ipaddr>
```

where

<ipaddr> is the IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.

<mask> is the address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP.

<ipaddr> is the IP address of the C-RP. This address must be one of the local PIM-SM enabled interfaces.

Command mode

Global configuration mode

no ip pim rp-candidate group rp

Use this command to remove a rendezvous point (RP) in the RP set.

Syntax

```
no ip pim rp-candidate group <ipaddr> <mask>
```

where

<ipaddr> is the IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.

<mask> is the address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP.

Command mode

Gobal configuration mode

ip pim static-rp

Use this command to enable a static RP.

Syntax

```
ip pim static-rp
```

When you enter this command, the following message appears:

WARNING: RP information learnt dynamically through BSR functionality will be lost.

Do you wish to enable Static RP? (y/n) ?

Command mode

Global configuration mode

no ip pim static-rp

Use this command to disable a static RP.

Syntax

```
no ip pim static-rp
```

When you enter this command, the following message appears:

WARNING: Static RP information will be lost.

Do you wish to disable Static RP? (y/n) ?

Command mode

Global configuration mode

ip pim static-rp

Use this command to add a static RP to the RP set.

Syntax

```
ip pim static-rp <group> <mask> <rp>
```

where

<group> is the IP address of the multicast group. When combined with the group mask, it identifies the range of the multicast addresses that the RP handles.

<mask> is the address mask of the multicast group. When combined with the group address, it identifies the range of the multicast addresses that the RP handles.

<rp> is the IP address of the static RP.

Command mode

Global configuration mode

no ip pim static-rp

Use this command to remove a static RP.

Syntax

```
no ip pim static-rp <group> <mask> <rp>
```

where

<group> is the IP address of the multicast group. When combined with the group mask, it identifies the range of the multicast addresses that the RP handles.

<mask> is the address mask of the multicast group. When combined with the group address, it identifies the range of the multicast addresses that the RP handles.

<rp> is the IP address of the static RP.

Command mode

Global configuration mode

show debug ip pim

Use this command to display the current PIM-SM debug trace flag settings on the switch.

Syntax

```
show debug ip pim
```

Command mode

Privileged EXEC mode

show interfaces vlan igmp

This command allows you to view the IGMP VLAN interfaces.

Syntax

```
show interfaces vlan igmp [<vid>]
```

where

vid is a VLAN ID from 1 to 4000. (Note that 1 to 2000 is the default, while 1 to 4000 is valid when the *vid-max4k* flag is set to true).

Command mode

User EXEC mode

show ip igmp

Use this command to display information about IGMP.

Syntax

```
show ip igmp
```

Parameters

This command includes the following options:

show ip igmp **followed by:**	
access	Displays information about IGMP multicast access filters.
cache	Displays information about IGMP cached groups.
[<count>]**group [<count>]**	Displays information about IGMP groups per port.
interface	Displays information about the IGMP interface (i.e., the IGMP querier).
mrdisc	Displays information about the multicast router discovery.
router-alert	Displays the IGMP router alert check status.
[]**sender [<count>]**	Displays information about the IGMP sender list.
snoop	Displays the status of IGMP snoop and proxy-snoop.
static	Displays information about the static and blocked ports for the IGMP-enabled interfaces.

Command mode

Privileged EXEC mode

For more information about IGMP operations, see *Configuring IP Multicast Routing Protocols*.

show ip igmp access

Once the access filter has been configured, this command allows you to view it.

Syntax

show ip igmp access

Command mode

Privileged EXEC mode

show ip igmp cache

This command allows you to view the IGMP cache.

Syntax

```
show ip igmp cache
```

Command mode

User EXEC mode

show ip igmp group

This command allows you to view an IGMP group. This command displays dynamic and static groups, with both dynamic and static groups being counted separately. For example, if the same group has dynamic and static members, that group is counted twice.

Syntax

```
show ip igmp group [<count>]
```

where

<count> shows the total number of dynamic groups and the number of static group ports. For example, in the case of a static group, each static member port is counted.

Command mode

User EXEC mode

show ip igmp group

You can use this command to view the count of IGMP group entries.

Syntax

```
show ip igmp group
```

Parameters

This command includes the following parameters:

show ip igmp group **followed by:**	
group <A.B.C.D>	Specifies the IP multicast group address.
member-subnet <a.b.c.d/x|a.b.c.d/x.x.x.x|default>	Specifies the IP multicast group address.
<cr>	Indicates a Carriage return.

Command mode

User EXEC mode

show ip igmp interface

Use this command to view the IGMP interface such as the IGMP querier.

Syntax

```
show ip igmp interface
```

Parameters

This command includes the following parameters:

show ip igmp interface **followed by:**	
<cr>	Indicates a Carriage return.
[{fastethernet|gigabitethernet} {slot/port[-slot/port][, ...]}]	Specifies the ports.
[vlan <1-4000>]	Specifies the VLAN ID in the range 1 to 4000.

Command mode

User EXEC mode

show ip igmp mrdisc

You can use this command to view the IGMP multicast router discovery parameters on a specific VLAN.

Syntax

```
show ip igmp mrdisc
```

Command mode

User EXEC mode

show ip igmp router-alert

This command allows you to view the router alert check status.

Syntax

```
show ip igmp router-alert
```

Command mode

User EXEC mode

show ip igmp sender

You can use this command to view the IGMP sender.

Syntax

```
show ip igmp sender
```

Parameters

This command includes the following parameters:

show ip igmp sender **followed by:**	
count	Shows the number of entries.
<cr>	Shows the IP sender with the host and the multicast group.
group <A.B.C.D>	Specifies the IP address of the multicast group address.
member-subnet <a.b.c.d/x|a.b.c.d/x.x.x.x|default>	Specifies the member IP address and network mask.

Command mode

User EXEC mode

show ip igmp snooping

You can use this command to view the IGMP snoop, snoop queriers and proxy status.

Syntax

```
show ip igmp snooping
```

Command mode

User Exec mode

show ip igmp snoop-trace

Use this command to show multicast hardware information.

Syntax

```
show ip igmp snoop-trace [source <value>] [group
<value>]
```

where

[source <value>] specifies the source IP address in the format a.b.c.d.

[group <value>] specifies the group IP address in the format a.b.c.d.

Command mode

User EXEC mode

show ip igmp static

Once static member members have been added, this command allows you to view the static entries.

Syntax

```
show ip igmp static
```

Command mode

User EXEC mode

show ip igmp stream-limit

Use this command to show multicast stream limitation members on an interface.

Syntax

```
show ip igmp stream-limit {interface}
```

where

{interface} shows multicast stream limitation members on an interface.

Command mode

Privileged EXEC mode

show ip igmp sys

You can use this command to view the IGMP system parameters.

Syntax

```
show ip igmp sys
```

Command mode

User EXEC mode

show ip mroute static-source-group

Use this command to display information about the static source-groups on the current interface.

Syntax

```
show ip mroute static-source-group [<A.B.C.D>]
```

where

<A.B.C.D> is the multicast source address for the specific static source-group entry.

Command mode

Privileged EXEC mode

show ip pim

Use this command to display the global status of PIM-SM on the switch.

Syntax

```
show ip pim
```

Command mode

Privileged EXEC mode

show ip pim active-rp

Use this command to display information about the active rendezvous point (RP) for a specific group.

Syntax

```
show ip pim active-rp [>ipaddr]
```

where

ipaddr is the IP address of the multicast group.

Command mode

Privileged EXEC mode

show ip pim bsr

Use this command to display information for a bootstrap router.

Syntax

```
show ip pim bsr
```

Command mode

Privileged EXEC mode

show ip pim interface

Use this command to display information about a PIM-SM interface.

Syntax

```
show ip pim interface
```

Command mode

Privileged EXEC mode

show ip pim interface vlan

Use this command to display information about the PIM-SM interface setup for VLANs.

Syntax

```
show ip pim interface vlan
```

Command mode

Privileged EXEC mode

show ip pim mroute

Use this command to display information from the route table.

Syntax

```
show ip pim mroute
```

Command mode

Privileged EXEC mode

show ip pim static-rp

Use this command to display information about a static RP.

Syntax

```
show ip pim static-rp
```

Command mode

Privileged EXEC mode

show ip pim neighbor

Use this command to display information for the PIM-SM virtual neighbor.

Syntax

```
show ip pim neighbor
```

Command mode

Privileged EXEC mode

show ip pim rp-candidate

Use this command to display candidate RP information.

Syntax

```
show ip pim rp-candidate
```

Command mode

Privileged EXEC mode

show ip pim virtual-neighbor

Use this command to display information about the neighboring routers configured with PIM-SM.

Syntax

```
show ip pim virtual-neighbor
```

Command mode

Privileged EXEC mode

Quality of Service commands

This chapter describes NNCLI Quality of Service (Qos) commands and their parameters.

Quality of Service Commands
"show qos policy-stats" (page 425)
"show qos map 8021p-to-class-map" (page 426)
"show qos map 8021p-to-drop-precedence-map" (page 426)
"show qos map class-to-8021p-map" (page 426)
"show qos map class-to-8021p-policed-map" (page 426)
"show qos map dscp-to-cos-policed-map" (page 427)

For more information about QoS, see *Nortel Ethernet Routing Switch 8300 Configuration — QoS and Filter using the NNCLI (NN46200-501)*.

interface FastEthernet/GigabitEthernet

Use this command to enter the interface configuration mode for Fast Ethernet interfaces.

Syntax

```
interface FastEthernet <ports>
interface GigabitEthernet <ports>
```

where

`<ports>` specifies the applicable ports associated with FastEthernet interfaces in port list form: `{slot/port [-slot/port][, ...]}`.

Command mode

Global configuration mode

Next command mode

Interface configuration mode

For more information about configuring port interfaces, see *Nortel Ethernet Routing Switch 8300 Configuration — QoS and Filter using the NNCLI (NN46200-501)*.

qos

Use this command to configure the QoS level on a port. The default is level 1, and level 7 is reserved for network traffic.

Syntax

```
qos
```

Parameter

This command includes the following options:

qos **followed by:**	
port <ports>	Specifies the applicable ports in port list form: **{slot/port [-slot/port] [, ...]}**.
8021p-override	Enables the Differentiated Service IEEE 802.1P override feature.
qos-level <level>	Sets the QoS level (0 to 7) associated with the traffic service class. Level 7 is reserved and cannot be set.
shaper [rate <value>] [burst-size <value>]	Enables or disables shaper on the port. **[rate <value>]** sets the shaping rate in Mbps. ***Note 1:*** The actual shaping rate might be different from the configured rate due to the rate granularity of the shaper. The range is from 1 to 10000Mbps and the default is **10**. ***Note 2:*** The actual burst size might be different from the configured size due to the granularity of the shaper. The range is from 4 to 16000KB, and the default is **4**.
trust-dscp enable	Enables or disables DSCP being trusted in an IPv4/6 packet. When enabled the **dscp-to-cos-map** will be used to decide on packet's traffic class and 802.1p value. This allows applications to activate Layer-3 based CoS on trusted interface. Default is disabled. ***Note:*** Trust DSCP can only be enabled on either 8348GTX or 8348GTX-PWR modules when in the GigabitEthenet level of NNCLI
update-dynamic-mac-qos-level	Enables or disable updating of the the qos level. The default is disable.

Command mode

Interface configuration mode

qos 8021p-override

Use this command to enable the Differentiated Service IEEE 802.1P override feature.

Syntax

```
qos 8021p-override
```

Command mode

Interface configuration mode

no qos 8021p-override

Use this command to disable the Differentiated Service IEEE 802.1P override feature.

Syntax

```
no qos 8021p-override
```

Command mode

Interface configuration mode

qos shaper

Use this command to enable the shaper configured on a port.

Syntax

```
qos shaper
```

Command mode

Interface configuration mode

qos shaper rate

Use this command to set the shaper rate

Syntax

```
qos shaper rate <1-10000>
```

Command mode

Interface configuration mode

qos shaper burst size

Use this command to set the shaper burst size

Syntax

```
qos shaper burst-size <4-16000>
```

Command mode

Interface configuration mode

no qos shaper

Use this command to disable the shaper configured on a port.

Syntax

```
no qos shaper
```

Command mode

Interface configuration mode

qos trust-dscp enable

Use this command to enable DSCP being trusted in an IPv4/6 packet.

Note 1: Trust DSCP can only be enabled on either 8348GTX or 8348GTX-PWR modules when in the GigabitEthenet level of NNCLI

Note 2: Trust DSCP should be enabled on the filter associated with the same port for consistent trust dscp operation.

Syntax

```
qos trust-dscp enable
```

Command mode

Interface GigabitEthernet configuration mode

no qos trust-dscp enable

Use this command to disable DSCP being trusted in an IPv4/6 packet.

Syntax

```
no qos trust-dscp enable
```

Command mode

Interface GigabitEthernet configuration mode

qos update-dynamic-mac-qos-level

Use this command to enable the MAC QoS level and override the port's QoS level.

Syntax

```
qos update-dynamic-mac-qos-level
```

Command mode

Interface configuration mode

no qos update-dynamic-mac-qos-level

Use this command to disable the MAC QoS level and override the port's QoS level.

Syntax

```
no qos update-dynamic-mac-qos-level
```

Command mode

Interface configuration mode

qos map

Use this command to configure QoS mapping tables.

Syntax

```
qos map [8021p-to-class-map <802.1p> <traffic-class> ]
[8021p-to-drop-precedence-map <802.1p> <drop-precedence>
] [class-to-8021p-map <traffic-class> <802.1p> ]
[class-to-8021p-policed-map <conformance-level> <dscp>
<traffic-class> <8021p> ] [dscp-to-cos-policed-map
<conformance-level> <dscp> <traffic-class> <8021p>
<drop-precedence> ]
```

Parameter

This command includes the following options:

`qos map` **followed by:**	
`8021p-to-class-map <802.1p> <traffic-class>`	Maps the value of the IEEE802.1 p bit (0 to 7) of the incoming packet to one of the traffic classes (0 to 7).
`8021p-to-drop-precedence-map <802.1p> <drop-precedence>`	Maps the value of the IEEE802.1 p bit (0 to 7) of the incoming packet to one of the following levels: • low • medium • high Packets marked with a higher drop precedence will be dropped first during periods of congestion.
`class-to-8021p-map <traffic-class> <802.1p>`	Maps the value of the traffic class (0 to 7) to the IEEE802.1 p bit (0 to 7) of the incoming packet.

qos map **followed by:**	
class-to-8021p-policed-map <conformance-level> <traffic-class> <802.1p>	Maps the value of the traffic class (0 to 7) to the IEEE802.1 p bit (0 to 7) of the incoming packet based on one of the following conformance levels. • **red** means the packet exceeds the PIR (Peak Information Rate). • **yellow** means the packet does not exceed the PIR, but it does exceed the CIR (Committed Information Rate). • **green** means the packet does not exceed the CIR. The conformance level is the outcome of policing and indicates the behavior of a traffic flow.
dscp-to-cos-policed-map <conformance-level> <dscp> <traffic-class> <8021p> <drop-precedence>	Maps the value of the DSCP (0 to 63) to the CoS of the incoming packet based on one of the following conformance levels. • **red** means the packet exceeds the PIR (Peak Information Rate). • **yellow** means the packet does not exceed the PIR, but it does exceed the CIR (Committed Information Rate). • **green** means the packet does not exceed the CIR. DSCP has the following options: cs0, af11, af12, af13, cs3, c4. The conformance level is the outcome of policing and indicates the behavior of a traffic flow. After the conformance level, enter the p bit value (0 to 7), the traffic class value (0 to 7), and the drop precedence level (low | medium | high).

Command mode

Global configuration mode

qos policy create

Use this command to create a Quality of Service policy.

Syntax

```
qos policy <policy-id> create [<enable|disable>] [name
<value> ] [cir <value> ] [cbs <value> ] [pir <value> ] [pbs
<value> ]
```

where

<policy-id> specifies the QoS policy ID number and is a unique ID in the range from 1 to 128.

Parameter

This command includes the following options:

qos policy <policy-id> create **followed by:**	
<enable|disable>	Enables or disables the policy you just created. The default is disable.
name <value>	Names the policy. You can use up to 33 characters to identify the policy. The range is 0 to 32. If you do not assign a name, the switch automatically assigns one.
cir <value>	Sets the Committed Information Rate (CIR) in Kbps. The CIR is used to measure against a traffic stream. The CIR specifies the rate at which incoming traffic is measured against to be considered at a high level of conformance. The range is from 64 to 10000000, and the default is **1000**.
cbs <value>	Sets the Committed Burst Size (CBS) in Kbps. The CBS is used to measure against a traffic stream. The CBS specifies the maximum burst size that is supported for flows to be considered to be at a high level of conformance. The range is from 2 to 512000, and the default is **200**.

qos policy <policy-id> create **followed by:**	
pir <value>	Sets the Peak Information Rate (PIR) in Kbps. The PIR is used to measure against a traffic stream. The PIR specifies the rate at which incoming traffic can arrive to be considered at a medium level of conformance. The range is from 64 to 10000000, and the default is 1000.
pbs <value>	Sets the Peak Burst Size (PBS) in Kbps. The PBS is used to measure against a traffic stream. The PBS specifies the maximum burst size that is supported for flows to be considered to be at a medium level of conformance. The range is from 2 to 512000, and the default is 200.

Command mode

Global configuration mode

no qos policy

Use this command to delete a Quality of Service policy.

Syntax

```
no qos policy <policy-id>
```

Command mode

Interface configuration mode

qos policy action

Use this command to configure an existing Quality of Service policy.

Syntax

```
qos policy <policy-id> action [drop rmk-cos] [rmk-8021p]
[rmk-dp]
```

Parameter

This command includes the following options:

qos policy <policy-id> action **followed by:**	
drop	Configures the policy to drop non-conforming traffic.
rmk-cos	Configures the policy to re-mark CoS parameters. The CoS parameters are re-marked according to the DSCP to CoS mapping table.
rmk-8021p	Configures the policy to re-mark the 802.1 user priority parameters. The user priority is re-marked according to the TrafficClass to 8021p mapping table.
rmk-dp	Configures the policy to re-mark drop precedence according to the conformance level.

Command mode

Global configuration mode

no qos policy action

Use this command to delete a Quality of Service policy.

Syntax

```
no qos policy <policy-id>action [drop] [rmk-cos] [rmk-8021p]
[rmk-dp]
```

Parameter

This command includes the following options:

no qos policy <policy-id> action **followed by:**	
drop	Configures the policy to drop non-conforming traffic.
rmk-cos	Configures the policy to re-mark CoS parameters. The CoS parameters are re-marked according to the DSCP to CoS mapping table.
rmk-8021p	Configures the policy to re-mark the 802.1 user priority parameters. The user priority is re-marked according to the TrafficClass to 8021p mapping table.
rmk-dp	Configures the policy to re-mark drop precedence according to the conformance level.

Command mode

Interface configuration mode

qos policy modify

Use this command to configure an existing Quality of Service policy.

Syntax

```
qos policy <policy-id> modify [name <value> ] [cir
<value> ] [cbs <value> ] [pir <value> ] [pbs <value> ]
```

Parameter

This command includes the following options:

qos policy <policy-id> modify **followed by:**	
name <value>	Changes the name of the policy. The range is 0 to 32 characters to identify the policy.
cir <value>	Changes the Committed Information Rate (CIR) in Kbps. The range is from 64 to 10000000, and the default is 1000.
cbs <value>	Changes the Committed Burst Size (CBS) in Kbps. The range is from 2 to 512000, and the default is 200.
pir <value>	Changes the Peak Information Rate (PIR) in Kbps. The range is from 64 to 10000000, and the default is 1000.
pbs <value>	Changes the Peak Burst Size (PBS) in Kbps. The range is from 2 to 512000, and the default is 2.

Command mode

Global configuration mode

qos egress-counter-set

Use this command to configure an egress counter that displays the statistics you want to monitor.

Syntax

```
qos egress-counter-set <counter_set_id> [port <port_num> ]
[vlan <vlan_id> ] [queue <vlan_id> ] [dp <dp_level> ]
```

where

`<counter_set_id>` is a value in the range from 1 to 40.

Parameter

This command includes the following options:

`qos egress-counter-set <counter_set_id>` **followed by:**	
`port <port_num>`	Configures the port(s) that you want the counter set to monitor. If you configure one or more ports, the switch disables MONITOR ALL PORTS, which is enabled by default.
`vlan <vlan_id>`	Configures the VLAN that you want the counter set to monitor. If you configure a VLAN, the switch disables MONITOR ALL VLANS, which is enabled by default.
`queue <vlan_id>`	Configures the tx queue ID (0 to 7) that you want the counter set to monitor. If you configure a queue, the switch disables MONITOR ALL Qs, which is enabled by default.
`dp <dp_level>`	Configures the Drop Precedence level (low, medium or high) that you want the counter set to monitor. If you configure a Drop Precedence level, the switch disables MONITOR ALL DPs, which is enabled by default.

Command mode

Global configuration mode

no qos egress-counter-set

Use this command to delete an egress counter set.

Syntax

```
no qos egress-counter-set <counter_set_id>
```

Command mode

Interface configuration mode

show qos egress-stats

Use this command to display information about the QoS egress counter set.

Syntax

```
show qos egress-stats [ <counter_set_id> ]
```

where

`<counter_set_id>` is a value in the range from 1 to 40.

Command mode

Privileged EXEC mode

show qos egress-counter-set

Use this command to display information about the QoS egress counter set.

Syntax

```
show qos egress-counter-set [ <counter_set_id> ]
```

where

`<counter_set_id>` is a value in the range from 1 to 40.

Command mode

Privileged EXEC mode

qos map-qos-level-override

Use this command to map the MAC QoS-level override setting.

Syntax

```
qos map-qos-level-override
```

Command mode

Global configuration mode

show qos policy

Use this command to display information about the QoS policies.

Syntax

```
show qos policy [ <policy-id> ]
```

where

`<policy-id>` specifies the QoS policy ID number. The range is 1 to 128.

Command mode

Privileged EXEC mode

show qos policy-stats

Use this command to display the QoS policy statistics.

Syntax

```
show qos policy-stats [ <policy-id> ]
```

where

<policy-id> specifies the QoS policy ID number. The range is 1 to 128.

Command mode

Privileged EXEC mode

show qos map 8021p-to-class-map

Use this command to display how the switch maps 802.1p user priority to traffic class levels.

Syntax

```
show qos map 8021-to-class-map
```

Command mode

Privileged EXEC mode

show qos map 8021p-to-drop-precedence-map

Use this command to display how the switch maps 802.1p bits to drop precedence.

Syntax

```
show qos map 8021-to-drop-precedence-map
```

Command mode

Privileged EXEC mode

show qos map class-to-8021p-map

Use this command to display how the switch maps traffic class levels to an 802.1p user priority.

Syntax

```
show qos map class-to-8021p-map
```

Command mode

Privileged EXEC mode

show qos map class-to-8021p-policed-map

Use this command to display how the switch maps traffic class levels to an 802.1p user priority.

Syntax

```
show qos map class-to-8021p-policed-map
```

Command mode

Privileged EXEC mode

show qos map dscp-to-cos-policed-map

Use this command to display how the switch maps DSCP to layer 2 Class of Service (CoS).

Syntax

`show qos map dscp-to-cos-policed-map`

where

`<conformance-level>` is the outcome of policing and indicates the behavior of a traffic flow.

Command mode

Privileged EXEC mode

Web server commands

This chapter describes NNCLI web server commands and their parameters.

Web Server Commands
"web-server" (page 429)
"web-server password" (page 430)
"no web-server" (page 430)
"no web-server" (page 430)

web-server

Use this command to enable and manage or disable the Web server interface.

Syntax

```
web-server [def-display-rows <integer> ] [help-tftp
<filename> ] [http-port <integer> ]
```

Parameters

This command includes the following optional parameters:

web-server **followed by:**	
[def-display-rows <integer>]	Specifies the number of rows displayed per page. The range of values is 10 to 100.
[help-tftp <filename>]	Specifies the file name, location, and path for the Web server HTML Help file. The target can be flash, pcmcia, or a TFTP IP address. The range of values is a string of 0 to 256 characters.
[http-port <integer>]	Specifies the http port of the Web server. The range of values is 1 to 49151.

Command mode

Global configuration mode

web-server password

Use this command to specify passwords for access to the Web server interface.

Syntax

```
web-server password <ro> <username> <passwd>
```

Parameters

This command includes the following parameters:

web-server password **followed by:**	
<ro>	Specifies a read-only access level to the Web server interface.
<username>	Specifies the user's login name. The range of values is a string up to 20 characters. The default is **ro**.
<passwd>	Specifies the password associated with **<username>**. The range of values is a string up to 20 characters. The default is **ro**.

Command mode

Global configuration mode

no web-server

Use this command to turn off Web access.

Syntax

```
no web-server
```

Command mode

Privileged EXEC mode

show web-server

Use this command to display whether or not Web access is enabled, as well as password and access information.

Syntax

```
show web-server
```

Command mode

Privileged EXEC mode

POE commands

This chapter describes NNCLI POE commands and their parameters.

Quality of Service Commands
"show poe port-stats" (page 441)
"show poe power-measurement" (page 441)

interface FastEthernet/GigabitEthernet

Use this command to enter the interface configuration mode for the Fast Ethernet/Gigabit Ethernet interfaces

Syntax

```
interface FastEthernet/GigabitEthernet <ports>
```

Command mode

Global configuration mode

interface FastEthernet

Use this command to enter into the interface configuration mode for Fast Ethernet interfaces.

Syntax

```
interface FastEthernet <ports>
```

where

`<ports>` specifies the applicable ports associated with FastEthernet interfaces in port list form: `{slot/port [-slot/port][, ...]}`.

Command mode

Global configuration mode

poe detect-control

Use this command to specify detect control for Power over Ethernet ports.

Syntax

```
poe detect-control [port <ports>] <auto|test>
```

Parameter

This command includes the following options:

poe detect control **followed by:**	
[ports <ports>]	Specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.
auto | test	Specifes automatic or test detection.

Command mode

Interface configuration mode

poe detection-control

Use this command to configure power detection control for the Power over Ethernet ports.

Syntax

```
poe detection-control
```

Parameter

This command includes the following options:

poe detection-control **followed by:**	
[ports <ports>]	Specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.
auto | test	Specifes automatic or test detection.

Command mode

Interface GigabitEthernet mode

poe fw-upgrade slot

Use this command to perform a firmware upgrade for a PoE card in a slot.

Syntax

```
poe fw-upgrade slot <slots>
```

Command mode

Global configuration mode

poe limit

Use this command to configure the power limit for the Power over Ethernet ports.

Syntax

```
poe limit [port <ports>] <3..16>
```

Parameters

This command includes the following parameters:

poe limit [port <ports>] <3..16> followed by:	
[ports <ports>]	Specifies the applicable ports in port list form: {slot/port [-slot/port] [, ...]}.
<3-16>	The value to set for the port PoE power limit.

Command mode

Interface GigabitEthernet mode

poe limit

Use this command to set the power limit for Power over Ethernet ports.

Syntax

```
poe limit <3-16> [port <ports> ]
```

Command mode

Interface configuration mode

poe notification slot

Use this command to set the notification control for Power over Ethernet.

Syntax

```
poe notification [slot <slots> ]
```

Command mode

Global configuration mode

no poe notification

Use this command to turn off notification control.

Syntax

```
no poe notification [slot <slots> ]
```

Command mode

Global configuration mode

poe port admin

Use this command to configure the admin for the Power over Ethernet ports.

Syntax

```
poe port <ports> admin <enable|disable>
```

Command mode

Interface GigabitEthernet mode

poe priority

Use this command to configure the power priority for the Power over Ethernet ports.

Syntax

```
poe priority port <ports> <low|high|critical>
```

where

port<ports> Specifies the applicable ports in port list form: **{slot/port [-slot/port][, ...]}**

<low|high|critical> specify the power priorites.

Command mode

Interface GigabitEthernet mode

poe priority

Use this command to set port priority for Power over Ethernet.

Syntax

```
poe priority [port <ports>] <low|high|critical>
```

Command mode

Interface configuration mode

poe priority

Use this command to enable Power over Ethernet on a particular slot or slots.

Syntax

```
poe priority [slot <slots>] <low|high|critical>
```

Command mode

Global configuration mode

poe shutdown

Use this command to shut down Power over Ethernet on specified ports.

Syntax

```
poe shutdown [port <ports> ]
```

Command mode

Interface configuration mode

no poe shutdown

Use this command to specify no shutdown of Power over Ethernet.

Syntax

```
no poe shutdown [port <ports> ]
```

Command mode

Interface configuration mode

poe shutdown

Use this command to disable Power over Ethernet for specified slots.

Syntax

```
poe shutdown slot <slots>
```

Command mode

Global configuration mode

no poe shutdown

Use this command to specify disabling the Power over Ethernet function for specified ports.

Syntax

```
no poe shutdown port [port <ports>]
```

Parameters

This command includes the following parameters:

`no poe shutdown port` **followed by:**	
`<portlist>`	Selects the portlist {port[-port][,...]}.

Command mode

Interface GigabitEthernet mode

no poe shutdown

Use this command to specify disabling the Power over Ethernet function for specified slots.

Syntax

```
no poe shutdown [slot <slots>]
```

Command mode

Global configuration mode

poe type

Use this command to set the port type for Power over Ethernet.

Syntax

```
poe type [port <ports>] <other|telephone|webcam|wire-
less>
```

Parameters

This command includes the following parameters:

poe type **followed by:**	
port <ports>	Specifies ports as the poe port type.
other	Specifies another device as the poe port type.
telephone	Specifies a telephone poe port type.
webcam	Specifies webcam as the poe port type.
wireless	Specifies wireless as the poe port type.

poe type port

Use this command to configure the type of Power over Ethernet ports.

Syntax

```
poe type port <ports> <other|telephone|webcam|wireless>
```

Parameters

This command includes the following parameters:

config poe type **followed by:**	
port <ports>	Specifies ports as the poe port type.
other	Specifies another device as the poe port type.

`config poe type` **followed by:**	
`telephone`	Specifies a telephone poe port type.
`webcam`	Specifies webcam as the poe port type.
`wireless`	Specifies wireless as the poe port type.

Command mode
Interface GigabitEthernet mode

Command mode
Interface configuration mode

poe usage-threshold
Use this command to set the usage threshold for Power over Ethernet for a particular slot or slots.

Syntax
```
poe usage-threshold [slot <slots> ]
```

Command mode
Global configuration mode

show poe main-status
Use this command to show the poe main status by slot.

Syntax
```
show poe main-status [slot <slot id> ]
```

Command mode
Privileged Exec mode

show poe port-status
Use this command to display the current status of the Power over Ethernet port.

Syntax
```
show poe port-status [ <ports> ]
```

Command mode
Privileged Exec mode

show poe sys-status
Use this command to display the system status for Power over Ethernet.

Syntax

```
show poe sys-status
```

Command mode

Privileged EXEC mode

show poe port-stats

Use this command to display the port statistics for the Power over Ethernet ports.

Syntax

```
show poe port-stats [port <ports>]
```

Command mode

Privileged EXEC mode

show poe power-measurement

Use this command to display power measurement for Power over Ethernet.

Syntax

```
show poe power-measurement [port <ports>]
```

Command mode

Privileged Exec mode

VCT commands

This chapter describes NNCLI VCT commands and their parameters.

VCT Commands
"show vct" (page 443)
"vct test" (page 443)

show vct

This command displays a virtual cable test or displays Virtual Cable Tester (VCT) information for a range of ports.

Syntax

```
show vct <portlist>
```

Parameters

This command includes the following parameters:

show vct **followed by:**	
<portlist>	Displays a virtual cable test on the specified ports. **portlist** specify the ports in the portlist form **{ slot/port [- slot/port][, ...]}**.

Command mode

User EXEC mode

vct test

This command specifies a virtual cable test.

Syntax

```
vct test <portlist>
```

Parameters

This command includes the following parameters:

`vct test` **followed by:**	
`<portlist>`	Starts a virtual cable test on the specified ports. `portlist` specify the ports in the portlist form `{ slot/port [- slot/port ][, ...]}`.

Command mode

Global configuration mode

Index

Nortel Ethernet Routing Switch 8300

Command Reference — NNCLI

Publication: NN46200-306
Document status: Standard
Document version: 03.01
Document date: 27 August 2007

To provide feedback or report a problem in the document, go to www.nortel.com/documentfeedback

Sourced in Canada and the United States of America.