Part No. 216490-B
July 2004

4655 Great America Parkway
Santa Clara, CA 95054

NNCLI Configuration Guide for BoSS Software Release 3.5 for BayStack 460 and 470 Switches

216490-B

NORTEL NETWORKS™

Copyright © 2004 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Autotopology, BayStack, BaySecure, Business Policy Switch 2000, Nortel Networks, the Nortel Networks logo, Optivity, Optivity Policy Services, Preside, and Quick2Config are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Java is a trademark of Sun Microsystems, Inc.

Acrobat and Adobe are trademarks of Adobe Systems, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

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 Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. 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).

International regulatory statements of conformity

This is to certify that the Nortel Networks BayStack 460 and 470 switches were evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC - Electromagnetic Emissions – CISPR 22, Class A
- EMC - Electromagnetic Immunity – CISPR 24
- Electrical Safety – IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed below.

National electromagnetic compliance (EMC) statements of compliance

FCC statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

ICES statement (Canada only)

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Nortel Networks BayStack 460 and 470 switches) do not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Nortel Networks BayStack 460 and 470 switches) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

CE marking statement (Europe only)

EN 55 022 statements

This is to certify that the Nortel Networks BayStack 460 and 470 switches are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

Caution: This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case the user may be required to take appropriate measures.

EN 55 024 statement

This is to certify that the Nortel Networks BayStack 460 and 470 switches are shielded against the susceptibility to radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of
EN 55 024 (CISPR 24).

EC Declaration of Conformity

This product conforms to the provisions of the R&TTE Directive 1999/5/EC.

VCCI statement (Japan/Nippon only)

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

　この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI statement for BayStack 460 and 470 (Taiwan only)

This is a Class A product based on the standard of the Bureau of Standards, Metrology and Inspection (BSMI) CNS 13438, Class A.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者 會被要求採取某些適當的對策。

MIC notice for BayStack 460 and 470 (Republic of Korea only)

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Ministry of Information and Communications (MIC). This device may not be sold for use in a non-business application.

Observe the Regulatory Marking label on the bottom surface of the chassis for specific certification information pertaining to this model. Each model in the BayStack Series which is approved for shipment to/usage in Korea is labeled as such, with all appropriate text and the appropriate MIC reference number.

National safety statements of compliance

CE marking statement (Europe only)

EN 60 950 statement

This is to certify that the Nortel Networks BayStack 460 and 470 switches are in compliance with the requirements of EN 60 950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance.

NOM statement BayStack 460 and 470 switches (Mexico only)

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Méxicana (NOM):

Exporter: Nortel Networks, Inc.
4655 Great America Parkway
Santa Clara CA 95054 USA

Importer: Nortel Networks de México, S.A. de C.V.
Avenida Insurgentes Sur #1605
Piso 30, Oficina
Col. San Jose Insurgentes
Deleg-Benito Juarez
México D.F. 03900

Tel: 52 5 480 2100

Fax: 52 5 480 2199

Input: BayStack 460, BayStack 470

100 - 120 VAC 16A 50 to 60 Hz

200 - 240 VAC 12 A 50 to 60 Hz

Información NOM (unicamente para México)

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Méxicana (NOM):

Exportador: Nortel Networks, Inc.
4655 Great America Parkway
Santa Clara, CA 95054 USA

Importador: Nortel Networks de México, S.A. de C.V.
Avenida Insurgentes Sur #1605
Piso 30, Oficina
Col. San Jose Insurgentes
Deleg-Benito Juarez
México D.F. 03900

Tel: 52 5 480 2100

Fax: 52 5 480 2199

Embarcar a: BayStack 460, BayStack 470

100 - 120 VAC 16A 50 to 60 Hz

200 - 240 VAC 12 A 50 to 60 Hz

Nortel Networks Inc. 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 MERCHANTABLITITY 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 forgoing 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**
   a. 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-Odd entities) and 48 C.F.R. 227.7202 (for Odd entities).

b. 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.

c. 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.

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

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. 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.

Revision History

Date Revised	Version	Reason for revision
July 2004	1.00	Incorporated new features for BoSS 3.5

Contents

Chapter 3

Chapter 4

Chapter 6
Virtual Local Area Networks 257

Chapter 7

Chapter 8

Chapter 9

Figures

Tables

Preface

The Nortel Networks* Command Line Interface (CLI) is one tool used to configure and manage BayStack switches. The CLI allows you to set up, configure, and manage your switch.

You can manage the switch with a number of tools. You can use either graphical user interface (GUI), the Java* Device Manager (DM) or the Web-based management system. You can use the console interface (CI menus), or you can use the command line interface (CLI).

For more information on using the DM, refer to *Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

For more information on using the Web-based management system, refer to *Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

For more information on using the CI menus and general information on using and configuring the switch, refer to *NNCLI Configuration Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

About this guide

This guide provides information about using the features and capabilities of the CLI to manage switching operations, as well as a complete list of CLI commands.

Network management tools and interfaces

- Console interface

The console interface (CI) allows you to configure and manage the switch locally or remotely. Access the CI menu and screens locally through a console terminal attached to your BayStack 470-24T, remotely through a dial-up modem connection, or in-band through a Telnet session.

- Web-based management

  You can manage the network from the World Wide Web and can access the Web-based Graphical User Interface (GUI) through the HTML-based browser located on your network. The GUI allows you to configure, monitor, and maintain your network through Web browsers. You can also download software using the Web. For information about Web-based management, see *Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

- Java-based Device Manager

  The Device Manager is set of Java-based graphical network management applications that is used to configure and manage BayStack 470-24T. For more information on the Device Manager, see *Reference for the Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

- Command Line Interface (CLI)

  The CLI is used to automate general management and configuration of the BayStack 470-48T. Use the CLI through a Telnet connection or through the serial port on the console. For more information on the CLI commands, see *NNCLI Configuration Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

- Any generic SNMP-based network management software.

  You can use any generic SNMP-based network management software to configure and manage a BayStack 470-24T.

- Telnet

  Telnet allows you to access the CLI and CI menu and screens locally using an in-band Telnet session.

- Nortel Networks Preside* Network Configuration System

  Allows you to configure the BayStack switches with a single system.

Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, bridging, and IP
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies

Before using this guide, you must complete the procedures discussed in the *BayStack 470-24T Switch Installation Instructions.*

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
`ip default-gateway <XXX.XXX.XXX.XXX>`,
you enter
`ip default-gateway 192.32.10.12`

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:

`http-server {enable|disable}`
the options for are `enable` or `disable`.

brackets ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.

Example: If the command syntax is:

`show ip [bootp]`,
you can enter either:

`show ip` or `show ip bootp`.

`plain Courier text`

Indicates command syntax and system output.

Example:

```
TFTP Server IP Address:  192.168.100.15
```

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:

`cli password <serial|telnet>`,
you must enter either `cli password serial` or `cli password telnet`, but not both.

H.H.H.

Enter a MAC address in this format (XXXX.XXXX.XXXX).

Related publications

For more information about managing or using the switches, refer to the following publications:

- *Release Notes for the BayStack 460-24T-PWR Switch* (part number 213297-A)
- *Release Notes for the BayStack 470-24T 10/100/1000 Switch Software Version 3.0* (part number 212864-C)
- *BayStack 460-24T-PWR Switch Installation Instructions* (part number 213318-A)
- *Installing the BayStack 470-24T 10/100/1000 Switch* (part number 212794-A)
- *Using the BayStack 460-24T-PWR Switch* (part number 213293-A)
- Using the BayStack 470-24T 10/100/1000 Switch Software Version 3.0 (part number 212791-C)
- Getting Started with the BayStack 470-24T 10/100/1000 Switch Management Software Operations (part number 213909-A)
- *Reference for the BayStack-460-24T-PWR Switch Management Software* (part number 213295-A)
- *Reference for the BayStack 470-24T 10/100/1000 Switch Management Software Version 3.0* (part number 212789-C)
- *Using Web-based Management for the BayStack 460-24T-PWR Switch* (part number 213294-A)
- *Using Web-based Management for the BayStack 470-24T 10/100/1000 Switch Software Version 3.0* (part number 212792-C)
- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (part number 312865-B)

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. (The product family for the BayStack 470-24T is Data and Internet.) Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

Obtaining technical assistance

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

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www130.nortelnetworks.com/cgi-bin/eserv/common/essContactUs.jsp URL.

Chapter 1 CLI basics

You can manage the switch with a number of tools. You can use either graphical user interface (GUI), the Java Device Manager (DM) or the Web-based management system. You can use the console interface (CI menus), or you can use the command line interface (CLI).

For more information on using the DM, refer to *Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

For more information on using the Web-based management system, refer to *Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

For more information on using the CI menus, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

The command line interface (CLI) is a management tool that provides methods for configuring, managing, and monitoring the operational functions of the switch. You access the CLI through a direct connection to the switch console port, or remotely using Telnet. For a complete, alphabetical list of CLI commands, refer to Appendix A, “Command List.

This chapter discusses the following CLI topics:

- “Accessing the CLI ”, next
- “CLI command modes” on page 45
- “CLI help” on page 49
- “Basic navigation” on page 49
- “Numbering ports” on page 55
- “How to comment and run scripts” on page 59
- “Managing basic system information” on page 59

- "Stacking compatibility" on page 62
- "MDA compatibility" on page 63

Accessing the CLI

You access the CI menus using Telnet or a direct connection to the switch from a terminal or personal computer (PC). You can use any terminal or PC with a terminal emulator as the CLI command station. Be sure the terminal has the following features:

- 9600 bits per second (b/s), 8 data bits, 1 stop bit, no parity, no flow control
- Serial terminal-emulation program such as Terminal or Hyperterm for Windows NT* or Hyperterm for Windows* 95 or Windows 98
- Cable and connector to match the male DTE connector (DB-9) on the switch console port, with the DCE/DTE switch on the switch management module set to DTE
- VT100 Arrows checked in the Terminal Preferences window under Terminal Options, and Block Cursor unchecked; VT-100/ANSI checked under Emulation

To access the CLI:

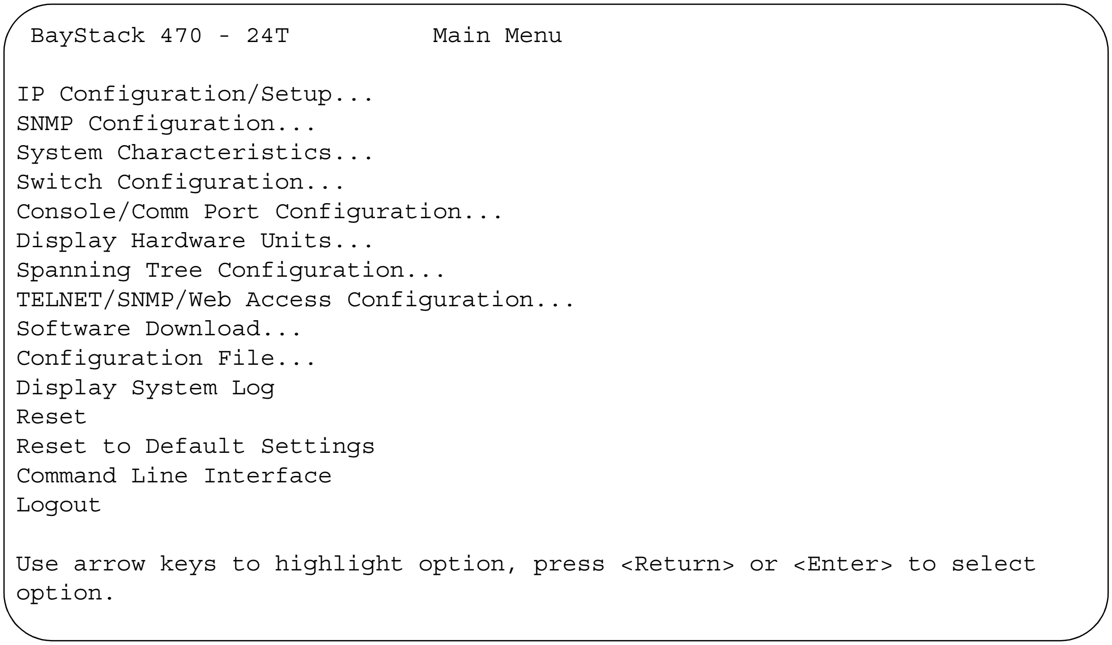
1 When you access the switch, the following banner appears (Figure 1).

Table 1 BayStack switch banner

```
********************************************************
* Nortel Networks
* Copyright (c) 1996,2000,2001, 2002
* All Rights Reserved
* BayStack 470-24T 10/100/1000 Switch
* Ver: HW:Rev 1    FW:3.0.0.5    SW:v3.0.0.28
************************************************************
***
Enter Ctrl-Y to begin.
```

2 Press [Ctrl]+Y, and the Main Menu appears on the console screen (Figure 1) with the top line highlighted.

Figure 1 Main Menu for Switch console interface



```
 BayStack 470 - 24T          Main Menu

IP Configuration/Setup...
SNMP Configuration...
System Characteristics...
Switch Configuration...
Console/Comm Port Configuration...
Display Hardware Units...
Spanning Tree Configuration...
TELNET/SNMP/Web Access Configuration...
Software Download...
Configuration File...
Display System Log
Reset
Reset to Default Settings
Command Line Interface
Logout

Use arrow keys to highlight option, press <Return> or <Enter> to select
option.
```

3 Using the Down Arrow key, scroll down to Command Line Interface, and press [Enter]. The CLI cursor appears as one of the following depending on your switch product number:

```
460-24T-PWR>
BS470>
```

The `>` sign at the end of the name of the switch indicates that the CLI opens in User EXEC mode. Refer to "CLI command modes ", next, to select the command mode you want to use (and are authorized to use).

CLI command modes

Most CLI commands are available only under a certain command mode. The switch has the following four command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration

The User EXEC mode is the default mode; it is also referred to as exec. This command mode is the initial mode of access upon first powering-up the switch. In this command mode, the user can access only a subset of the total CLI commands; however, the commands in this mode are available while the user is in any of the other four modes. The commands in this mode are those you would generally need, such as ping and logout.

Commands in the Privileged EXEC mode are available to all other modes except the User EXEC mode. The commands in this mode allow you to perform basic switch-level management tasks, such as downloading the software image, setting passwords, and booting the switch. The Privileged EXEC mode is also referred to as privExec mode.

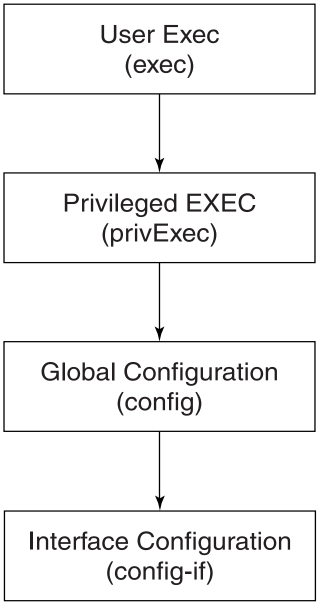
The last two command modes allow you to change the configuration of the switch. Changes made in these command modes are immediately applied to the switch configuration and saved to non-volatile memory (NVRAM).

The Global Configuration commands allow you to set and display general configurations for the switch, such as the IP address, SNMP parameters, Telnet access, and VLANs. The Global Configuration mode is also referred to as config mode.

The Interface Configuration commands allow you to configure parameters for each port, such as speed, duplex mode, and rate-limiting. The Interface Configuration mode is also referred to as config-if mode.

Figure 2 provides an illustration of the hierarchy of CLI command modes.

Figure 2 CLI command mode hierarchy



You can see a specific value for each command mode at the prompt line, and you can use specific commands to enter or exit each command mode (Table 2). Additionally, you can only enter command modes from specific modes and only exit to specific command modes.

Table 2 Command mode prompts and entrance/exit commands

Command mode	**Prompt**	**Enter/exit command**

User EXEC
(exec)
	`460-24T-PWR>`
	`BS470>`
		• Default mode, automatically enter
		• `logout` or `exit` to quit CLI

Privileged EXEC
(privExec)
	`460-24T-PWR#`
	`BS470#`
		• `enable` to enter from User EXEC mode
		• `logout` or `exit` to quit CLI

Table 2 Command mode prompts and entrance/exit commands (Continued)

Command mode	Prompt	Enter/exit command

Global Configuration (config)	`460-24T-PWR(config)#`
	`BS470(config)#`
		• `configure` to enter from Privileged EXEC mode
		• `logout` to quit CLI; `end` or `exit` to exit to Privileged EXEC mode

Interface Configuration (config-if)	`460-24T-PWR(config-if)#`
	`BS470(config-if)#`
		• `interface FastEthernet {<portnum>|all}` to enter from Global Configuration mode
		• `logout` to quit CLI; `end` to exit to Privileged EXEC mode; `exit` to exit to Global Configuration mode

The prompt displays the switch name, `460-24T-PWR,` or `BS470-24T` and the current CLI command mode:

- User EXEC— `460-24T-PWR>,` or `BS470>`
- Privileged EXEC— `460-24T-PWR#,` or `BS470#`
- Global Configuration— `460-24T-PWR(config)#,` or `BS470(config)#`
- Interface Configuration— `460-24T-PWR(config-if)#,` or `BS470(config-if)#`

See Appendix A, “Command List”, for a complete, alphabetical list of all CLI commands and where they are explained.

The initial command mode in CLI depends on your access level when you log into the switch CI menus:

- With no password protection, you enter the CLI in userExec mode, and use the `enable` command to move to the privExec command mode.
- If you log into the CI menus with read-only access, you enter the CLI in userExec mode and cannot access any other CLI command modes.
- If you log into the CI menus with read-write access, you enter the CLI in privExec mode and use the commands to move to the other command modes.

CLI help

When you navigate through the CLI, online help is available at all levels. Entering a portion of the command, space, and a question mark (**?**) at the prompt results in a list of all options for that command.

Refer to "help command" on page 51 for more information about the specific types of online help.

Basic navigation

This section discusses basic navigation around the CLI and between the command modes. As you see, the CLI incorporates various shortcut commands and keystrokes to simplify its use. The following topics are covered in this section:

- "General navigation commands ", next
- "Keystroke navigation" on page 50
- "help command" on page 51
- "no command" on page 52
- "default command" on page 52
- "logout command" on page 53
- "enable command" on page 53
- "configure command" on page 53
- "interface command" on page 54
- "disable command" on page 54
- "end command" on page 55
- "exit command" on page 55

General navigation commands

When you enter**?** at any point in the CLI session, the system retrieves help information for whatever portion of the command you entered thus far. Refer to "help command" on page 51 for more information.

The system records the last command in a CLI session. However, the last command is not saved across reboots.

Add the word `no` to the beginning of most CLI configuration commands to clear or remove the parameters of the actual command. For example, when you enter the command `ip stack address 192.32.154.126`, you set the IP stack address. However, when you enter `no ip stack address`, the system returns the IP address to zero. See Appendix A, "Command List" for an alphabetical list of `no` commands.

Add the word `default` to the beginning of most CLI configuration commands returns the parameters of the actual command to the factory default values. Refer to Appendix A, "Command List" for an alphabetical list of `default` commands.

When you enter a portion of the command and the [Tab] key, the system finds the first unambiguous match of a command and displays that command. For example, if you enter `down`+[Tab], the system displays `download`.

Keystroke navigation

You can change the location of the cursor using the key combinations shown in Table 3.

Table 3 Keystroke navigation

Key combination	Function
[Ctrl]+A	Start of line
[Ctrl]+B	Back 1 character
[Ctrl]+C	Abort command
[Ctrl]+D	Delete the character indicated by the cursor
[Ctrl]+E	End of line
[Ctrl]+F	Forward 1 character
[Ctrl]+H	Delete character left of cursor (Backspace key)
[Ctrl]+I &	Command/parameter completion
[Ctrl]+K & [Ctrl]+R	Redisplay line
[Ctrl]+N or [Down arrow]	Next history command
[Ctrl]+P or [Up arrow]	Previous history command

Table 3 Keystroke navigation

Key combination	**Function**
[Ctrl]+T	Transpose characters
[Ctrl]+U	Delete entire line
[Ctrl]+W	Delete word left of cursor
[Ctrl]+X	Delete all characters to left of cursor
[Ctrl]+z	Exit Global Configuration mode (to Privileged EXEC mode)
?	Context-sensitive help
[Esc]+c & [Esc]+u	Capitalize character at cursor
[Esc]+l	Change character at cursor to lowercase
[Esc]+b	Move back 1 word
[Esc]+d	Delete 1 word to the right
[Esc]+f	Move 1 word forward

help command

The help command is in all command modes and displays a brief message about using the CLI help system. The syntax for the help command is:

```
help
```

The help command has no parameters or variables.

Figure 3 shows the output from the help command.

Figure 3 `help` command output in privExec mode

```
BS470#help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command
argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is
entered and you want to know what arguments match the input (e.g.
'show pr?'.)
```

no command

The `no` command is always used as a prefix to a configuration command, and it negates the action performed by that command. The effect of the `no` command is to remove or to clear the configuration controlled by the specified command. Various `no` commands are in the config and config-if command modes.

Refer to Appendix A, "Command List" for an alphabetical listing of all `no` commands.

Note: Not all configuration commands support the `no` prefix command.

default command

The `default` command is always used as a prefix to a configuration command, and it restores the configuration parameters to default values. The default values are specified by each command.

Refer to Appendix A, "Command List" for an alphabetical listing of all `default` commands.

Note: Not all commands support the `default` prefix command.

logout command

The `logout` command logs you out of the CLI session and returns you to the Main Menu of the console interface (CI) menus (Figure 1). The syntax for the `logout` command is:

```
logout
```

The `logout` command is in all command modes.

The `logout` command has no parameters or variables.

enable command

The `enable` command changes the command mode from User EXEC to privExec mode. The syntax for the `enable` command is:

```
enable
```

The `enable` command is in the exec command mode.

The `enable` command has no parameters or variables.

Note: You must have read-write access to the switch to use the `enable` command.

configure command

The `configure` command moves you to the Global Configuration (config) command mode and identifies the source for the configuration commands. The syntax for the `configure` command is:

```
configure {terminal|network|memory}
```

The `configure` command is in the privExec command mode.

Table 4 describes the parameters and variables for the `configure` command.

Table 4 `configure` command parameters and variables

Parameters and variables	Description

`terminal|`
`network|`
`memory`
	Specifies the source for the configuration commands for the switch:
	• `terminal`—allows you to enter config mode to enter configuration commands
	• `network`—allows you to set up parameters for auto-loading a script at boot-up or for loading and executing a script immediately
	• `memory`—not supported on the switch

interface command

The `interface` command moves you to the Interface Configuration (config-if) command mode. The syntax for the `interface` command is:

```
interface FastEthernet {<portlist>}
```

The `interface` command is in the config command mode.

Table 5 describes the parameters and variables for the `interface` command.

Table 5 interface command parameters and variables

Parameters and variables	Description
<portlist>	Specifies the portlist you want to be affected by all the commands issued in the config-if command mode.

disable command

The `disable` command returns you to the User EXEC (exec) command mode. The syntax for the `disable` command is:

```
disable
```

The `disable` command is in the privExec command mode.

The `disable` command has no parameters or variables.

end command

The `end` command moves you to the priv Exec mode from either the Global Configuration (config) mode or the Interface Configuration (config-if) mode.

The syntax for the `end` command is:

```
end
```

The `end` command has no parameters or variables.

exit command

The `exit` command moves you around the command modes:

- In User EXEC (exec) and Privileged EXEC (privExec) command modes, `exit` allows you to quit the CLI session.
- In Global Configuration (config) mode, `exit` moves you back to the privExec command mode.
- In Interface Configuration (config-if) command mode, `exit` moves you back to the config mode.

The syntax for the `exit` command is:

```
exit
```

The `exit` command has no parameters or variables.

Numbering ports

The BayStack 470-24T operates in standalone mode. The BayStack 470-24T has 24 10/100 Mb/s ports on the front. Thus, you have a maximum of 26 ports on one BayStack 470-24T.

The BayStack 470-48T operates in standalone mode. The BayStack 470-48T has 48 10/100 Mb/s ports on the front. Thus, you have a maximum of 48 ports on one BayStack 470-48T.

The BayStack 460-24T-PWR can operate either in standalone mode or in stack mode. The BayStack 460-24T-PWR have 24 10/100 Mb/s ports on the front, as well as an uplink slot that allows you to attach a media dependent adapter (MDA). The MDAs available for the uplink can have up to 4 ports. Thus, you have a maximum of 28 ports on one BayStack 460-24T-PWR switch.

Note: The MDA do not supply power to PoE (Power Over Ethernet) devices. Only unit ports, 1-24 can supply power to PoE devices.

In stack mode, the BayStack 460-24T-PWR operate either in Pure Stack mode or in Hybrid Stack mode. The Hybrid Stack mode is when you are working with a combination of other BayStack switches in one stack.

Note: The Hybrid stack mode is not supported in this release of the BayStack 460-24T-PWR switch, the BayStack 470-24T switch, or the BayStack 470-48T switch.

When you are working with a standalone BayStack 460-24T-PWR switch, ensure that the operational mode is set for Pure Stack. (Refer to "show stack-oper-mode command" on page 73 and "stack oper-mode command" on page 73 for information on operational mode commands.)

Note: The variable `portlist` replaces the use of variables *`portnum`*, *`port-num,`* and `all` for ports.

The CLI uses the variable *`<portlist>`* when a command specifies one or more ports for the command. The format of the variable *`<portlist>`* is different if you are working with a standalone switch or with a stack (either Pure Stack or Hybrid Stack).

Numbering port in standalone mode

When you are working with a standalone BayStack 460-24T-PWR switch, ensure that the operational mode is set for the Pure Stack mode.

In standalone mode, use the *`<portlist>`* variable in the following formats:

- A single port number—an integer between 1 through 26
  - Example: `7` means port 7
- A range of port numbers—a pair of port numbers between 1 and 26 separated by a dash
  - Example: `1-3` means ports 1, 2, and 3
  - Example: `5-24` means all ports from port 5 through port 24
- A list of port numbers and/or port ranges, separated by commas
  - Example: `1,3,7` means ports 1, 3, and 7
  - Example: `1-3,9-11` means ports 1, 2, 3, 9, 10, and 11
  - Example: `1,3-5,9-11,15` means ports 1, 3, 4, 5, 9, 10, 11, and 15
- `none` means no ports (not case-sensitive)
- `all` means all the ports on the standalone switch, including any MDA ports (not case-sensitive)

You can also use the unit/port convention discussed in "Numbering port in stacked mode ", next, with a standalone BayStack 460-24T-PWR switch as long as the unit number is always 1.

Numbering port in stacked mode

In stacked mode, either Pure Stack mode or Hybrid Stack Mode, use the *`<portlist>`* variable to represent the number of the unit within the stack, followed by a forward slash (/), followed by port number(s). The unit numbers are always integers between 1 and 8, and the port numbers are always integers between 1 and 26. You can also use `none` to indicate none of the ports in the stack or `all` to indicate all of the ports in the stack.

Note: The Hybrid stack mode is not supported in this release of the BayStack 460-24T-PWR switch.

In stacked mode, use the `<portlist>` variable in the following formats:

- A single port number—an integer for the unit, followed by /, and an integer for the port number
  - — Example: `1/7` means unit 1 port 7
  - — Example: `3/24` means unit 3, port 24
- A range of port numbers—an integer for the unit, followed by /, and integers for the port number between 1 and 26 separated by a dash
  - — Example: `1/1-3` means unit 1, ports 1, 2, and 3
  - — Example: `3/5-26` means unit 3, port 5 through port 26
- A unit with no ports specified—an integer for the unit, followed by /, and the word `none` (not case-sensitive)
  - — `3/none` means unit 3 with no ports
- A unit with all ports specified—an integer for the unit, followed by /, and the word `all` (not case-sensitive)
  - — `3/all` means unit 3 with all ports
- A list of port numbers, port ranges, and/or units with all ports or no ports—using the unit/port format—separated by commas
  - — Example: `1/1,2/3,3/7` means unit 1 port 1; unit 2, port 3; and unit 3, port 7
  - — Example: `1/1-3,3/9-11` means unit 1, ports 1, 2, 3; and unit 3, ports 9, 10, and 11
  - — Example: `1/1,4/3-5,5/9-11,7/15` means unit 1, port 1; unit 4, ports 3, 4, 5; unit 5, ports 9, 10, 11; and unit 7, port 15
  - — Example: `1/3,3/ALL,4/NONE` means unit 1, port 3; unit 3, all ports; and unit 4, no ports
- `none` means no ports in the stack (not case-sensitive)
- `all` means all the ports in the stack, including all MDA ports (not case-sensitive)

To view the unit numbers in the stack, enter the `show stack-info` command (see "show stack-info command" on page 74). You must be in the Privileged EXEC (privExec) mode to enter this command.

Refer to *Using the Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches* guide, for more information on numbering units within the stack.

How to comment and run scripts

You can use the CLI interactively, or you can load and execute CLI “scripts.” CLI scripts are loaded in one of the following ways:

- By entering the `configure network` command.
- By manually loading the script in the console menu.
- By automatically loading the script at boot-up

Managing basic system information

This section shows you how to view basic system information, such as the current software version and the stack mode; you can renumber the units within a stack. The following topic is covered:

- “show sys-info command ”, next
- “show stack-info command” on page 61

Refer to *Using the Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*, for more information on the operation of the stack mode, including unit numbering.

show sys-info command

The `show sys-info` command displays the current system characteristics, which includes HW rev, FW rev, date of manufacture (DOM), and Hardware deviation number. The syntax for the `show sys-info` command is:

```
show sys-info
```

The `show sys-info` command is in the privExec command mode.

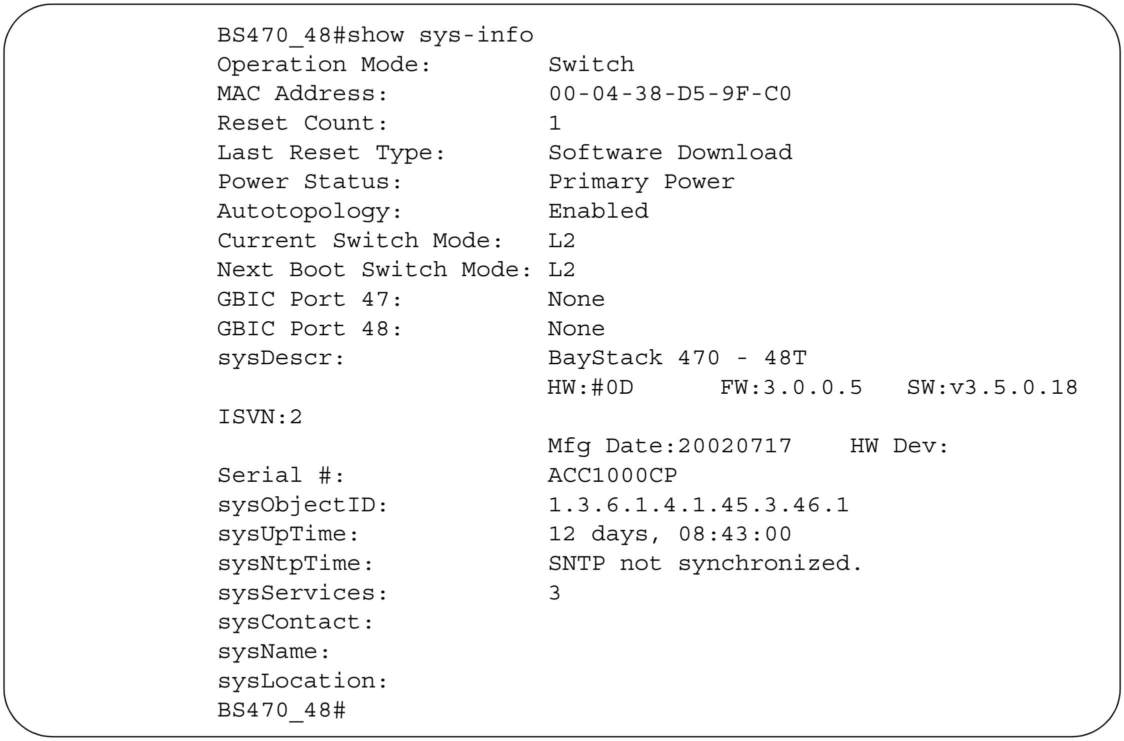
The `show sys-info` command has no parameters or variables.

Figure 4 and Figure 5 displays sample output from the `show sys-info` command.

Figure 4 `show sys-info` command output

```
BS460_24T_PWR#show sys-info
Operation Mode:        Switch
MAC Address:           00-09-97-29-1F-00
Reset Count:           1
Last Reset Type:       Software Download
Power Status:          Primary Power
Autotopology:          Enabled
Current Switch Mode:   L2
Next Boot Switch Mode: L2
Local MDA Type:        None
PoE Module FW:         7013.2
sysDescr:              BayStack 460 - 24T - PWR
                       HW:00       FW:3.0.0.5   SW:v3.5.0.18
ISVN:2
                       Mfg Date:20021102    HW Dev:
Serial #:              SDNIHR007B
sysObjectID:           1.3.6.1.4.1.45.3.49.1
sysUpTime:             12 days, 07:04:49
sysNtpTime:            SNTP not synchronized.
sysServices:           3
sysContact:
sysName:
sysLocation:
BS460_24T_PWR#show sys-info
```

Figure 5 `show sys-info` command output



```
BS470_48#show sys-info
Operation Mode:        Switch
MAC Address:           00-04-38-D5-9F-C0
Reset Count:           1
Last Reset Type:       Software Download
Power Status:          Primary Power
Autotopology:          Enabled
Current Switch Mode:   L2
Next Boot Switch Mode: L2
GBIC Port 47:          None
GBIC Port 48:          None
sysDescr:              BayStack 470 - 48T
                       HW:#0D      FW:3.0.0.5   SW:v3.5.0.18
ISVN:2
                       Mfg Date:20020717    HW Dev:
Serial #:              ACC1000CP
sysObjectID:           1.3.6.1.4.1.45.3.46.1
sysUpTime:             12 days, 08:43:00
sysNtpTime:            SNTP not synchronized.
sysServices:           3
sysContact:
sysName:
sysLocation:
BS470_48#
```

To change the system contact, name, or location, refer to the `snmp-server` command.

show stack-info command

The `show stack-info` command displays the current stack information, which includes unit numbers, MDA and cascade attachments, and software version for all units. The syntax for the `show stack-info` command is:

```
show stack-info
```

The `show stack-info` command is in the privExec command mode.

The `show stack-info` command has no parameters or variables.

Figure 6 displays sample output from the `show stack-info` command.

Figure 6 `show stack-info` command output

```
460-24T-PWR#show stack-info
Unit #  Switch Model      MDA Model    Cascade MDA  SW Version
------  ----------------  -----------  ----------- ------------
1       460-24T-PWR       None         400-ST1      v2.3.0.05
2       460-24T-PWR       None         400-ST1      v2.3.0.05
```

Stacking compatibility

You can stack the switch up to 8 units high. There are two types of stacks:

- Pure switch—This stack has *only* one model switch. It is sometimes referred to as a pure stack. The stack operational mode for this type of stack is Pure 460 Mode.
- Hybrid—This stack has a combination of BayStack switches. It is sometimes referred to as a mixed stack. The stack operational mode for this type of stack is Hybrid Mode.

Note: The Hybrid stack mode is not supported in this release of the software. You can only stack the same model switches in this release.

When you work with the switch in standalone mode, ensure that the stack operational mode shows Pure Mode, and does not show Hybrid Mode.

All BayStack 460-24T-PWR switches in the stack must be running the identical version of software.

When you are working with a mixed stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for all switches must be the same. If the ISVNs are not the same, the stack does not operate.

In summary, the stacking software compatibility requirements are as follows:

- Pure switch stack—All units must be running the same software version.
- Pure BayStack 450 stack—All units must be running the same software version.
- Hybrid stack:
  - All Baystack units must be running the same software version.
  - All software versions must have the identical ISVN.

Note: The Hybrid stack mode is not supported in this release of the BayStack 460-24T-PWR switch, the BayStack 470-24T switch, or the BayStack 470-48T switch.

MDA compatibility

Note: The MDA do not supply power to PoE (Power Over Ethernet) devices. Only unit ports, 1-24 can supply power to PoE devices.

The switch provides support for many Nortel Networks MDAs that use a variety of media, including Gigabit Interface Converters (GBICs) and CWDM.

Refer to *Installing Media Dependent Adapters (MDA)s* and *Installing Gigabit Interface Converters, SFPs, and CWDM SFP Gigabit Interface Converters* for more information on installation, technical specifications, connectors, and cabling for the GBIC MDAs. Contact your Nortel Networks representative for a complete listing of compatible MDAs.

Chapter 2
System configuration

In the switch, the Command Line Interface (CLI) commands allow you to display and modify the switch configuration while the switch is operating.

This chapter includes information about the system configuration, such as Configuring the switch IP address, downloading and uploading your software, and customizing your system. This chapter covers the following topics:

- "Configuring the switch IP address, subnet mask and default gateway ", next
- "Pinging the switch" on page 75
- "Using DNS to ping and telnet" on page 76
- "Configuring the switch with a BootP/Dynamic IP Configuration" on page 80
- "IP/BootP configuration retention on downgrade" on page 81
- "Configuration Management" on page 81
- "Downloading and uploading your software" on page 90
- "Customizing your system" on page 95
- "Displaying the ARP table" on page 127
- "Displaying interfaces" on page 128
- "Displaying unit uptime" on page 130
- "Displaying port statistics" on page 131
- "Enabling and disabling autosave" on page 134
- "Setting time on network elements using Simple Network Time Protocol (SNTP)" on page 136
- "Enabling remote login" on page 142
- "Enabling traffic separation" on page 147
- "Saving the configuration to NVRAM" on page 149
- "Trap notification when configuration changes are saved to NVRAM" on page 149

- "Replacing a unit" on page 150

Configuring the switch IP address, subnet mask and default gateway

IP notation

You enter IP addresses and subnet masks in one of the following two ways in the CLI. You can always enter an IP address in dotted decimal notation (XXX.XXX.XXX.XXX), specifying both the IP address and the subnet mask in dotted-decimal notation.

Assigning and clearing IP addresses

Using the CLI, you can assign IP addresses and gateway addresses, clear these addresses, and view configured IP addresses. This section covers these topics:

- "ip address command ", next
- "no ip address command" on page 67
- "ip default-gateway command" on page 68
- "no ip default-gateway command" on page 68
- "show ip command" on page 69

ip address command

The `ip address` command sets the IP address and subnet mask for the switch or a stack. The syntax for the `ip address` command is:

```
ip address [switch|stack|unit] <XXX.XXX.XXX.XXX> [netmask
<XXX.XXX.XXX.XXX>]
```

The `ip address` command is in the config command mode.

If you do not enter either the stack or switch parameter, the system automatically modifies the stack IP address when in stack mode and modifies the switch IP address when in standalone mode.

Table 6 describes the parameters and variables for the `ip address` command.

Table 6 ip address command parameters and variables

Parameters and variables	Description
`switch|stack|unit`	Sets the switch, stack, or other unit IP address and netmask.
`XXX.XXX.XXX.XXX`	Enter IP address in dotted decimal notation; netmask is optional.
`netmask`	Sets the IP subnet mask for the switch or stack.

Note: When you change the IP address or subnet mask, you may lose connection to Telnet and the Web.

no ip address command

The `no ip address` command clears the IP address and subnet mask. This command sets the IP address and subnet mask for a switch to all zeros (0). The syntax for the `no ip address` command is:

```
no ip address {switch|stack|unit}
```

The `no ip address` command is in the config command mode.

Table 7 describes the parameters and variables for the `no ip address` command.

Table 7 `no` ip address command parameters and variables

Parameters and variables	Description
`switch|stack|unit`	Zeros out the IP address and subnet mask for the switch, stack, or other unit in the stack.

Note: When you change the IP address or subnet mask, you may lose connection to Telnet and the Web. You also disable any new Telnet connection, and you must connect to the serial console port to configure a new IP address.

ip default-gateway command

The `ip default-gateway` command sets the IP default gateway address for a switch or a stack to use. The syntax for the `ip default-gateway` command is:

```
ip default-gateway <XXX.XXX.XXX.XXX>
```

The `ip default-gateway` command is in the config command mode.

Table 8 describes the parameters and variables for the `ip default-gateway` command.

Table 8 ip default-gateway command parameters and variables

Parameters and variables	**Description**
XXX.XXX.XXX.XXX	Enter the dotted-decimal IP address of the default IP gateway.

Note: When you change the IP gateway, you may lose connection to Telnet and the Web.

no ip default-gateway command

The `no ip default-gateway` command sets the IP default gateway address to zeros (0). The syntax for the `no ip default-gateway` command is:

```
no ip default-gateway
```

The `no ip default-gateway` command is in the config command mode.

The `no ip default-gateway` command has no parameters or variables.

Note: When you change the IP gateway address, you may lose connection to Telnet and the Web. You also may disable any new Telnet connection be required to connect to the serial console port to configure a new IP gateway address.

show ip command

The `show ip` command displays the IP configurations, specifically BootP mode, stack address, switch address, subnet mask, and gateway address. This command displays the parameters for what is configured, what is in use, and the last BootP. The syntax for the `show ip` command is:

```
show ip [bootp] [default-gateway] [address [switch|stack]]
```

The `show ip` command is in the exec command mode. If you do not enter any parameters, this command displays all the IP-related configuration information.

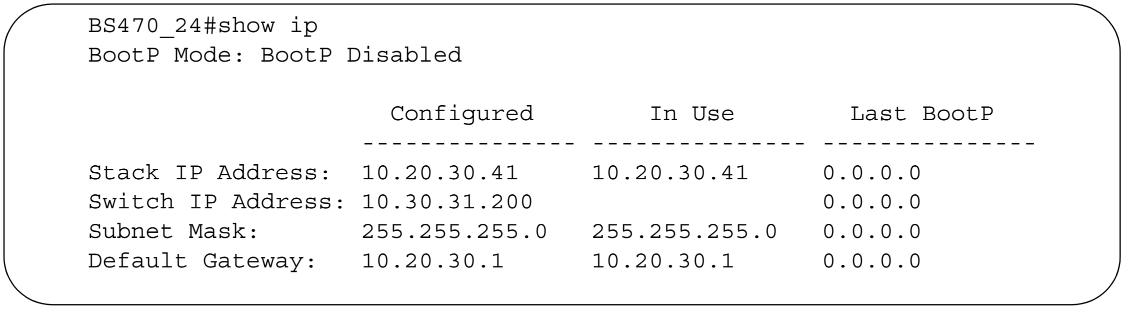
Table 9 describes the parameters and variables for the `show ip` command.

Table 9 `show ip` command parameters and variables

Parameters and variables	Description
`bootp`	Displays BootP-related IP information.
`default-gateway`	Displays the IP address of the default gateway.
`address`	Displays the current IP address.
`switch|stack`	Specifies current IP address of the switch or stack.

Figure 7 displays a sample output of the `show ip` command.

Figure 7 `show ip` command output



```
BS470_24#show ip
BootP Mode: BootP Disabled

                   Configured        In Use         Last BootP
                  --------------- --------------- ---------------
Stack IP Address: 10.20.30.41     10.20.30.41     0.0.0.0
Switch IP Address: 10.30.31.200                   0.0.0.0
Subnet Mask:      255.255.255.0   255.255.255.0   0.0.0.0
Default Gateway:  10.20.30.1      10.20.30.1      0.0.0.0
```

Assigning and clearing IP addresses for specific units

You can assign IP addresses for a specific units within a stack. This section covers these topics:

- "ip address unit command ", next
- "no ip address unit command" on page 71
- "default ip address unit command" on page 72

ip address unit command

The `ip address unit` command sets the IP address and subnet mask for a specific standalone unit or a specific unit in a stack. The syntax for the `ip address unit` command is:

```
ip address unit <1-8> A.B.C.D
```

The `ip address unit` command is in the config command mode.

Table 10 describes the parameters and variables for the `ip address unit` command.

Table 10 ip address `unit` command parameters and variables

Parameters and variables	Description
<1-8>	Sets the unit you are assigning an IP address.
A.B.C.D	Enter IP address in dotted decimal notation.

Note: When you change the IP address or subnet mask, you may lose connection to Telnet and the Web.

no ip address unit command

The `no ip address unit` command sets the IP address for the specified unit to all zeros (0). The syntax for the `no ip address unit` command is:

```
no ip address unit <1-8>
```

The `no ip address unit` command is in the config command mode.

Table 11 describes the parameters and variables for the `no ip address unit` command.

Table 11 no ip address `unit` command parameters and variables

Parameters and variables	Description
<1-8>	Zeros out the IP address for the specified unit.

Note: When you change the IP address or subnet mask, you may lose connection to Telnet and the Web. You also disable any new Telnet connection, and you must connect to the serial console port to configure a new IP address.

default ip address unit command

The `default ip address unit` command sets the IP address for the specified unit to all zeros (0). The syntax for the `default ip address unit` command is:

```
default ip address unit <1-8>
```

The `default ip address unit` command is in the config command mode.

Table 12 describes the parameters and variables for the `default ip address unit` command.

Table 12 default ip address `unit` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Zeros out the IP address for the specified unit.

Note: When you change the IP gateway, you may lose connection to Telnet and the Web.

Configuring the stack operational mode

This section shows you how to view and set the stack operational mode. The following topics are covered:

- "show stack-oper-mode command ", next
- "stack oper-mode command" on page 73
- "show stack-info command" on page 74

Refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches* for more information on stack operation, including features that require specific operational modes and adding switches to the stack.

show stack-oper-mode command

The `show stack-oper-mode` command displays the current operational mode of the stack and the mode set for the next switch reboot. The display shows either:

- Pure BayStack 460-24T-PWR Stack, Pure BayStack 470-24T Stack, or Pure BayStack 470-48T Stack
- Hybrid Stack

Note: The Hybrid Stack mode is not supported in this release of the BayStack 470-24T

The syntax for the `show stack-oper-mode` command is:

```
show stack-oper-mode
```

The `show stack-oper-mode` command is in the privExec command mode.

The `show stack-oper-mode` command has no parameters or variables.

Figure 8 displays sample output from the `show stack-oper-mode` command.

Figure 8 `show stack-oper-mode` command output

```
BS470#show stack-oper-mode
Current Operational Mode: BS 470 Stack
Next Boot Operational Mode: BS 470 Stack
```

stack oper-mode command

The `stack oper-mode` command allows you to set the stack operational mode, which becomes active at the next reboot of the switch or stack. The syntax for the `stack oper-mode` command is:

```
stack oper-mode {BS470|hybrid}
```

The `stack oper-mode` command is in the config command mode.

Table 13 describes the parameters and variables for the `stack oper-mode` command.

Table 13 stack oper-mode command parameters and variables

Parameters and variables	Description
`BS470|hybrid`	Sets the stack operational mode for the next boot: • `BS470`—Pure BayStack 470-24T Stack mode. This means *only* BayStack 470-24T switches either standalone or in a stack. • `hybrid`—Hybrid Stack mode. This means a mixture of BayStack 470-24T or BayStack 470-48T and BayStack 460 switches in a stack.
`BS460|hybrid`	Sets the stack operational mode for the next boot: • `BS460`—Pure 460 Stack mode. This means *only* BayStack 460-24T-PWR switches either standalone or in a stack. • `hybrid`—Hybrid Stack mode. This means a mixture of BayStack 470-24T and BayStack 460 switches in a stack. Note: Hybrid Stack mode is not supported in this release of the BayStack 470-24T.

Note: You must reboot the system for the stack operation mode you entered in the CLI to take effect.

show stack-info command

The `show stack-info` command displays the current stack information, which includes unit numbers, cascade attachments, and software version for all units. The syntax for the `show stack-info` command is:

```
show stack-info
```

The `show stack-info` command is in the privExec command mode.

The `show stack-info` command has no parameters or variables.

Figure 9 displays sample output from the `show stack-info` command.

Figure 9 `show stack-info` command output

```
BS470#show stack-info
Unit #  Switch Model     GBIC Model Cascade GBIC SW Version
----------------------------------------------------------
1       BS 47000000000000 None       None        v3.0.0.00
```

Renumber unit command

The `renumber unit` command changes the unit number of each switch. The syntax for the `renumber unit` command is:

```
renumber unit
```

The `renumber unit` command is in the config command mode.

The `renumber unit` command has no parameters or variables.

Note: This command does not take effect until you reset the stack.

Pinging the switch

You can ping from a BayStack 470-24T. This ability greatly enhances the ease of network management. The ping command tests the network connection to another network device. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device. The local IP address must be set before issuing the ping command.

For more information on the CLI commands, see “ping command” on page 77.

Using DNS to ping and telnet

Using the DNS client, you can ping or telnet to a host server or to a host by name. To use this feature, you must configure at least one domain name server; you may also configure a default domain name. If you configure a default domain name, that name is appended to hostnames that do not contain a dot. The default domain name and addresses are saved in NVRAM.

The hostnames for ping and telnet cannot be longer than 63 alphanumeric characters, and the default DNS domain name cannot be longer than 255 characters. This section covers these commands:

- "show ip dns command ", next
- "ping command" on page 77
- "ip name-server command" on page 78
- "no ip name-server command" on page 79
- "ip domain-name command" on page 79
- "no ip domain-name command" on page 80
- "default ip domain-name command" on page 80

show ip dns command

The `show ip dns` command displays the DNS domain name, as well as any configured DNS servers. The syntax for the `show ip dns` command is:

```
show ip dns
```

The `show ip dns` command is in the exec command mode.

The `show ip dns` command has no parameters or variables.

Figure 10 displays sample output from the `show ip dns` command.

Figure 10 `show ip dns` command output

```
BS470-48#show ip dns
DNS Default Domain name: us.nortel.com
DNS Servers
- - - - - - -
47.82.2.10
0.0.0.0
0.0.0.0
BS470-48#
```

ping command

The `ping` command tests the network connection to another network device. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device. The local IP address must be set before issuing the `ping` command.

You can ping a host using either its IP address or hostname.

The syntax for the `ping` command is:

```
ping <A.B.C.D or Hostname>
```

The `ping` command is in the exec command mode.

Table 14 describes the parameters and variables for the `ping` command.

Table 14 ping command parameters and variables

Parameters and variables	**Description**
<A.B.C.D or Hostname>	Specify: • the IP address of the target device in dotted-decimal notation • the hostname of the device to ping (The hostname can be a simple name, such as fred; in this case the DNS domain name, if set, is appended. Or the hostname can be a full hostname, such as fred.ca.nortel.com.)

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.

Figure 11 displays sample `ping` responses.

Figure 11 `ping` command responses

```
BS470_48#ping 10.10.40.29
Host is reachable
```

There is no default value for this command.

ip name-server command

The `ip name-server` command adds one or more DNS servers’ IP addresses. The syntax for the `ip name-server` command is:

```
ip name-server <A.B.C.D>
```

The `ip name-server` command is in the config command mode.

Note: You can add up to 3 servers; adding one at a time.

Table 15 describes the parameters and variables for the `ip name-server` command.

Table 15 ip name-server command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of a DNS server.

The default value is 0.0.0.0.

no ip name-server command

The `no ip name-server` command removes one or more DNS servers' IP addresses. The syntax for the `no ip name-server` command is:

```
no ip name-server <A.B.C.D>
```

The `no ip name-server` command is in the config command mode.

Table 16 describes the parameters and variables for the `no ip name-server` command.

Table 16 no ip name-server command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of a DNS server.

The default value is 0.0.0.0.

ip domain-name command

The `ip domain-name` command sets the system's DNS domain name. The syntax for the `ip domain-name` command is:

```
ip domain-name [<LINE>]
```

The `ip domain-name` command is in the config command mode.

Table 17 describes the parameters and variables for the `ip domain-name` command.

Table 17 ip domain-name command parameters and variables

Parameters and variables	Description
<LINE>	Enter a DNS domain name.

The default value for this command is an empty string.

no ip domain-name command

The `no ip domain-name` command clears the system's DNS domain name (sets it to an empty string). The syntax for the `no ip domain-name` command is:

```
no ip domain-name
```

The `no ip domain-name` command is in the config command mode.

The `no ip domain-name` command has no parameters or variables.

default ip domain-name command

The `default ip domain-name` command clears the system's DNS domain name (set it to an empty string). The syntax for the `default ip domain-name` command is:

```
default ip domain-name
```

The `default ip domain-name` command is in the config command mode.

The `default ip domain-name` command has no parameters or variables.

Configuring the switch with a BootP/Dynamic IP Configuration

The BayStack 470-24T have a unique 48-bit hardware address, or MAC address, that is printed on a label on the back panel. Use this MAC address when you configure the network BootP server to recognize BootP requests from BayStack 470-24T. A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask and the IP address of the default router (default gateway).

IP/BootP configuration retention on downgrade

When downgrading a unit with BoSS Software for Policy Switches version 3.0.3 and later, the system will default all configuration, except for the following:

- Stack operation mode
- IP configuration
- BootP mode

Previous releases of Policy Switch software retained the Stack Operational Mode only on software downgrade. This change allows a remotely accessed switch to maintain its accessibility after downgrade and/or not require the user re-enter this basic information which should remained unchanged after a downgrade.

Configuration Management

The Configuration File Menu screen allows you to upload and download the configuration parameters of a BayStack 470-24T to a TFTP server. You can also download an ASCII configuration file from a TFTP server.

Binary upload and binary download

The Configuration File upload/download are of two types:

- Binary config file upload/download
- ASCII config file upload/download

These options allow you to store your switch configuration parameters on a TFTP server. You can retrieve the configuration parameters of a standalone switch and use the retrieved parameters to automatically configure a replacement switch. You must set up the file on your TFTP server and set the filename read/write permission to enabled before you can save the configuration parameters.

Automatically loading an ASCII configuration file

This section discusses how to download a configuration file when the system boots. You use standard CLI commands to modify the configuration file you want to download. This section covers these commands:

- "configure-network command ", next
- "show config-network command" on page 83

configure-network command

The `configure-network` command allows you to load and execute a script immediately and to configure parameters to automatically download a configuration file when you reboot the switch or stack. The syntax for the `configure-network` command is:

```
configure-network [load-on-boot
{disable|use-bootp|use-config}] [filename <WORD>] [address
<XXX.XXX.XXX.XXX>]
```

The `configure-network` command is in the exec mode.

Note: When you enter the `configure-network` command with no parameters, the system prompts you for the script file name and TFTP server address and then downloads the script.

Table 18 describes the parameters and variables for the `configure-network` command.

Table 18 configure-network command parameters and variables

Parameters and variables	Description
`load-on-boot {disable|use-bootp|use-config}`	Specifies the settings for automatically loading a configuration file when the system boots: • `disable`—disables the automatic loading of config file • `use-boot`—specifies using the BootP file as the automatically loaded config file • `use-config`—specifies using the ASCII configuration file as the automatically loaded config file Note: If you omit this parameter, the system immediately downloads and runs the ASCII config file.
`filename <`*`WORD`*`>`	Specifies the file name. Note: If you omit this parameter and do not specify BootP, the system uses the configured file name.
`address <`*`XXX.XXX.XXX.XXX`*`>`	Specifies the TFTP server from which to load the file. Enter the IP address in dotted-decimal notation. Note: If you omit this parameter and do not specify BootP, the system uses the configured address.

Note: When you specify the file name or address, these parameters are changed at the next reboot, even if you do not specify load-on-boot.

show config-network command

The `show config-network` command displays information regarding the automatic loading of the configuration file, including the current status of this feature, the file name, the TFTP server address, and the status of the previous automatic configuration command. The syntax for the `show config-network` command is:

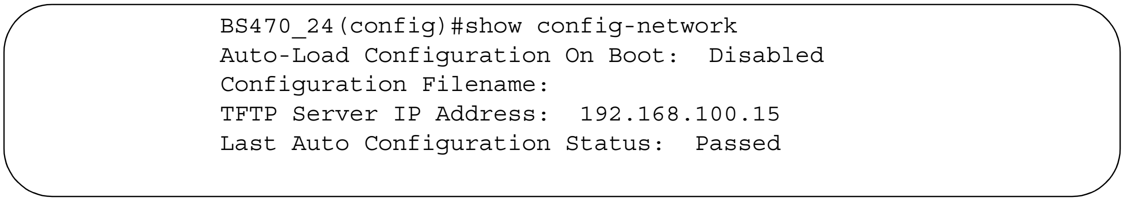
```
show config-network
```

The `show config-network` command is in the privExec mode.

The `show config-network` command has no parameters or variables.

The output for the `show config-network` command is shown in Figure 12,

Figure 12 `show config-network` **command**



```
BS470_24(config)#show config-network
Auto-Load Configuration On Boot:  Disabled
Configuration Filename:
TFTP Server IP Address:  192.168.100.15
Last Auto Configuration Status:  Passed
```

ASCII Configuration Generator (ACG)

The ACG application allows you to save a switch's provisioning information to an external file and download this information to a switch from an external file server.

Note: The external file server must support TFTP.

You can use ACG to:

- Display the current configuration on the CLI.
- Store the current configuration in an external file.
- Load configuration from an external file
- Load configuration at boot time

This section covers the ACG commands available and includes:

- "show running-config ", next
- "copy running-config" on page 86
- "configure network" on page 86
- "configure network load-on-boot" on page 89

show running-config

The `show running-config` command displays the current switch configuration information. The syntax for the `show running-config` command is:

```
show running-config
```

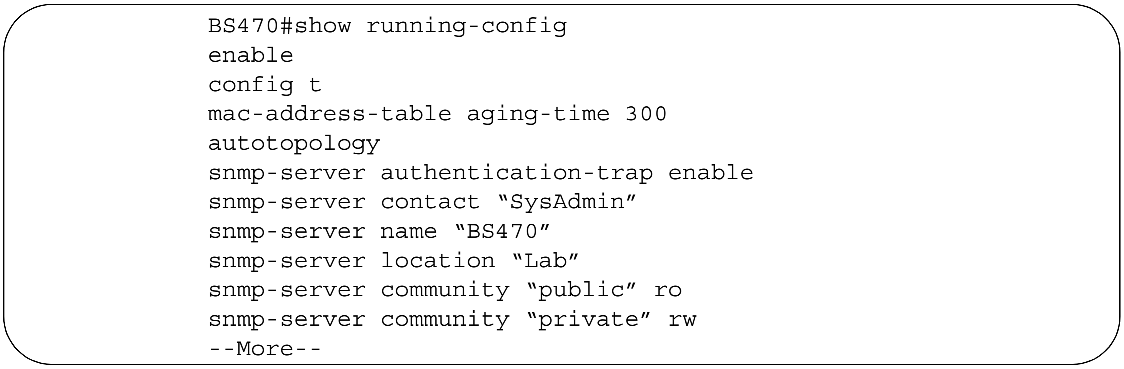
The `show running-config` command is in the privExec command mode.

Note: The `show running-config` command is available, but its use is restricted, when a user has read-only access.

The `show running-config` command has no parameters or variables.

Figure 13 displays a sample output of the `show running-config` command.

Figure 13 `show running-config` command output



```
BS470#show running-config
enable
config t
mac-address-table aging-time 300
autotopology
snmp-server authentication-trap enable
snmp-server contact “SysAdmin”
snmp-server name “BS470”
snmp-server location “Lab”
snmp-server community “public” ro
snmp-server community “private” rw
--More--
```

copy running-config

The `copy running-config` command copies the current switch configuration as an ASCII file on the TFTP server. The syntax for the `copy running-config` command is:

```
copy running-config tftp [address <A.B.C.D>] filename <WORD>
```

Note: The `copy config` command will copy a binary configuration file to the TFTP server. To store the configuration as an ASCII file, you must use the `copy running-config` command.

The `copy running-config` command is in the privExec command mode.

Table 19 describes the parameters and variables for the `copy running-config` command.

Table 19 copy running-config command parameters and variables

Parameters and variables	Description
address <A.B.C.D>	Specifies the TFTP server IP address; enter in dotted-decimal notation.
filename <WORD>	Specifies the name of the existing ASCII configuration file on the TFTP server. This file must be read/write enabled.

Figure 14 displays a sample output of the `copy running-config` command.

Figure 14 `copy running-config` command output

```
BS470#copy running-config tftp address 134.177.118.56 filename
config.txt
%Contacting TFTP host: 134.177.118.56.
%ACG Configuration file successfully written.
BS470#
```

configure network

The `configure network` command loads configuration from an external file on to the switch. The syntax for the `configure network` command is:

```
configure network [address <A.B.C.D>] [filename <WORD>]
```

The `configure network` command is in the PrivExec mode, Global configuration mode, and Interface configuration mode.

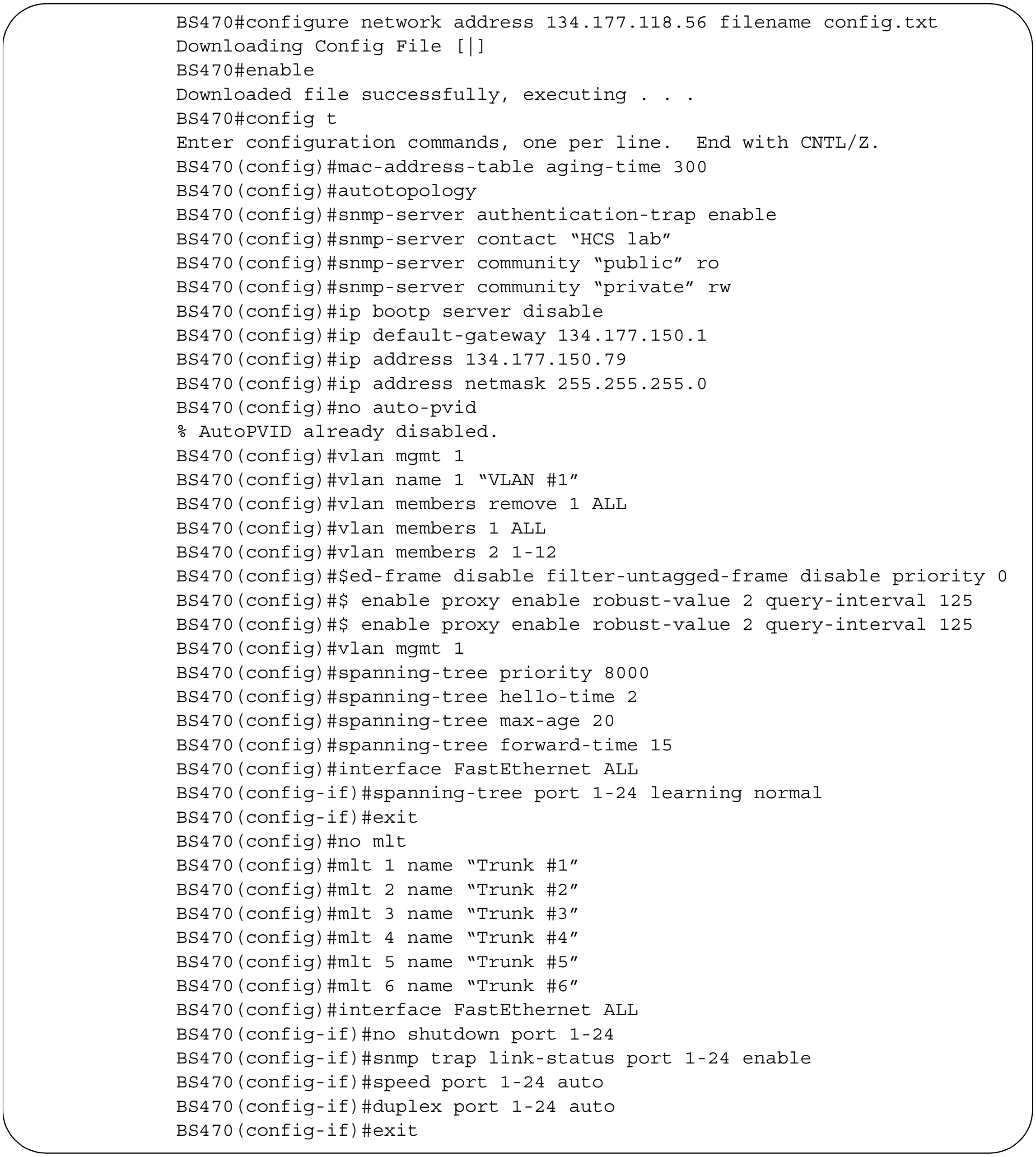
Table 20 describes the parameters and variables for the `configure network` command.

Table 20 configure network command parameters and variables

Parameters and variables	Description
address <A.B.C.D>	Specifies the TFTP server IP address; enter in dotted-decimal notation.
filename <WORD>	Enter the name of the ASCII configuration file you want to copy from the TFTP server.

Figure 15 displays a sample output of the `configure network` command.

Figure 15 `configure network` command output



```
BS470#configure network address 134.177.118.56 filename config.txt
Downloading Config File [|]
BS470#enable
Downloaded file successfully, executing . . .
BS470#config t
Enter configuration commands, one per line.  End with CNTL/Z.
BS470(config)#mac-address-table aging-time 300
BS470(config)#autotopology
BS470(config)#snmp-server authentication-trap enable
BS470(config)#snmp-server contact “HCS lab”
BS470(config)#snmp-server community “public” ro
BS470(config)#snmp-server community “private” rw
BS470(config)#ip bootp server disable
BS470(config)#ip default-gateway 134.177.150.1
BS470(config)#ip address 134.177.150.79
BS470(config)#ip address netmask 255.255.255.0
BS470(config)#no auto-pvid
% AutoPVID already disabled.
BS470(config)#vlan mgmt 1
BS470(config)#vlan name 1 “VLAN #1”
BS470(config)#vlan members remove 1 ALL
BS470(config)#vlan members 1 ALL
BS470(config)#vlan members 2 1-12
BS470(config)#$ed-frame disable filter-untagged-frame disable priority 0
BS470(config)#$ enable proxy enable robust-value 2 query-interval 125
BS470(config)#$ enable proxy enable robust-value 2 query-interval 125
BS470(config)#vlan mgmt 1
BS470(config)#spanning-tree priority 8000
BS470(config)#spanning-tree hello-time 2
BS470(config)#spanning-tree max-age 20
BS470(config)#spanning-tree forward-time 15
BS470(config)#interface FastEthernet ALL
BS470(config-if)#spanning-tree port 1-24 learning normal
BS470(config-if)#exit
BS470(config)#no mlt
BS470(config)#mlt 1 name “Trunk #1”
BS470(config)#mlt 2 name “Trunk #2”
BS470(config)#mlt 3 name “Trunk #3”
BS470(config)#mlt 4 name “Trunk #4”
BS470(config)#mlt 5 name “Trunk #5”
BS470(config)#mlt 6 name “Trunk #6”
BS470(config)#interface FastEthernet ALL
BS470(config-if)#no shutdown port 1-24
BS470(config-if)#snmp trap link-status port 1-24 enable
BS470(config-if)#speed port 1-24 auto
BS470(config-if)#duplex port 1-24 auto
BS470(config-if)#exit
```

configure network load-on-boot

The `configure network load-on-boot` command is used to configure the switch to automatically download a configuration file when you reboot the switch. The syntax for the `configure network load-on-boot` command is:

```
configure network load-on-boot {disable|use-bootp|
use-config} [address <A.B.C.D>] filename <WORD>
```

The `configure network load-on-boot` command is in the PrivExec mode, Global configuration mode, and Interface configuration mode.

Table 21 describes the parameters and variables for the `configure network load-on-boot` command.

Table 21 configure network load-on-boot command parameters

Parameters and variables	Description
{disable|use-bootp|use-config}	Specifies the settings for automatically loading a configuration file when the system boots: • disable—disables the automatic loading of the configuration file • use-bootp—specifies using the BootP file as the automatically loaded configuration file • use-config—specifies using the ASCII configuration file as the automatically loaded configuration file
address <A.B.C.D>	Specifies the TFTP server IP address; enter in dotted-decimal notation.
filename <WORD>	Enter the name of the ASCII configuration file you want to copy from the TFTP server.

Figure 16 displays a sample output of the `configure network load-on-boot` command.

Figure 16 `configure network load-on-boot` command output

```
BS470#configure network load-on-boot use-config address 134.177.118.56
filename config.txt
BS470#
```

Downloading and uploading your software

You can download the switch software image that is located in non-volatile flash memory. To download the switch software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch IP address, refer to "Assigning and clearing IP addresses" on page 66.

Caution: Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

You also download the Power over Ethernet (PoE) image using the NNCLI.

This section covers the following topics:

- "download command ", next
- "Observing LED indications" on page 92
- "Upgrading software images" on page 94

download command

The `download` command upgrades the software for the switch. You can upgrade the software image, the diagnostics image, and/or the PoE image. If you upgrade to a stack configuration, the entire stack is upgraded, and the new image is loaded onto every unit of the stack.

Note: The default downloading process without this command, is that the unit resets after downloading.

The syntax for the `download` command is:

```
download [address <ip>] {image <image-name>|image-if-newer
<image-name>|diag <filename>}[no-reset]
```

The `download` command is in the privExec command mode.

Table 22 describes the parameters and variables for the `download` command.

Table 22 download command parameters and variables

Parameters and variables	Description
address <ip>	Specifies the TFTP server you want to use. Note: If this parameter is omitted, the system goes to the server specified by the `tftp-server` command.
image <image-name>	Enter the name of the software image you want to download.
image-if-newer <image-name>	Enter the name of the software image you want to download if newer than the current running image.
diag <filename>	Enter the name of the diagnostics image you want to download.
no-reset	Download the specified software without resetting the unit.

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Take care not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

When the download process is complete, the switch automatically resets (unless you specify no-reset) and the new software image initiates a self-test. The system returns a message after successfully downloading a new image. Figure 17 displays a sample output of the download command.

Figure 17 download message

```
Download Image [/]
Saving Image [-]
Finishing Upgrading Image
```

During the download process, the unit is not operational. You can monitor the progress of the download process by observing the LED indications.

Observing LED indications

Note: When you upgrade the software in a mixed stack, or Hybrid Stack operational mode, all the BU LEDs on all switch units may light or blink. you may disregard these lights at this time.
The Hybrid Stack mode is not supported in this release of the BayStack 460-24T-PWR.

Table 23 describes the LED indications during the software download process for the BayStack 470-24T switch.

Table 23 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs ports 1 to 24:** The LEDs blink in succession from both ends and criss-cross at the center of the switch.
2	The switch erases the flash memory.	**100 Mb/s LEDs ports 1 and 24 stay lit**.
3	The switch programs the new software image into the flash memory.	**Same as phase 1**.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Note: When you upgrade the software in a mixed stack, or Hybrid Stack operational mode, all the BU LEDs on all BayStack 470-48T units may light or blink. you may disregard these lights at this time.
The Hybrid Stack mode is not supported in this release of the BayStack 460-24T-PWR.

Table 24 describes the LED indications during the software download process for BayStack 460-24T-PWR switch.

Table 24 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs (ports 18 to 24 only):** The LEDs begin to turn on in succession beginning with port 24, which indicates the progress of the download process. When LEDs 18 to 24 are all on, the switch has received the new software image successfully.
2	The switch erases the flash memory.	**100 Mb/s port status LEDs (ports 1 to 12 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that various sectors of the switches flash memory are being erased. When LEDs 1 to 12 are all on, the switches flash memory has been erased.
3	The switch programs the new software image into the flash memory.	**100 Mb/s port status LEDs (ports 1 to 8 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that the new software image is being programmed into the switches flash memory. When LEDs 1 to 8 are all on, the new software image has been programmed successfully into the switches flash memory.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Table 25 describes the LED indications during the software download process for the BayStack 470-48T switch.

Table 25 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs ports 1 to 48:** The LEDs blink in succession from both ends and criss-cross at the center of the switch.
2	The switch erases the flash memory.	**100 Mb/s LEDs ports 1 and 48 stay lit**.

Table 25 LED Indications during the software download process (Continued)

Phase	Description	LED Indications
3	The switch programs the new software image into the flash memory.	**Same as phase 1**.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Upgrading software images

You follow a different procedure depending on your switch model and if you are using a Pure Stack or a Hybrid Stack.

The stacking software compatibility requirements are as follows:

- Pure Stack—All units must be running the same software version.
- Hybrid Stack—All units must be running the same software version and all software versions must have the identical ISVN.

Note: The Hybrid Stack mode is not supported in this release of the BayStack 460-24T-PWR.

This section discusses the following topics:

- "Upgrading software in a Pure 460 Stack ", next
- "Upgrading software in a Pure BayStack 470-24T Stack" on page 95
- "Upgrading software in a Pure BayStack 470-48T Stack" on page 95
- "Customizing your system" on page 95

Upgrading software in a Pure 460 Stack

To download, or upgrade, software in a Pure 460 stack:

1 Enter `download [address <ip>] image 460.img`.

The system resets and opens to the BayStack 460-24T-PWR banner. Refer to "Setting the CLI password" on page 162 to return to the CLI.

2 Enter `download [address <ip>] diag` **`460diags.bin`**.

The system resets and opens to the BayStack 460-24T-PWR banner. Refer to "Setting the CLI password" on page 162 to return to the CLI.

Upgrading software in a Pure BayStack 470-24T Stack

To download, or upgrade, software in a BayStack 470-24T switch:

1 Enter `download [address <ip>] image` **`BS470_24.img`**.

The system resets and opens to the BayStack 470-24T banner. Refer to "Setting the CLI password" on page 162 to return to the CLI.

2 Enter `download [address <ip>] diag` **`BS470_24diags.bin`**.

The system resets and opens to the BayStack 470-24T banner. Refer to "Setting the CLI password" on page 162 to return to the CLI.

Upgrading software in a Pure BayStack 470-48T Stack

To download, or upgrade, software in a BayStack 470-48T switch:

1 Enter `download [address <ip>] image` **`BS470.img`**.

The system resets and opens to the BayStack 470-48T banner. Refer to "Setting the CLI password" on page 162 to return to the CLI.

2 Enter `download [address <ip>] diag` **`BS470diags.bin`**.

The system resets and opens to the BayStack 470-48T banner. Refer to "Setting the CLI password" on page 162 to return to the CLI.

Customizing your system

You can customize your system using the following CLI commands. This section covers:

- "Setting the terminal ", next
- "Displaying system information" on page 99
- "Setting boot parameters" on page 101
- "Setting TFTP parameters" on page 104
- "Customizing the opening banner" on page 106
- "Setting SNMP parameters" on page 109
- "Configuring remote network monitoring (RMON)" on page 113
- "Setting the system event log" on page 122
- "Setting the default management system" on page 127

Setting the terminal

You can view the terminal settings, set them to default settings, or customize the terminal settings. This section covers:

- "show terminal command ", next
- "default terminal command" on page 97
- "terminal command" on page 97
- "show cli command" on page 98

show terminal command

The `show terminal` command displays the current serial port information, which includes connection speed, as well as the terminal width and length in number of characters. The syntax for the `show terminal` command is:

```
show terminal
```

The `show terminal` command is in the exec command mode.

The `show terminal` command has no parameters or variables.

Figure 18 displays the output from the `show terminal` command.

Figure 18 `show terminal` command output

```
BS470_24#show terminal
Terminal speed: 9600
Terminal width: 79
Terminal length: 23
```

default terminal command

The `default terminal` command configures default settings for the terminal. These settings are transmit and receive speeds, terminal length, and terminal width. The syntax for the `default terminal` command is:

```
default terminal {speed|width|length}
```

The `default terminal` command is in the exec mode.

Table 26 describes the parameters and variables for the `default terminal` command.

Table 26 default terminal command parameters and variables

Parameters and variables	Description
`speed|width|length`	Sets the defaults • `speed`—transmit and receive baud rates for the terminal; default is 9600 baud • `width`—width of the terminal display; default is 79 characters • `length`—Length of the terminal display; default is 24 characters

terminal command

The `terminal command` configures the settings for the terminal. These settings are transmit and receive speeds, terminal length, and terminal width. The syntax of the `terminal` command is:

```
terminal speed {2400|4800|9600|19200|38400}|length
<1-132>|width <1-132>
```

The `terminal command` is in the exec mode.

Table 27 describes the parameters and variables for the `terminal` command.

Table 27 terminal command parameters and variables

Parameters and variables	Description
`speed {2400|4800|9600|19200|38400}`	Sets the transmit and receive baud rates for the terminal. You can set the speed at one of the five options shown; default is 9600.
`length`	Sets the length of the terminal display in characters; default is 24.
`width`	Sets the width of the terminal display in characters; default is 79.

show cli command

The `show cli` command displays the current CLI settings. The syntax for the `show cli` command is:

```
show cli [info|password]
```

The `show cli` command is in the exec command mode.

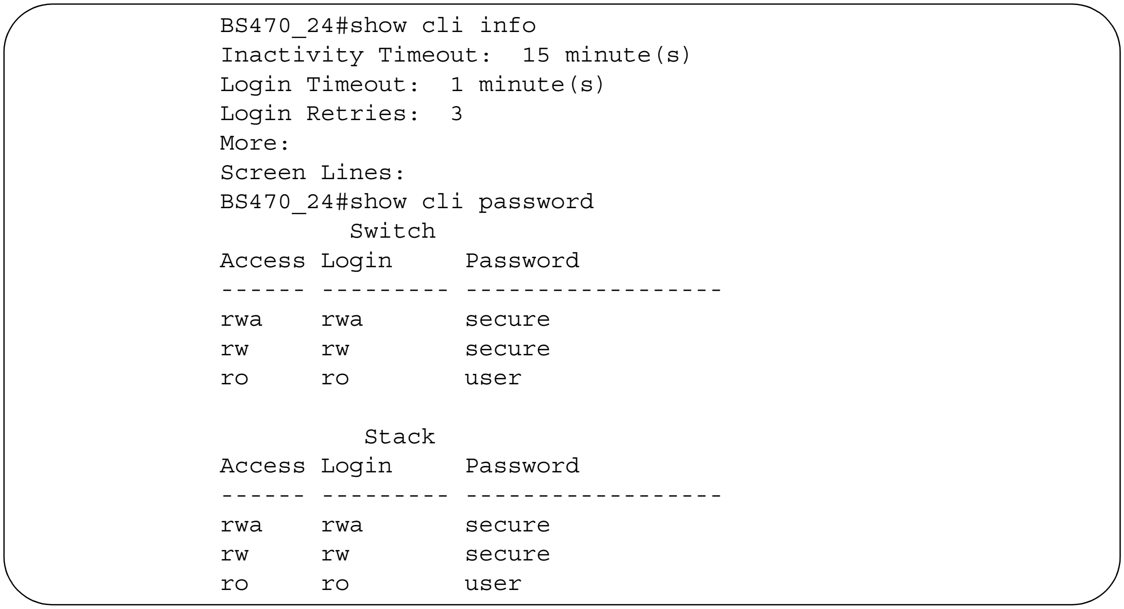
Table 28 describes the parameters and variables for the `show cli` command.

Table 28 show cli command parameters and variables

Parameters and variables	Description
`info`	Displays general CLI settings.
`password`	Displays CLI usernames and passwords.

Figure 19 displays the output from the `show cli` command.

Figure 19 `show cli` command output



```
BS470_24#show cli info
Inactivity Timeout:  15 minute(s)
Login Timeout:  1 minute(s)
Login Retries:  3
More:
Screen Lines:
BS470_24#show cli password
         Switch
Access Login     Password
------ --------- ------------------
rwa    rwa       secure
rw     rw        secure
ro     ro        user

          Stack
Access Login     Password
------ --------- ------------------
rwa    rwa       secure
rw     rw        secure
ro     ro        user
```

Displaying system information

The `show sys-info` command displays the current system characteristics, which includes HW rev, FW rev, date of manufacture (DOM), and Hardware deviation number. The syntax for the `show sys-info` command is:

```
show sys-info
```

The `show sys-info` command is in the privExec command mode.

The `show sys-info` command has no parameters or variables.

Figure 20 and Figure 21 displays sample output from the `show sys-info` command.

Figure 20 `show sys-info` command output

```
BS460_24T_PWR#show sys-info
Operation Mode:        Switch
MAC Address:           00-09-97-29-1F-00
Reset Count:           1
Last Reset Type:       Software Download
Power Status:          Primary Power
Autotopology:          Enabled
Current Switch Mode:   L2
Next Boot Switch Mode: L2
Local MDA Type:        None
PoE Module FW:         7013.2
sysDescr:              BayStack 460 - 24T - PWR
                       HW:00       FW:3.0.0.5   SW:v3.5.0.18
ISVN:2
                       Mfg Date:20021102    HW Dev:
Serial #:              SDNIHR007B
sysObjectID:           1.3.6.1.4.1.45.3.49.1
sysUpTime:             12 days, 07:04:49
sysNtpTime:            SNTP not synchronized.
sysServices:           3
sysContact:
sysName:
sysLocation:
BS460_24T_PWR#show sys-info
```

Figure 21 `show sys-info` command output

```
BS470_48#show sys-info
Operation Mode:        Switch
MAC Address:           00-04-38-D5-9F-C0
Reset Count:           1
Last Reset Type:       Software Download
Power Status:          Primary Power
Autotopology:          Enabled
Current Switch Mode:   L2
Next Boot Switch Mode: L2
GBIC Port 47:          None
GBIC Port 48:          None
sysDescr:              BayStack 470 - 48T
                       HW:#0D      FW:3.0.0.5   SW:v3.5.0.18
ISVN:2
                       Mfg Date:20020717    HW Dev:
Serial #:              ACC1000CP
sysObjectID:           1.3.6.1.4.1.45.3.46.1
sysUpTime:             12 days, 08:43:00
sysNtpTime:            SNTP not synchronized.
sysServices:           3
sysContact:
sysName:
sysLocation:
BS470_48#
```

To change the system contact, name, or location, refer to the `snmp-server` command.

Setting boot parameters

You can reboot the switch or stack and configure BootP. The topics covered in this section are:

- "boot command ", next
- "ip bootp server command" on page 102
- "stack bootp-mac-addr-type command" on page 103
- "no ip bootp server command" on page 104
- "default ip bootp server command" on page 104

boot command

The `boot` command performs a soft-boot of the switch. The syntax for the `boot` command is:

```
boot [default] [unit <unitno>]
```

The `boot` command is in the privExec command mode.

Table 29 describes the parameters and variables for the `boot` command.

Table 29 boot command parameters and variables

Parameters and variables	Description
`default`	Restores switch to factory-default settings after rebooting.
`unit <unitno>`	Specifies which unit of the stack to be rebooted. This command is available only in stack mode. Enter the unit number of the switch you want to reboot.

Note: When you reset to factory defaults, the switch retains the last reset count, and reason for last reset; these parameters are not changed to factory defaults.

ip bootp server command

The `ip bootp server` command configures BootP on the current instance of the switch or server. You use this command if you want to change the value of BootP from the default value, which is BootP when needed.The syntax for the `ip bootp server` command is:

```
ip bootp server {last|needed|disable|always}
```

The `ip bootp server` command is in the config command mode.

Table 30 describes the parameters and variables for the `ip bootp server` command.

Table 30 ip bootp server command parameters and variables

Parameters and variables	Description
last|needed|disable|always	Specifies when to use BootP: • always—Always use BootP • disable—never use BootP • last—use BootP or the last known address • needed—use BootP only when needed NOTE: The default value is to use BootP when needed.

stack bootp-mac-addr-type command

The `stack bootp-mac-addr-type` command allows you to choose which MAC address is used for BootP operation when running in a stack. This option is available only on a stack consisting of all the same models of switches that are set for the stack operational mode of Pure Stack. The syntax for the `stack bootp-mac-address-type` command is:

```
stack bootp-mac-addr-type {base-unit|stack}
```

The `stack bootp-mac-addr-type` command is in the config command mode.

Table 31 describes the parameters and variables for the `stack boot-mac-addr-type` command.

Table 31 stack boot-mac-addr-type command parameters and variables

Parameters and variables	Description
`base-unit|stack`	Specifies location of BootP MAC address: • `base-unit`—use the base unit MAC address for BootP • `stack`—use the stack MAC address for BootP

no ip bootp server command

The `no ip bootp server` command disables the BootP server. The syntax for the `no ip bootp server` command is:

```
no ip bootp server
```

The `no ip bootp server` command is in the config command mode.

The `no ip bootp server` command has no parameters or variables.

default ip bootp server command

The `default ip bootp server` command disables the BootP server. The syntax for the `default ip bootp server` command is:

```
default ip bootp server
```

The `default ip bootp server` command is in the config command mode.

The `default ip bootp server` command has no parameters or variables.

Setting TFTP parameters

You can display the IP address of the TFTP server, assign an IP address you want to use for a TFTP server, copy a configuration file to the TFTP server, or copy a configuration file from the TFTP server to the switch to use to configure the switch. This section covers:

- "show tftp-server command ", next
- "tftp-server command" on page 105
- "no tftp-server command" on page 106
- "copy config tftp command" on page 106
- "copy config tftp command" on page 106

show tftp-server command

The `show tftp-server` command displays the IP address of the server used for all TFTP-related transfers. The syntax for the `show tftp-server` command is:

```
show tftp-server
```

The `show tftp-server` command is in the privExec command mode.

The `show tftp-server` command has no parameters or variables.

Figure 22 displays a sample output of the `show tftp-server command`.

Figure 22 `show tftp-server` command output

```
BS470_24#show tftp-server
TFTP Server IP address : 192.168.100.15
```

tftp-server command

The `tftp-server` command assigns the address for the switch to use for TFTP services. The syntax for the `tftp-server` command is:

```
tftp-server <XXX.XXX.XXX.XXX>
```

The `tftp-server` command is in the config command mode.

Table 32 describes the parameters and variables for the `tftp-server` command.

Table 32 tftp-server command parameters and variables

Parameters and variables	Description
XXX.XXX.XXX.XXX	Enter the dotted-decimal IP address of the server you want to use for TFTP services.

no tftp-server command

The `no tftp-server` command clears the TFTP server IP address to `0.0.0.0`. The syntax of the `no tftp-server` command is:

```
no tftp-server
```

The `no tftp-server` command is in the config command mode.

The `no tftp-server` command has no parameters or variables.

copy config tftp command

The `copy config tftp` command copies the current configuration file onto the TFTP server. The syntax for the `copy config tftp` command is:

```
copy config tftp [address <XXX.XXX.XXX.XXX>] filename <WORD>
```

The `copy config tftp` command is in the privExec command mode.

Table 33 describes the parameters and variables for the `copy config tftp` command.

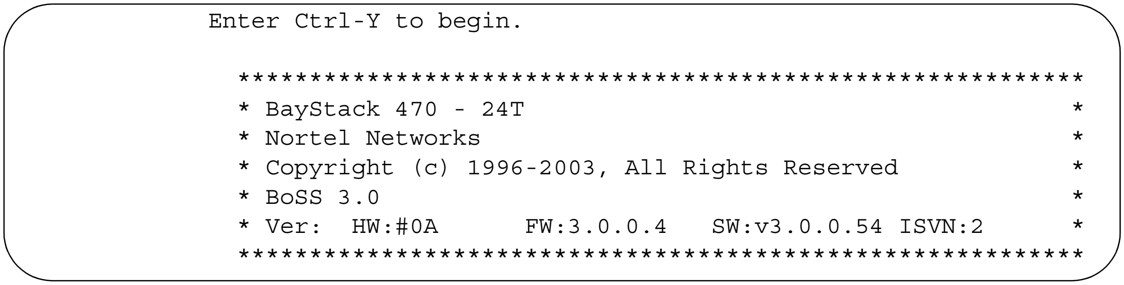
Table 33 copy config tftp command parameters and variables

Parameters and variables	Description
`[address <XXX.XXX.XXX.XXX>]`	Specifies the TFTP server IP address; enter in dotted-decimal notation.
`filename <WORD>`	Specifies that you want to copy the configuration file onto the TFTP server. Enter the name you want the configuration file to have on the TFTP server.

Customizing the opening banner

You can customize the opening banner that appears when you connect to the switch console port or Telnet to the switch. The part you can customize is the “BAYSTACK,” written in asterisks when it is opened the first time. You cannot customize the portion that displays “Enter Ctrl-Y to begin” (Figure 23).

Figure 23 Portion of opening banner you *cannot* customize



```
         Enter Ctrl-Y to begin.

           ***********************************************************
           * BayStack 470 - 24T                                      *
           * Nortel Networks                                         *
           * Copyright (c) 1996-2003, All Rights Reserved            *
           * BoSS 3.0                                                *
           * Ver:  HW:#0A      FW:3.0.0.4   SW:v3.0.0.54 ISVN:2      *
           ***********************************************************
```

The banner cannot exceed 11215 bytes, or 15 rows x 80 columns plus line termination characters.

The banner control setting is saved to NVRAM, and both the banner file and control setting are distributed to all units within a stack.

You must create the custom banner one line at a time using the Nortel Networks Command Line Interface (NNCLI). Additionally, you can download the customer banner using the ASCII configuration file.

This sections describes the NNCLI commands you must use to customize and display the banner that displays when you connect to the switch console port or Telnet to the switch. The following topics are discussed:

- "show banner command ", next
- "banner command for displaying banner" on page 108
- "banner command for creating banner" on page 109
- "no banner command" on page 109

show banner command

The `show banner` command displays the banner. The syntax for the `show banner` command is:

```
show banner [static|custom]
```

The `show banner` command is in the privExec command mode.

Table 34 describes the parameters and variables for the `show banner` command.

Table 34 `show banner` command parameters and variables

Parameters and variables	Description
static|custom	Displays which banner is currently set to display • static • custom

Figure 24 displays a sample output of the `show banner` command.

Figure 24 `show banner` command output

```
BS470_24T#show banner
Current banner setting: CUSTOM
```

banner command for displaying banner

The `banner` command for displaying banner specifies the banner displayed at startup; either static or custom. The syntax for the `banner` command for displaying banner is:

```
banner [static|custom]
```

The `banner` command for displaying banner is in privExec command mode.

Table 35 describes the parameters and variables for the `banner` command.

Table 35 `banner` command for displaying banner parameters and variables

Parameters and variables	Description
static|custom	Sets the display banner as: • static • custom

banner command for creating banner

The banner command for creating banner allows you to create a custom banner. The syntax for the banner command for creating banner is:

```
banner <line number> <text>
```

The banner command for creating banner is in the privExec command mode.

Table 36 describes the parameters and variables for the banner command.

Table 36 banner command for creating banner parameters and variables

Parameters and variables	Description
<line number>	Enter the banner line number you are setting. The range is 1 to 15.
<text>	Enter the character string you want to display. The range is 1 to 80.

no banner command

The no banner command allows you to clear all lines of a previously stored custom banner. The syntax for the no banner command is:

```
no banner
```

The no banner command is in the privExec command mode.

Setting SNMP parameters

You can set various SNMP parameters and traps, as well as disable SNMP traps. This section covers:

- "snmp-server command ", next
- "no snmp-server command" on page 111
- "snmp trap link-status command" on page 111
- "no snmp trap link-status command" on page 112
- "default snmp trap link-status command" on page 113

snmp-server command

The `snmp-server` command configures various SNMP parameters. The syntax for the `snmp-server` command is:

```
snmp-server {{enable|disable}|authentication-trap|community
<community-string> [ro|rw] contact <text>|host <host-ip>
<community-string>|location <text>|name <text>}
```

The `snmp-server` command is in the config command mode.

Table 37 describes the parameters and variables for the `snmp-server` command.

Table 37 snmp-server command parameters and variables

Parameters and variables	Description
`authentication-trap enable / disable`	Enables generation of SNMP authentication failure traps.
`community <community-string>`	Changes the read-only (`ro`) or read-write (`rw`) community strings for SNMP v1 and SNMPv2c access. Enter a community string that works as a password and permits access to the SNMP protocol.
`ro|rw`	Specifies read-only or read-write access. Stations with `ro` access can only retrieve MIB objects, and stations with `rw` access can retrieve and modify MIB objects. Note: If neither `ro` nor `rw` is specified, `ro` is assumed (default).
`contact <text>`	Specifies the SNMP sysContact value; enter an alphanumeric string.
`host <host-ip> <community-string>`	Configures an SNMP trap destination: • *host-ip*—enter a dotted-decimal IP address of a host that is to be the trap destination • *community-string*—enter a community string that works as a password and permits access to the SNMP protocol
`location <text>`	Specifies the SNMP sysLocation value; enter an alphanumeric string.
`name <text>`	Specifies the SNMP sysName value; enter an alphanumeric string.

no snmp-server command

The `no snmp-server command` disables SNMP or clears the configuration. If you omit the parameters, this command disables SNMP access. The syntax for the `no snmp-server` command is:

```
no snmp-server [authentication-trap|community [ro|rw]
contact|host [<host-ip> <community-string>] |location| name]
```

The `no snmp-server` command is in the config command mode.

Table 38 describes the parameters and variables for the `snmp-server` command.

Table 38 no snmp-server command parameters and variables

Parameters and variables	Description
`enable|disable`	With no parameters, disables SNMP access.
`authentication-trap`	Disables authentication failure traps.
`community`	Disables the community string.
`ro|rw`	Disables either read-only or read-write access.
`contact <text>`	Clears the SNMP sysContact value.
`host <host-ip> <community-string>`	Removes an SNMP trap destination or all destinations.
`location`	Clears the SNMP sysLocation value.
`name`	Clears the SNMP sysName value

Note: Disabling SNMP access also locks you out of the Device Manager management system.

snmp trap link-status command

The `snmp trap link-status` command enables the linkUp/linkDown traps for the port. The syntax of the command is:

```
snmp trap link-status [port <portlist>]
```

The `snmp trap link-status` command is in the config-if command mode.

Table 39 describes the parameters and variables for the `snmp trap link-status` command.

Table 39 snmp trap link-status command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to enable the linkUp/linkDown traps on. Enter the port numbers or `all`. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

no snmp trap link-status command

The `no snmp trap link-status` command disables the linkUp/linkDown traps for the port. The syntax of the command is:

```
no snmp trap link-status [port <portlist>]
```

The `no snmp trap link-status` command is in the config-if command mode.

Table 40 describes the parameters and variables for the `no snmp trap link-status` command.

Table 40 no snmp trap link-status command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable the linkUp/linkDown traps on. Enter the port numbers or `all`. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

default snmp trap link-status command

The `default snmp trap link-status` command disables the linkUp/linkDown traps for the port. The syntax of the command is:

```
default snmp trap link-status [port <portlist>]
```

The `default snmp trap link-status` command is in the config-if command mode.

Table 41 describes the parameters and variables for the `default snmp trap link-status` command.

Table 41 default snmp trap link-status command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable the linkUp/linkDown traps on. Enter the port numbers or `all`. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Configuring remote network monitoring (RMON)

This section covers the RMON commands available and includes the following topics:

- "show rmon alarm ", next
- "show rmon event" on page 114
- "show rmon history" on page 115
- "show rmon stats" on page 116
- "rmon alarm" on page 117
- "no rmon alarm" on page 118
- "rmon event" on page 119
- "no rmon event" on page 119
- "rmon history" on page 120
- "no rmon history" on page 121

- “rmon stats” on page 121
- “no rmon stats” on page 122

show rmon alarm

The `show rmon alarm` command displays information for RMON alarms. The syntax for the `show rmon alarm` command is:

```
show rmon alarm
```

The `show rmon alarm` command is in the privExec mode.

The `show rmon alarm` command has no parameters or variables.

Figure 25 displays a sample output of the `show rmon alarm` command.

Figure 25 `show rmon alarm` command output

```
BS470_24#show rmon alarm
                                         Sample      Rising         Falling
Index Interval Variable                   Type  Threshold Event Threshold Event
----- -------- ------------------------- ------ --------- ----- --------- -----
1     30       ifInOctets.1              delta  500       1     10        1
```

show rmon event

The `show rmon event` command displays information regarding RMON events. The syntax for the `show rmon event` command is:

```
show rmon event
```

The `show rmon event` command is in the privExec mode.

The `show rmon event` command has no parameters or variables. Figure 26 displays a sample output of the `show rmon event` command.

Figure 26 `show rmon event` command output

```
BS470_24#show rmon event
Index Log Trap Description
----- --- ---- ----------------------------------------------------
1     Yes Yes  'Rising or Falling alarm on received octets'
```

show rmon history

The `show rmon history` command displays information regarding RMON history. The syntax for the `show rmon history` command is:

```
show rmon history
```

The `show rmon history` command is in the privExec mode.

The `show rmon history` command has no parameters or variables.

Figure 27 displays a sample output of the `show rmon history` command.

Figure 27 `show rmon history` command output

```
BS470_24#show rmon history
Index Unit/Port Buckets Requested Buckets Granted Interval
----- --------- ----------------- --------------- --------
1     1/1       15                15              30
2     1/2       15                15              30
3     1/3       15                15              30
4     1/4       15                15              30
5     1/5       15                15              30
6     1/6       15                15              30
7     1/7       15                15              30
8     1/8       15                15              30
9     1/9       15                15              30
10    1/10      15                15              30
11    1/11      15                15              30
12    1/12      15                15              30
13    1/13      15                15              30
14    1/14      15                15              30
15    1/15      15                15              30
16    1/16      15                15              30
17    1/17      15                15              30
18    1/18      15                15              30
19    1/19      15                15              30
20    1/20      15                15              30
--More--
```

show rmon stats

The `show rmon stats` command displays information regarding RMON statistics. The syntax for the `show rmon stats` command is:

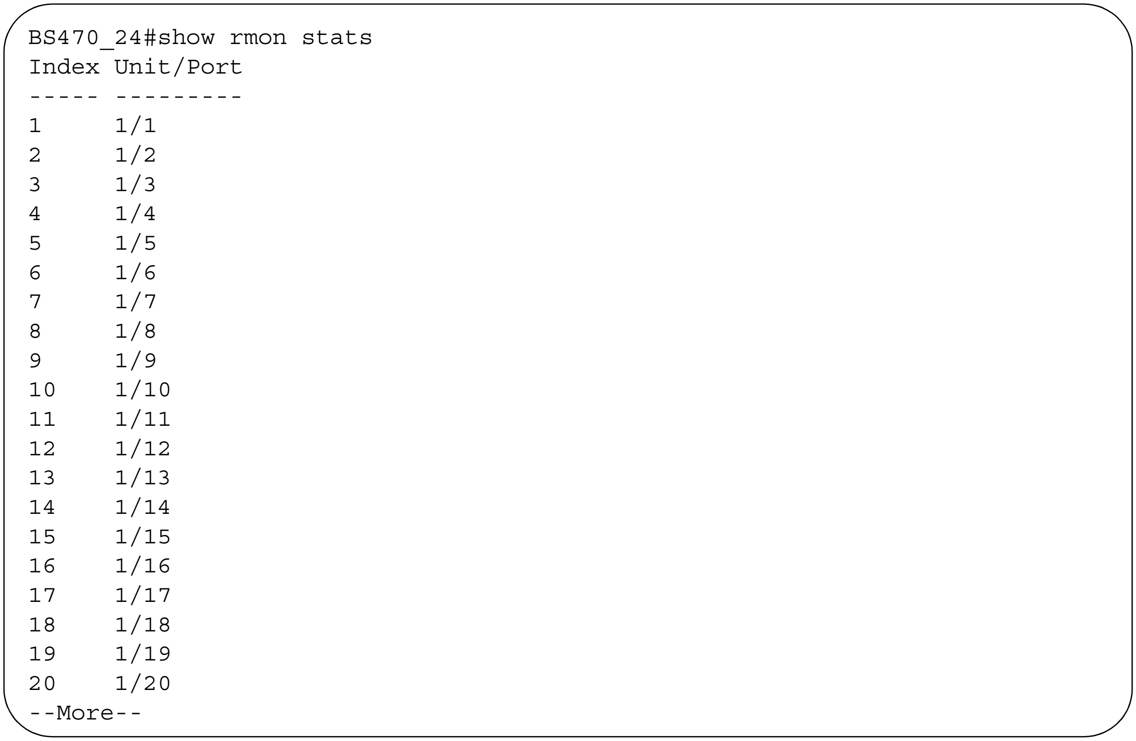
```
show rmon stats
```

The `show rmon stats` command is in the privExec mode.

The `show rmon stats` command has no parameters or variables.

Figure 28 displays a sample output of the `show rmon stats` command.

Figure 28 `show rmon stats` command output



```
BS470_24#show rmon stats
Index Unit/Port
----- ---------
1     1/1
2     1/2
3     1/3
4     1/4
5     1/5
6     1/6
7     1/7
8     1/8
9     1/9
10    1/10
11    1/11
12    1/12
13    1/13
14    1/14
15    1/15
16    1/16
17    1/17
18    1/18
19    1/19
20    1/20
--More--
```

rmon alarm

The `rmon alarm` command allows you to set RMON alarms and thresholds. The syntax for the `rmon alarm` command is:

```
rmon alarm <1-65535> <WORD> <1-2147483647> {absolute|delta}
rising threshold <-2147483648-2147483647> [<1-65535>]
falling-threshold <-2147483648-2147483647> [<1-65535>]
[owner <LINE>]
```

The `rmon alarm` command is in the config command mode.

Table 42 describes the parameters and variables for the `rmon alarm` command.

Table 42 rmon alarm command parameters and variables

Parameters and variables	Description
`<1-65535>`	Unique index for the alarm entry.
`<WORD>`	The MIB object to be monitored. This is an *OID*, and for most available objects, an English name may be used.
`<1-2147483647>`	The sampling interval, in seconds.
`absolute`	Use absolute values (value of the MIB object is compared directly with thresholds).
`delta`	Use delta values (change in value of the MIB object between samples is compared with thresholds).
`rising-threshold <-2147483648-2147483647> [<1-65535>]`	The first integer value is the rising threshold value. The optional second integer specifies the event entry to be triggered when the rising threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered.
`falling-threshold <-2147483648-2147483647> [<1-65535>]`	The first integer value is the falling threshold value. The optional second integer specifies the event entry to be triggered when the falling threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered.
`[owner <LINE>]`	Specifies an owner string to identify alarm entry.

no rmon alarm

The `no rmon alarm` command deletes RMON alarm table entries. When the variable is omitted, all entries in the table are cleared. The syntax for the `no rmon alarm` command is:

```
no rmon alarm [<1-65535>]
```

The `no rmon alarm` command is in the config command mode.

Table 43 describes the parameters and variables for the `no rmon alarm` command.

Table 43 no rmon alarm command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the alarm entry.

rmon event

The `rmon event` command allows you to configure RMON event log and trap settings. The syntax for the `rmon event` command is:

```
rmon event <1-65535> [log] [trap] [description <LINE>]
[owner <LINE>]
```

The `rmon event` command is in the config command mode.

Table 44 describes the parameters and variables for the `rmon event` command.

Table 44 rmon event command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the event entry.
[log]	Record events in the log table.
[trap]	Generate SNMP trap messages for events.
[description <*LINE*>]	Specify a textual description for the event.
[owner <*LINE*>]	Specify an owner string to identify the event entry

no rmon event

The `no rmon event` command deletes RMON event table entries. When the variable is omitted, all entries in the table are cleared. The syntax for the `no rmon event` command is:

```
no rmon event [<1-65535>]
```

The `no rmon event` command is in the config command mode.

Table 45 describes the parameters and variables for the `no rmon event` command.

Table 45 no rmon event command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the event entry.

rmon history

The `rmon history` command allows you to configure RMON history settings. The syntax for the `rmon history` command is:

```
rmon history <1-65535> <LINE> <1-65535> <1-3600>
[owner <LINE>]
```

The `rmon history` command is in the config command mode.

Table 46 describes the parameters and variables for the `rmon history` command.

Table 46 rmon history command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the history entry.
<LINE>	Specify the port number to be monitored.
<1-65535>	The number of history buckets (records) to keep.
<1-3600>	The sampling rate (how often a history sample is collected).
[owner *<LINE>*]	Specify an owner string to identify the history entry.

no rmon history

The `no rmon history` command deletes RMON history table entries. When the variable is omitted, all entries in the table are cleared. The syntax for the `no rmon history` command is:

```
no rmon history [<1-65535>]
```

The `no rmon history` command is in the config command mode.

Table 47 describes the parameters and variables for the `no rmon history` command.

Table 47 no rmon history command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the history entry.

rmon stats

The `rmon stats` command allows you to configure RMON statistic settings. The syntax for the `rmon stats` command is:

```
rmon stats <1-65535> <port> [owner <LINE>]
```

The `rmon stats` command is in the config command mode.

Table 48 describes the parameters and variables for the `rmon stats` command.

Table 48 rmon stats command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the stats entry.
<port>	Specifies a port for the stats.
[owner *<LINE>*]	Specifies an owner string to identify the stats entry.

no rmon stats

The `no rmon stats` turns off RMON statistics. When the variable is omitted, all table entries are cleared. The syntax for the `no rmon stats` command is:

```
no rmon stats [<1-65535>]
```

The `no rmon stats` command is in the config command mode.

Table 49 describes the parameters and variables for the `no rmon stats` command.

Table 49 no rmon stats command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the stats entry.

Setting the system event log

You can set the system event log to log different levels of events. This section covers:

- "show logging ", next
- "logging" on page 124
- "no logging" on page 124
- "set logging" on page 125
- "no set logging" on page 125
- "default logging" on page 126
- "clear logging command" on page 126

show logging

The `show logging` command displays the current contents of the system event log. The default value displays all levels in chronological order. The syntax for the `show logging` command is:

```
show logging [config|critical|serious|informational]
```

The `show logging` command is in the privExec command mode.

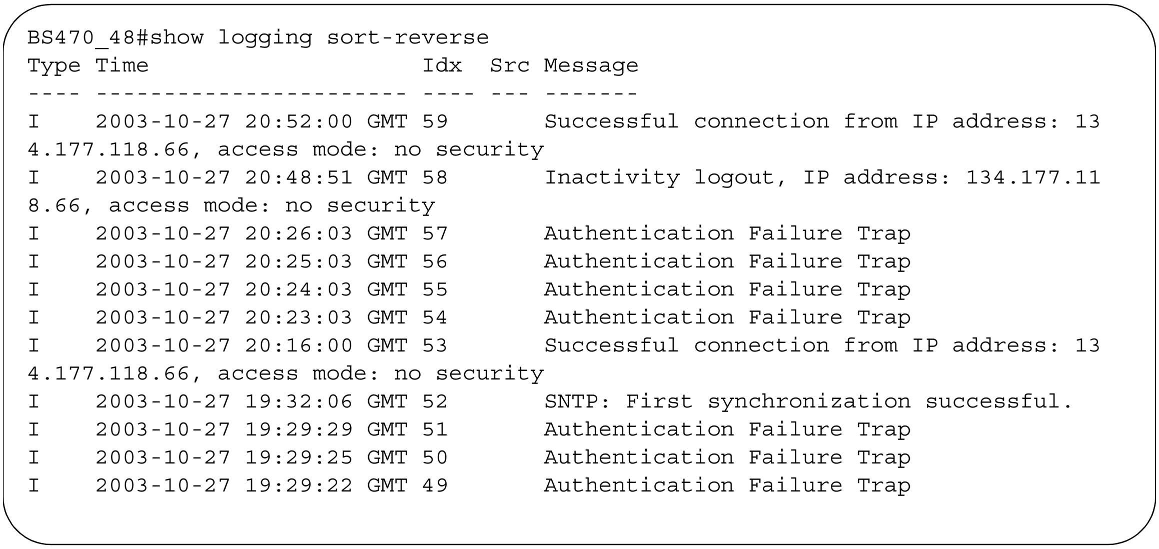
Table 50 describes the parameters and variables for `show logging` command.

Table 50 `show logging` command parameters and variables

Parameters and variables	Description
`config`	Displays configuration log messages. (This command parameter is only available with the BayStack 470-24T switch.)
`critical`	Displays critical log messages.
`serious`	Displays serious log messages.
`informational`	Displays informational log messages.

Figure 29 shows the output of the `show logging`#sort-reverse command.

Figure 29 `show logging sort-reverse` command output



```
BS470_48#show logging sort-reverse
Type Time                    Idx  Src Message
---- ----------------------- ---- --- -------
I    2003-10-27 20:52:00 GMT 59       Successful connection from IP address: 13
4.177.118.66, access mode: no security
I    2003-10-27 20:48:51 GMT 58       Inactivity logout, IP address: 134.177.11
8.66, access mode: no security
I    2003-10-27 20:26:03 GMT 57       Authentication Failure Trap
I    2003-10-27 20:25:03 GMT 56       Authentication Failure Trap
I    2003-10-27 20:24:03 GMT 55       Authentication Failure Trap
I    2003-10-27 20:23:03 GMT 54       Authentication Failure Trap
I    2003-10-27 20:16:00 GMT 53       Successful connection from IP address: 13
4.177.118.66, access mode: no security
I    2003-10-27 19:32:06 GMT 52       SNTP: First synchronization successful.
I    2003-10-27 19:29:29 GMT 51       Authentication Failure Trap
I    2003-10-27 19:29:25 GMT 50       Authentication Failure Trap
I    2003-10-27 19:29:22 GMT 49       Authentication Failure Trap
```

logging

The logging command configures the system settings for the system event log of the BayStack 470-24T switch. The syntax for the logging command is:

```
logging [enable|disable]
[level critical|serious|informational]
[nv-level critical|serious|informational|none]
```

The logging command is in the config command mode.

Table 51 describes the parameters and variables for the logging command.

Table 51 logging command parameters and variables

Parameters and variables	Description
enable|disable	Enables or disables the event log (default is enabled).
level critical|serious|informational	Specifies the level of logging stored in DRAM.
nv-level critical|serious|informational|none	Specifies the level of logging stored in non-volatile memory (NVRAM).

no logging

The no logging command disables the BayStack 470-24T system event log. The syntax for the no logging command is:

```
no logging
```

The no logging command is in the config command mode.

The no logging command has no parameters or variables.

set logging

The set logging command configures the system settings of the system event log for the BayStack 470-48T switch or BayStack 460-24T switch. The syntax for the set logging command is:

```
set logging [enable|disable] [level
critical|serious|informational] [nv-level
critical|serious|informational|none]
```

The set logging command is in the config command mode.

Table 52 describes the parameters and variables for the set logging command.

Table 52 set logging command parameters and variables

Parameters and variables	Description
enable|disable	Enables or disables the event log (default is enabled).
level critical|serious|informational	Specifies the level of logging stored in DRAM.
nv-level critical|serious|informational|none	Specifies the level of logging stored in NVRAM.

no set logging

The no set logging command disables the BayStack 470-48T or the BayStack 460-24T system event log. The syntax for the no set logging command is:

```
no set logging
```

The no set logging command is in the config command mode.

The no set logging command has no parameters or variables.

default logging

The `default logging` command configures the system settings as the factory default settings for the BayStack 470-24T system event log. The syntax for the `default logging` command is:

```
default logging
```

The `default logging` command is in the config command mode.

The `default logging` command has no parameters or variables, default set logging

default set logging

The `default set logging` command configures the system settings as the factory default settings for the BayStack 470-48T or the BayStack 460-24T system event log. The syntax for the `default set logging` command is:

```
default set logging
```

The `default set logging` command is in the config command mode.

The `default set logging` command has no parameters or variables.

clear logging command

The `clear logging` command clears all log messages in DRAM. The syntax for the `clear logging` command is:

```
clear logging [nv]
```

The `clear logging` command is in the privExec command mode.

Table 53 shows the parameters and values for the `clear logging` command.

Table 53 clear logging command parameters and values

Parameters and values	Description
`nv`	Clears all log messages in both DRAM and non-volatile memory (NVRAM).

Setting the default management system

The `cmd-interface` command allows you to set the default management interface when you use the console port or Telnet.

The syntax for the `cmd-interface` command is:

```
cmd-interface [cli|menu]
```

The `cmd-interface` command is in the privExec command mode.

Displaying the ARP table

The `show arp-table` command displays the arp table of the device. The syntax for the `show arp-table` command is:

```
show arp-table
```

The `show arp-table` command is in the exec command mode.

The `show arp-table` command has no parameters or variables.

Figure 30 displays a sample output of the `show arp-table` command.

Figure 30 `show arp-table` command output

```
BS470_24#show arp-table
Port IP Address      MAC Address
---- --------------- -----------------
24   10.30.40.1      00:00:A2:0B:3D:45
```

Displaying interfaces

You can view the status of all interfaces on the switch, including MultiLink Trunk membership, link status, autonegotiation, and speed.

show interfaces command

The `show interfaces` command displays the current configuration and status of all interfaces. The syntax for the `show interfaces` command is:

`show interfaces [names] [<`*`portlist`*`>]`

The `show interfaces` command is in the exec command mode.

Table 54 describes the parameters and variables for the `show interfaces` command.

Table 54 show interfaces command parameters and variables

Parameters and variables	Description

`names`
`<`*`portlist`*`>`
	Displays the interface names; enter specific ports if you want to see only those.

Figure 31 displays a sample output of the `show interfaces names` command.

Figure 31 `show interfaces names` command output

```
BS470_24 SW 3.0 in SC2-02 LAB>show interfaces names 1-3
Port Name
---- ----------------------------------------------------------------
1     LabBldg4
2     Testing
3     Floor1Bldg2
```

Figure 32 displays a sample output of the `show interfaces` command without the names variable.

Figure 32 `show interfaces` command output

```
BayStack 470 3.0#show interfaces
              Status                           Auto                        Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation Speed    Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
1          Enable  Down Down Enabled  Enabled
2          Enable  Down Down Enabled  Enabled
3          Enable  Down Down Enabled  Enabled
4          Enable  Down Down Enabled  Enabled
5          Enable  Down Down Enabled  Enabled
6          Enable  Down Down Enabled  Enabled
7          Enable  Down Down Enabled  Enabled
8          Enable  Down Down Enabled  Enabled
9          Enable  Down Down Enabled  Enabled
10         Enable  Down Down Enabled  Enabled
11         Enable  Down Down Enabled  Enabled
12         Enable  Down Down Enabled  Enabled
13         Enable  Down Down Enabled  Enabled
14         Enable  Up   Up   Enabled  Enabled     10M
15         Enable  Down Down Enabled  Enabled
16         Enable  Down Down Enabled  Enabled
17         Enable  Down Down Enabled  Enabled
18         Enable  Down Down Enabled  Enabled
19         Enable  Down Down Enabled  Enabled
--More--
```

Show cmd-interface command

The `show cmd-interface` command displays the current default interface. The syntax for the `show cmd-interface` command is:

```
show cmd-interface
```

Figure 33 displays a sample output of the `show cmd-interface` command.

Figure 33 `show cmd-interface` command output

```
-- ---------------------------------------------------------
BS460_24T_PWR#show cmd-interface
Default interface: Menu
BS460_24T_PWR#
```

Displaying unit uptime

You can display the uptime for each unit in a stack. Unit stack uptime collects the stack uptime for each unit in a stack and reports this information when requested. This allows you to determine how long each unit has been connected to the stack. You must use the Nortel Networks Command Line Interface (NNCLI) commands system to display the unit uptimes.

The `show stack-info uptime` command displays the uptime for all units in the stack.

The syntax for the `show stack-info uptime` command is:

```
show stack-info uptime
```

The `show stack-info uptime` command is in the privExec command mode.

The `show stack-info uptime` command has no parameters or variables.

Figure 34 displays sample output from the `show stack-info uptime` command.

Figure 34 `show stack-info uptime` command output

```
BS470_24T#show stack-info uptime
Unit# Switch Model     Unit UpTime
----- ---------------- --------------------
1     BayStack 470-24T 4 days, 21:38:46
2     BayStack 470-24T 4 days, 21:38:46
3     BayStack 470-24T 4 days, 21:38:46
4     BayStack 470-24T 4 days, 21:38:46
5     BayStack 470-24T 4 days, 21:38:44
6     BayStack 470-24T 4 days, 21:38:46
```

Displaying port statistics

You can display the statistics for a port for both received and transmitted traffic. This section covers:

- "show port-statistics command ", next
- "clear-stats command" on page 133

show port-statistics command

The `show port-statistics` command displays the statistics for the port on both received and transmitted traffic. The syntax for the `show port-statistics` command is:

`show port-statistics [port <`*`portlist`*`>]`

The `show port-statistics` command is in the config-if command mode.

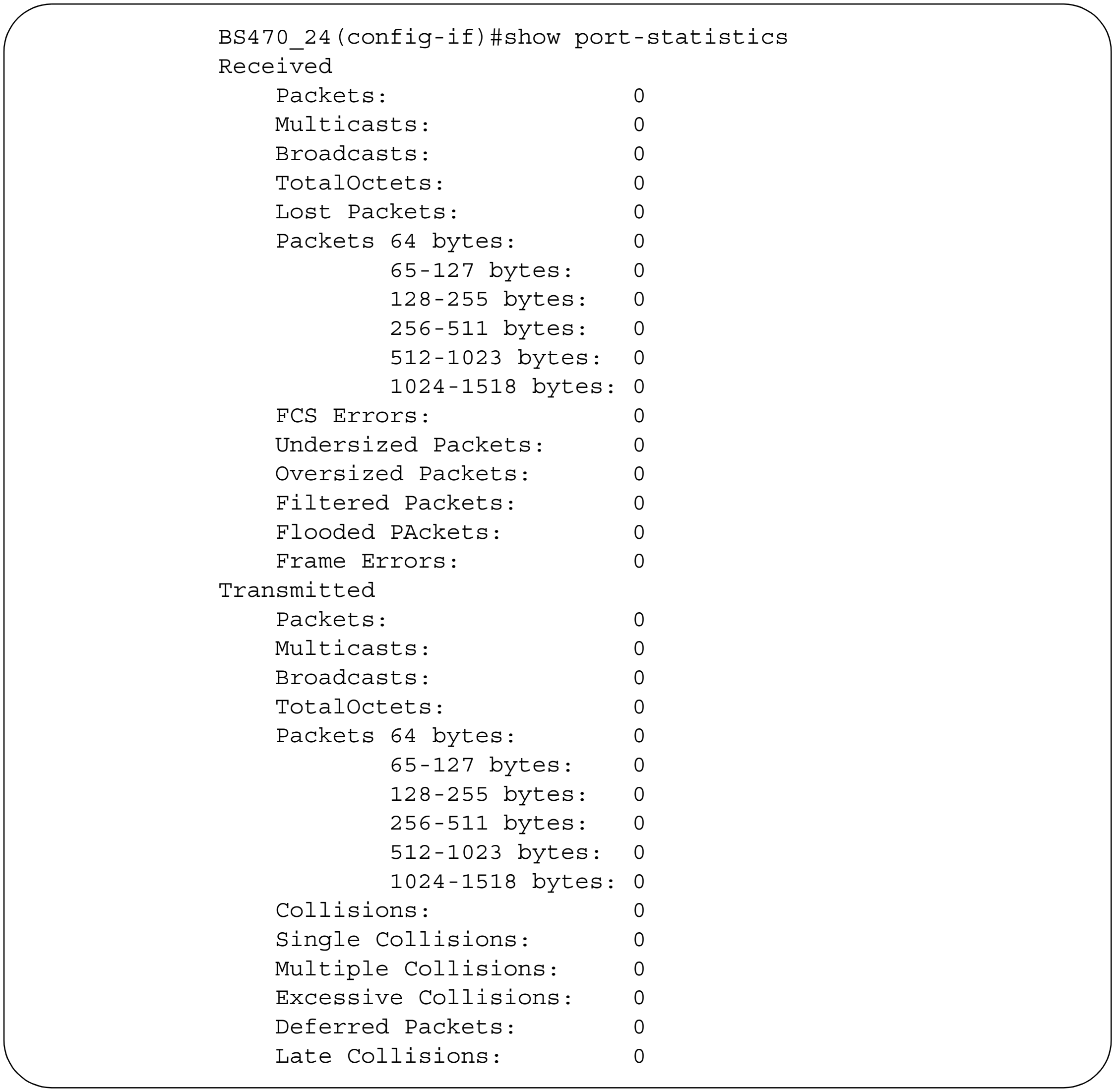
Table 55 describes the parameters and variables for the `show port-statistics` command.

Table 55 show port-statistics command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to configure to display statistics on; enter the port numbers. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Figure 35 displays sample output from the `show port-statistics` command.

Figure 35 `show port-statistics` command output



```
BS470_24(config-if)#show port-statistics
Received
    Packets:                 0
    Multicasts:              0
    Broadcasts:              0
    TotalOctets:             0
    Lost Packets:            0
    Packets 64 bytes:        0
            65-127 bytes:    0
            128-255 bytes:   0
            256-511 bytes:   0
            512-1023 bytes:  0
            1024-1518 bytes: 0
    FCS Errors:              0
    Undersized Packets:      0
    Oversized Packets:       0
    Filtered Packets:        0
    Flooded PAckets:         0
    Frame Errors:            0
Transmitted
    Packets:                 0
    Multicasts:              0
    Broadcasts:              0
    TotalOctets:             0
    Packets 64 bytes:        0
            65-127 bytes:    0
            128-255 bytes:   0
            256-511 bytes:   0
            512-1023 bytes:  0
            1024-1518 bytes: 0
    Collisions:              0
    Single Collisions:       0
    Multiple Collisions:     0
    Excessive Collisions:    0
    Deferred Packets:        0
    Late Collisions:         0
```

clear-stats command

The `clear-stats command` clears all statistical information for the specified port. All counters are set to zero (0). The syntax for the `clear-stats` command is:

```
clear-stats [port <portlist>]
```

The `clear-stats` command is in the config-if command mode.

Table 56 describes the parameters and variables for the `clear-stats` command.

Table 56 clear-stats command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to clear of statistical information; enter the port numbers. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Enabling and disabling autosave

You can enable or disable the autosave feature of your unit. Autosave automatically saves your configuration information across reboots. This section covers these commands:

- “show autosave command ”, next
- “autosave enable command” on page 135
- “no autosave enable command” on page 135
- “default autosave enable command” on page 136

Note: You can use the CLI command `copy config nvram` to force a manual save of the configuration when autosave is disabled.

show autosave command

The `show autosave` command displays the status of the autosave feature, either enabled or disabled. The syntax for the `show autosave` command is:

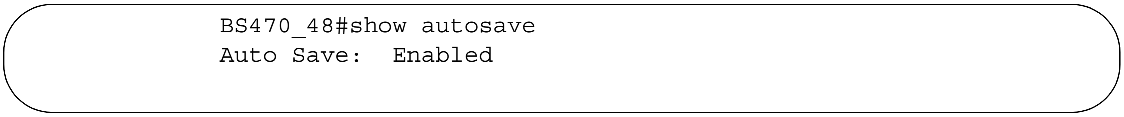
```
show autosave
```

The `show autosave` command is in the privExec command mode.

The `show autosave` command has no parameters or variables.

Figure 36 displays sample output from the `show autosave` command.

Figure 36 `show autosave` command output



```
BS470_48#show autosave
Auto Save:  Enabled
```

autosave enable command

The `autosave enable` command enables the autosave feature. The syntax for the `autosave enable` command is:

```
autosave enable
```

The `autosave enable` command is in the config command mode.

The `autosave enable` command has no parameters or variables.

no autosave enable command

The `no autosave enable` command disables the autosave feature. The syntax for the `no autosave enable` command is:

```
no autosave enable
```

The `no autosave enable` command is in the config command mode.

The `no autosave enable` command has no parameters or variables.

default autosave enable command

The `default autosave enable` command defaults the autosave feature to the default value of enabled. The syntax for the `default autosave enable` command is:

```
default autosave enable
```

The `default autosave enable` command is in the config command mode.

The `default autosave enable` command has no parameters or variables.

Setting time on network elements using Simple Network Time Protocol (SNTP)

The Simple Network Time Protocol (SNTP) feature synchronizes the Universal Coordinated Time (UCT) to an accuracy within 1 second. This feature adheres to the IEEE RFC 2030 (MIB is the s5agent). With this feature, the system can obtain the time from any RFC 2030-compliant NTP/SNTP server.

➡ **Note:** If you have trouble using this feature, try various NTP servers. Some NTP servers may be overloaded or currently inoperable.

- "show sntp command ", next
- "show sys-info command" on page 137
- "sntp enable command" on page 138
- "no sntp enable command" on page 139
- "sntp server primary address command" on page 139
- "sntp server secondary address command" on page 140
- "no sntp server command" on page 140
- "sntp sync-now command" on page 141
- "sntp sync-interval command" on page 141

show sntp command

The `show sntp` command displays the SNTP information, as well as the configured NTP servers. The syntax for the `show sntp` command is:

```
show sntp
```

The `show sntp` command is in the privExec command mode.

The `show sntp` command has no parameters or variables.

Figure 37 displays sample output from the `show sntp` command.

Figure 37 `show sntp` command output

```
BS470_48#show sntp
SNTP Status:                    Enabled
Primary server address:         47.82.2.10
Secondary server address:       47.81.2.10
Sync interval:                  24 hours
Last sync source:               47.82.2.10
Primary server sync failures:   0
Secondary server sync failures: 0
Last sync time:                 2003-10-27 19:32:17 GMT
Next sync time:                 2003-10-28 19:32:17 GMT
Current time:                   2003-10-27 19:47:35 GMT
```

show sys-info command

The `show sys-info` command displays the current system characteristics.

Note: You must have SNTP enabled and configured to display GMT time.

The syntax for the `show sys-info` command is:

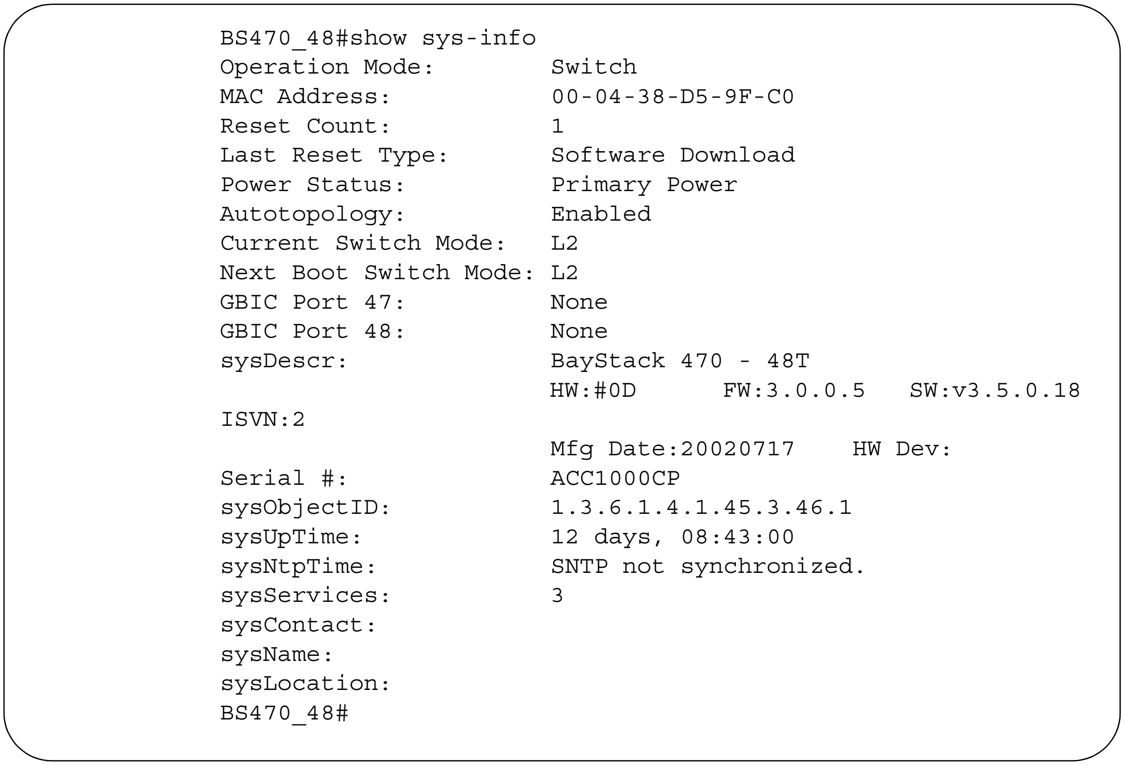
```
show sys-info
```

The `show sys-info` command is in the privExec command mode.

The `show sys-info` command has no parameters or variables.

Figure 38 displays sample output from the `show sys-info` command.

Figure 38 `show sys-info` command output



```
BS470_48#show sys-info
Operation Mode:        Switch
MAC Address:           00-04-38-D5-9F-C0
Reset Count:           1
Last Reset Type:       Software Download
Power Status:          Primary Power
Autotopology:          Enabled
Current Switch Mode:   L2
Next Boot Switch Mode: L2
GBIC Port 47:          None
GBIC Port 48:          None
sysDescr:              BayStack 470 - 48T
                       HW:#0D      FW:3.0.0.5   SW:v3.5.0.18
ISVN:2
                       Mfg Date:20020717    HW Dev:
Serial #:              ACC1000CP
sysObjectID:           1.3.6.1.4.1.45.3.46.1
sysUpTime:             12 days, 08:43:00
sysNtpTime:            SNTP not synchronized.
sysServices:           3
sysContact:
sysName:
sysLocation:
BS470_48#
```

sntp enable command

Note: The default setting for SNTP is disabled.

The `sntp enable` command enables SNTP. The syntax for the `sntp enable` command is:

```
sntp enable
```

The `sntp enable` command is in the config command mode.

The `sntp enable` command has no parameters or variables.

no sntp enable command

The `no sntp enable` command disables SNTP. The syntax for the `no sntp enable` command is:

```
no sntp enable
```

The `no sntp enable` command is in the config command mode.

The `no sntp enable` command has no parameters or variables.

sntp server primary address command

The `sntp server primary address` command specifies the IP addresses of the primary NTP server. The syntax for the `sntp server primary address` command is:

```
sntp server primary address <A.B.C.D>
```

The `sntp server primary address` command is in the config command mode.

Table 57 describes the parameters and variables for the `sntp server primary address` command.

Table 57 `sntp server primary address` command parameters and variables

Parameters and variables	**Description**
<A.B.C.D>	Enter the IP address of the primary NTP server.

The default is 0.0.0.0.

sntp server secondary address command

The `sntp server secondary address` command specifies the IP addresses of the secondary NTP server. The syntax for the `sntp server secondary address` command is:

```
sntp server secondary address <A.B.C.D>
```

The `sntp server secondary address` command is in the config command mode.

Table 58 describes the parameters and variables for the `sntp server secondary address` command.

Table 58 `sntp server secondary address` command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of the secondary NTP server.

The default is 0.0.0.0.

no sntp server command

The `no sntp server` command clears the NTP server IP addresses. The syntax for the `no sntp server` command is:

```
no sntp server <primary|secondary>
```

The `no sntp server` command is in the config command mode.

Table 59 describes the parameters and variables for the `no sntp server` command.

Table 59 `no sntp server` command parameters and variables

Parameters and variables	Description
<primary|secondary>	Enter the NTP server you want to clear: • primary—clears the IP address for the primary NTP server • secondary—clears the IP address for the secondary NTP server

sntp sync-now command

The `sntp sync-now` command forces a manual synchronization with the NTP server.

Note: You must have SNTP enabled before this command can take effect.

The syntax for the `sntp sync-now` command is:

```
sntp sync-now
```

The `sntp sync-now` command is in the config command mode.

The `no sntp sync-now` command has no parameters or variables.

sntp sync-interval command

The `sntp sync-interval` command specifies recurring synchronization with the NTP server in hours relative to initial synchronization. The syntax for the `sntp sync-interval` command is:

```
sntp sync-interval <0-168>
```

The `sntp sync-interval` command is in the config command mode.

Table 60 describes the parameters and variables for the `sntp sync-interval` command.

Table 60 `sntp sync-interval` command parameters and variables

Parameters and variables	Description
<0-168>	Enter the number of hours you want for periodic synchronization with the NTP server. NOTE: 0 is boot-time only, and 168 is once a week; the default value is 24 hours.

Enabling remote login

This feature provides an enhanced level of logging by replicating system messages onto a syslog server. System log messages from several switches can be collected at a central location, which alleviates the network manager querying each switch individually to interrogate the log files. This section covers the following commands:

- "show logging ", next
- "logging remote enable command" on page 144
- "no logging remote enable command" on page 144
- "logging remote address command" on page 145
- "no logging remote address command" on page 145
- "logging remote level command" on page 146
- "no logging remote level command" on page 146
- "default logging remote level command" on page 147

show logging

The `show logging` command displays the configuration and the current contents of the system event log. The syntax for the `show logging` command is:

```
show logging [config] [critical] [informational] [serious]
[sort-reverse]
```

The show logging command is in the privExec command mode.

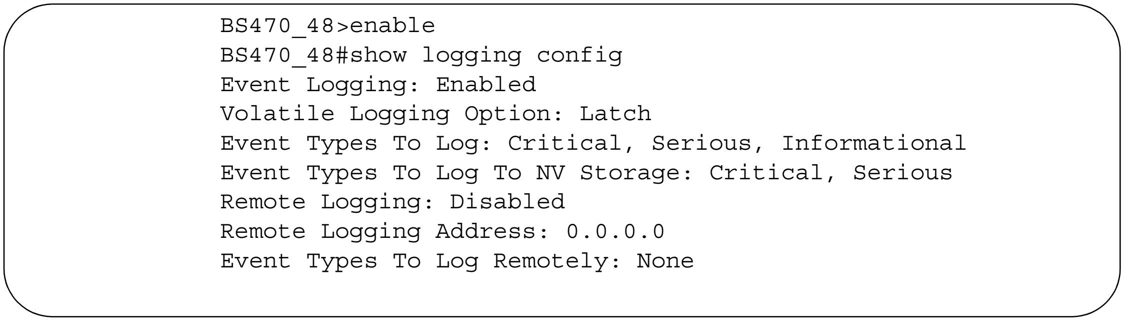
Table 61 describes the parameters and variables for the show logging command.

Table 61 show logging command parameters and variables

Parameters and variables	Description
config	Displays the configuration of event logging.
critical	Displays critical log messages.
informational	Displays informational log messages.
serious	Displays serious log messages.
sort-reverse	Displays log messages in reverse chronological order (beginning with most recent).

Figure 39 shows the output of the show logging config command.

Figure 39 `show logging config` command output



```
BS470_48>enable
BS470_48#show logging config
Event Logging: Enabled
Volatile Logging Option: Latch
Event Types To Log: Critical, Serious, Informational
Event Types To Log To NV Storage: Critical, Serious
Remote Logging: Disabled
Remote Logging Address: 0.0.0.0
Event Types To Log Remotely: None
```

logging remote enable command

Note: The default value for remote logging is disabled

The `logging remote enable` command enables logging syslog messages to a remote server. The syntax for the `remote logging enable` command is:

```
logging remote enable
```

The `logging remote enable` command is in the config command mode.

The `logging remote enable` command has no parameters or variables.

no logging remote enable command

The `no logging remote enable` command disables sending syslog messages to a remote server. The syntax for the `no logging remote enable` command is:

```
no logging remote enable
```

The `no remote logging enable` command is in the config command mode.

The `no remote logging enable` command has no parameters or variables.

logging remote address command

The `logging remote address` command sets the remote server for receiving the syslog messages; you enter the IP address of the server you want. The syntax for the `logging remote address` command is:

```
logging remote address <A.B.C.D>
```

The `logging remote address` command is in the config command mode.

Table 62 describes the parameters and variables for the `logging remote address` command.

Table 62 `logging remote address` command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Specifies the IP address of the remote server in dotted-decimal notation.

The default address is 0.0.0.0.

no logging remote address command

The `no logging remote address` command clears the IP address of the remote server. The syntax for the `no logging remote address` command is:

```
no logging remote address
```

The `no logging remote address` command is in the config command mode.

The `no logging remote address` command has no parameters or variables.

logging remote level command

The `logging remote level` command sets the severity level of the logs you send to the remote server. The syntax for the `logging remote level` command is:

```
logging remote level {critical|informational|serious}
```

The `logging remote level` command is in the config command mode.

Table 63 describes the parameters and variables for the `logging remote level` command.

Table 63 `logging remote level` command parameters and variables

Parameters and variables	Description
{criticallseriousl informational}	Specifies the severity level of the log messages to be sent to the remote server: • critical • informational • serious

There is no default value for this command.

no logging remote level command

The `no logging remote level` command removes any severity level of the log messages that you send to the remote server; it reverts to None. The syntax for the `no logging remote level` command is:

```
no logging remote level
```

The `no logging remote level` command is in the config command mode.

The `no logging remote level` command has no parameters or variables.

default logging remote level command

The default logging remote level command sets the severity level of the logs you send to the remote server to the default value, which is None. The syntax for the default logging remote level command is:

```
default logging remote level
```

The default logging remote level command is in the config command mode.

The default logging remote level command has no parameters or variables.

Copper GBIC support

A new full-sized GBIC is supported. This GBIC supports 1000BaseT and works only on BayStack 470 units.

Enabling traffic separation

You can separate traffic on the network such that IP packets are forwarded to a pre-defined CDN port using the traffic separation mode. Enabling this feature also ensures that both control and data PPPoE packets are forwarded to a pre-defined ISP port.

To enable traffic separation, use the following command:

```
config switch mode <l2|traffic-separation>
```

The config switch mode command is in the privExec command mode.

Table 64 describes the parameters and variables for the `config switch mode` command.

Table 64 `config switch mode` command parameters and variables

Parameters and values	Description
`<l2|traffic-separation>`	Enter traffic-separation to enable the traffic separation feature.

Default traffic-separation restrict

This command sets the mode for traffic separation restrict to Layer3 restriction, The user will not be allowed to create new L3 policies. This command is similar to the `traffic-separation restrict` command.

This command can be executed in the Global Configuration mode and there are no parameters associated with this command.

No traffic-separation restrict

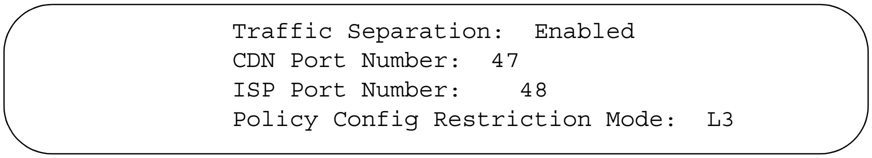
This command sets the mode for traffic separation restrict, to no restriction. The user is allowed to create all types of L3 policies.There are no restrictions on creation of policies.

This command can be executed in the Global Configuration mode and has no associated parameters.

show traffic-separation

This command displays the current traffic separation settings, including the traffic separation restrict mode. Figure 40 shows the output of this command.

Figure 40 `show traffic restriction` command output



```
Traffic Separation:  Enabled
CDN Port Number:  47
ISP Port Number:    48
Policy Config Restriction Mode:  L3
```

Saving the configuration to NVRAM

You can save your configuration parameters to Non-Volatile RAM (NVRAM) using the CLI. This section covers the following topic:

- “copy config nvram ”, next

copy config nvram

The `copy config nvram` copies the current configuration to NVRAM. The syntax for the `copy config nvram` command is:

```
copy config nvram
```

The `copy config nvram` command is in the privExec command mode.

The `copy config nvram` command has no parameters or variables.

➡ **Note:** The system automatically issues the `copy config nvram` command periodically.

Trap notification when configuration changes are saved to NVRAM

When configuration changes are written to non-volatile memory, a trap (bsnConfigurationSavedToNvram) is sent to the trap receiver indicating that a change has occurred to the configuration of the device. This trap will also appear as an event in the volatile system log.

For each standalone and stack configuration, you need to configure a trap destination. Use the following CLI commands.

snmp-server community trap notify-view snmpv1Objs command

snmp-server host <a.b.c.d> v1 trap command

Replacing a unit

Unit Replacement allows you to upgrade a standalone unit with the configuration of the inactive unit off-line, before adding it to the stack. This is also called a staging operation.

It also allows you to retrieve a single unit configuration from a binary configuration file of a stack. The unit can then be inserted into the stack without requiring a reboot of the entire stack.

You can replace a unit in the stack using the following commands:

- "Copy tftp config unit command ", next
- "stack replace unit command" on page 151

Copy tftp config unit command

The `copy tftp config unit` command downloads the configuration of the unit you wish to replace, to a replacement unit. Use this command in standalone mode. The syntax for the `copy tftp config unit` command is:

```
copy tftp config unit <unit #>
```

The `copy tftp config unit` command is in the privExec command mode.

Table 65 describes the parameters and variables for the `copy tftp config unit` command.

Table 65 `copy tftp config unit` command parameters and variables

Parameters and variables	Description
`<unit #>`	Enter the number of the unit you want to replace.

stack replace unit command

The `stack replace unit` command prepares the stack to receive the replacement unit. Use this command in stack mode. The syntax for the `stack replace unit` command is:

```
stack replace unit <1-8>
```

The `stack replace unit` command is in the privExec command mode.

Table 66 describes the parameters and variables for the `stack replace unit` command.

Table 66 `stack replace unit` command parameters and variables

Parameters and variables	Description
`<1-8>`	Enter the number of the replacement unit.

Chapter 3
Network Management

This chapter includes information about the RMON, SNMP, configuring the port-mirroring and enabling autotopology.

This chapter covers the following topics:

- "RMON ", next
- "SNMP" on page 154
- "Using port-mirroring" on page 154
- "Enabling Autotopology" on page 157

For more information on port-mirroring, as well as configuration directions using the console interface (CI) menu, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

For more information on configuring these features using the Web-based management system, refer to *Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

For more information on configuring these features using the Device Manager, refer to *Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

RMON

You can set and display the RMON parameters for alarms, events, history, and statistics using the NNCLI command.

For more information on the NNCLI commands, see "Configuring remote network monitoring (RMON)" on page 113.

SNMP

You can set various SNMP parameters and traps, as well as disable SNMP traps using the NNCLI command.

For more information on the NNCLI commands, see "Setting SNMP parameters" on page 109.

Using port-mirroring

Note: For guidelines to port-mirroring, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

You use port-mirroring to monitor traffic. This section covers the following commands:

- "show port-mirroring command ", next
- "port-mirroring command" on page 155
- "no port-mirroring command" on page 157

show port-mirroring command

The `show port-mirroring` command displays the port-mirroring configuration. The syntax for the `show port-mirroring` command is:

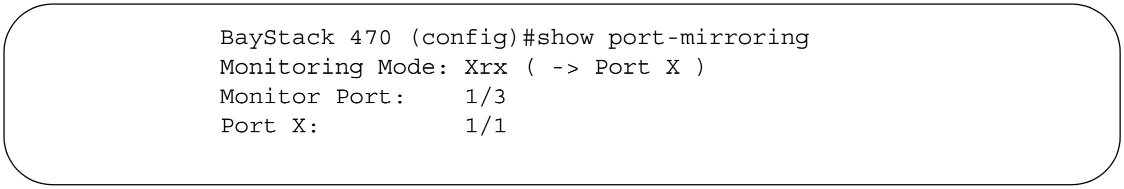
```
show port-mirroring
```

The `show port-mirroring` command is in the privExec command mode.

The `show port-mirroring` command has no parameters or variables.

Figure 41 displays sample output from the `show port-mirroring` command.

Figure 41 `show port-mirroring` command output



```
BayStack 470 (config)#show port-mirroring
Monitoring Mode: Xrx ( -> Port X )
Monitor Port:    1/3
Port X:          1/1
```

port-mirroring command

The `port-mirroring` command sets the port-mirroring configuration. The syntax of the `port-mirroring` command is:

```
port-mirroring mode
{disable |
Xrx monitor-port <portlist> mirror-port-X <portlist>|
Xtx monitor-port <portlist> mirror-port-X <portlist>|
XrxOrXtx monitor-port <portlist>
mirror-port-X <portlist> mirror-port-Y <portlist>|
XrxOrYtx monitor-port <portlist>
mirror-port-X <portlist> mirror-port-Y <portlist>|
XrxYtx monitor-port <portlist>
mirror-port-X <portlist> mirror-port-Y <portlist>|
XrxYtxOrYrxXtx monitor-port <portlist>
mirror-port-X <portlist> mirror-port-Y <portlist>|
Asrc monitor-port <portlist> mirror-MAC-A <macaddr>|
Adst monitor-port <portlist> mirror-MAC-A <macaddr>|
AsrcOrAdst monitor-port <portlist>
mirror-MAC-A <macaddr>|
AsrcBdst monitor-port <portlist>
mirror-MAC-A <macaddr> mirror-MAC-B <macaddr>|
AsrcBdstOrBsrcAdst monitor-port <portlist>
mirror-MAC-A <macaddr> mirror-MAC-B <macaddr>}
```

Note: In this command, *`portlist`* must specify only a single port

The `port-mirroring` command is in the config command mode.

Table 67 describes the parameters and variables for the `port-mirroring` command.

Table 67 `port-mirroring` command parameters and variables

Parameters and variables	Description
`disable`	Disables port-mirroring.
`monitor-port`	Specifies the monitor port.
`mirror-port-X`	Specifies the mirroring port X.
`mirror-port-Y`	Specifies the mirroring port Y.
`mirror-MAC-A`	Specifies the mirroring MAC address A.
`mirror-MAC-B`	Specifies the mirroring MAC address B.
`portlist`	Enter the port numbers.
`Xrx`	Mirror packets received on port X.
`Xtx`	Mirror packets transmitted on port X.
`XrxOrXtx`	Mirror packets received or transmitted on port X.
`XrxYtx`	Mirror packets received on port X and transmitted on port Y. Note: Do not use this mode for mirroring broadcast and multicast traffic.
`XrxYtxOrXtxYrx`	Mirror packets received on port X and transmitted on port Y or packets received on port Y and transmitted on port X. Note: Do not use this mode for mirroring broadcast and multicast traffic.
`macaddr`	Enter the MAC address in format H.H.H.
`Asrc`	Mirror packets with source MAC address A.
`Adst`	Mirror packets with destination MAC address A.
`AsrcOrAdst`	Mirror packets with source or destination MAC address A.
`AsrcBdst`	Mirror packets with source MAC address A and destination MAC address B.
`AsrcBdstOrBsrcAdst`	Mirror packets with source MAC address A and destination MAC address B or packets with source MAC address B and destination MAC address A.

no port-mirroring command

The `no port-mirroring` command disables port-mirroring. The syntax of the `no port-mirroring command` is:

```
no port-mirroring
```

The `no port-mirroring` command is in the config command mode.

The `no port-mirroring` command has no parameters or variables.

Enabling Autotopology

You can enable the Optivity* Autotopology* protocol using the CLI. Refer to the www.nortelnetworks.com/documentation URL for information on Autotopology. (The product family for Optivity and Autotopology is Data and Internet.). This section covers the following commands:

- "autotopology command ", next
- "no autotopology command" on page 158
- "default autotopology command" on page 158
- "show autotopology settings" on page 158
- "show autotopology nmm-table" on page 159

autotopology command

The `autotopology` command enables the Autotopology protocol. The syntax for the `autotopology` command is:

```
autotopology
```

The `autotopology` command is in the config command mode.

The `autotopology` command has no parameters or variables.

no autotopology command

The `no autotopology` command disables the Autotopology protocol. The syntax for the `no autotopology` command is:

```
no autotopology
```

The `no autotopology` command is in the config command mode.

The `no autotopology` command has no parameters or variables.

default autotopology command

The `default autotopology` command enables the Autotopology protocol. The syntax for the `default autotopology` command is:

```
default autotopology
```

The `default autotopology` command is in the config command mode.

The `default autotopology` command has no parameters or variables.

show autotopology settings

The `show autotopology settings` command displays information on the Autotopology configuration. The syntax for the `show autotopology settings` command is:

```
show autotopology settings
```

The `show autotopology settings` command is in the privExec mode.

The `show autotopology settings` command has no parameters or variables. Figure 42 displays a sample output of the `show autotopology settings` command.

Figure 42 `show autotopology settings` command output

```
BS470_24#show autotopology settings
Autotopology:  Enabled
Last NMM Table Change:  4578
Maximum NMM Table Entries:  100
Current NMM Table Entries:  1
```

show autotopology nmm-table

The `show autotopology nmm-table` command displays information about the network management module (NMM) table. The syntax for the `show autotopology nmm-table` command is:

```
show autotopology nmm-table
```

The `show autotopology nmm-table` command is in the privExec mode.

The `show autotopology nmm-table` command has no parameters or variables.

Figure 43 displays a sample output of the `show autotopology nmm-table` command.

Figure 43 `show autotopology nmm-table` command output

```
BS470_48#show autotopology nmm-table
LSlot                                                                    RSlot
LPort IP Addr          Seg ID   MAC Addr     Chassis Type     BT LS   CS   RPort
----- --------------- -------- ------------ ---------------- -- --- ----  ---
 0/ 0 134.177.150.80  0x000000 000438D59FC1 BayStack 470     12 Yes HTBT    NA
 1/ 1 134.177.150.6   0x000108 000F6A7DC121 BayStack 425-48T 12 Yes HTBT   1/ 8
 1/ 1 134.177.150.79  0x000101 000997291F01 BayStack 460-24T-PWR 12 Yes HTBT
1/ 1
BS470_48#
```

Chapter 4
Using security in your system

This chapter describes the security commands available with the CLI. This chapter covers the following topics:

- "Securing your system ", next
- "Securing your network" on page 207

For more information on these security features, as well as using the console interface (CI) menus, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

For more information on configuring these security features using the Web-based management system, refer to *Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

For more information on configuring these security features using the Device Manager, refer to *Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

Securing your system

You can secure your system using the following CLI commands.

- "Setting the CLI password ", next
- "Configuring the IP manager list" on page 163
- "Changing the http port number" on page 168
- "Setting Telnet access" on page 170
- "Configuring Secure Shell (SSH)" on page 173
- "Enabling or disabling the server for Web-based management" on page 182

- "Configuring SNMPv3" on page 183
- "Configuring the RADIUS-based management password authentication" on page 204

Setting the CLI password

You can set passwords using the `cli password` command for selected types of access using the CLI, Telnet, or RADIUS security.

For more information on Telnet access, refer to "Setting Telnet access" on page 170. For more information on using RADIUS security with the CLI, refer to "Configuring the RADIUS-based management password authentication" on page 204.

cli password command

The `cli password` is in two forms and performs the following functions for either the switch or the entire stack:

- Changes the password for access through the serial console port and Telnet
- Specifies changing the password for serial console port or Telnet access and whether to authenticate password locally or with the RADIUS server

The syntax for the `cli password` commands are:

```
cli password {switch|stack} {ro|rw} <WORD> <WORD>
```

```
cli password {switch|stack} {serial|telnet}
{none|local|radius}
```

The `cli password` command is in the config command mode.

Table 68 describes the parameters and variables for the `cli password` command.

Table 68 cli password command parameters and variables

Parameters and variables	**Description**
`switch|stack`	Specifies you are modifying the settings on the switch or stack. Note: If you omit this parameter, the system modifies the information for the current mode.
`ro|rw`	Specifies you are modifying the read-only (ro) password or the read-write (rw) password.
<*WORD*> <*WORD*>	Enter your username for the first variable, and your password for the second variable.
`serial|telnet`	Specifies you are modifying the password for serial console access or for Telnet access.
`none|local|radius`	Specifies the password you are modifying: • `none`—disables the password • `local`—use the locally defined password for serial console or Telnet access • `radius`—use RADIUS authentication for serial console or Telnet access

Configuring the IP manager list

When enabled, the IP manager list determines which source IP addresses are allowed access to the switch. No other source IP addresses have access to the switch. You configure the IP manager list using the following commands:

- "show ipmgr command ", next
- "ipmgr command for management system" on page 165
- "no ipmgr command for management system" on page 166
- "ipmgr command for source IP address" on page 167
- "no ipmgr command for source IP address" on page 168

show ipmgr command

The `show ipmgr` command displays whether Telnet, SNMP, and Web access are enabled; whether the IP manager list is being used to control access to Telnet, SNMP, and the Web-based management system; and the current IP manager list configuration. The syntax for the `show ipmgr` command is:

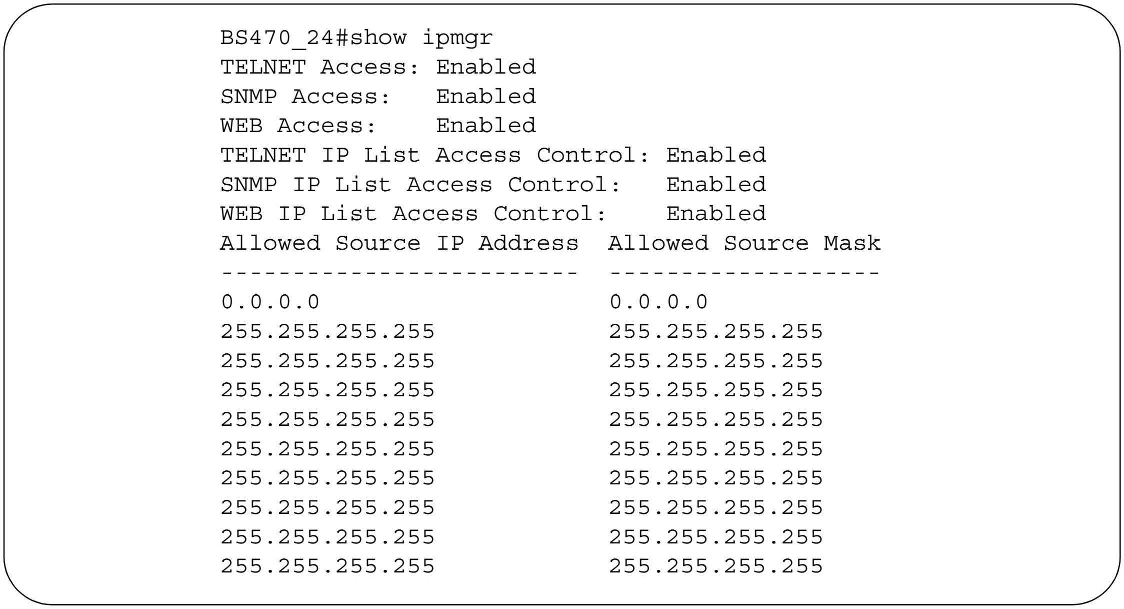
```
show ipmgr
```

The `show ipmgr` command is in the privExec command mode.

The `show ipmgr` command has no parameters or variables.

Figure 44 displays sample output from the `show ipmgr` command.

Figure 44 `show ipmgr` command output



```
BS470_24#show ipmgr
TELNET Access: Enabled
SNMP Access:   Enabled
WEB Access:    Enabled
TELNET IP List Access Control: Enabled
SNMP IP List Access Control:   Enabled
WEB IP List Access Control:    Enabled
Allowed Source IP Address  Allowed Source Mask
-------------------------  -------------------
0.0.0.0                     0.0.0.0
255.255.255.255             255.255.255.255
255.255.255.255             255.255.255.255
255.255.255.255             255.255.255.255
255.255.255.255             255.255.255.255
255.255.255.255             255.255.255.255
255.255.255.255             255.255.255.255
255.255.255.255             255.255.255.255
255.255.255.255             255.255.255.255
255.255.255.255             255.255.255.255
```

ipmgr command for management system

The `ipmgr` command for the management systems enables the IP manager list for Telnet, SNMP, or HTTP access. The syntax for the `ipmgr` command for the management systems is:

```
ipmgr {telnet|snmp|http} [source-ip <1-10> <XXX.XXX.XXX.XXX>
[mask <XXX.XXX.XXX.XXX>]]
```

The `ipmgr` command for the management systems is in the config mode.

Table 69 describes the parameters and variables for the `ipmgr` command.

Table 69 ipmgr command for system management parameters and variables

Parameters and variables	Description
`telnet|snmp|http`	Enables IP manager list checking for access to various management systems: • `telnet`—provides list access using Telnet access • `snmp`—provides list access using SNMP, including the Device Manager • `http`—provides list access using the Web-based management system
`source-ip <1-10> <XXX.XXX.XXX.XXX>`	Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation.
`[mask <XXX.XXX.XXX.XXX>]`	Specifies the subnet mask from which access is allowed; enter IP mask in dotted-decimal notation.

no ipmgr command for management system

The `no ipmgr` command disables the IP manager list for Telnet, SNMP, or HTTP access. The syntax for the `no ipmgr` command for the management systems is:

```
no ipmgr {telnet|snmp|http}
```

The `no ipmgr` command is in the config mode.

Table 70 describes the parameters and variables for the `no ipmgr` command.

Table 70 no ipmgr command for management system

Parameters and variables	Description
`telnet|snmp |http`	Disables IP manager list checking for access to various management systems: • `telnet`—disables list check for Telnet access • `snmp`—disables list check for SNMP, including the Device Manager • `http`—disables list check for the Web-based management system

ipmgr command for source IP address

The `ipmgr` command for source IP addresses allows you to enter the source IP addresses or address ranges that you allow to access the switch or the stack. The syntax for the `ipmgr` command for source IP addresses is:

```
ipmgr {source-ip <1-10> <XXX.XXX.XXX.XXX>
[mask <XXX.XXX.XXX.XXX>]}
```

The `ipmgr` command for the source IP addresses is in the config mode

Table 71 describes the parameters and variables for the `ipmgr` command for the source IP addresses

Table 71 ipmgr command for source IP addresses parameters and variables

Parameters and variables	Description
`source-ip <1-10> <XXX.XXX.XXX.XXX>`	Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation.
`[mask <XXX.XXX.XXX.XXX>]`	Specifies the subnet mask from which access is allowed; enter IP mask in dotted-decimal notation.

no ipmgr command for source IP address

The `no ipmgr` command for source IP addresses disables access for specified source IP addresses or address ranges and denies them access to the switch or the stack. The syntax for the `no ipmgr` command for source IP addresses is:

```
no ipmgr {source-ip [<1-10>]}
```

The `no ipmgr` command for the source IP addresses is in the config mode

Table 72 describes the parameters and variables for the `no ipmgr` command for the source IP addresses.

Table 72 no ipmgr command for source IP addresses parameters and variables

Parameters and variables	Description
`source-ip [<1-10>]`	When you specify an option, it sets the IP address and mask for the specified entry to 255.255.255.255 and 255.255.255.255. When you omit the optional parameter, it resets the list to factory defaults.

Changing the http port number

Beginning with software release 3.1, you can configure the HTTP port. This feature provides enhanced security and network access. The default HTTP port typically used to communicate between the Web client and the server is the well-known port 80. With this feature, you can change the HTTP port.

You can configure this feature using the following commands:

- "show http-port command ", next
- "http-port command" on page 169
- "default http-port" on page 170

show http-port command

The `show http-port` command displays the port number of the HTTP port. The syntax for the `show http-port` command is:

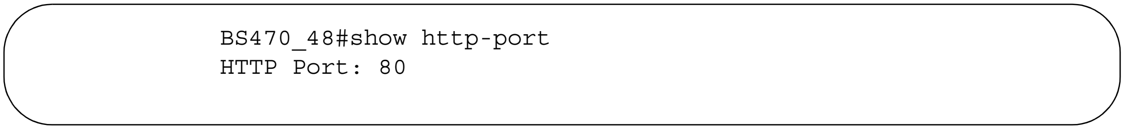
```
show http-port
```

The `show http-port` command is in the privExec command mode.

The `show http-port` command has no parameters or variables.

Figure 45 displays sample output from the `show http-port` command.

Figure 45 `show http-port` command output



```
BS470_48#show http-port
HTTP Port: 80
```

http-port command

The `http-port` command sets the port number for the HTTP port. The syntax for the `http-port` command is:

```
http-port <1024-65535>
```

The `http-port` command is in the config command mode.

Table 73 describes the parameters and variables for the `http-port` command.

Table 73 `http-port` command parameters and variables

Parameters and variables	Description
<1024-65535>	Enter the port number you want to be the HTTP port.

Note: To set the HTTP port to 80, use the `default http-port` command.

The default value for this parameter is port 80.

default http-port

The `default http-port` command sets the port number for the HTTP port to the default value of 80. The syntax for the `default http-port` command is:

```
default http-port
```

The `default http-port` command is in the config command mode.

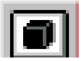
The `default http-port` command has no parameters or variables.

Setting Telnet access

You can also access the CLI through a Telnet session. To access the CLI remotely, the management port must have an assigned IP address and remote access must be enabled. You can log on to the switch using Telnet from a terminal that has access to the switch.

To open a Telnet session from Device Manager, click on the Telnet icon on the toolbar (Figure 46) or click Action > Telnet on the Device Manager toolbar.

Figure 46 Telnet icon on Device Manager toolbar



Note: Multiple users can access the CLI system simultaneously, through the serial port, Telnet, and modems. The maximum number of simultaneous users is four plus one each at the serial port for a maximum of 12 users. All users can configure simultaneously.

You can view the Telnet allowed IP addresses and settings, change the settings, or disable the Telnet connection. This section covers the following topics:

- "show telnet-access command ", next
- "telnet-access command" on page 171
- "no telnet-access command" on page 172
- "default telnet-access command" on page 173

show telnet-access command

The `show telnet-access` command displays the current settings for Telnet access. The syntax for the `show telnet-access` command is:

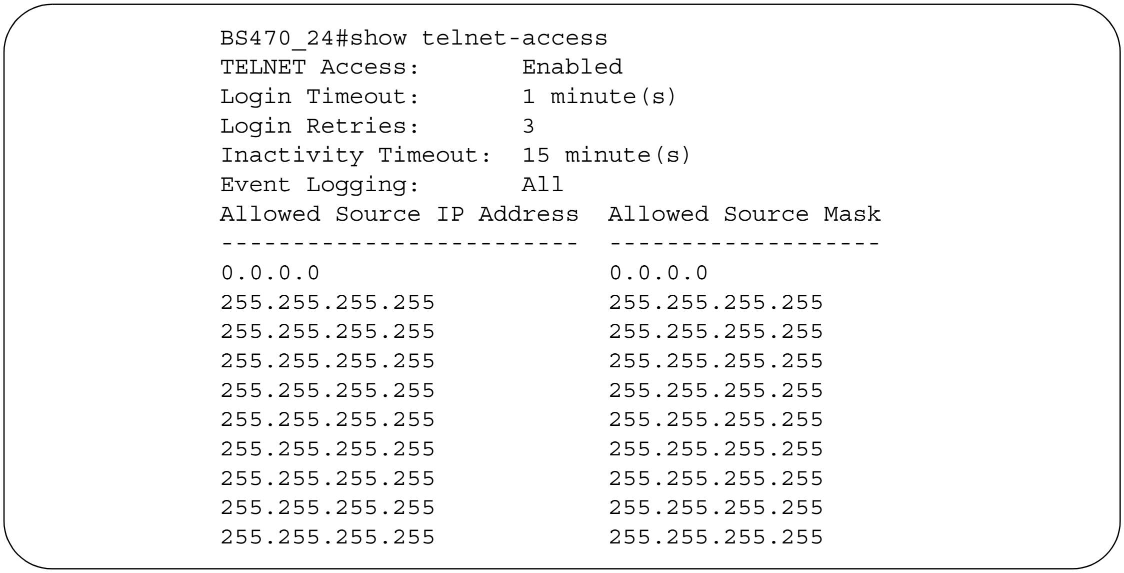
```
show telnet-access
```

The `show telnet-access` command is in the privExec command mode.

The `show telnet-access` command has no parameters or variables.

Figure 47 displays sample output from the `show telnet-access` command.

Figure 47 `show telnet-access` command output



```
BS470_24#show telnet-access
TELNET Access:        Enabled
Login Timeout:        1 minute(s)
Login Retries:        3
Inactivity Timeout:   15 minute(s)
Event Logging:        All
Allowed Source IP Address  Allowed Source Mask
-------------------------  -------------------
0.0.0.0                    0.0.0.0
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
```

telnet-access command

The `telnet-access` command allows you to configure the Telnet connection used to manage the switch. The syntax for the `telnet-access` command is:

```
telnet-access [enable|disable] [login-timeout <1-10>]
[retry <1-100>] [inactive-timeout <0-60>]
[logging {none|access|failures|all}]
[source-ip <1-10> <XXX.XXX.XXX.XXX>[mask <XXX.XXX.XXX.XXX>]]
```

The `telnet-access` command is in the config command mode.

Table 74 describes the parameters and variables for the `telnet-access` command.

Table 74 `telnet-access` command parameters and variables

Parameters and variables	Description
`enable|disable`	Enables or disables Telnet connections.
`login-timeout <1-10>`	Specifies the time in minutes to wait between initial Telnet connection and accepted password before closing the Telnet connection; enter an integer between 1 and 10.
`retry <1-100>`	Specifies the number of times the user can enter an incorrect password before closing the connection; enter an integer between 1 and 100.
`inactive timeout <0-60>`	Specifies in minutes how long to wait before closing an inactive session; enter an integer between 0 and 60.
`logging {none|access|failures|all}]`	Specifies what types of events you want to save in the event log: • `none`—do not save access events in the log • `access`—save access events in the log • `failure`—save failed access events in the log • `all`—save all access events in the log
`[source-ip <1-10> <XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]`	Specifies the source IP address that allow connections. Enter the IP address as an integer or in dotted-decimal notation. Specifies the subnet mask that allow connections; enter IP mask in dotted-decimal notation. Note: These are the same source IP addresses as in the IP Manager list. For more information on the IP Manager list see "Configuring the IP manager list" on page 163.

no telnet-access command

The `no telnet-access` command allows you to disable the Telnet connection. The syntax for the `no telnet-access` command is:

```
no telnet-access [source-ip [<1-10>]]
```

The `no telnet-access` command is in the config mode.

Table 75 describes the parameters and variables for the `no telnet-access` command.

Table 75 `no telnet-access` command parameters and variables

Parameters and variables	Description
`source-ip [<1-10>]`	Disables the Telnet access. When you do *not* use the optional parameter, the source-ip list is cleared, meaning the 1st index is set to 0.0.0.0./0.0.0.0. and the 2nd to 10th indexes are set to 255.255.255.255/255.255.255.255. When you *do* specify a source-ip value, the specified pair is set to 255.255.255.255/255.255.255.255. Note: These are the same source IP addresses as in the IP Manager list. For more information on the IP Manager list, see "Configuring the IP manager list" on page 163.

default telnet-access command

The `default telnet-access` command sets the Telnet settings to the default values. The syntax for the `default telnet-access` command is:

```
default telnet-access
```

The `default telnet-access` command is in the config command mode.

The `default telnet-access` command has no parameters or variables.

Configuring Secure Shell (SSH)

Note: Refer to the release notes accompanying your software release for the latest information on how to download the SSH-enabled image file. The SSH server will not function without the use of this image.

The secure shell protocol provides secure access to the CLI interface. With the CLI system, you can use the following commands:

- "show ssh global command ", next

- "show ssh session command" on page 175
- "show ssh download-auth-key command" on page 176
- "ssh dsa-key command" on page 176
- "no ssh dsa-key command" on page 177
- "ssh command" on page 177
- "no ssh command" on page 177
- "ssh secure command" on page 178
- "ssh max-sessions command" on page 178
- "ssh timeout command" on page 179
- "ssh dsa-auth command" on page 179
- "no ssh dsa-auth command" on page 179
- "ssh pass-auth command" on page 180
- "no ssh pass-auth command" on page 180
- "ssh port command" on page 180
- "ssh download-auth-key" on page 181
- "default ssh command" on page 181

show ssh global command

The `show ssh global` command displays the secure shell configuration information. The syntax for the `show ssh global` command is:

```
show ssh global
```

The `show ssh global` command is in the privExec command mode.

The `show ssh global` command has no parameters or variables.

Figure 48 displays sample output from the `show ssh global` command.

Figure 48 `show ssh global` command output

```
BS_470_24T#show ssh global
Active SSH Sessions      :  2
Version                  :  Version 2 only
Port                     :  22
Max. Sessions            :  2
Timeout                  :  60
DSA Key Size             :  1024
DSA Authentication       :  True
Password Authentication :  True
Public Key TFTP Server   :  134.177.152.12
Public Key File Name     :  pubkey.txt
Enabled                  :  True
```

show ssh session command

The `show ssh session` command displays the secure shell session information. The session information includes the session ID and the host IP address. A host address of 0.0.0.0 indicates no connection for that session ID. The syntax for the `show ssh session` command is:

```
show ssh session
```

The `show ssh session` command is in the privExec command mode.

The `show ssh session` command has no parameters or variables.

Figure 49 displays sample output from the `show ssh session` command.

Figure 49 `show ssh session` command output

```
BS470_24_24T#show ssh session
Session  Host
-------  ---------------
0        134.177.152.12
1        0.0.0.0
```

show ssh download-auth-key command

The `show ssh download-auth-key` command displays the results of the most recent attempt to download the DSA public key from the TFTP server. The syntax for the `show ssh download-auth-key` command is:

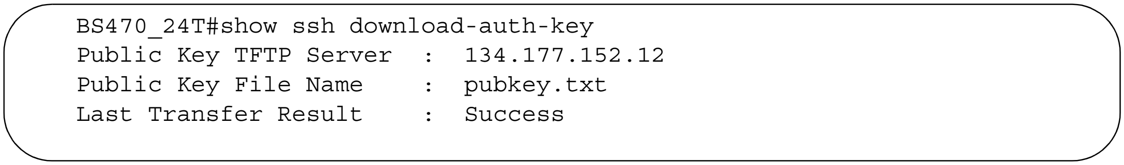
```
show ssh download-auth-key
```

The `show ssh download-auth-key` command is in the privExec command mode.

The `show ssh download-auth-key` command has no parameters or variables.

Figure 50 displays sample output from the `show ssh session` command.

Figure 50 `show ssh download-auth-key` command output



```
BS470_24T#show ssh download-auth-key
Public Key TFTP Server  :  134.177.152.12
Public Key File Name    :  pubkey.txt
Last Transfer Result    :  Success
```

ssh dsa-key command

The `ssh dsa-key` command initiates generation of a DSA host key at next system reboot. If a key size is specified, a key of this size (in bytes) is generated. If no key size is specified, the previous provisioned key size (or default of 1024) is used. This command can only be executed in the SSH disable mode. The syntax of the `ssh dsa-key` command is:

```
ssh dsa-key-gen [<512-1024>]
```

The `ssh dsa-key-gen` command is in the config command mode.

Table 76 describes the parameters and variables for the `ssh dsa-key-gen` command.

Table 76 `ssh dsa-key-gen` command parameters and variables

Parameters and variables	Description
<512-1024>	Sets the SSH host key size. Can be a value from 512 to 1-24. Default is 1024.

no ssh dsa-key command

The `no ssh dsa-key-gen` command deletes the DSA host key in the switch. The syntax of the `no ssh dsa-key-gen` command is:

```
no ssh dsa-key
```

The `no ssh dsa-key` command is in the config command mode.

There are no parameters or variables for the `no ssh dsa-key` command.

ssh command

The `ssh` command enables the SSH server on the BayStack 470-24T in non-secure mode. In addition to accepting SSH connections, the BayStack 470-24T continues to accept Web, SNMP, and Telnet connections while in this mode. The syntax of the `ssh` command is:

```
ssh
```

The `ssh` command is in the config command mode.

There are no parameters or variables for the `ssh` command.

no ssh command

The `no ssh` command disables the SSH server on the BayStack 470-24T. The syntax of the `no ssh` command is:

```
no ssh
```

The `no ssh` command is in the config command mode.

There are no parameters or variables for the `no ssh` command.

ssh secure command

The `ssh secure` command enables the SSH server on the BayStack 470-24T in secure mode. In secure mode, the BayStack 470-24T does not accept Web, SNMP, or Telnet connections. The syntax of the `ssh secure` command is:

```
ssh secure
```

The `ssh secure` command is in the config command mode.

There are no parameters or variables for the `ssh secure` command.

ssh max-sessions command

The `ssh max-sessions` command allows you to set the maximum number of simultaneous SSH sessions allowed. The syntax of the `ssh max-sessions` command is:

```
ssh max-sessions <0-2>
```

The `ssh max-sessions` command is in the config command mode.

Table 77 describes the parameters and variables for the `ssh max-sessions` command.

Table 77 `ssh max-sessions` command parameters and variables

Parameters and variables	Description
<0-2>	Specifies the maximum number of SSH sessions allowed. Default is 2.

ssh timeout command

The `ssh timeout` command sets the timeout value for session authentication. The syntax of the `ssh timeout` command is:

```
ssh timeout <1-120>
```

The `ssh timeout` command is in the config command mode.

Table 78 describes the parameters and variables for the `ssh timeout` command.

Table 78 `ssh timeout` command parameters and variables

Parameters and variables	Description
<1-120>	Specifies the timeout value for authentication. Default is 60.

ssh dsa-auth command

The `ssh dsa-auth` command enables DSA authentication. The syntax of the `ssh dsa-auth` command is:

```
ssh dsa-auth
```

The `ssh dsa-auth` command is in the config command mode.

There are no parameters or variables for the `ssh dsa-auth` command.

no ssh dsa-auth command

The `no ssh dsa-auth` command disables DSA authentication. The syntax of the `no ssh dsa-auth` command is:

```
no ssh dsa-auth
```

The `no ssh dsa-auth` command is in the config command mode.

There are no parameters or variables for the `no ssh dsa-auth` command.

ssh pass-auth command

The `ssh pass-auth` command enables password authentication. The syntax of the `ssh pass-auth` command is:

```
ssh pass-auth
```

The `ssh pass-auth` command is in the config command mode.

There are no parameters or variables for the `ssh pass-auth` command.

no ssh pass-auth command

The `no ssh pass-auth` command disables password authentication. The syntax for the `no ssh pass-auth` command is:

```
no ssh pass-auth
```

The `no ssh pass-auth` command is in the config command mode.

There are no parameters or variables for the `no ssh pass-auth` command.

ssh port command

The `ssh port` command sets the SSH connection port. The syntax of the `ssh port` command is:

```
ssh port <1-65535>
```

The `ssh port` command is in the config command mode.

Table 79 describes the parameters and variables for the `ssh port` command.

Table 79 `ssh port` command parameters and variables

Parameters and variables	Description
<1-65535>	Specifies the SSH connection port. Default is 22.

ssh download-auth-key

The `ssh download-auth-key` command downloads the client public key from the TFTP server to the BayStack 470-24T. The syntax for the `ssh download-auth-key` command is:

```
ssh download-auth-key [address <XXX.XXX.XXX.XXX>]
[key-name <file>]
```

The `ssh download-auth-key` command is in the config command mode.

Table 80 describes the parameters and variables for the `ssh download-auth-key` command.

Table 80 `ssh download-auth-key` command parameters and variables

Parameters and variables	Description
`address <XXX.XXX.XXX.XXX>`	The IP address of the TFTP server.
`key-name <file>`	The name of the public key file on the TFTP server.

default ssh command

The `default ssh` command resets the specific secure shell configuration parameter to the default value. The syntax of the `default ssh` command is:

```
default ssh
[dsa-auth|dsa-key|max-sessions|pass-auth|port|timeout]
```

The `default ssh` command is in the config command mode.

Table 81 describes the parameters and variables for the `default ssh` command.

Table 81 `default ssh` command parameters and variables

Parameters and variables	Description
`dsa-auth`	Resets dsa-auth to the default value. Default is True.
`dsa-key`	Resets the dsa-key size to the default value of 1024 bits.

Table 81 `default ssh` command parameters and variables (Continued)

Parameters and variables	Description
`max-sessions`	Resets the maximum number of simultaneous sessions to the default of 2.
`pass-auth`	Resets pass-auth to the default value. Default is True.
`port`	Resets the port number for SSH connections to the default. Default is 22.
`timeout`	Resets the timeout value for session authentication to the default. Default is 60.

Enabling or disabling the server for Web-based management

You can enable or disable the Web server for the Web-based management system. For information on using the Web-based management system, refer to *Using Web-based Management for the BayStack 460-24T-PWR Switch, Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

This section discusses the following commands:

- "web-server ", next
- "no web-server" on page 183

web-server

The `web-server` command enables or disables the Web server that you can use for Web-based management. The syntax for the `web-server` command is:

```
web-server {enable|disable}
```

The `web-server` command is in the config mode.

Table 82 describes the parameters and variables for the `web-server` command.

Table 82 `web-server` command parameters and variables

Parameters and variables	Description
`enable|disable`	Enables or disables the Web server.

no web-server

The `no web-server` command disables the Web server that you use for Web-based management. The syntax for the `no web-server` command is:

```
no web-server
```

The `no web-server` command is in the config mode.

The `no web-server` command has no parameters or variables.

Configuring SNMPv3

The switch provides the following CLI commands for SNMPv3:

- "show snmp-server command ", next
- "snmp-server command" on page 185
- "no snmp-server command" on page 185
- "snmp-server authentication-trap command" on page 186
- "no snmp-server authentication-trap command" on page 186
- "default snmp-server authentication-trap command" on page 187
- "snmp-server community for read/write command" on page 187
- "snmp-server community command" on page 188
- "no snmp-server community command" on page 189
- "default snmp-server community command" on page 190
- "snmp-server contact command" on page 191
- "no snmp-server contact command" on page 191
- "default snmp-server contact command" on page 191

- "snmp-server host for old-style table command" on page 192
- "snmp-server host for new-style table command" on page 193
- "no snmp-server host for old-style table command" on page 194
- "no snmp-server host for new-style table command" on page 194
- "default snmp-server host command" on page 195
- "snmp-server location command" on page 195
- "no snmp-server location command" on page 196
- "default snmp-server location command" on page 196
- "snmp-server name command" on page 196
- "no snmp-server name command" on page 197
- "default snmp-server name command" on page 197
- "snmp-server user command" on page 198
- "no snmp-server user command" on page 199
- "snmp-server view command" on page 200
- "no snmp-server view command" on page 201
- "snmp trap link-status command" on page 202
- "no snmp trap link-status command" on page 202
- "default snmp trap link-status command" on page 203
- "snmp-server bootstrap command" on page 204

show snmp-server command

The `show snmp-server` command displays SNMP configuration. The syntax for the `show snmp-server` command is:

```
show snmp-server {community|host|user|views}
```

The `show snmp-server` command is in the privExec command mode.

Table 83 describes the parameters and variables for the `show snmp-server` command.

Table 83 `show snmp-server` command parameters and variables

Parameters and variables	Description
`community|host|user|view`	Displays SNMPv3 configuration information: • community strings as configured in SNMPv3 MIBs • trap receivers as configured in SNMPv3 MIBs • SNMPv3 users, including views accessible to each user • SNMPv3 views
`view/views`	Displays SNMPv3 views.

snmp-server command

The `snmp-server` command enables or disables the SNMP server. The syntax for the `snmp-server` command is:

```
snmp-server {enable|disable}
```

The `snmp-server` command is in the config command mode.

Table 84 describes the parameters and variables for the `snmp-server` command.

Table 84 `snmp-server` command parameters and variables

Parameters and variables	Description
`enable|disable`	Enables or disables the SNMP server.

no snmp-server command

The `no snmp-server` command disables SNMP access. The syntax for the `no snmp-server` command is:

```
no snmp-server
```

The `no snmp-server` command is in the config command mode.

The `no snmp-server` command has no parameters or variables.

➡ **Note:** Disabling SNMP access also locks you out of the Device Manager management system.

snmp-server authentication-trap command

The `snmp-server authentication-trap` command enables or disables the generation of SNMP authentication failure traps. The syntax for the `snmp-server authentication-trap` command is:

```
snmp-server authentication-trap {enable|disable}
```

The `snmp-server authentication-trap` command is in the config command mode.

Table 85 describes the parameters and variables for the `snmp-server authentication-trap` command.

Table 85 `snmp-server authentication-trap` command

Parameters and variables	Description
`enable|disable`	Enables or disables the generation of authentication failure traps.

no snmp-server authentication-trap command

The `no snmp-server authentication-trap` command disables generation of SNMP authentication failure traps. The syntax for the `no snmp-server authentication-trap` command is:

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

The `no snmp-server authentication-trap` command is in the config command mode.

The `no snmp-server authentication-trap` command has no parameters or variables.

default snmp-server authentication-trap command

The `default snmp-server authentication-trap` command restores SNMP authentication trap configuration to the default settings. The syntax for the `default snmp-server authentication-trap` command is:

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

The `default snmp-server authentication-trap` command is in the config command mode.

The `default snmp-server authentication-trap` command has no parameters or variables.

snmp-server community for read/write command

The `snmp-server community command` for read/write modifies the community strings for SNMP v1 and SNMPv2c access. The syntax for the `snmp-server community` for read/write command is:

```
snmp-server community <community-string> [ro|rw]
```

The `snmp-server community` for read/write command is in the config command mode.

This command configures a single read-only or a single read-write community. A community configured using this command does not have access to any of the SNMPv3 MIBs. The community strings created by this command are controlled by the SNMP Configuration screen in the console interface.

This command affects community strings that were created prior to BoSS 3.0. These community strings will have a fixed MIB view.

Table 86 describes the parameters and variables for the `snmp-server community` for read/write command.

Table 86 `snmp-server community for read/write` command

Parameters and variables	Description
<community-string>	Changes community strings for SNMP v1 and SNMPv2c access. Enter a community string that works as a password and permits access to the SNMP protocol. If you set the value to ‘NONE’, it is disabled.
`ro|rw`	Specifies read-only or read-write access. Stations with `ro` access can only retrieve MIB objects, and stations with `rw` access can retrieve and modify MIB objects. **Note**: If neither `ro` nor `rw` is specified, `ro` is assumed (default).

snmp-server community command

The `snmp-server community` command allows you to create community strings with varying levels of read, write, and notification access based on SNMPv3 views. These community strings are separate from those created using the `snmp-server community` for read/write command.

This command affects community strings stored in the SNMPv3 snmpCommunityTable, which allows several community strings to be created. These community strings may have any MIB view.

The syntax for the `snmp-server community` command is:

```
snmp-server community <community-string>
{read-view <view-name>|write-view <view-name>|
notify-view <view-name>}
```

The `snmp-server community` command is in the config command mode.

Table 87 describes the parameters and variables for the `snmp-server community` command.

Table 87 `snmp-server community` command parameters and variables

Parameters and variables	Description
<*community-string*>	Enter a community string to be created with access to the specified views.
`read-view` <*view-name*>	Changes the read view used by the new community string for different types of SNMP operations. • *view-name*—specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
`write-view` <*view-name*>	Changes the write view used by the new community string for different types of SNMP operations. • *view-name*—specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
`notify-view` <*view-name*>	Changes the notify view settings used by the new community string for different types of SNMP operations. • *view-name*—specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.

no snmp-server community command

The `no snmp-server community` command clears the snmp-server community configuration. The syntax for the `no snmp-server community` command is:

```
no snmp-server community {ro|rw|<community-string>}
```

The `no snmp-server community` command is in the config command mode.

If you do not specify a read-only or read-write community parameter, all community strings are removed, including all communities controlled by the `snmp-server community` command and the `snmp-server community` for read-write command.

If you specify read-only or read-write, then just the read-only or read-write community is removed. If you specify the name of a community string, then the community string with that name is removed.

Table 88 describes the parameters and variables for the `no snmp-server community` command.

Table 88 `no snmp-server community` command parameters and variables

Parameters and variables	Description
`ro|rw|`	Sets the specified old-style community string's value to 'NONE', thereby disabling it.
<community-string>	Deletes the specified community string from the SNMPv3 MIBs (i.e., from the new-style configuration).

default snmp-server community command

The `default snmp-server community` command restores the community string configuration to the default settings. The syntax for the `default snmp-server community` command is:

```
default snmp-server community [ro|rw]
```

The `default snmp-server community` command is in the config command mode.

If the read-only or read-write parameter is omitted from the command, then all communities are restored to their default settings. The read-only community is set to Public, the read-write community is set to Private, and all other communities are deleted.

Table 89 describes the parameters and variables for the `default snmp-server community` command.

Table 89 default snmp-server community command parameters

Parameters and variables	Description
`ro|rw`	Restores the read-only community to 'public', or the read-write community to 'private'.

snmp-server contact command

The `snmp-server contact` command configures the SNMP sysContact value. The syntax for the `snmp-server contact` command is:

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

The `snmp-server contact` command is in the config command mode.

Table 90 describes the parameters and variables for the `snmp-server contact` command.

Table 90 `snmp-server contact` command parameters and variables

Parameters and variables	Description
`<text>`	Specifies the SNMP sysContact value; enter an alphanumeric string.

no snmp-server contact command

The `no snmp-server contact` command clears the sysContact value. The syntax for the `no snmp-server contact` command is:

```
no snmp-server contact
```

The `no snmp-server contact` command is in the config command mode.

The `no snmp-server contact` command has no parameters or variables.

default snmp-server contact command

The `default snmp-server contact` command restores the sysContact value to the default value. The syntax for the `default snmp-server contact` command is:

```
default snmp-server contact
```

The `default snmp-server contact` command is in the config command mode.

The `default snmp-server contact` command has no parameters or variables.

snmp-server host for old-style table command

The `snmp-server host` for old-style table command adds a trap receiver to the old-style trap-receiver table. The table has a maximum of four entries, and the entries can generate only SNMPv1 traps. This command controls the contents of the s5AGTrpRcvrTable which is the set of trap destinations controlled by the SNMP Configuration screen in the console interface.

The syntax for the `snmp-server host` for old-style table command is:

```
snmp-server host <host-ip> <community-string>
```

The `snmp-server host` for old-style table command is in the config command mode.

Table 91 describes the parameters and variables for the `snmp-server host` for old-style table command.

Table 91 snmp-server host for old-style table command parameters

Parameters and variables	Description
<host-ip>	Enter a dotted-decimal IP address of a host that will be the trap destination.
<community-string>	Enter a community string that works as a password and permits access to the SNMP protocol.

snmp-server host for new-style table command

The `snmp-server host` for new-style table command adds a trap receiver to the new-style configuration (that is, to the SNMPv3 tables) You can create several entries in this table, and each can generate v1, v2c, or v3 traps. Note that you must have previously configured the community string or user that is specified, with a notify-view. The syntax for the `snmp-server host` for new-style table command is:

```
snmp-server host <host-ip> {v1 <community-string>|
v2c <community-string>| v3 {auth|no-auth|auth-priv}
<username>}
```

The `snmp-server host` for new-style table command is in the config command mode.

Table 92 describes the parameters and variables for the `snmp-server host` for new-style table command.

Table 92 snmp-server host for new-style table command parameters

Parameters and variables	Description
`<host-ip>`	Enter a dotted-decimal IP address of a host that will be the trap destination.
`v1 <community-string>`	Using v1 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels may be created.
`v2c <community-string>`	Using v2c creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels may be created.
`v3 {auth|no-auth|auth-priv}`	Using v3 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels may be created: Enter the following variables: • `auth|no-auth`—specifies whether SNMPv3 traps should be authenticated • `auth-priv`—this parameter is only available if the image has full SHA/DES support.
`<username>`	Specifies the SNMPv3 username for trap destination; enter an alphanumeric string.

no snmp-server host for old-style table command

The `no snmp-server host` for old-style table command deletes trap receivers from the old-style table. The syntax for the `no snmp-server host` for old-style table command is:

```
no snmp-server host [<host-ip> [<community-string>]]
```

The `no snmp-server host` for old-style table command is in the config command mode.

If you do not specify any parameters, this command deletes all trap destinations from the s5AgTrpRcvrTable and from SNMPv3 tables.

Table 93 describes the parameters and variables for the `no snmp-server host` for old-style table command.

Table 93 no snmp-server host for old-style table command parameters

Parameters and variables	**Description**

`<host-ip>`
`[<community-string>]`
	Enter the following variables:
	• *host-ip*—IP address of a trap destination host.
	• *community-string*— community string that works as a password and permits access to the SNMP protocol.
	If both parameters are omitted, nothing is cleared.
	If a host IP is included, the community-string is required or an error is reported.

no snmp-server host for new-style table command

The `no snmp-server` for new-style table command deletes trap receivers from the new-style table (SNMPv3 MIB). Any trap receiver matching the IP address and SNMP version is deleted. The syntax for the `no snmp-server host` for new-style table command is:

```
no snmp-server host <host-ip> {v1|v2c|v3}
```

The `no snmp-server host` for new-style table command is in the config command mode.

Table 94 describes the parameters and variables for the `no snmp-server host` for new-style table command.

Table 94 `no snmp-server host for new-style` command parameters

Parameters and variables	Description
<host-ip>	Enter the IP address of a trap destination host.
v1|v2c|v3	Specifies trap receivers in the SNMPv3 MIBs.

default snmp-server host command

The `default snmp-server host` command restores the old-style table to defaults (that is, it clears the table). The syntax for the `default snmp-server host` command is:

```
default snmp-server host
```

The `default snmp-server host` command is in the config command mode.

The `default snmp-server host` command has no parameters or variables.

snmp-server location command

The `snmp-server location` command configures the SNMP sysLocation value. The syntax for the `snmp-server location` command is:

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

The `snmp-server location` command is in the config command mode.

Table 95 describes the parameters and variables for the `snmp-server location` command.

Table 95 `snmp-server location` command parameters and variables

Parameters and variables	Description
<text>	Specifies the SNMP sysLocation value; enter an alphanumeric string of up to 255 characters.

no snmp-server location command

The `no snmp-server location` command clears the SNMP sysLocation value. The syntax for the `no snmp-server location` command is:

```
no snmp-server location <text>
```

The `no snmp-server location` command is in the config command mode.

Table 96 describes the parameters and variables for the `no snmp-server location` command.

Table 96 `no snmp-server location` command parameters and variables

Parameters and variables	Description
<text>	Specifies the SNMP sysLocation value. Enter a string of up to 255 characters.

default snmp-server location command

The `default snmp-server location` command restores sysLocation to the default value. The syntax for the `default snmp-server location` command is:

```
default snmp-server location
```

The `default snmp-server location` command is in the config command mode.

The `default snmp-server location` command has no parameters or variables.

snmp-server name command

The `snmp-server name` command configures the SNMP sysName value. The syntax for the `snmp-server name` command is:

```
snmp-server name <text>
```

The `snmp-server name` command is in the config command mode.

Table 97 describes the parameters and variables for the `snmp-server name` command.

Table 97 `snmp-server name` command parameters and variables

Parameters and variables	Description
<text>	Specifies the SNMP sysName value; enter an alphanumeric string of up to 255 characters.

no snmp-server name command

The `no snmp-server name` command clears the SNMP sysName value. The syntax for the `no snmp-server name` command is:

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

The `no snmp-server name` command is in the config command mode.

Table 98 describes the parameters and variables for the `no snmp-server name` command.

Table 98 `no snmp-server name` command parameters and variables

Parameters and variables	Description
<text>	Specifies the SNMP sysName value; enter an alphanumeric string of up to 255 characters.

default snmp-server name command

The `default snmp-server name` command restores sysName to the default value. The syntax for the `default snmp-server name` command is:

```
default snmp-server name
```

The `default snmp-server name` command is in the config command mode.

Table 99 describes the parameters and variables for the `default snmp-server name` command.

Table 99 `default snmp-server name` command parameters and variables

Parameters and variables	Description
`<text>`	Specifies the SNMP sysName value; enter an alphanumeric string of up to 255 characters.

snmp-server user command

The `snmp-server user` command creates an SNMPv3 user. The syntax for the `snmp-server user` command is:

```
snmp-server user <username> [read-view <view-name>]
[write-view <view-name>][notify-view <view-name>]
[{md5|sha} <password>[read-view <view-name>]
[write-view <view-name>][notify-view <view-name>]
[des <password> [read-view <view-name>]
[write-view <view-name>][notify-view <view-name>]
```

The `snmp-server user` command is in the config command mode.

The `sha` and `des` parameters are available only if the switch image has full SHA/DES support.

There are three sets of read/write/notify views shown in the command. The first set specifies unauthenticated access. The second set specifies authenticated access. The third set specifies authenticated and encrypted access.

You can only specify authenticated access if the `md5` or `sha` parameter is included. Likewise, you can only specify authenticated and encrypted access, if the `des` parameter is included.

If you omit the authenticated view parameters, authenticated access uses the views specified for unauthenticated access. If you omit all of the authenticated and encrypted view parameters, the authenticated and encrypted access uses the same views used for authenticated access. These views are the unauthenticated views, if all the authenticated ones are also omitted.

Table 100 describes the parameters and variables for the `snmp-server user` command.

Table 100 `snmp-server user` command parameters and variables

Parameters and variables	Description
<*username*>	Specifies the user names; enter an alphanumeric string of up to 255 characters.
md5 <*password*>	Specifies the use of an md5 password. • *password*—specifies the new user md5 password; enter an alphanumeric string. If this parameter is omitted, the user is created with only unauthenticated access rights.
read-view <*view-name*>	Specifies the read view to which the new user has access: • *view-name*—specifies the viewname; enter an alphanumeric string of up to 255 characters.
write-view <*view-name*>	Specifies the write view to which the new user has access: • *view-name*—specifies the viewname; enter an alphanumeric string of up to 255 characters.
notify-view <*view-name*>	Specifies the notify view to which the new user has access: • *view-name*—specifies the viewname; enter an alphanumeric string of up to 255 characters.
sha/des	Specifies either SHA authentication or DES privacy encryption.

no snmp-server user command

The `no snmp-server user` command deletes the specified user. The syntax for the `no snmp-server user` command is:

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

The `no snmp-server user` command is in the config command mode.

Table 101 describes the parameters and variables for the `no snmp-server user` command.

Table 101 `no snmp-server user` command parameters and variables

Parameters and variables	Description
<username>	Specifies the user to be removed.

snmp-server view command

The `snmp-server view` command creates an SNMPv3 view. The view is a set of MIB object instances which may be accessed. The syntax for the `snmp-server view` command is:

```
snmp-server view <view-name> <OID> [<OID> [<OID> [<OID>
[<OID> [<OID> [<OID> [<OID> [<OID> [<OID>]]]]]]]]]
```

The `snmp-server view` command is in the config command mode.

Table 102 describes the parameters and variables for the `snmp-server view` command.

Table 102 `snmp-server view` **command parameters and variables**

Parameters and variables	**Description**
<viewname>	Specifies the name of the new view; enter an alphanumeric string.
<OID>	Specifies Object identifier. *OID* may be entered as a MIB object English descriptor, a dotted form *OID*, or a mix of the two. Each *OID* may also be preceded by a '+' or '-' sign (if this is omitted, a '+' sign is implied). For the dotted form, a sub-identifier can be a '*' indicating a wildcard. Here are some examples of valid *OID* parameters: • `sysName` • `+sysName` • `-sysName` • `+sysName.0` • `+ifIndex.1` • `-ifEntry.*.1` (matches all objects in the if Table with an instance of 1, i.e., the entry for interface #1) • `1.3.6.1.2.1.1.1.0` (dotted form of `sysDescr`) The `'+'` or `'-'` indicates whether the specified *OID* is included in or excluded from, respectively, the set of MIB objects that are accessible using this view. For example, if you create a view like this: • `snmp-server view myview +system -sysDescr` And you use that view for the read-view of a user, then the user can read only the system group, except for `sysDescr`.

no snmp-server view command

The `no snmp-server view` command deletes the specified view. The syntax for the `no snmp-server view` command is:

```
no snmp-server view <viewname>
```

The `no snmp-server view` is in the config command mode.

Table 103 describes the parameters and variables for the `no snmp-server view` command.

Table 103 `no snmp-server view` command parameters and variables

Parameters and variables	Description
<viewname>	Specifies the name of the view to be removed. If no view is specified, all views are removed.

snmp trap link-status command

The `snmp trap link-status` command enables the linkUp/linkDown traps for the port. The syntax of the command is:

```
snmp trap link-status [port <portlist>]
```

The `snmp trap link-status` command is in the config-if command mode.

Table 104 describes the parameters and variables for the `snmp trap link-status` command.

Table 104 `snmp trap link-status` command parameters and variables

Parameters and variables	Description
port *<portlist>*	Specifies the port numbers to enable the linkUp/linkDown traps on. Enter the port numbers or All. **Note**: If you omit this parameter, the system uses the port number specified with the `interface` command.

no snmp trap link-status command

The `no snmp trap link-status` command disables the linkUp/linkDown traps for the port. The syntax of the `no snmp trap link-status` command is:

```
no snmp trap link-status [port <portlist>]
```

The `no snmp trap link-status` command is in the config-if command mode.

Table 105 describes the parameters and variables for the `no snmp trap link-status` command.

Table 105 `no snmp trap link-status` command parameters

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable the linkUp/linkDown traps on. Enter the port numbers or all. **Note**: If you omit this parameter, the system uses the port number specified with the `interface` command.

default snmp trap link-status command

The `default snmp trap link-status` command disables the linkUp/linkDown traps for the port. The syntax of the command is:

```
default snmp trap link-status [port <portlist>]
```

The `default snmp trap link-status` command is in the config-if command mode.

Table 106 describes the parameters and variables for the `default snmp trap link-status` command.

Table 106 `default snmp trap link-status` command parameters

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable the linkUp/linkDown traps on. Enter the port numbers or all. **Note**: If you omit this parameter, the system uses the port number specified with the `interface` command.

snmp-server bootstrap command

The `snmp-server bootstrap` command allows you to specify how you wish to secure SNMP communications, as described in the SNMPv3 standards. It creates an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (in RFC 3414 and 3415). It consists of a set of initial users, groups, and views. This `snmp-server bootstrap` command deletes ALL existing SNMP configurations, so it should be used with care.

The syntax for the `snmp-server bootstrap` command is:

```
snmp-server bootstrap <minimum-secure> | <semi-secure>
|<very-secure>
```

The `snmp-server bootstrap` command is in the config command mode.

Table 107 describes the parameters and variables for the `snmp-server bootstrap` command.

Table 107 `snmp-server bootstrap` command parameters and variables

Parameters and variables	Description
<minimum-secure>	Specifies a minimum security configuration that allows read access to everything via noAuthNoPriv, and write access to everything via authNoPriv.
<semi-secure>	Specifies a partial security configuration that allows read access to a small subset of system information using noAuthNoPriv, and read and write access to everything using authNoPriv.
<very-secure>	Specifies a maximum security configuration that allows no access.

Configuring the RADIUS-based management password authentication

Using a the RADIUS protocol and a server, you can configure the switch for authentication. With the CLI system, you can use the following commands:

- “show radius-server command ”, next
- “radius-server command” on page 205
- “no radius-server command” on page 206
- “radius-server password fallback” on page 206

show radius-server command

The `show radius-server` command displays the RADIUS server configuration. The syntax for the `show radius-server` command is:

```
show radius-server
```

The `show radius-server` command is in the privExec command mode.

The `show radius-server` command has no parameters or variables.

Figure 51 displays sample output from the `show radius-server` command.

Figure 51 `show radius-server` command output

```
BS470_24#show radius-server
host: 0.0.0.0
Secondary-host: 0.0.0.0
port: 1645
key:
BS470_24#
```

radius-server command

The `radius-server` command changes the RADIUS server settings. The syntax for the `radius-server` command is:

```
radius-server host <address> [secondary-host <address>]
port <num> key <string>
```

The `radius-server` command is in the config command mode.

Table 108 describes the parameters and variables for the `radius-server` command.

Table 108 `radius-server` command parameters and variables

Parameters and variables	Description
host *<address>*	Specifies the primary RADIUS server. Enter the IP address of the RADIUS server.
secondary-host *<address>*	Specifies the secondary RADIUS server Enter the IP address of the secondary RADIUS server.
port *<num>*	Enter the port number of the RADIUS server.
key *<string>*	Specifies a secret text string that is shared between the switch and the RADIUS server. Enter the secret string, which is an alphanumeric string up to 16 characters.

no radius-server command

The `no radius-server` command clears the RADIUS server settings. The syntax for the `no radius-server` command is:

```
no radius-server
```

The `no radius-server` command is in the config command mode.

The `no radius-server` command has no parameters or values.

radius-server password fallback

The `radius-server password fallback` command enables you to configure password fallback as an option when using RADIUS authentication for login and password. The syntax for the `radius-server password fallback` command is:

```
radius-server password fallback
```

The `radius-server password fallback` command is in the config command mode.

Securing your network

You can secure your network using the following CLI commands.

- "Configuring MAC address filter-based security ", next
- "Configuring EAPOL-based security" on page 214

Configuring MAC address filter-based security

You configure the BaySecure* application using MAC addresses with the following commands:

- "show mac-security command ", next
- "show mac-security mac-da-filter command" on page 208
- "mac-security command" on page 209
- "mac-security mac-address-table address command" on page 210
- "mac-security security-list command" on page 211
- "no mac-security command" on page 211
- "no mac-security mac-address-table command" on page 212
- "no mac-security security-list command" on page 212
- "mac-security command for specific ports" on page 213
- "mac-security mac-da-filter command" on page 214

show mac-security command

The `show mac-security` command displays configuration information for the BaySecure application. The syntax for the `show mac-security` command is:

```
show mac-security {config|mac-address-table
[address <macaddr>] |port|security-lists}
```

The `show mac-security` command is in the privExec command mode.

Table 109 describes the parameters and variables for the `show mac-security` command.

Table 109 `show mac-security` command parameters and variables

Parameters and variables	Description
`config`	Displays general BaySecure configuration.
`mac-address-table [address <macaddr>]`	Displays contents of BaySecure table of allowed MAC addresses: • `address`—specifies a single MAC address to display; enter the MAC address
`port`	Displays the BaySecure status of all ports.
`security-lists`	Displays port membership of all security lists.

Figure 52 displays sample output from the `show mac-security` command.

Figure 52 `show mac-security` command output

```
BS470_24#show mac-security config
MAC Address Security: Disabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
Generate SNMP Trap on Intrusion: Disabled
Current Learning Mode: Disabled
Learn by Ports:
```

show mac-security mac-da-filter command

The `show mac-security mac-da-filter` command displays configuration information for filtering MAC destination addresses (DAs). You can filter packets from up to 10 MAC DAs. The syntax for the `show mac-security mac-da-filter` command is:

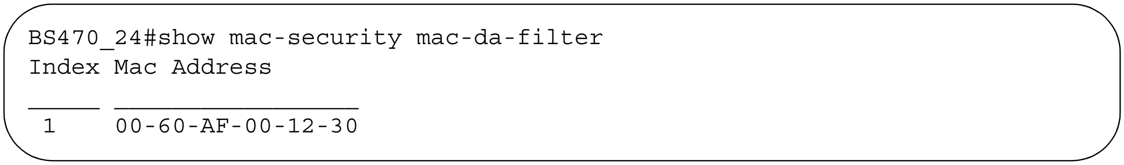
```
show mac-security mac-da-filter
```

The `show mac-security mac-da-filter` command is in the privExec command mode.

The `show mac-security mac-da-filter` command has no parameters or variables.

Figure 53 displays sample output from the `show mac-security mac-da-filter` command.

Figure 53 `show mac-security mac-da-filter` command output



```
BS470_24#show mac-security mac-da-filter
Index Mac Address

_____ _________________
 1    00-60-AF-00-12-30
```

mac-security command

The `mac-security` command modifies the BaySecure configuration. The syntax for the `mac-security` command is:

```
mac-security [disable|enable] [filtering {enable|disable}]
[intrusion-detect {enable|disable|forever}]
[intrusion-timer <1-65535>] [learning-ports <portlist>]
[learning {enable|disable}] [snmp-lock {enable|disable}]
[snmp-trap {enable|disable}]
```

The `mac-security` command is in the config command mode.

Table 110 describes the parameters and variables for the `mac-security` command.

Table 110 `mac-security` command parameters and variables

Parameters and variables	Description
`disable|enable`	Disables or enables MAC address-based security.
`filtering {enable|disable}`	Enables or disables destination address (DA) filtering on intrusion detected.
`intrusion-detect {enable|disable|forever}`	Specifies partitioning of a port when an intrusion is detected: • `enable`—port is partitioned for a period of time • `disabled`—port is not partitioned on detection • `forever`—port is partitioned until manually changed

Table 110 `mac-security` command parameters and variables (Continued)

Parameters and variables	Description
`intrusion-timer <1-65535>`	Specifies, in seconds, length of time a port is partitioned when an intrusion is detected; enter the number of you want.
`learning-ports <portlist>`	Specifies MAC address learning. Learned addresses are added to the table of allowed MAC addresses. Enter the ports you want to learn; it can be a single port, a range of ports, several ranges, all, or none.
`learning {enable|disable}`	Specifies MAC address learning: • `enable`—enables learning by ports • `disable`—disables learning by ports
`snmp-lock {enable|disable}`	Enables or disables a lock on SNMP write-access to the BaySecure MIBs.
`snmp-trap {enable|disable}`	Enables or disables trap generation upon intrusion detection.

mac-security mac-address-table address command

The `mac-security mac-address-table address` command assigns either a specific port or a security list to the MAC address. This removes any previous assignment to the specified MAC address and creates an entry in the BaySecure table of allowed MAC addresses. The syntax for the `mac-security mac-address-table address` command is:

```
mac-security mac-address-table address <H.H.H.>
{port <portlist>|security-list <1-32>}
```

Note: In this command, *`portlist`* must specify only a single port

The `mac-security mac-address-table address` command is in the config command mode.

Table 111 describes the parameters and variables for the `mac-security mac-address-table address` command.

Table 111 `mac-security mac-address-table address` command

Parameters and variables	Description
`<H.H.H.>`	Enter the MAC address in the form of H.H.H.

`port <portlist>|`
`security-list <1-32>`
	Enter the port number or the security list number.

mac-security security-list command

The `mac-security security-list` command assigns a list of ports to a security list. The syntax for the `mac-security security-list` command is:

```
mac-security security-list <1-32> <portlist>
```

The `mac-security security-list` command is in the config command mode.

Table 112 describes the parameters and variables for the `mac-security security-list` command.

Table 112 `mac-security security-list` command parameters

Parameters and variables	Description
`<1-32>`	Enter the number of the security list you want to use.
`<portlist>`	Enter a list or range of port numbers.

no mac-security command

The `no mac-security` command disables MAC source address-based security. The syntax for the `no mac-security` command is:

```
no mac-security
```

The `no mac-security` command is in the config command mode.

The `no mac-security` command has no parameters or values.

no mac-security mac-address-table command

The `no mac-security mac-address-table` command clears entries from the MAC address security table. The syntax for the `no mac-security mac-address-table` command is:

```
no mac-security mac-address-table {address <H.H.H.> |
port <portlist>|security-list <1-32>}
```

The `no mac-security mac-address-table` command is in the config command mode.

Table 113 describes the parameters and variables for the `no mac-security mac-address-table` command.

Table 113 `no mac-security mac-address-table` command

Parameters and variables	Description
`address <H.H.H.>`	Enter the MAC address in the form of H.H.H.
`port <portlist>`	Enter a list or range of port numbers.
`security-list <1-32>`	Enter the security list number.

no mac-security security-list command

The `no mac-security security-list` command clears the port membership of a security list. The syntax for the `no mac-security security-list` command is:

```
no mac-security security-list <1-32>
```

The `no mac-security security-list` command is in the config command mode.

Table 114 describes the parameters and variables for the `no mac-security security-list` command.

Table 114 `no mac-security security-list` command parameters

Parameters and variables	Description
`<`*`1-32`*`>`	Enter the number of the security list you want to clear.

mac-security command for specific ports

The `mac-security` command for specific ports configures the BaySecure status of specific ports. The syntax for the `mac-security` command for specific ports is:

```
mac-security [port <portlist>] {disable|enable|learning}
```

The `mac-security` command for specific ports is in the config-if command mode

Table 115 describes the parameters and variables for the `mac-security` command for specific ports.

Table 115 `mac-security` command for a single port parameters

Parameters and variables	Description
`port <`*`portlist`*`>`	Enter the port numbers.
`disable|enable|learning`	Directs the specific port: • `disable`—disables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is being performed • `enable`—enables BaySecure on the specified port and removes the port from the list of ports for which MAC address learning is being performed • `learning`—disables BaySecure on the specified port and adds these port to the list of ports for which MAC address learning is being performed

mac-security mac-da-filter command

The `mac-security mac-da-filter` command allows you to filter packets from up to 10 specified MAC DAs. You also use this command to delete such a filter and then receive packets from the specified MAC DA**.** The syntax for the `mac-security mac-da-filter` command is:

```
mac-security mac-da-filter {add|delete}<H.H.H.>
```

The `mac-security mac-da-filter` command is in the config command mode.

Table 116 describes the parameters and variables for the `mac-security mac-da-filter` command.

Table 116 `mac-security mac-da-filter` command parameters

Parameters and variables	Description
`{add|delete}` *<H.H.H>*	Add or delete the specified MAC address; enter the MAC address in the form of H.H.H.

Note: Ensure that you do not enter the MAC address of the management unit.

Configuring EAPOL-based security

You configure the security based on the Extensible Authentication Protocol over LAN (EAPOL) using the following CLI commands:

- "show eapol command ", next
- "eapol command" on page 216
- "eapol command for modifying parameters" on page 217

show eapol command

The `show eapol` command displays the status of the EAPOL-based security. The syntax for the `show eapol` command is:

```
show eapol [port <portlist>]
```

The `show eapol` command is in the privExec command mode.

Table 117 describes the parameters and variables for the `show eapol` command.

Table 117 `show eapol` command parameters and variables

Parameters and variables	Description
port *<portlist>*	Enter a list or range of port numbers. If left blank, EAPOL status of all ports will be displayed.

The `show eapol` command displays the current status of the EAPOL parameters.

Figure 54 displays the `show eapol` command output.

Figure 54 `show eapol` command output

```
BS460_24T_PWR#show eapol
EAPOL Administrative State:  Disabled
EAPOL User-Based Policies :  Disabled
     Admin         Admin Oper ReAuth ReAuth Quiet  Xmit   Supplic Server  Max
Port Status   Auth Dir   Dir  Enable Period Period Period Timeout Timeout Req
---- -------- ---- ----- ---- ------ ------ ------ ------ ------- ------- ---
1    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
2    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
3    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
4    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
5    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
6    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
7    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
8    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
9    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
10   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
11   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
12   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
13   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
14   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
15   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
16   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
17   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
----More ----
```

eapol command

The `eapol` command enables or disables EAPOL-based security. The syntax of the `eapol` command is:

```
eapol {disable|enable}
```

The `eapol` command is in the config command mode.

Table 118 describes the parameters and variables for the `eapol` command.

Table 118 `eapol` command parameters and variables

Parameters and variables	Description
`disable|enable`	Disables or enables EAPOL-based security.

eapol command for modifying parameters

The eapol command for modifying parameters modifies EAPOL-based security parameters for a specific port. The syntax of the eapol command for modifying parameters is:

```
eapol [port <portlist>] [init]
[status authorized|unauthorized|auto]
[traffic-control in-out|in]
[re-authentication enable|disable]
[re-authentication-interval <num>]
[re-authentication-period <1-604800>] [re-authenticate]
[quiet-interval <num>] [transmit-interval <num>]
[supplicant-timeout <num>]
[server-timeout <num>][max-request <num>]
```

The eapol command for modifying parameters is in the config-if command mode.

Table 119 describes the parameters and variables for the eapol command for modifying parameters

Table 119 eapol command for modifying parameters and variables

Parameters and variables	Description
port *<portlist>*	Specifies the ports to configure for EAPOL; enter the port numbers you want. Note: If you omit this parameter, the system uses the port number specified when you issued the interface command.
init	Re-initiates EAP authentication.
status authorized|unauthorized|auto	Specifies the EAP status of the port: • authorized—port is always authorized • unauthorized—port is always unauthorized • auto—port authorization status depends on the result of the EAP authentication
traffic-control in-out|in	Sets the level of traffic control: • in-out—if EAP authentication fails, both ingressing and egressing traffic are blocked • in—if EAP authentication fails, only ingressing traffic is blocked

Table 119 `eapol` command for modifying parameters and variables

Parameters and variables	Description
`re-authentication enable|disable`	Enables or disables re-authentication.
`re-authentication-interval <num>`	Enter the number of seconds you want between re-authentication attempts; range is 1 to 604800. Use either this variable or the re-authentication-period variable; do not use both variables because the two variables control the same setting.
`re-authentication-period <1-604800>`	Enter the number of seconds you want between re-authentication attempts. Use either this variable or the re-authentication-interval variable; do not use both variables because the two variables control the same setting.
`re-authenticate`	Specifies an immediate re-authentication.
`quiet-interval <num>`	Enter the number of seconds you want between an authentication failure and the start of a new authentication attempt; range is 1 to 65535.
`transmit-interval <num>`	Specifies a waiting period for response from supplicant for EAP Request/Identity packets. Enter the number of seconds you want to wait; range is 1-65535.
`supplicant-timeout <num>`	Specifies a waiting period for response from supplicant for all EAP packets except EAP Request/Identity packets. Enter the number of seconds you want to wait; range is 1-65535.
`server-timeout <num>`	Specifies a waiting period for response from the server. Enter the number of seconds you want to wait; range is 1-65535
`max-request <num>`	Enter the number of times to retry sending packets to supplicant.

Chapter 5 Ethernet port management

This chapter describes how to enable a port, name a port, enable rate limit and display the status for the Power over Ethernet (PoE) configuration. This chapter covers the following topics:

- "Enabling or disabling a port ", next
- "Naming ports" on page 221
- "Setting port speed" on page 223
- "Enabling flow control" on page 227
- "Enabling rate-limiting" on page 229
- "Enabling Custom Autonegotiation Advertisements (CANA)" on page 234
- "Displaying PoE configuration" on page 238
- "Configuring FEFI" on page 242
- "Configuring SFFD" on page 243
- "Configuring power parameters on the switch" on page 246
- "Configuring power parameters on the ports" on page 253

Refer to the *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches* for more information on the PoE feature on the switch. Refer to Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches for information on configuring these features using the Web-based management system, and refer to *Reference for the Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches* for configuration information for the DM.

➡ **Note:** For information on downloading the PoE image, refer to "download command" on page 90.

Enabling or disabling a port

You can enable or disable a port using the CLI. This section covers the following commands:

- "shutdown command ", next
- "no shutdown command" on page 220

shutdown command

The `shutdown` command disables the port. The syntax for the `shutdown` command is:

```
shutdown [port <portlist>]
```

The `shutdown` command is in the config-if command mode.

Table 120 describes the parameters and variables for the `shutdown` command.

Table 120 `shutdown` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to shut down or disable. Enter the port numbers you want to disable. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

no shutdown command

The `no shutdown` command enables the port. The syntax for the `no shutdown` command is:

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

The `no shutdown` command is in the config-if command mode.

Table 121 describes the parameters and variables for the `no shutdown` command.

Table 121 `no shutdown` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to enable. Enter the port numbers you want to enable. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Naming ports

You can name a port using the CLI. This section covers the following commands:

- "name command ", next
- "no name command" on page 222
- "default name command" on page 222

name command

The `name` command allows you to name ports or to change the name. The syntax for the `name` command is:

```
name [port <portlist>] <LINE>
```

The `name` command is in the config-if command mode.

Table 122 describes the parameters and variables for the `name` command.

Table 122 `name` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to name. Note: If you omit this parameter, the system uses the port number you specified in the `interface` command.
`<LINE>`	Enter up to 26 alphanumeric characters.

no name command

The `no name` command clears the port names; it resets the field to an empty string. The syntax for the `no name` command is:

```
no name [port <portlist>]
```

The `no name` command is in the config-if command mode.

Table 123 describes the parameters and variables for the `no name` command.

Table 123 `no name` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to clear of names. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

default name command

The `default name` command clears the port names; it resets the field to an empty string. The syntax for the `default name` command is:

```
default name [port <portlist>]
```

The `default name` command is in the config-if command mode.

Table 124 describes the parameters and variables for the `default name` command.

Table 124 `default name` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to clear of names. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Setting port speed

You can set the speed and duplex mode for a port. This section covers:

- "speed command ", next
- "default speed command" on page 224
- "duplex command" on page 225
- "default duplex command" on page 226

speed command

The `speed` command sets the speed of the port. The syntax for the `speed` command is:

```
speed [port <portlist>] {10|100|1000|auto}
```

The `speed` command is in the config-if command mode.

Note: You cannot *enable* autonegotiation on fiber optic ports.

Table 125 describes the parameters and variables for the `speed` command.

Table 125 `speed` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to configure the speed. Enter the port numbers you want to configure. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.
`10|100|1000|auto`	Sets speed to: • `10`—10 Mb/s • `100`—100 Mb/s • `1000`—1000 Mb/s or 1 GB/s • `auto`—autonegotiation

Note: When you set the port speed for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

default speed command

The `default speed` command sets the speed of the port to the factory default speed. The syntax for the `default speed` command is:

```
default speed [port <portlist>]
```

The `default speed` command is in the config-if command mode.

Table 126 describes the parameters and variables for the `default speed` command.

Table 126 `default speed` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to set the speed to factory default. Enter the port numbers you want to set. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

duplex command

The `duplex` command specifies the duplex operation for a port. The syntax for the `duplex` command is:

```
duplex [port <portlist>] {full|half|auto}
```

The `duplex` command is in the config-if command mode.

Note: You cannot *enable* autonegotiation on fiber optic ports.

Table 127 describes the parameters and variables for the duplex command.

Table 127 duplex command parameters and variables

Parameters and variables	Description
port *<portlist>*	Specifies the port number to configure the duplex mode. Enter the port number you want to configure, or all to configure all ports simultaneously. Note: If you omit this parameter, the system uses the port number specified with the interface command.
full|half|auto	Sets duplex to: • full—full-duplex mode • half—half-duplex mode • auto—autonegotiation

Note: When you set the duplex mode for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

default duplex command

The default duplex command sets the duplex operation for a port to the factory default duplex value. The syntax for the default duplex command is:

```
default duplex [port <portlist>]
```

The default duplex command is in the config-if command mode.

Table 128 describes the parameters and variables for the `default duplex` command.

Table 128 `default duplex` command parameters and variables

Parameters and variables	Description
`port` *`<portlist>`*	Specifies the port numbers to reset the duplex mode to factory default values. Enter the port numbers you want to configure, or `all` to configure all ports simultaneously. The default value is autonegotiation. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Note: You cannot *enable* autonegotiation on fiber optic ports.

Enabling flow control

If you use a Gigabit Interface Connector (GBIC) with the switch, you control traffic on this port using the `flowcontrol` command. This section covers the following commands:

- "flowcontrol command ", next
- "no flowcontrol command" on page 228
- "default flowcontrol command" on page 229

flowcontrol command

The `flowcontrol` command is used only on Gigabit Interface Connector ports and controls the traffic rates during congestion. The syntax for the `flowcontrol` command is:

```
flowcontrol [port <portlist>]
{asymmetric|symmetric|auto|disable}
```

The `flowcontrol` command is in the config-if mode.

Table 129 describes the parameters and variables for the `flowcontrol` command.

Table 129 `flowcontrol` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to configure for flow control. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.
`asymmetric|symmetric|auto|disable`	Sets the mode for flow control: • `asymmetric`—enables the local port to perform flow control on the remote port • `symmetric`—enables the local port to perform flow control • `auto`—sets the port to automatically determine the flow control mode (default) • `disable`—disables flow control on the port

no flowcontrol command

The `no flowcontrol` command is used only on Gigabit Ethernet ports and disables flow control. The syntax for the `no flowcontrol command` is:

```
no flowcontrol [port <portlist>]
```

The `no flowcontrol` command is in the config-if mode.

Table 130 describes the parameters and variables for the `no flowcontrol` command.

Table 130 `no flowcontrol` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable flow control. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

default flowcontrol command

The `default flowcontrol` command is used only on Gigabit Ethernet ports and sets the flow control to auto, which automatically detects the flow control. The syntax for the `default flowcontrol` command is:

```
default flowcontrol [port <portlist>]
```

The `default flowcontrol` command is in the config-if mode.

Table 131 describes the parameters and variables for the `default flowcontrol` command.

Table 131 `default flowcontrol` command parameters and variables

Parameters and variables	**Description**
`port <portlist>`	Specifies the port numbers to default to auto flow control. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Enabling rate-limiting

You can limit the percentage of multicast traffic, or broadcast traffic, or both using the CLI. For more information on rate-limiting, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

This section covers:

- "show rate-limit command ", next
- "rate-limit command" on page 231
- "no rate-limit command" on page 232
- "default rate-limit command" on page 233

show rate-limit command

The `show rate-limit` command displays the rate-limiting settings and statistics. The syntax for the `show rate-limit` command is:

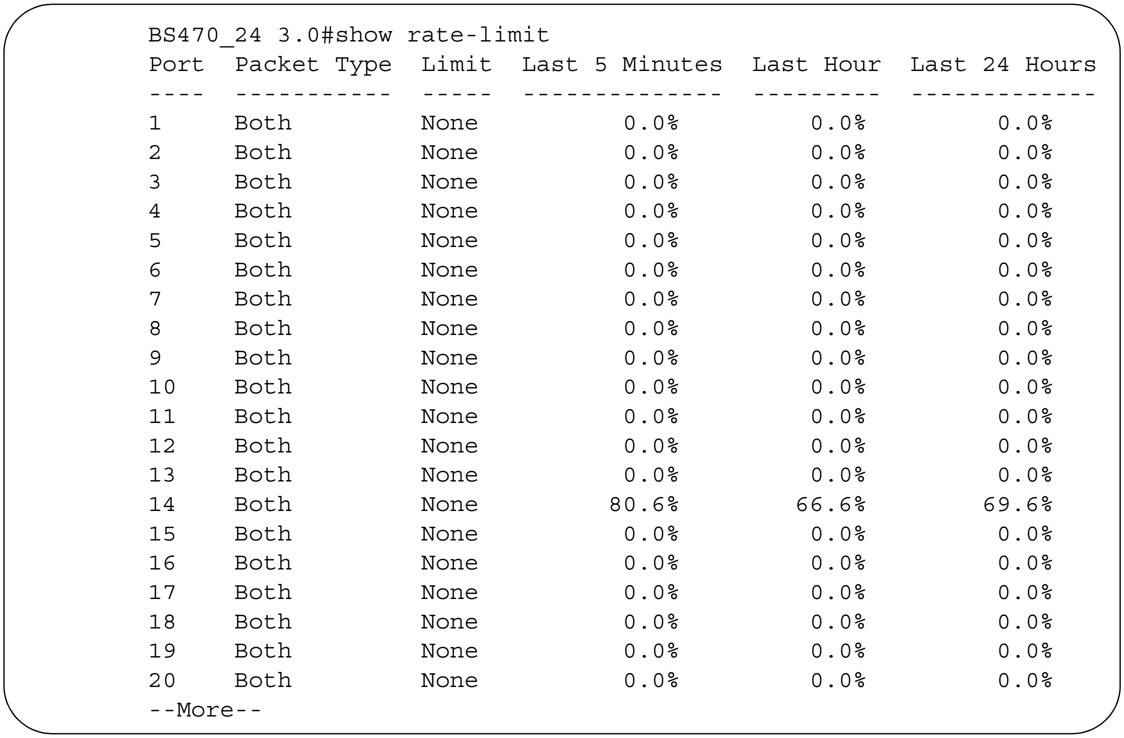
```
show rate-limit
```

The `show rate-limit` command is in the privExec command mode.

The `show rate-limit` command has no parameters or variables.

Figure 55 displays sample output from the `show rate-limit` command.

Figure 55 `show rate-limit` command output



```
BS470_24 3.0#show rate-limit
Port  Packet Type  Limit  Last 5 Minutes  Last Hour  Last 24 Hours
----  -----------  -----  --------------  ---------  -------------
1     Both         None             0.0%       0.0%           0.0%
2     Both         None             0.0%       0.0%           0.0%
3     Both         None             0.0%       0.0%           0.0%
4     Both         None             0.0%       0.0%           0.0%
5     Both         None             0.0%       0.0%           0.0%
6     Both         None             0.0%       0.0%           0.0%
7     Both         None             0.0%       0.0%           0.0%
8     Both         None             0.0%       0.0%           0.0%
9     Both         None             0.0%       0.0%           0.0%
10    Both         None             0.0%       0.0%           0.0%
11    Both         None             0.0%       0.0%           0.0%
12    Both         None             0.0%       0.0%           0.0%
13    Both         None             0.0%       0.0%           0.0%
14    Both         None            80.6%      66.6%          69.6%
15    Both         None             0.0%       0.0%           0.0%
16    Both         None             0.0%       0.0%           0.0%
17    Both         None             0.0%       0.0%           0.0%
18    Both         None             0.0%       0.0%           0.0%
19    Both         None             0.0%       0.0%           0.0%
20    Both         None             0.0%       0.0%           0.0%
--More--
```

rate-limit command

The `rate-limit` command configures rate-limiting on the port. The syntax for the `rate-limit` command is:

```
rate-limit [port <portlist>]
{multicast <pct>| broadcast <pct>| both <pct>}
```

The `rate-limit` command is in the config-if command mode.

Table 132 describes the parameters and variables for the `rate-limit` command.

Table 132 `rate-limit` command parameters and variables

Parameters and values	Description
`port <portlist>`	Specifies the port numbers to configure for rate-limiting. Enter the port numbers you want to configure. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.
`multicast <pct>|broadcast <pct>|both <pct>`	Applies rate-limiting to the type of traffic. Enter an integer between 1 and 10 to set the rate-limiting percentage: • `multicast`—applies rate-limiting to multicast packets • `broadcast`—applies rate-limiting to broadcast packets • `both`—applies rate-limiting to both multicast and broadcast packets

no rate-limit command

The `no rate-limit` command disables rate-limiting on the port. The syntax for the `no rate-limit` command is:

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

The `no rate-limit` command is in the config-if command mode.

Table 133 describes the parameters and variables for the `no rate-limit` command.

Table 133 `no rate-limit` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable from rate-limiting. Enter the port numbers you want to disable. Note: If you omit this parameter, the system uses the port number you specified in the `interface` command.

default rate-limit command

The `default rate-limit` command restores the rate-limiting value for the specified port to the default setting. The syntax for the `default rate-limit` command is:

```
default rate-limit [port <portlist>]
```

The `default rate-limit` command is in the config-if command mode.

Table 134 describes the parameters and variables for the `default rate-limit` command.

Table 134 `default rate-limit` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to reset rate-limiting to factory default. Enter the port numbers you want to set rate-limiting to default on. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Enabling Custom Autonegotiation Advertisements (CANA)

You can control the capabilities that are advertised by the BayStack switch as part of the auto-negotiation process using the Custom Autonegotiation Advertisements (CANA) feature. When auto-negotiation is disabled, the hardware is configured for a single (fixed) speed and duplex value. When auto-negotiation is enabled, the advertisement made by the switch is a constant value based upon all speed and duplex modes supported by the hardware. When auto-negotiating, the switch selects the highest common operating mode supported between it and its link partner.

This section covers:

- "show auto-negotiation-advertisements command ", next
- "show auto-negotiation-capabilities command" on page 235
- "auto-negotiation-advertisements command" on page 236
- "no auto-negotiation-advertisements command" on page 237
- "default auto-negotiation-advertisements command" on page 238

show auto-negotiation-advertisements command

The `show auto-negotiation-advertisements` command displays the current autonegotiation advertisements. The syntax for the `show auto-negotiation-advertisements` command is:

```
show auto-negotiation-advertisements [port <portlist>]
```

The `show auto-negotiation-advertisements` command is in the userExec command mode.

Table 135 describes the parameters and variables for the `show auto-negotiation-advertisements` command.

Table 135 `show auto-negotiation-advertisements` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want the current autonegotiation advertisements displayed.

Figure 56 displays sample output from the `show auto-negotiation-advertisements` command.

Figure 56 `show auto-negotiation-advertisements` command output

```
BS460_24T_PWR#show auto-negotiation-advertisements port 4,8,10
Port Autonegotiation Advertised Capabilities
------------------------------------------------------
4    10Full 10Half 100Full 100Half
8    10Full 10Half 100Full 100Half
10   10Full 10Half 100Full 100Half
```

show auto-negotiation-capabilities command

The `show auto-negotiation-capabilities` command displays the hardware advertisement capabilities for the switch. The syntax for the `show auto-negotiation-capabilities` command is:

```
show auto-negotiation-capabilities [port <portlist>]
```

The `show auto-negotiation-capabilities` command is in the userExec command mode.

Table 136 describes the parameters and variables for the `show auto-negotiation-capabilities` command.

Table 136 `show auto-negotiation-capabilities` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want the autonegotiation capabilities displayed.

Figure 57 displays sample output from the `show auto-negotiation-capabilities` command.

Figure 57 `show auto-negotiation-capabilities` command output

```
BS460_24T_PWR#show auto-negotiation-capabilities port 5,6,10
Port Autonegotiation Capabilities
---- ----------------------------------------------------------------
5    10Full 10Half 100Full 100Half
6    10Full 10Half 100Full 100Half
10   10Full 10Half 100Full 100Half
BS460_24T_PWR#
```

auto-negotiation-advertisements command

The `auto-negotiation-advertisements` command configures advertisements for the switch. The syntax for the `auto-negotiation-advertisements` command is:

```
auto-negotiation-advertisements [port <portlist>] [10-full]
[10-half] [100-full] [100-half] [1000-full] [1000-half]
[asymm-pause-frame] [pause-frame]
```

The `auto-negotiation-advertisements` command is in the interface configuration command mode.

Table 137 describes the parameters and variables for the `auto-negotiation-advertisements` command.

Table 137 `auto-negotiation-advertisements` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want to configure advertisements.

`[10-full] [10-half]`
`[100-full] [100-half]`
`[1000-full] [1000-half]`
`[asymm-pause-frame]`
`[pause-frame]`
	These are speed-duplex-pause settings. Any combination of these settings is allowed, but parameters must be given in the order shown.

no auto-negotiation-advertisements command

The `no auto-negotiation-advertisements` command clears all advertisements for the switch. This command is used for testing. The syntax for the `no auto-negotiation-advertisements` command is:

```
no auto-negotiation-advertisements [port <portlist>]
```

Note: The use of this command affects traffic and brings down the link.

The `no auto-negotiation-advertisements` command is in the interface configuration command mode.

Table 138 describes the parameters and variables for the `no auto-negotiation-advertisements` command.

Table 138 `no auto-negotiation-advertisements` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want to clear all advertisements.

default auto-negotiation-advertisements command

The `default auto-negotiation-advertisements` command sets default advertisements for the switch. The syntax for the `default auto-negotiation-advertisements` command is:

```
default auto-negotiation-advertisements [port <portlist>]
```

The `default auto-negotiation-advertisements` command is in the interface configuration command mode.

Table 139 describes the parameters and variables for the `default auto-negotiation-advertisements` command.

Table 139 `default auto-negotiation-advertisements` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want to set default advertisements.

Displaying PoE configuration

You display the status for the PoE configuration on the BayStack 470-24T using the NNCLI, using the following commands:

- "show poe-main-status command ", next
- "show poe-port-status command" on page 240
- "show poe-power-measurement command" on page 241

show poe-main-status command

The `show poe-main-status` command displays the current PoE configuration of the BayStack 470-24T, and per port PoE settings. The syntax for the `show poe-main-status` command is:

```
show poe-main-status [unit <1-8>]
```

The `show poe-main-status` command is in the exec command mode.

Table 140 describes the parameters and variables for the `show poe-main-status` command.

Table 140 `show poe-main-status` **command parameters and variables**

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to display the power statistics. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.

Figure 58 displays sample output from the `show poe-main-status` command.

Figure 58 `show poe-main-status` **command output**

```
460-24T-PWR>show poe-main-status
PoE Main Status - Unit# 1
--------------------------------------------------
Available DTE Power           : 200 Watts
DTE Power Status              : Normal
DTE Power Consumption         : 0 Watts
DTE Power Usage Threshold     : 80 %
Power Pairs                   : Spare
Traps Control Status          : Enable
PD Detect Type                : 802.3af
Power Source Present          : AC Only
DC Source Type                : BayStack 10
DC Source Configuration       : Power Sharing
```

Note: Refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches* for complete information on power sources and power configuration.
The Power Source Present displays the current power source for the switch: AC Only, DC Only, or AC and DC.

show poe-port-status command

The `show poe-port-status` command displays the status, power status, power limit, and port priority of each port. The syntax for the `show poe-port-status` command is:

```
show poe-port-status [port <portlist>]
```

The `show poe-port-status` command is in the exec command mode.

The DTE Power Status displays error messages if the port is not providing power. The following messages may appear:

- Detecting—port detecting IP device requesting power
- Delivering power—port delivering requested power to device
- Invalid PD—port detecting device that is not valid to request power
- Deny low priority—power disabled from port because of port setting and demands on power budget
- Overload—power disabled from port because port overloaded
- Test—port in testing mode
- Error—none of the other conditions apply

Table 141 describes the parameters and variables for the `show poe-port-status` command.

Table 141 `show poe-port-status` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you wan to display the status. Note: If you omit this parameter, the system displays all ports

Figure 59 displays sample output from the `show poe-port-status` command.

Figure 59 `show poe-port-status` command output

```
460-24T-PWR>show poe-port-status
           Admin      Current               Limit
Unit/Port  Status     Status               (Watts)  Priority
---------  -------    -----------------    -------  --------
1/1        Enable     Detecting            16       Low
1/2        Enable     Detecting            16       Low
1/3        Enable     Detecting            16       Low
1/4        Enable     Detecting            16       Low
1/5        Enable     Detecting            16       Low
1/6        Enable     Detecting            16       Low
1/7        Enable     Detecting            16       Low
1/8        Enable     Detecting            16       Low
1/9        Enable     Detecting            16       Low
1/10       Enable     Detecting            16       Low
1/11       Enable     Detecting            16       Low
1/12       Enable     Detecting            16       Low
1/13       Enable     Detecting            16       Low
1/14       Enable     Detecting            16       Low
1/15       Enable     Detecting            16       Low
1/16       Enable     Detecting            16       Low
1/17       Enable     Detecting            16       Low
1/18       Enable     Detecting            16       Low
1/19       Enable     Detecting            16       Low
1/20       Enable     Detecting            16       Low
1/21       Enable     Detecting            16       Low
1/22       Enable     Detecting            16       Low
1/23       Enable     Detecting            16       Low
1/24       Enable     Detecting            16       Low
--More--
```

show poe-power-measurement command

The `show poe-power-measurement` command displays the voltage, current and power values for each powered device connected to each port. The syntax for the `show poe-power-measurement` command is:

`show poe-power-measurement [port <`*`portlist`*`>]`

The `show poe-power-measurement` command is in the exec command mode.

Table 142 shows the variables and parameters for the `show poe-power-measurement` command.

Table 142 show poe-power-measurement command parameters

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to display the power measurements. Note: If you omit this parameter, the system displays all ports.

Figure 60 displays sample output from the `show poe-power-measurement` command.

Figure 60 `show poe-power-measurement` command output

```
460-24T-PWR>show poe-power-measurement
Unit/Port   Volt(V)   Current(mA)    Power(Watt)
---------   -------   -----------    ---------------
1/1         0.0       0              0.000
1/2         0.0       0              0.000
1/3         0.0       0              0.000
1/4         0.0       0              0.000
1/5         0.0       0              0.000
1/6         0.0       0              0.000
1/7         0.0       0              0.000
1/8         0.0       0              0.000
1/9         0.0       0              0.000
-More--
```

Configuring FEFI

When a fiber optic transmission link to a remote device fails, the remote device indicates the failure and the port is disabled. To use Far End Fault Indication (FEFI), the user must enable autonegotiation on the port.

Configuring SFFD

When a partial fiber break occurs, data is lost on one side of a link. Single Fiber Fault Detection (SFFD) detects this error condition, and causes the port that is losing data to go down. This stops the loss of data.

The Single Fiber Fault Detection feature is enabled on a port by port basis for the BayStack 470-24T and 470-48T GBIC ports. At present, you can access this feature through the NNCLI.

Single Fiber Fault Detection (SFFD) has the following requirements and limitations:

- SFFD must be implemented on both sides of a link. For example: Passport 8600 and BoSS 3.0
- SFFD must be enabled on a per-port basis
- By default, SFFD is disabled on all ports
- SFFD takes about 50 seconds to detect a fault
- Once a link is repaired, the link recovers automatically

This section lists the CLI commands that are used on the BayStack products to support the SFFD feature:

- "show sffd command ", next
- "sffd enable command" on page 244
- "no sffd enable command" on page 245
- "default sffd enable command" on page 245

show sffd command

The `show sffd` command displays the SFFD configuration information for all ports with the SFFD feature. The display also indicates whether the SFFD feature is enabled or disabled. The syntax of the `show sffd` command is:

```
show sffd
```

The `show sffd` command is in ALL of the NNCLI modes (e.g., User EXEC, Privileged EXEC, Global Configuration, and Interface Configuration).

The `show sffd` command has no parameters or variables.

Figure 61 displays the `show sffd` command output.

Figure 61 `show sffd` command output

```
 BS470-48T#show sffd
Port  SFFD Mode
----  ---------
47     Disabled
BS470-48T#
```

sffd enable command

The `sffd enable` command enables the SFFD feature on specified ports, and is only available in the NNCLI using the interface configuration mode. The syntax of the `sffd enable` command is:

```
sffd [port <portlist>] enable
```

The `sffd enable` command is in the config-if command mode.

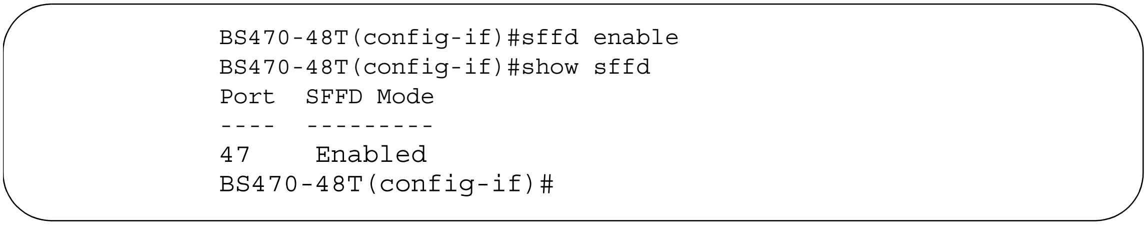
Table 143 describes the parameters and variables for the `sffd enable` command.

Table 143 `sffd enable` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to enable the SFFD feature. The portlist may be separated by commas or dashes. For example: 2/16, 3/16, or 2/26 - 2/27. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Figure 62 displays sample output from the `sffd enable` command.

Figure 62 `sffd enable` command output



```
BS470-48T(config-if)#sffd enable
BS470-48T(config-if)#show sffd
Port  SFFD Mode
----  ---------
47     Enabled
BS470-48T(config-if)#
```

no sffd enable command

The `no sffd enable` command disables the SFFD feature on specified ports, and is only available in the NNCLI using the interface configuration mode. The syntax of the `no sffd enable` command is:

```
no sffd [port <portlist>] enable
```

The `no sffd enable` command is in the config-if command mode.

Table 144 describes the parameters and variables for the `no sffd enable` command.

Table 144 `no sffd enable` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable the SFFD feature. The portlist may be separated by commas or dashes. For example: 2/16, 3/16, or 2/26 - 2/27. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

default sffd enable command

The `default sffd enable` command changes the SFFD feature on specified ports to the factory default setting. The factory default setting is disabled. The syntax of the `default sffd enable` command is:

```
default sffd [port <portlist>] enable
```

The `default sffd enable` command is in the config-if command mode.

Table 145 describes the parameters and variables for the `default sffd enable` command.

Table 145 `default sffd enable` command parameters and variables

Parameters and variables	Description
port <*portlist*>	Specifies the port numbers to change the SFFD feature to the factory default of disabled. The portlist may be separated by commas or dashes. For example: 2/16, 3/16, or 2/26 - 2/27. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Configuring power parameters on the switch

You configure power parameters for each BayStack 470-24T using the NNCLI. You can configure the DC power source, the power pairs, and the power usage with this management system. This section covers the following topics:

- "poe poe-dc-source-type command ", next
- "poe poe-dc-source-conf command" on page 247
- "poe poe-pd-detect-type command" on page 248
- "poe poe-power-pairs command" on page 249
- "poe poe-power-usage-threshold command" on page 251
- "poe poe-trap command" on page 251
- "no poe-trap command" on page 252

poe poe-dc-source-type command

The `poe poe-dc-source-type` command allows you to set the type of external DC power source you are using with the switch. The syntax for the `poe poe-dc-source-type` command is:

```
poe poe-dc-source-type [unit <1-8>] {baystack10|nes}
```

The `poe poe-dc-source-type` command is in the config mode.

Table 146 describes the parameters and variables for the `poe poe-dc-source-type` command.

Table 146 `poe poe-dc-source-type` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number that you want to configure for an external power source. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.
`baystack10|nes`	Sets the type of external DC power source you are using: • `baystack10`—sets the external DC power source as the BayStack 10 PSU • `nes`—sets the external DC power source as the Intergy* Network Energy Source (NES) from Invensys Energy Systems Note: The default setting is `baystack10`. You set this parameter whether or not you are physically attached to an external power source. For more information on power sharing, RPSU, and UPS DC source type options, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

poe poe-dc-source-conf command

The `poe poe-dc-source-conf` command allows you to configure the type of power sharing you want to use on the BayStack 470-24T. The syntax for the `poe poe-dc-source-conf` command is:

```
poe poe-dc-source-conf [unit <1-8>] {powersharing|rpsu|ups}
```

The `poe poe-dc-source-conf` command is in the config mode.

Table 147 describes the parameters and variables for the `poe poe-dc-source-conf` command.

Table 147 `poe poe-dc-source-conf` **command parameters and variables**

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to configure the power-sharing option. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.
`powersharing|rpsu|ups`	Sets the type of powersharing for the BayStack 470-24T: • `powersharing` • `rpsu` • `ups` Note: The default setting is `powersharing`. You set this parameter whether or not you are physically attached to an external power source. For more information on power sharing, RPSU, and UPS DC source type options, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

poe poe-pd-detect-type command

The `poe poe-pd-detect-type` command sets the method the BayStack 470-24T uses to detect the power devices connected to the front ports. The syntax for the `poe poe-pd-detect-type` command is:

```
poe poe-pd-detect-type [unit <1-8>]
{802dot3af|802dot3af_and_legacy}
```

The `poe poe-pd-detect-type` command is in the config mode.

Note: You must ensure that this setting is the correct one for the IP appliance you are using with the switch. Please note this setting applies to the entire switch, not port-by-port. So, you must ensure that this setting is configured correctly for *all* the IP appliances you have on a specified switch.

Table 148 describes the parameters and variables for the `poe poe-pd-detect-type` command.

Table 148 `poe poe-pd-detect-type` command parameters and variables

Parameters and variables	**Description**
`unit <1-8>`	Enter the unit number for which you want to configure the power option detection. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.
`802dot3af|802dot3af_and_legacy`	Sets the detection method the switch use to detect power needs of devices connected to front ports: • `802dot3af` • `802dot3af_and_legacy` Note: The default setting is 802dot3af. Ensure that the power detection method you choose for the BayStack 470-24T matches that used by the IP devices you are powering. Refer to *Using the Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches* for information on power detection.

poe poe-power-pairs command

The `poe poe-power-pairs` command sets the RJ-45 connector pins on the front port that you will use to deliver power to the device. The syntax for the `poe poe-power-pairs` command is:

```
poe poe-power-pairs [unit <1-8>] {spare|signal}
```

The `poe poe-power-pairs` command is in the config mode.

➡ **Note:** You must ensure that this setting is the correct one for the IP appliance you are using with the switch. Please note this setting applies to the entire switch, not port-by-port. So, you must ensure that this setting is configured correctly for *all* the IP appliances you have on a specified switch.

Table 149 describes the parameters and variables for the `poe poe-power-pairs` command.

Table 149 `poe poe-power-pairs` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to configure the power pairs. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.
`spare|signal`	Sets the type of external DC power source you are using: • `spare`—sets power-carrying pins to the spare set • `signal`—sets power-carrying pins to the signal set The default value is spare. Refer to *Using the Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches* for complete information on power pairs. Note: Ensure that the power pair you choose for the BayStack 470-24T matches the power pair used by the IP devices you are powering. Each unit uses the same power pairs; you cannot configure this on each port.

poe poe-power-usage-threshold command

The `poe poe-power-usage-threshold` command allows you to set a percentage usage threshold above which the system sends a trap for each BayStack 470-24T. The syntax for the `poe poe-power-usage-threshold` command is:

```
poe poe-power-usage-threshold [unit <1-8>] <1-99>
```

The `poe poe-power-usage-threshold` command is in the config mode.

Table 150 describes the parameters and variables for the `poe poe-power-usage-threshold` command.

Table 150 `poe poe-power-usage-threshold` command parameters

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to configure the trap generation. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.
`<1-99>`	Enter the percentage of total available power you want the switch to use prior to sending a trap. Note: The default setting is 80%.

poe poe-trap command

The `poe poe-trap` command enables the traps for the PoE functions on the BayStack 470-24T. The syntax for the `poe poe-trap` command is:

```
poe poe-trap [unit <1-8>]
```

The `poe poe-trap` command is in the config mode.

Table 151 describes the parameters and variables for the `poe poe-trap` command.

Table 151 `poe poe-trap` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to enable traps. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.

no poe-trap command

The `no poe-trap` command disables the traps for the PoE functions on the BayStack 470-24T. The syntax for the `no poe-trap` command is:

```
no poe-trap [unit <1-8>]
```

The `no poe-trap` command is in the config mode.

Table 152 describes the parameters and variables for the `no poe-trap` command.

Table 152 `no poe-trap` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to disable traps. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.

Configuring power parameters on the ports

You can configure power parameters for each port on the BayStack 470-24T using the NNCLI. You enable the power and set the power limit and power priority on each port. This section covers the following topics:

- "no poe-shutdown command ", next
- "poe poe-shutdown command" on page 253
- "poe poe-priority command" on page 254
- "poe poe-limit command" on page 255

no poe-shutdown command

The `no poe-shutdown` command enables power to the port. The syntax for the `no poe-shutdown` command is:

```
no poe-shutdown [port <portlist>]
```

The `no poe-shutdown` command is in the config-if mode.

Table 153 describes the parameters and variables for the `no poe-shutdown` command.

Table 153 `no poe-shutdown` command parameters and variables

Parameters and variables	**Description**
`port <portlist>`	Enter the port number you want to enable power on. The default value is enabled. Note: If you omit this parameter, the system uses the port entered with the `interface FastEthernet` command.

poe poe-shutdown command

The `poe poe-shutdown` command disables power to the port. The syntax for the `poe poe-shutdown` command is:

```
poe poe-shutdown [port <portlist>]
```

The `poe poe-shutdown` command is in the config-if mode.

Table 154 describes the parameters and variables for the `poe poe-shutdown` command.

Table 154 `poe poe-shutdown` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the port number you want to disable power on. The default value is enabled. Note: If you omit this parameter, the system uses the port entered with the `interface FastEthernet` command.

poe poe-priority command

The `poe poe-priority` command allows you to set the power priority for each port to low, high, or critical. The system uses the port power priority settings to distribute power to the ports depending on the available power budget. The syntax for the `poe poe-priority` command is:

```
poe poe-priority [port <portlist>] {low|high|critical}
```

The `poe poe-priority` command is in the config-if mode.

Table 155 describes the parameters and variables for the `poe poe-priority` command.

Table 155 `poe poe-priority` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the port number(s) you want to disable power on. Note: If you omit this parameter, the system uses the port entered with the `interface FastEthernet` command.
`low|high|critical`	Sets the port priority as: • `low` • `high` • `critical` Note: The default setting is low. When two ports have the same priority and one must be shut down, the port with the higher port number is shut down first. For more information on port priority and overall power balancing, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

poe poe-limit command

The `poe poe-limit` command sets the maximum power allowed to a port. The syntax for the `poe poe-limit` command is:

```
poe poe-limit [port <portlist>] <3-20>
```

The `poe poe-limit` command is in the config-if mode.

Table 156 describes the parameters and variables for the `poe poe-limit` command.

Table 156 `poe poe-limit` command parameters and variables

Parameters and variables	Description
<3-20>	Enter the maximum number of Watts you want to allow to the specified port. The range is 3W to 20W; the default value is 16W.
`ports`	Enter the port number you want to disable power on. Note: If you omit this parameter, the system uses the port entered with the `interface FastEthernet` command.

Chapter 6
Virtual Local Area Networks

This chapter describes how to configure and display VLANs using a variety of command modes, depending on whether you are working with ports, protocol-based VLANs, or MAC source address-based VLANs. You can also enable or disable the automatic PVID feature.This chapter covers the following topics:

- "Creating a VLAN ", next
- "Deleting a VLAN" on page 260
- "Changing the management VLAN assignment" on page 262
- "Changing the VLAN name" on page 263
- "Displaying VLAN information" on page 263
- "Creating, deleting and displaying a MAC address-based VLAN" on page 266
- "Displaying IP multicast sessions in your network" on page 272
- "Configuring automatic PVID" on page 273
- "Configuring VLAN-related port settings" on page 274
- "Configuring an 802.1Q VLAN workgroups" on page 276
- "IEEE 802.1Q tagging" on page 276

Refer to the *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches* for more information on VLANs, as well as configuration directions using the console interface (CI) menus. Refer to Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches for information on configuring these features using the Web-based management system, and refer to Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches for configuration information for the DM.

➡ **Note:** The standalone or stack of switches must be operating in Pure Stack mode. Refer to "Configuring the stack operational mode" on page 72 for information on configuring the stack operational mode.

Refer to Appendix A, "Command List for an alphabetical list of the VLAN commands.

➡ **Note:** For guidelines for configuring VLANs, spanning tree groups, and MLTs, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

Creating a VLAN

You can create a VLAN using the CLI.

vlan create command

The `vlan create` command allows you to create a VLAN. You can create a VLAN by setting the state of a previously non-existent VLAN.

The syntax for the `vlan create` command is:

```
vlan create <1-4094>] [name <line>]
type
{macsa|
port|
protocol-ipEther2|
protocol-ipx802.3|
protocol-ipx802.2|
protocol-ipxSnap|
protocol-ipxEther2|
protocol-ApltkEther2Snap|
protocol-decEther2|
protocol-decOtherEther2|
protocol-sna802.2|
protocol-snaEther2|
protocol-Netbios|
protocol-xnsEther2|
protocol-vinesEther2|
protocol-ipv6Ether2|
protocol-Userdef <4096-65534>|
protocol-RarpEther2}
[learning {IVL|SVL}]
```

The `vlan create` command is in the config command mode.

Table 157 describes the parameters and variables for the `vlan create` command.

Table 157 `vlan create` command parameters and variables

Parameters and variables	Description
`<1-4094>`	Enter the number of the VLAN to create.
`name <line>`	Enter the name of the VLAN to create.
`type`	Enter the type of VLAN to create: • macsa—MAC source address-based • port—port-based • protocol—protocol-based (see following list)
`protocol-ipEther2`	Specifies an ipEther2 protocol-based VLAN.
`protocol-ipx802.3`	Specifies an ipx802.3 protocol-based VLAN.
`protocol-ipx802.2`	Specifies an ipx802.2 protocol-based VLAN.
`protocol-ipxSnap`	Specifies an ipxSnap protocol-based VLAN.
`protocol-ipxEther2`	Specifies an ipxEther2 protocol-based VLAN.
`protocol-ApltkEther2Snap`	Specifies an ApltkEther2Sanp protocol-based VLAN.
`protocol-decEther2`	Specifies a decEther2 protocol-based VLAN.
`protocol-decOtherEther2`	Specifies a decOtherEther2 protocol-based VLAN.
`protocol-sna802.2`	Specifies an sna802.2 protocol-based VLAN.
`protocol-snaEther2`	Specifies an snaEther2 protocol-based VLAN.
`protocol-Netbios`	Specifies a NetBIOS protocol-based VLAN.
`protocol-xnsEther2`	Specifies an xnsEther2 protocol-based VLAN.

Table 157 `vlan create` command parameters and variables (Continued)

Parameters and variables	Description
`protocol-vinesEther2`	Specifies a vinesEther2 protocol-based VLAN.
`protocol-ipv6Ether2`	Specifies an ipv6Ether2 protocol-based VLAN.
`protocol-Userdef <4096-65534>`	Specifies a user-defined protocol-based VLAN.
`protocol-RarpEther2`	Specifies an RarpEther2 protocol-based VLAN.
`learning {IVL|SVL}`	Enter the type of learning you want for the VLAN: • IVL—independent VLAN learning • SVL—shared VLAN learning **Note**: IVL is available *only* when you are operating in the Pure BS 470-24T stack mode. **Note:** The Hybrid stack mode is not supported on this release of the BayStack 470-24T.

Note: This command fails if the VLAN already exists.

Deleting a VLAN

You can delete a VLAN using the CLI. This section covers the following commands:

- "vlan delete command ", next
- "no vlan command" on page 261

vlan delete command

The `vlan delete` command allows you to delete a VLAN. The syntax for the `vlan delete` command is:

```
vlan delete <1-4094>
```

The `vlan delete` command is in the config command mode.

Table 158 describes the parameters and variables for the `vlan delete` command.

Table 158 `vlan delete` command parameters and variables

Parameters and variables	Description
<1-4094>	Enter the number of the VLAN to delete.

no vlan command

The `no vlan` command allows you to delete a VLAN. The syntax for the `no vlan` command is:

```
no vlan <1-4094>
```

The `no vlan` command is in the config command mode.

Table 159 describes the parameters and variables for the `no vlan` command.

Table 159 `no vlan` command parameters and variables

Parameters and variables	Description
<1-4094>	Enter the number of the VLAN to delete. Omitting this variable will remove all VLANs except for VLAN1, which cannot be deleted.

Changing the management VLAN assignment

You can change the management VLAN assignment using the CLI. This section covers the following commands:

- "vlan mgmt command ", next
- "default vlan mgmt command" on page 262

vlan mgmt command

The `vlan mgmt` command allows you to set a VLAN as the management VLAN. The syntax for the `vlan mgmt` command is:

```
vlan mgmt <1-4094>
```

The `vlan mgmt` command is in the config command mode.

Table 160 describes the parameters and variables for the `vlan mgmt` command.

Table 160 `vlan mgmt` command parameters and variables

Parameters and variables	Description
<1-4094>	Enter the number of the VLAN you want to serve as the management VLAN.

default vlan mgmt command

The `default vlan mgmt` command resets the management VLAN to VLAN1. The syntax for the `default vlan mgmt` command is:

```
default vlan mgmt
```

The `default vlan mgmt` command is in the config command mode.

The `default vlan mgmt` command has no variables or parameters.

Changing the VLAN name

You can change the VLAN name using the CLI.

vlan name command

The `vlan name` command allows you to change the name of an existing VLAN. The syntax for the `vlan name` command is:

```
vlan name <1-4094> <line>
```

The `vlan name` command is in the config command mode.

Table 161 describes the parameters and variables for the `vlan name` command.

Table 161 `vlan name` command parameters and variables

Parameters and variables	**Description**
<1-4094>	Enter the number of the VLAN you want to change the name of.
<line>	Enter the new name you want for the VLAN.

Displaying VLAN information

You can display the VLAN information using the CLI. This section covers the following commands:

- "show vlan interface info command ", next
- "show vlan interface vids command" on page 265

show vlan interface info command

The `show vlan interface info` command displays VLAN settings associated with a port, including tagging information, PVID number, priority, and filtering information for tagged, untagged, and unregistered frames. The syntax for the `show vlan interface info` command is:

```
show vlan interface info [<portlist>]
```

The `show vlan interface info` command is in the privExec command mode.

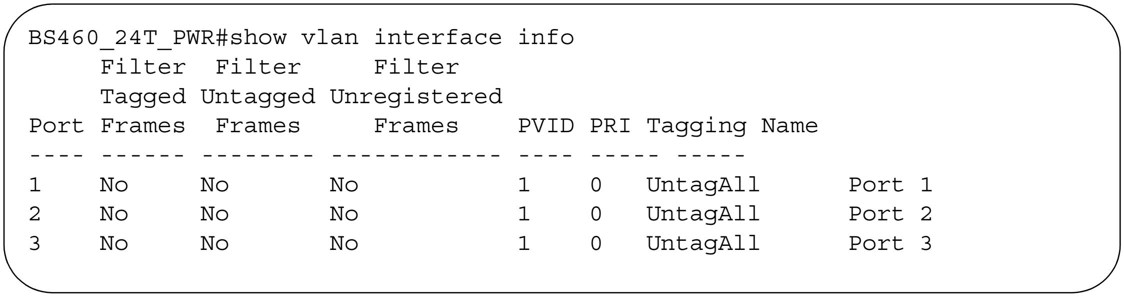
Table 162 describes the parameters and variables for the `show vlan interface info` command.

Table 162 `show vlan` command interface info parameters and variables

Parameters and variables	Description
<portlist>	Enter the list of ports you want the VLAN information for, or enter all to display all ports.

Figure 63 displays sample output from the `show vlan interface info` command.

Figure 63 `show vlan interface info` command output



```
BS460_24T_PWR#show vlan interface info
     Filter  Filter     Filter
     Tagged Untagged Unregistered
Port Frames  Frames     Frames     PVID PRI Tagging Name
---- ------ -------- ------------ ---- ----- -----
1    No     No       No           1    0   UntagAll      Port 1
2    No     No       No           1    0   UntagAll      Port 2
3    No     No       No           1    0   UntagAll      Port 3
```

show vlan interface vids command

The `show vlan interface vids` command displays port memberships in VLANs. The syntax for the `show vlan interface vids` command is:

```
show vlan interface vids [<portlist>]
```

The `show vlan interface vids` command is in the privExec command mode.

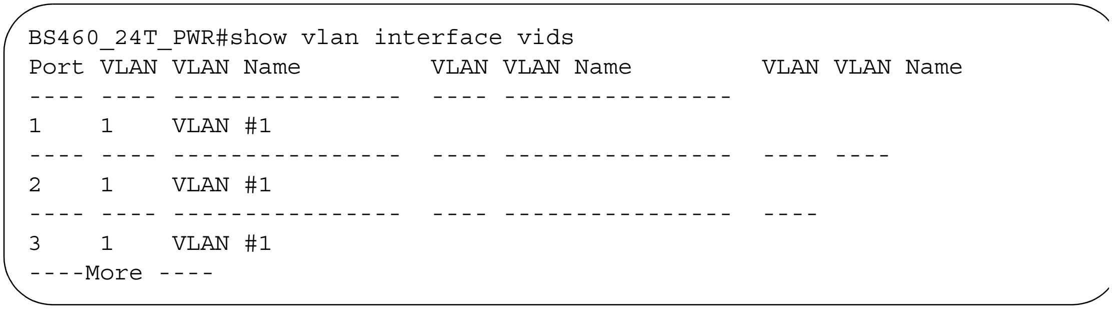
Table 163 describes the parameters and variables for the `show vlan interface vids` command.

Table 163 `show vlan interface vids` command parameters and variables

Parameters and variables	Description
<portlist>	Enter the list of ports you want the VLAN information for, or enter all to display all ports.

Figure 64 displays sample output from the `show vlan interface vids` command.

Figure 64 `show vlan interface vids` output



```
BS460_24T_PWR#show vlan interface vids
Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
---- ---- ----------------  ---- ----------------
1    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----
2    1    VLAN #1
---- ---- ----------------  ---- ----------------  ----
3    1    VLAN #1
----More ----
```

Creating, deleting and displaying a MAC address-based VLAN

You can create, delete and display a MAC address-based VLAN using the following CLI commands:

- "vlan mac-address command ", next
- "no vlan mac-address command" on page 267
- "show vlan mac-address command" on page 267
- "Managing MAC address forwarding database table" on page 268

vlan mac-address command

The `vlan mac-address` command adds MAC addresses to MAC source-address-based VLANs. The `vlan mac-address` syntax is:

```
vlan mac-address <1-4094> address <H.H.H>
```

The `vlan mac-address` command is in the config command mode.

Table 164 describes the parameters and variables for the `vlan mac-address` command.

Table 164 `vlan mac-address` command parameters and variables

Parameters and variables	Description
<1-4094>	Enter the number of the VLAN you want to add a MAC source address to.
address *<H.H.H.>*	Enter the MAC source address to assign to the VLAN.

no vlan mac-address command

The `no vlan mac-address` command removes MAC addresses from MAC source-address-based VLANs. The `no vlan mac-address` syntax is:

```
no vlan mac-address <1-4094> address <H.H.H>
```

The `no vlan mac-address` command is in the config command mode.

Table 165 describes the parameters and variables for the `no vlan mac-address` command.

Table 165 `no vlan mac-address` command parameters and variables

Parameters and variables	Description
<1-4094>	Enter the number of the VLAN you want to remove a MAC source address from.
address *<H.H.H.>*	Enter the MAC source address to remove from the VLAN.

show vlan mac-address command

The `show vlan mac-address` command displays the configured MAC address for a MAC source address-based VLAN. The syntax for the `show vlan mac-address` command is:

```
show vlan mac-address <1-4094> [address H.H.H]
```

The `show vlan mac-address` command is in the privExec mode.

Table 166 describes the parameters and variables for the `show vlan mac-address` command.

Table 166 `show vlan mac-address` command parameters and variables

Parameters and variables	Description
<1-4094>	Enter the number of the VLAN you want to display MAC source addresses for.
`address H.H.H`	Specifies a particular MAC address to display; enter the MAC address in the H.H.H. format. Note: If you omit this parameter, the system displays the entire table.

Figure 65 displays sample output from the `show vlan mac-address` command.

Figure 65 `show vlan mac-address` command output

```
BS470_24(config)#show vlan mac-address 6
Active MAC Addresses
---------------------------------------------------------
08-00-01-02-02-03
```

Managing MAC address forwarding database table

This section shows you how to view the contents of the MAC address forwarding database table, as well as setting the age-out time for the addresses. The following topics are covered:

- “show mac-address-table command ”,” next
- “mac-address-table aging-time command” on page 270
- “default mac-address-table aging-time command” on page 271
- “stack bootp-mac-addr-type command” on page 271

show mac-address-table command

The `show mac-address-table` command displays the current contents of the MAC address forwarding database table. You can now filter the MAC Address table by port number.

The syntax for the `show mac-address-table` command is:

```
show mac-address-table [vid <1-4094>] [aging-time] [address
<H.H.H>] [port <portlist>]
```

The `show mac-address-table` command is in the privExec command mode.

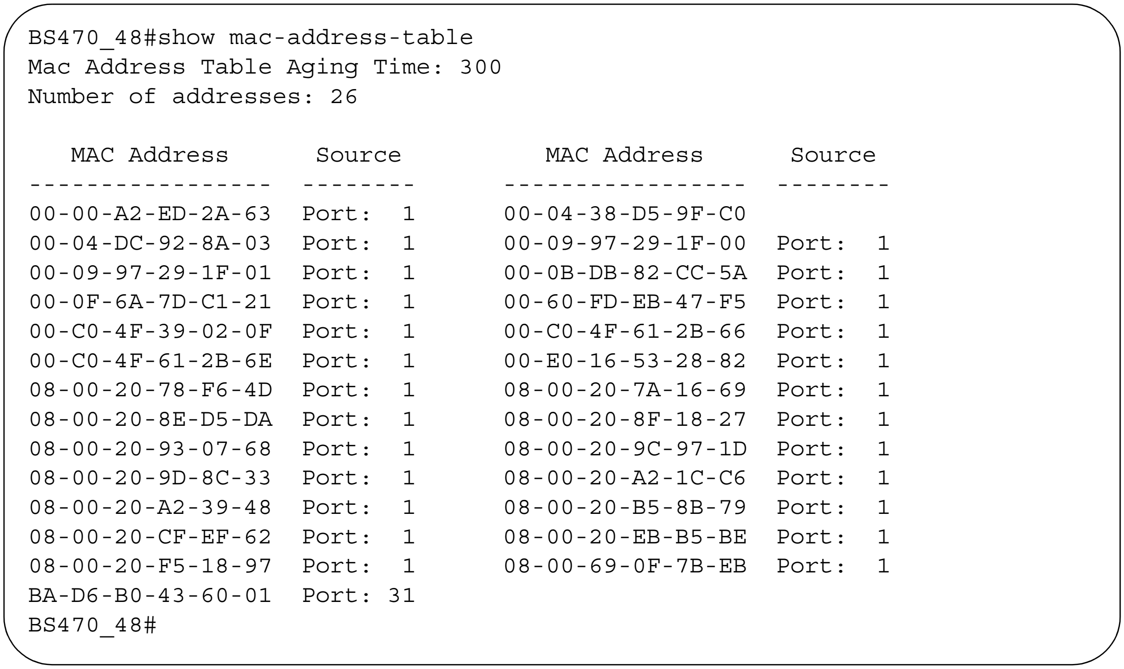
Table 167 describes the parameters and variables for the `show mac-address-table` command.

Table 167 `show mac-address-table` command parameters and variables

Parameters and variables	Description
`vid <1-4094>`	Enter the number of the VLAN for which you want to display the forwarding database. Default is to display the management VLAN's database.
`aging-time`	Displays the time in seconds after which an unused entry is removed from the forwarding database.
`address <H.H.H>`	Displays a specific MAC address if it exists in the database. Enter the MAC address you want displayed.

Figure 66 displays sample output from the `show mac-address-table` command.

Figure 66 `show mac-address-table` command output



```
BS470_48#show mac-address-table
Mac Address Table Aging Time: 300
Number of addresses: 26

   MAC Address      Source          MAC Address      Source
-----------------  --------      -----------------  --------
00-00-A2-ED-2A-63  Port:  1      00-04-38-D5-9F-C0
00-04-DC-92-8A-03  Port:  1      00-09-97-29-1F-00  Port:  1
00-09-97-29-1F-01  Port:  1      00-0B-DB-82-CC-5A  Port:  1
00-0F-6A-7D-C1-21  Port:  1      00-60-FD-EB-47-F5  Port:  1
00-C0-4F-39-02-0F  Port:  1      00-C0-4F-61-2B-66  Port:  1
00-C0-4F-61-2B-6E  Port:  1      00-E0-16-53-28-82  Port:  1
08-00-20-78-F6-4D  Port:  1      08-00-20-7A-16-69  Port:  1
08-00-20-8E-D5-DA  Port:  1      08-00-20-8F-18-27  Port:  1
08-00-20-93-07-68  Port:  1      08-00-20-9C-97-1D  Port:  1
08-00-20-9D-8C-33  Port:  1      08-00-20-A2-1C-C6  Port:  1
08-00-20-A2-39-48  Port:  1      08-00-20-B5-8B-79  Port:  1
08-00-20-CF-EF-62  Port:  1      08-00-20-EB-B5-BE  Port:  1
08-00-20-F5-18-97  Port:  1      08-00-69-0F-7B-EB  Port:  1
BA-D6-B0-43-60-01  Port: 31
BS470_48#
```

There are no default values for this command.

mac-address-table aging-time command

The `mac-address-table aging-time` command sets the time that the switch retains unseen MAC addresses. The syntax for the `mac-address-table aging-time command` is:

```
mac-address-table aging-time <10-1000000>
```

The `mac-address-table aging-time` command is in the config command mode.

Table 168 describes the parameters and variables for the `mac-address-table aging-time` command.

Table 168 `mac-address-table aging-time` **command parameters**

Parameters and variables	Description
<10-1000000>	Enter the aging time in seconds that you want for MAC addresses before they are flushed.

default mac-address-table aging-time command

The `default mac-address-table aging-time` command sets the time that the switch retains unseen MAC addresses to 300 seconds. The syntax for the `default mac-address-table aging-time` command is:

```
default mac-address aging-time
```

The `default mac-address-table aging-time` command is in the config command mode.

The `default mac-address-table aging-time` command has no parameters or variables.

stack bootp-mac-addr-type command

The `stack bootp-mac-addr-type` command allows you to choose which MAC address is used for BootP operation when running in a stack. This option is available only on a stack consisting of all BayStack 470-24T that is set for stack operational mode. The syntax for the `stack bootp-mac-address-type` command is:

```
stack bootp-mac-addr-type {base-unit|stack}
```

The `stack bootp-mac-addr-type` command is in the config command mode.

Table 169 describes the parameters and variables for the `stack boot-mac-addr-type` command.

Table 169 `stack boot-mac-addr-type` command parameters and variables

Parameters and variables	Description
`base-unit|` `stack`	Specifies location of BootP MAC address: • `base-unit`—use the base unit MAC address for BootP • `stack`—use the stack MAC address for BootP

Displaying IP multicast sessions in your network

You can display the membership of multicast groups using the CLI.

show vlan multicast membership command

The `show vlan multicast membership` command displays the IP multicast sessions in the network. The syntax for the `show vlan multicast membership` command is:

```
show vlan multicast membership <1-4094>
```

The `show vlan multicast membership` command is in the privExec mode.

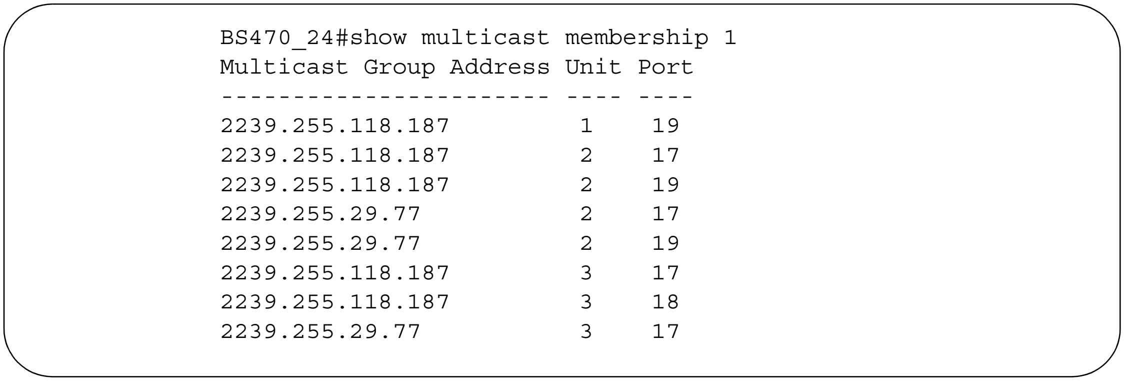
Table 170 describes the parameters and variables for the `show vlan multicast membership` command.

Table 170 `show vlan multicast membership` command parameters and variables

Parameters and variables	Description
<1-4094>	Specifies the VLAN to display IP multicast sessions.

Figure 67 displays sample output from the `show vlan multicast membership` command.

Figure 67 `show vlan multicast membership` command output



```
BS470_24#show multicast membership 1
Multicast Group Address Unit Port
----------------------- ---- ----
2239.255.118.187          1    19
2239.255.118.187          2    17
2239.255.118.187          2    19
2239.255.29.77            2    17
2239.255.29.77            2    19
2239.255.118.187          3    17
2239.255.118.187          3    18
2239.255.29.77            3    17
```

Configuring automatic PVID

You can enable or disable the automatic PVID feature using the CLI. This section covers the following commands:

- “auto-pvid command ””, next
- “no auto-pvid command” on page 274

auto-pvid command

The `auto-pvid` command allows you to enable the automatic PVID feature. The syntax for the `auto-pvid` command is:

```
auto-pvid
```

The `auto-pvid` command is in the config command mode.

The `auto-pvid` command has no parameters or variables.

For more information on the automatic PVID feature, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

no auto-pvid command

The `no auto-pvid` command allows you to disable the automatic PVID feature. The syntax for the `no auto-pvid` command is:

```
no auto-pvid
```

The `no auto-pvid` command is in the config command mode.

The `no auto-pvid` command has no parameters or variables.

For more information on the automatic PVID feature, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

Configuring VLAN-related port settings

You can configure VLAN-related port setting using the CLI. This section covers the following commands:

- "vlan ports command "", next
- "vlan members command" on page 275

vlan ports command

The `vlan ports` command configures the VLAN-related settings for a port.The syntax for the `vlan ports` command is:

```
vlan ports [<portlist>] [tagging
{enable|disable|tagAll|untagAll|tagPvidOnly|untagPvidOnly}]
[pvid <1-4094>] [filter-tagged-frame {enable|disable}]
[filter-untagged-frame {enable|disable}]
[filter-unregistered-frames {enable|disable}]
[priority <0-7>] [name <line>]
```

The `vlan ports` command is in the config command mode.

Table 171 describes the parameters and variables for the `vlan ports` command.

Table 171 `vlan ports` command parameters and variables

Parameters and variables	Description
<*portlist*>	Enter the port number(s) you want to configure for a VLAN.
tagging {enable|disable|tagAll|untagAll|tagPvidOnly|untagPvidOnly}	Enables or disables the port as a tagged VLAN member for egressing packet.
pvid <*1-4094*>	Associates the port with a specific VLAN
filter-tagged-frame {enable|disable}	Enables or disables the port to filter received tagged packets.
filter-untagged-frame {enable|disable}	Enables or disables the port to filter received untagged packets.
filter-unregistered-frames {enable|disable}	Enables or disables the port to filter received unregistered packets.
priority <*0-7*>	Sets the port as a priority for the switch to consider as it forwards received packets.
name <*line*>	Enter the name you want for this port. Note: This option can only be used if a single port is specified in the <portlist>.

vlan members command

The `vlan members` command adds a port to or deletes a port from a VLAN. The syntax for the `vlan members` command is:

```
vlan members [add|remove] <1-4094> <portlist>
```

The `vlan members` command is in the config mode.

Table 172 describes the parameters and variables for the `vlan members` command.

Table 172 `vlan members` command parameters and variables

Parameters and variables	Description
`add|remove`	Adds a port to or removes a port from a VLAN. Note: If you omit this parameter, you are setting the exact port membership for the VLAN; the prior port membership of the VLAN is discarded and replaced by the new list of ports.
<1-4094>	Specifies the target VLAN.
`portlist`	Enter the list of port(s) you are adding, removing, or assigning to the VLAN.

Configuring an 802.1Q VLAN workgroups

BayStack 460-24T-PWR and BayStack 470 switches support up to 256 VLANs (maximum of 48 MAC source address-based VLANs) with IEEE 802.1Q tagging available per port.

Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in one VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN.

IEEE 802.1Q tagging

BayStack 460-24T-PWR and BayStack 470 switches operate in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 802.1Q tagging feature are:

- Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches for information on overriding the default values.

- Port VLAN identifier (PVID)—a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3. You can automatically assign the PVIDs.
- Tagged frame—the 32-bit field (VLAN tag) in the frame header that identifies the frame as belonging to a specific VLAN. Untagged frames are marked (tagged) with this classification as they leave the switch through a port that is configured as a tagged port.
- Untagged frame— a frame that does not carry any VLAN tagging information in the frame header.
- VLAN port members— a set of ports that form a broadcast domain for a specific VLAN. A port can be a member of one or more VLANs.
- Untagged member—a port that has been configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- Tagged member—a port that has been configured as a member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).
- User priority—a three-bit field in the header of a tagged frame. The field is interpreted as a binary number, therefore has a value of 0 - 7. This field allows the tagged frame to carry the user-priority across bridged LANs where the individual LAN segments may be unable to signal priority information.
- Port priority—the priority level assigned to *untagged* frames received on a port. This value becomes the user priority for the frame. *Tagged* packets get their user priority from the value contained in the 802.1Q frame header.
- Unregistered packet—a tagged frame that contains a VID where the receiving port is not a member of that VLAN.
- Filtering database identifier (FID)—the specific filtering/forwarding database within the BayStack Switch that is assigned to each VLAN. The current version of software assigns all VLANs to the same FID when it is running in the Hybrid Operational mode. This process is referred to as Shared VLAN Learning (SVL) in the IEEE 802.1Q specification. A VLAN may either share its filtering database with other VLANs (SVL) or have its own filtering database, which is called Independent VLAN Learning (IVL).

Chapter 7 Multilink Trunking

This chapter describes how to configure the Multi-Link Trunking (MLT) and Link Aggregation Group (LAG).

This chapter covers the following topics:

- "Using MLT ", next
- "Using Link Aggregation Group (LAG)" on page 282

For more information on a MLT, as well as configuration directions using the console interface (CI) menu, refer to *Using the Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

For more information on configuring these features using the Web-based management system, refer to *Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

For more information on configuring these features using the Device Manager, refer to *Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

Using MLT

Note: For guidelines to configuring STGs, VLANs, and MLTs, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

You configure Multi-Link Trunking (MLT) using the following commands:

- "show mlt command ", next

- "mlt command" on page 280
- "no mlt command" on page 281

show mlt command

The `show mlt` command displays the Multi-Link Trunking (MLT) configuration and utilization. The syntax for the `show mlt` command is:

```
show mlt [utilization <1-6>]
```

The `show mlt` command is in the privExec command mode.

Table 173 describes the parameters and variables for the `show mlt` command.

Table 173 `show mlt` command parameters and variables

Parameters and variables	Description
`utilization <1-6>`	Displays the utilization of the specified enabled MLT(s) in percentages.

Figure 68 displays sample output from the `show mlt` command.

Figure 68 `show mlt` command output

```
BS460_24T_PWR#show mlt
Trunk Name Members    STP Learn Bpdu   Mode   Status
----- ------------------------------- --------- ------ ---
1     Trunk #1 NONE       Normal     All     Basic  Disabled
2     Trunk #2 NONE       Normal     All     Basic  Disabled
```

mlt command

The `mlt` command configures a Multi-Link Trunk (MLT). The syntax for the `mlt` command is:

```
mlt <id> [name <trunkname>] [enable|disable]
[member <portlist>] [learning {disable|fast|normal}]
```

The `mlt` command is in the config command mode.

Table 174 describes the parameters and variables for the `mlt` command.

Table 174 `mlt` command parameters and variables

Parameters and variables	Description
`<id>`	Enter the trunk ID; range is 1 to 6.
`name <trunkname>`	Specifies a text name for the trunk; enter up to 16 alphanumeric characters.
`enable|disable`	Enables or disables the trunk.
`member <portlist>`	Enter the ports that you want as members of the trunk.
`learning <disable	fast	normal >`	Sets the STP learning mode.

Note: You can modify an MLT when it is enabled or disabled.

no mlt command

The `no mlt` command disables a Multi-Link Trunk (MLT), clearing all the port members. The syntax for the `no mlt` command is:

```
no mlt [<id>]
```

The `no mlt` command is in the config command mode.

Table 175 describes the parameters and variables for the `no mlt` command.

Table 175 `no mlt` command parameters and variables

Parameters and variables	Description
`<id>`	Enter the trunk ID to disable the trunk and to clear the port members of the specified trunk.

Using Link Aggregation Group (LAG)

With the switch, you can configure a LAG. To use LAG, you must also enable the Link Aggregation Control Protocol (LACP) on each port which is configured as part of the LAG.

You configure LACP using the following commands:

- "lacp system-priority command " next
- "default lacp system-priority command" on page 283
- "lacp mode command" on page 283
- "default lacp mode command" on page 284
- "lacp aggregation command" on page 284
- "no lacp aggregation command" on page 285
- "default lacp aggregation command" on page 285
- "lacp key command" on page 286
- "lacp priority command" on page 286
- "default lacp priority command" on page 287
- "lacp timeout-time command" on page 287
- "default lacp timeout-time command" on page 288
- "show lacp system command" on page 288
- "show lacp mlt command" on page 289
- "show lacp mlt <mlt-id> command" on page 289
- "show lacp port command" on page 290
- "show lacp debug member command" on page 291
- "show lacp stats command" on page 293

lacp system-priority command

The `lacp system-priority` command sets a system priority for LACP. The syntax for the `lacp system-priority` command is:

```
lacp system-priority [0-65535]
```

The `lacp system-priority` command is in the CLI Global Configuration mode.

Table 176 describes the parameters and variables for the `lacp system-priority` command.

Table 176 `lacp system-priority command` parameters and variables

Parameters and variables	Description
`[0-65535]`	Enter a system priority for LACP; range is 0 to `65535`.

default lacp system-priority command

The `default lacp system-priority` command sets the system priority for LACP as the default value of 32768. The syntax for the `default lacp system-priority` command is:

```
default lacp system-priority
```

The `default lacp system-priority` command is in the CLI Global Configuration mode.

lacp mode command

The `lacp mode` command sets the mode for an LACP port. The syntax for the `lacp mode` command is:

```
lacp mode [port <portlist>]  {off | passive | active}
```

The `lacp mode` command is in the CLI Global Configuration mode.

Table 177 describes the parameters and variables for the `lacp mode` command.

Table 177 `lacp mode command` parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to set LACP the mode.
port `{off	passive	active}`	Sets the LACP mode for the specified port to off, passive, or active; if port mode is selected as Passive or Active, port is ready to participate in LACP

default lacp mode command

The `default lacp mode` command puts an LACP port in the default off mode. The syntax for the `default lacp mode` command is:

```
default lacp mode [port <portlist>]
```

The `default lacp mode` command is in the CLI Global Configuration mode.

Table 178 describes the parameters and variables for the `default lacp mode` command.

Table 178 `default lacp mode command` parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports that you want to set in the LACP off mode by default.

lacp aggregation command

The `lacp aggregation` command enables lacp aggregation on the specified port(s). The syntax for the `lacp aggregation` command is:

```
lacp aggregation [port <portlist>] enable
```

The `lacp aggregation` command is in the CLI Global Configuration mode.

Table 179 describes the parameters and variables for the `lacp aggregation` command.

Table 179 `lacp aggregation command` parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to enable LACP aggregation.

no lacp aggregation command

The `no lacp aggregation` command disables lacp aggregation on the specified port(s). The syntax for the `no lacp aggregation` command is:

```
no lacp aggregation [port <portlist>] enable
```

The `no lacp aggregation` command is in the CLI Global Configuration mode.

Table 180 describes the parameters and variables for the `no lacp aggregation` command.

Table 180 `no lacp aggregation command` parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to disable LACP aggregation.

default lacp aggregation command

The `default lacp aggregation` command disables LACP aggregation on the the specified port(s) by default. The syntax for the `default lacp aggregation` command is:

```
default lacp aggregation [port <portlist>] enable
```

The `default lacp aggregation` command is in the CLI Global Configuration mode.

Table 181 describes the parameters and variables for the `default lacp aggregation` command.

Table 181 `default lacp aggregation command` parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to disable LACP aggregation by default.

lacp key command

The lacp key command assigns a key value for the specified port(s). The syntax for the lacp key command is:

```
lacp key [port <portlist>] <1-4095>
```

The lacp key command is in the CLI Global Configuration mode.

Table 182 describes the parameters and variables for the lacp key command.

Table 182 lacp key command parameters and variables

Parameters and variables	Description
port <portlist>	Enter the ports for which you want to assign an LACP key value.
<1-4095>	Enter an LACP key value for the port; range is 1 to 4095.

lacp priority command

The lacp priority command sets an LACP priority for the specified port(s). The syntax for the lacp priority command is:

```
lacp priority [port <portlist>] <0-255>
```

The lacp priority command is in the CLI Global Configuration mode.

Table 183 describes the parameters and variables for the lacp priority command.

Table 183 lacp priority command parameters and variables

Parameters and variables	Description
port <portlist>	Enter the ports for which you want to set LACP priority.
<0-255>	Enter a priority number for the port; range is 0 to 255.

default lacp priority command

The `default lacp priority` command sets the LACP priority for the specified port(s) as the default value of 128. The syntax for the `default lacp priority` command is:

```
default lacp priority [port <portlist>]
```

The `default lacp priority` command is in the CLI Global Configuration mode.

Table 184 describes the parameters and variables for the `default lacp priority` command.

Table 184 `default lacp priority command` parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to set the default LACP priority of 128.

lacp timeout-time command

The `lacp timeout-time` command sets an LACP timeout for the specified port(s). The syntax for the `lacp timeout-time` command is:

```
lacp timeout-time [port <portlist>] {short | long}
```

The `lacp timeout-time` command is in the CLI Global Configuration mode.

Table 185 describes the parameters and variables for the `lacp timeout-time` command.

Table 185 `lacp timeout-time command` parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to set an LACP timeout.
`port {short | long}`	Sets the a short or long LACP timeout for the port.

default lacp timeout-time command

The `default lacp timeout-time` command sets a short LACP timeout for the specified port(s) by default. The syntax for the `default lacp timeout-time` command is:

```
default lacp timeout-time [port <portlist>]
```

The `default lacp timeout-time` command is in the CLI Global Configuration mode.

Table 186 describes the parameters and variables for the `default lacp timeout-time` command.

Table 186 `default lacp timeout-time command` parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to set a short LACP timeout by default.

show lacp system command

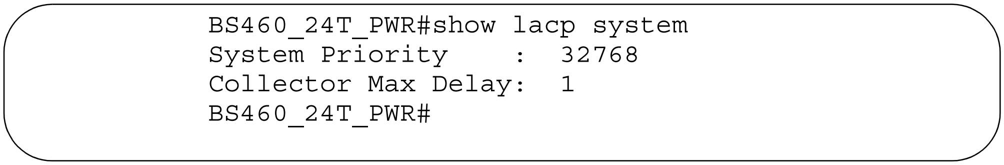
The `show lacp system` command displays LACP information for the entire system. The syntax for the `show lacp system` command is:

```
show lacp system
```

The `show lacp system` command is in the privExec mode.

Figure 69 displays a sample output for the `show lacp system` command.

Figure 69 `show lacp system` command output



```
BS460_24T_PWR#show lacp system
System Priority     :  32768
Collector Max Delay:   1
BS460_24T_PWR#
```

show lacp mlt command

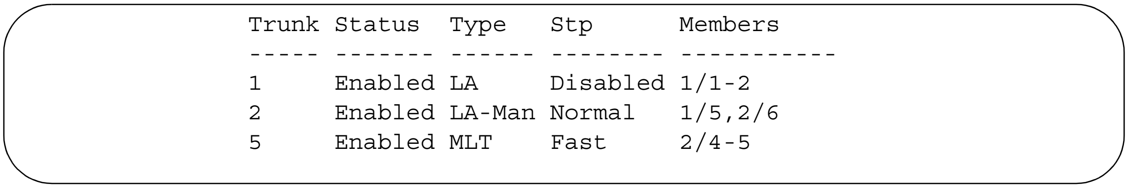
The `show lacp mlt` command displays LACP trunk summary information. The syntax for the `show lacp mlt` command is:

```
show lacp mlt
```

The `show lacp mlt` command is in the privExec mode.

Figure 70 displays a sample output for the `show lacp mlt` command.

Figure 70 `show lacp mlt` command output



```
Trunk Status  Type   Stp      Members
----- ------- ------ -------- -----------
1     Enabled LA     Disabled 1/1-2
2     Enabled LA-Man Normal   1/5,2/6
5     Enabled MLT    Fast     2/4-5
```

In this example,

- Trunk 1 is a Link Aggregation (LA) trunk.
- Trunk 2 is a manual LA trunk.
- Trunk 5 is an MLT trunk.

show lacp mlt <mlt-id> command

The `show lacp mlt <mlt-id>` command displays LACP trunk detail information. The syntax for the `show lacp mlt <mlt-id>` command is:

```
show lacp mlt <mlt-id>
```

The `show lacp mlt <mlt-id>` command is in the CLI Exec mode.

Table 187 describes the parameters and variables for the `show lacp mlt <mlt-id>` command.

Table 187 `show lacp mlt <mlt-id> command` parameters and variables

Parameters and variables	Description
`<mlt-id>`	Enter the ID of the MLT trunk for which you want detailed information.

Figure 71 displays a sample output for the `show lacp mlt <mlt-id>` command.

Figure 71 `show lacp mlt <mlt-id>` command output

```
Trunk          :   1
Status         :   Enabled
Type           :   LA
Stp:           :   Disabled
Actor Lag ID   :
xxxx-xxxxxxxxxxxx-xxxx
Partner Lag ID:
xxxx-xxxxxxxxxxxx-xxxx
Members        :   1/1-2
```

In this example, the Lag ID=System ID (Sys Priority+MAC) + group Key.

show lacp port command

The `show lacp port` command displays LACP port information. The syntax for the `show lacp port` command is:

```
show lacp port [<portlist>]
```

The `show lacp port` command is in the CLI Exec mode.

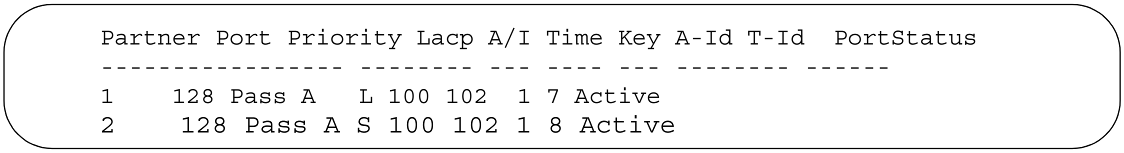
Table 188 describes the parameters and variables for the `show lacp port` command.

Table 188 `show lacp port command` parameters and variables

Parameters and variables	Description
`<portlist>`	Enter the ports for which you want information.

Figure 72 displays a sample output for the `show lacp port` command.

Figure 72 `show lacp port` command output



```
Partner Port Priority Lacp A/I Time Key A-Id T-Id  PortStatus
----------------- -------- --- ---- --- -------- ------
1    128 Pass A   L 100 102  1 7 Active
2    128 Pass A S 100 102 1 8 Active
```

In this example,

- Ports 1 and 2 are active members of aggregator 102.
- Port 3 is a standby member of aggregator 102.
- Trunk 1 is attached to aggregator 102.
- Port 23 is not in a trunk and up.
- Port 24 is not in a trunk and down.

Note: A=Aggregatable, I=Individual, S=Short timeout, L=Long timeout

show lacp debug member command

The `show lacp debug member` command displays LACP port debug information. The syntax for the `show lacp debug member` command is:

```
show lacp debug member [portlist]
```

The `show lacp debug member` command is in the CLI Exec mode.

Table 189 describes the parameters and variables for the `show lacp debug member` command.

Table 189 `show lacp debug member command` **parameters and variables**

Parameters and variables	Description
`[portlist]`	Enter the ports for which you want debug information.

Figure 73 displays a sample output for the `show lacp debug member` command.

Figure 73 `show lacp debug member` **command output**

```
 Partner
Port A-Id T-Id Rx State Mux State Partner Port
---- ---- ---- -------- ----------------
1    100  3    current  attached  40
```

The command may display the following terms.

LACP Receiving State:

- Current: Rx information is valid
- Expired: Rx information is invalid.
- Defaulted: Rx machine is defaulted.
- Initialized: Rx machine is initializing.
- LacpDisabled: LACP is disabled on this port.
- PortDisabled: Port is disabled.

Selection State:

- Detached: port is not attached to any aggregator.
- Waiting: port is waiting to attach to an aggregator.
- Attached: port is attached to an Aggregator.
- Ready: port is ready to Tx and Rx.

show lacp stats command

The show lacp stats command displays LACP port statistics. The syntax for the show lacp stats command is:

```
show lacp stats [port <portlist>]
```

The show lacp stats command is in the CLI Exec mode.

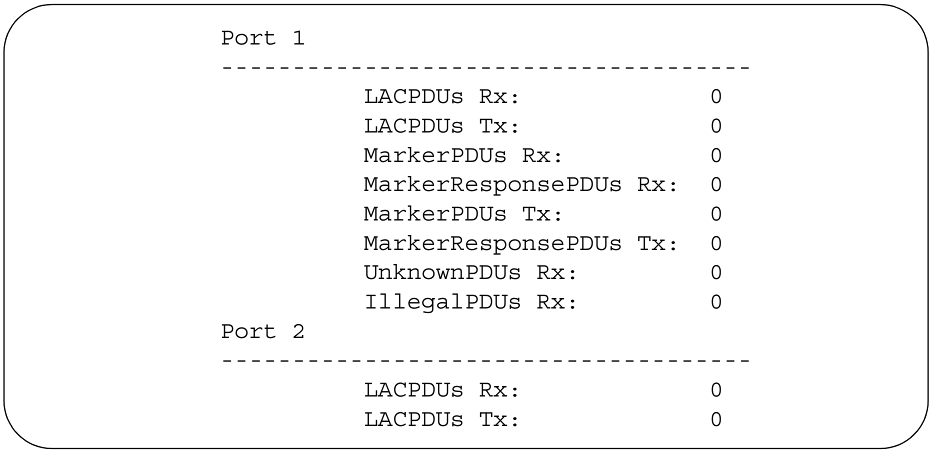
Table 190 describes the parameters and variables for the show lacp stats command.

Table 190 show lacp stats command parameters and variables

Parameters and variables	Description
port <portlist>	Enter the ports for which you want statistics.

Figure 74 displays a sample output for the show lacp stats command.

Figure 74 show lacp stats command output



```
Port 1
-------------------------------------
          LACPDUs Rx:              0
          LACPDUs Tx:              0
          MarkerPDUs Rx:           0
          MarkerResponsePDUs Rx:   0
          MarkerPDUs Tx:           0
          MarkerResponsePDUs Tx:   0
          UnknownPDUs Rx:          0
          IllegalPDUs Rx:          0
Port 2
-------------------------------------
          LACPDUs Rx:              0
          LACPDUs Tx:              0
```

You can configure LAG using the following commands:

- "lacp mlt command " next
- "no lacp mlt command" on page 294

lacp mlt command

The `lacp mlt` command is used to manually enable a LAG, and assign an MLT ID to the enabled LAG. The syntax for the `lacp mlt` command is:

```
lacp mlt <mlt-id> [learning {disable | fast | normal}]
<portlist>
```

The `lacp mlt` command is in the CLI Global Configuration mode.

Table 191 describes the parameters and variables for the `lacp mlt` command.

Table 191 `lacp mlt command` parameters and variables

Parameters and variables	Description
`<mlt-id>`	Enter the MLT ID for the enabled LAG.
`learning {disable | fast | normal }`	Sets the STP learning mode.
`<portlist>`	Enter the ports in the LAG.

no lacp mlt command

The `no lacp mlt` command is used to manually disable a LAG. The syntax for the `no lacp mlt` command is:

```
no lacp mlt <mlt-id>
```

The `no lacp mlt` command is in the CLI Global Configuration mode.

Table 192 describes the parameters and variables for the `no lacp mlt` command.

Table 192 `no lacp mlt command` parameters and variables

Parameters and variables	Description
`<mlt-id>`	Enter the MLT ID of the LAG that you want to disable.

Chapter 8
Spanning Tree

This chapter describes how to configure the Spanning Tree Protocol, Spanning tree groups and Advanced Spanning Tree Protocol (ASTP).

This chapter covers the following topics:

- "Using spanning tree ", next
- "Using Advanced Spanning Tree" on page 309

For more information on a spanning tree, as well as configuration directions using the console interface (CI) menu, refer to *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches*.

For more information on configuring these features using the Web-based management system, refer to *Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

For more information on configuring these features using the Device Manager, refer to *Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches.*

Using spanning tree

➡ **Note:** For detailed information on spanning tree parameters, spanning tree groups, and configuration guidelines, refer to *Using the BayStack 460-24T-PWR Switch Software, Using the BayStack 470-24T 10/100/1000 Switch Software Version 3.0., Using the BayStack 470-48T 10/100/1000 Switch Software Version 2.2.1.*

With the switch, you can configure multiple spanning tree groups (STGs). (Multiple spanning tree groups are available only when the Stack Operational Mode is set to Pure Stack.) The CLI allows you to configure spanning tree groups, to add or remove VLANs to the spanning tree groups, and to configure the usual spanning tree parameters and FastLearn. This section covers the following topics:

- "show spanning-tree command ", next
- "spanning-tree stp create command by STG" on page 299
- "spanning-tree stp delete command by STG" on page 300
- "spanning-tree stp enable command by STG" on page 300
- "spanning-tree stp disable command by STG" on page 301
- "spanning-tree command by STG" on page 302
- "default spanning-tree command by STG" on page 303
- "spanning-tree add-vlan command" on page 304
- "spanning-tree remove-vlan command" on page 305
- "spanning-tree command by port" on page 306
- "default spanning-tree command by port" on page 307
- "no spanning-tree command by port" on page 308

➡ **Note:** When you omit the spanning tree group parameter (`stp <1-8>`) in the any of the spanning tree commands, the commands operate on the default spanning tree group (spanning tree group 1).

show spanning-tree command

The `show spanning-tree` command displays spanning tree configuration information that is specific to either the spanning tree group or to the port. The syntax for the `show spanning-tree` command is:

```
show spanning-tree [stp <1-8>|vlans <1-4094>] {config|port|}
```

The `show spanning-tree` command is in the privExec command mode.

Table 193 describes the parameters and variables for the `show spanning-tree` command.

Table 193 `show spanning-tree` command parameters and variables

Parameters and variables	Description
`stp <1-8>`	Displays specified spanning tree group configuration; enter the number of the group you want displayed.
`vlans <1-4094>`	Displays specified vlans configuration; enter the number of the vlans you want displayed. (BP 2000)
`config|port`	Displays spanning tree configuration for: • `config`—the specified (or default) spanning tree group • `port`—the ports within the spanning tree group

Figure 76 displays sample output from the `show spanning-tree` command for the default spanning tree group (STP1). Figure 75 shows the spanning tree parameters by port.

Figure 75 `show spanning-tree` command output by port

```
BS460_24T_PWR#show spanning-tree stp 1 port
Port Trunk   Participation   Priority  Path Cost    State
---- -----  ---------------  --------  ---------  ----------
1           Normal Learning  128       100        Forwarding
2           Normal Learning  128       10         Forwarding
3           Normal Learning  128       10         Forwarding
4           Normal Learning  128       10         Forwarding
5           Normal Learning  128       10         Forwarding
6           Normal Learning  128       10         Forwarding
7           Normal Learning  128       10         Forwarding
8           Normal Learning  128       10         Forwarding
9           Normal Learning  128       10         Forwarding
10          Normal Learning  128       10         Forwarding
11          Normal Learning  128       10         Forwarding
12          Normal Learning  128       10         Forwarding
13          Normal Learning  128       10         Forwarding
14          Normal Learning  128       10         Forwarding
15          Normal Learning  128       10         Forwarding
16          Normal Learning  128       10         Forwarding
17          Normal Learning  128       10         Forwarding
18          Normal Learning  128       10         Forwarding
19          Normal Learning  128       10         Forwarding
20          Normal Learning  128       10         Forwarding
----More ----
```

Figure 76 `show spanning-tree` command output for spanning tree group

```
BS470_48#show spanning-tree config
Bridge Priority (hex):       8000
Designated Root:             8000000081C6A801
Root Port:                   1
Root Path Cost:              105
Hello Time:                  2 seconds
Maximum Age Time:            20 seconds
Forward Delay:               15 seconds
Bridge Hello Time:           2 seconds
Bridge Maximum Age Time:     20 seconds
Bridge Forward Delay:        15 seconds
Tagged BPDU on tagged port:  No
VID used for Tagged BPDU:    4001
STP Group State:             Active
STP Multicast Address:       01-80-C2-00-00-00
BS470_48#
```

spanning-tree stp create command by STG

Note: For guidelines to configuring STGs, VLANs, and MLTs, refer to *Using the BayStack 460-24T-PWR Switch Software, Using the BayStack 470-24T 10/100/1000 Switch Software Version 3.0.*, *Using the BayStack 470-48T 10/100/1000 Switch Software Version 2.2.1.*

The `spanning-tree stp create` command allows you to create a spanning tree group. The syntax for the `spanning-tree stp create` command is:

```
spanning-tree stp <1-8> create
```

The `spanning-tree stp create` command is in the config command mode.

Table 194 describes the parameters and variables for the `spanning-tree stp create` command.

Table 194 `spanning-tree stp create` command parameters and variables

Parameters and variables	Description
<1-8>	Enter the number of the spanning tree group you are creating (STG ID). You cannot create the default spanning tree group, which is number 1.

spanning-tree stp delete command by STG

The `spanning-tree stp delete` command allows you to delete a spanning tree group. The syntax for the `spanning-tree stp delete` command is:

```
spanning-tree stp <1-8> delete
```

The `spanning-tree stp delete` command is in the config command mode.

Table 195 describes the parameters and variables for the `spanning-tree stp delete` command.

Table 195 `spanning-tree stp delete` command parameters and variables

Parameters and variables	Description
<1-8>	Enter the number of the spanning tree group you are deleting (STG ID). You cannot delete the default spanning tree group, which is number 1.

spanning-tree stp enable command by STG

The `spanning-tree stp enable` command allows you to enable a spanning tree group. The syntax for the `spanning-tree stp enable` command is:

```
spanning-tree stp <1-8> enable
```

The `spanning-tree stp enable` command is in the config command mode.

Table 196 describes the parameters and variables for the `spanning-tree stp enable` command.

Table 196 `spanning-tree stp enable` command parameters and variables

Parameters and variables	Description
<1-8>	Enter the number of the spanning tree group you want to enable (STG ID). You cannot enable the default spanning tree group, which is number 1; it is always enabled.

spanning-tree stp disable command by STG

The `spanning-tree stp disable` command allows you to disable a spanning tree group. The syntax for the `spanning-tree stp disable` command is:

```
spanning-tree stp <1-8> disable
```

The `spanning-tree stp disable` command is in the config command mode.

Table 197 describes the parameters and variables for the `spanning-tree stp disable` command.

Table 197 `spanning-tree stp disable` command parameters

Parameters and variables	Description
<1-8>	Enter the number of the spanning tree group you want to disable (STG ID). You cannot disable the default spanning tree group, which is number 1d.

spanning-tree command by STG

The `spanning-tree` command by STG sets STP values by STG. The syntax for the `spanning-tree` command by STG is:

```
spanning-tree [stp <1-8>] [forward-time <4-30>]
[hello-time <1-10>] [max-age <6-40>] [priority <0-65535>]
[tagged-bpdu {enable|disable}] [tagged-bpdu-vid <1-4094]>
[multicast-address <H H.H.>]
```

The `spanning-tree` command by STG is in the config command mode.

Table 198 describes the parameters and variables for the `spanning-tree` command by STG.

Table 198 `spanning-tree` command by STG parameters and variables

Parameters and variables	Description
`stp <1-8>`	Specifies the spanning tree group you want; enter the STG ID.
`forward-time <4-30>`	Enter the forward time of the STG in seconds; range is 4-30. Default value is 15.
`hello-time <1-10>`	Enter the hello time of the STG in seconds; range is 1-10. Default value is 2.
`max-age <6-40>`	Enter the max-age of the STG in seconds; range is 6-40. Default value is 20.
`priority <0-65535>`	Enter the priority of the STG in seconds; range is 0-65535. Default value is 0x8000.
`tagged-bpdu {enable|disable}`	Allows you to set the BPDU as tagged or untagged. Default value for spanning tree group 1 (default group) is untagged; the default for the other groups is tagged.
`tagged-bpdu-vid <1-4094>`	Allows you to set the VLAN ID (VID) for the tagged BPDU. Default value is 4001-4008 for STG 1-8, respectively.
`multicast-address <H.H.H.>`	Allows you to set the spanning tree multicast address. Default value is 01-80-c2-00-00-00 (BayStack 460-24T-PWR).

default spanning-tree command by STG

The `default spanning-tree` command by STG restores the default spanning tree values for the spanning tree group. The syntax for the `default spanning-tree` command by STG is:

```
default spanning-tree [stp <1-8>] [forward-time]
[hello-time] [max-age] [priority] [tagged-bpdu]
[multicast-address]
```

The `default spanning-tree` command by STG is in the config command mode.

Table 199 describes the parameters and variables for the `default spanning-tree` command by STG.

Table 199 `default spanning-tree` command by STG parameters

Parameters and variables	Description
`stp <1-8>`	Disables the spanning tree group; enter the STG ID.
`forward-time`	Sets the forward time to default value—15 seconds.
`hello-time`	Sets the hello time to default value—2 seconds.
`max-age`	Sets the maximum age time to default value—20 seconds.
`priority`	Sets the priority to default value—0x8000.
`tagged-bpdu`	Sets the tagging to default value. Default value for spanning tree group 1 (default group) is untagged; the default for the other groups is tagged.
`multicast address`	Sets the default multicast address - 01-80-C2-00-00-00.

spanning-tree add-vlan command

Note: You can use the `spanning-tree add-vlan` command to move a VLAN from one spanning tree group to another group. You no longer must remove the VLAN from the first group.

The `spanning-tree add-vlan` command allows you to add a VLAN to a specified spanning tree group. The syntax for the `spanning-tree add-vlan` command is:

```
spanning-tree [stp <1-8>] add-vlan <1-4094>
```

The `spanning-tree add-vlan` command by port is in the config command mode.

Table 200 describes the parameters and variables for the `spanning-tree add-vlan` command.

Table 200 `spanning-tree add-vlan` command parameters and variables

Parameters and variables	Description
`stp <1-8>`	Specifies the spanning tree group you want to add the VLAN to; enter the STG ID. Note: If you omit this parameter, the system uses the default spanning tree group, 1.
`add-vlan <1-4094>`	Enter the VLAN you want to add to the spanning tree group.

Note: VLAN 1 is always in spanning tree group 1.

spanning-tree remove-vlan command

The `spanning-tree remove-vlan` command allows you to remove a VLAN from a specified spanning tree group. The syntax for the `spanning-tree remove-vlan` command is:

```
spanning-tree [stp <1-8>] remove-vlan <1-4094>
```

The `spanning-tree remove-vlan` command by port is in the config command mode.

Table 201 describes the parameters and variables for the `spanning-tree remove-vlan` command.

Table 201 `spanning-tree remove-vlan` command parameters

Parameters and variables	Description
`stp <1-8>`	Specifies the spanning tree group you want to remove the VLAN from; enter the STG ID. Note: If you omit this parameter, the system uses the default spanning tree group, 1.
`remove-vlan <1-4094>`	Enter the VLAN you want to remove from the spanning tree group.

Note: You cannot remove VLAN 1 from spanning tree group 1.

spanning-tree command by port

Note: For guidelines to configuring STGs, VLANs, and MLTs, refer to *Using the BayStack 460-24T-PWR Switch Software, Using the BayStack 470-24T 10/100/1000 Switch Software Version 3.0., Using the BayStack 470-48T 10/100/1000 Switch Software Version 2.2.1.*

The `spanning-tree` command by port sets Spanning Tree Protocol (STP) and multiple spanning tree group (STG) participation for the ports within the specified spanning tree group. The syntax for the `spanning-tree` command by port is:

```
spanning-tree [port <portlist>] [stp <1-8>]
[learning {disable|normal|fast}] [cost <1-65535>]
[priority <00|10|20|...|F0>]
```

or for BayStack 460-24T-PWR switches:

```
spanning-tree [port <portlist>] [stp <1-8>]
[learning {disable|normal|fast}] [cost <1-65535>]
[priority <0-255>]
```

The `spanning-tree` command by port is in the config-if command mode.

Table 202 describes the parameters and variables for the `spanning-tree` command by port.

Table 202 `spanning-tree` command by port parameters and variables

Parameters and variables	Description
`port <portlist>`	Enables spanning tree for the specified port or ports; enter port or ports you want enabled for spanning tree. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.
`stp <1-8>`	Specifies the spanning tree group you want; enter the STG ID.

Table 202 `spanning-tree` command by port parameters and variables

Parameters and variables	Description
`learning {disable|normal|fast}`	Specifies the STP learning mode: • `disable`—disables FastLearn mode • `normal`—changes to normal learning mode • `fast`—enables FastLearn mode
`cost <1-65535>`	Enter the path cost of the spanning tree; range is 1-.65535.
`priority <00|10|20|...|F0>`	Enter the priority value of the port; range is `00|10|20|...|F0`.
`priority <0-255>`	Enter the priority value of the spanning tree; range is 0-255 (BayStack 460-24T-PWR switches).

default spanning-tree command by port

The `default spanning-tree` command by port sets the spanning tree values for the ports within the specified spanning tree group to the factory default settings. The syntax for the `default spanning-tree` command by port is:

```
default spanning-tree [port <portlist>] [stp <1-8>]
[learning] [cost] [priority]
```

The `default spanning-tree` command by port is in the config-if command mode.

Table 203 describes the parameters and variables for the `default spanning-tree` command by port.

Table 203 `default spanning-tree` **command by port parameters**

Parameters and variables	Description
`port <portlist>`	Enables spanning tree for the specified port or ports; enter port or ports you want set to factory spanning tree default values. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.
`stp <1-8>`	Specifies the spanning tree group you want to set to factory default value; enter the STG ID. This command places the port into the default STG. Default value for STG is 1.
`learning`	Sets the spanning tree learning mode to factory default value. Default value for learning is normal mode.
`cost`	Sets the path cost to factory default value. Default value for path cost depends on the type of port.
`priority`	Sets the priority to factory default value. Default value for the priority is 0x80 (0x8000 for BayStack 460-24T-PWR switches).

no spanning-tree command by port

The `no spanning-tree` command by port disables spanning tree for a port in a specific spanning tree group. The syntax for the `no spanning-tree` command by port is:

```
no spanning-tree [port <portlist>] [stp <1-8>]
```

The `no spanning-tree` command by port is in the config-if command mode.

Table 204 describes the parameters and variables for the `no spanning-tree` command by port.

Table 204 `no spanning-tree` command by port parameters and variables

Parameters and variables	Description
`port <portlist>`	Disables spanning tree for the specified port or ports; enter port or ports you want enabled for STP. Note: If you omit this parameter, the system uses the port number you specified when you issued the `interface` command.
`stp <1-8>`	Disables the port in the specified spanning tree group; enter the STG ID.

Using Advanced Spanning Tree

The Advanced Spanning Tree Protocol (ASTP) application comprises Rapid Spanning Tree Protocol (RSTP) and Multi Spanning Tree Protocol (MSTP). With the switch, you can configure the RSTP and the MSTP applications. This section covers the following topics:

- "show spanning-tree rstp Config command ", next
- "show spanning-tree rstp statistics command" on page 311
- "show spanning-tree rstp status command" on page 311
- "show spanning-tree rstp port config command" on page 312
- "show spanning-tree rstp port statistics command" on page 313
- "show spanning-tree rstp port status command" on page 314
- "spanning-tree rstp command" on page 315
- "spanning- tree rstp port role command" on page 316
- "show spanning-tree mstp config command" on page 317
- "show spanning-tree mstp statistics command" on page 318
- "show spanning-tree mstp statistics command" on page 318
- "show spanning-tree mstp status command" on page 318
- "show spanning-tree mstp port config command" on page 319
- "show spanning-tree mstp port statistics command" on page 320

- “show spanning-tree mstp-msti config command” on page 321
- “show spanning-tree mstp msti statistics command” on page 322
- “Show spanning-tree mstp msti port config command” on page 323
- “show spanning-tree mstp msti port statistics command” on page 324
- “spanning-tree mstp command” on page 325
- “spanning- tree mstp port role command” on page 326
- “spanning-tree mstp region command” on page 327
- “spanning-tree mstp msti command” on page 328
- “spanning- tree mstp port role command” on page 326
- “No spanning-tree mstp msti command” on page 330
- “Spanning-tree mstp msti enable” on page 330
- “No spanning-tree mstp msti enable” on page 330

show spanning-tree rstp Config command

The `show spanning-tree rstp config` command displays the Rapid Spanning Tree Protocol (RSTP) related bridge-level configuration details. The syntax for the `show spanning-tree rstp config` command is:

```
show spanning-tree rstp info
```

The `show spanning-tree rstp config` command is in the privExec command mode.

Figure 77 displays sample output from the `show spanning-tree rstp config` command.

Figure 77 `show spanning-tree rstp config` command output

```
Stp Priority:                 8000
Stp Version:                  Rstp Mode
Bridge Max Age:               20 seconds
Bridge Hello Time:            2 seconds
Bridge Forward Delay Time:    15 seconds
Tx Hold Count:                3
PathCost Default Type:        32-bit
```

show spanning-tree rstp statistics command

The `show spanning-tree rstp statistics` command displays the Rapid Spanning Tree Protocol (RSTP) related bridge-level statistics. The syntax for the `show spanning-tree rstp statistics` command is:

```
show spanning-tree rstp statistics
```

The `show spanning-tree rstp statistics` command is in the privExec command mode.

Figure 78 displays sample output from the `show spanning-tree rstp statistics` command.

Figure 78 `show spanning-tree rstp statistics` command output

```
Rstp UP Count:                     1
Rstp DOWN Count:                   0
Count of Root Bridge Changes:     1
Stp Time since Topology Change:   111 seconds
Total No. Topology Changes:       1
```

show spanning-tree rstp status command

The `show spanning-tree rstp status` command displays the Rapid Spanning Tree Protocol (RSTP) related status information for the selected bridge.The syntax for the `show spanning-tree rstp status` command is:

```
show spanning-tree rstp status
```

The `show spanning-tree rstp status` command is in the privExec command mode.

Figure 79 displays sample output from the `show spanning-tree rstp status` command.

Figure 79 `show spanning-tree rstp status` command output

```
Designated Root:        40:00:00:E0:7B:3D:CA:38
Stp Root Cost:          200020
Stp Root Port:          37
Stp Max Age:            20 seconds
Stp Hello Time:         2 seconds
Stp Forward Delay Time:15 seconds
```

show spanning-tree rstp port config command

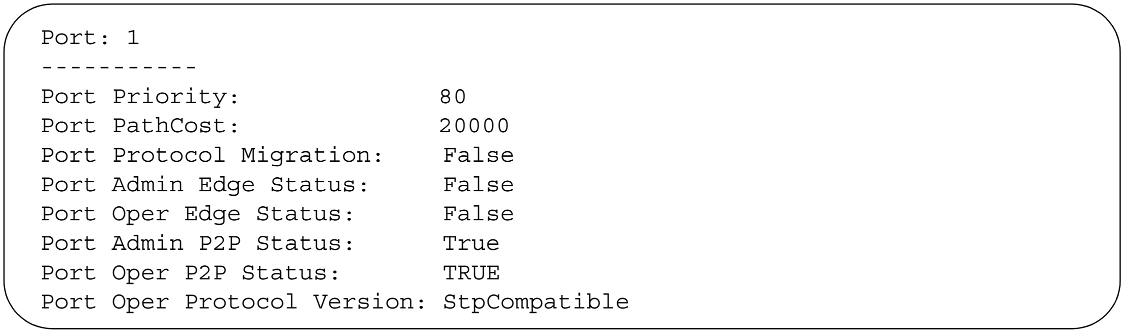
The `show spanning-tree rstp port config` command displays the Rapid Spanning Tree Protocol (RSTP) related port-level configuration details. The syntax for the `show spanning-tree rstp port config` command is:

```
show spanning-tree rstp port config[<portlist>]
```

The `show spanning-tree rstp port config` command is in the privExec command mode.

Figure 80 displays sample output from the `show spanning-tree rstp port config` command.

Figure 80 `show spanning-tree rstp port info` command output



```
Port: 1
-----------
Port Priority:              80
Port PathCost:              20000
Port Protocol Migration:    False
Port Admin Edge Status:     False
Port Oper Edge Status:      False
Port Admin P2P Status:      True
Port Oper P2P Status:       TRUE
Port Oper Protocol Version: StpCompatible
```

show spanning-tree rstp port statistics command

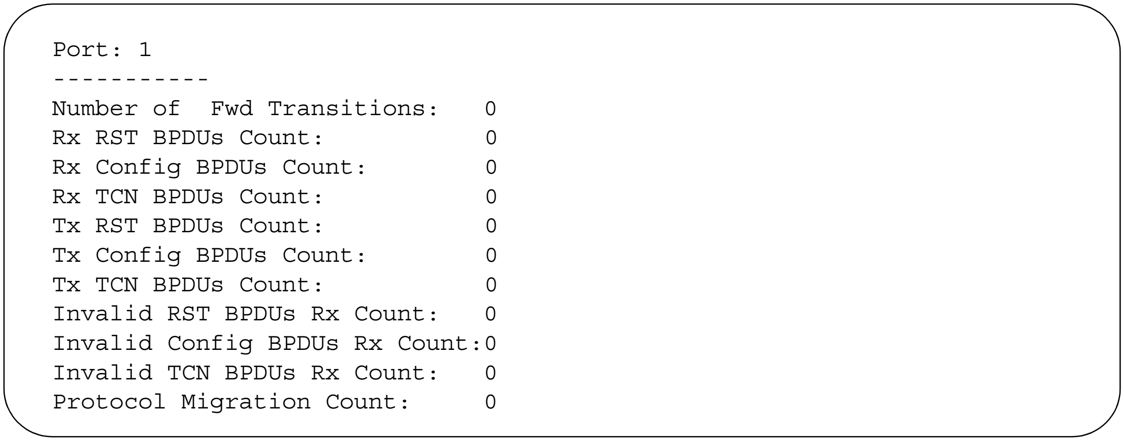
The `show spanning-tree rstp port statistics` command displays the Rapid Spanning Tree Protocol (RSTP) related port-level statistics. The syntax for the `show spanning-tree rstp port statistics` command is:

```
show spanning-tree rstp port statistics [<portlist>]
```

The `show spanning-tree rstp port statistics` command is in the privExec command mode.

Figure 81 displays sample output from the `show spanning-tree rstp port statistics` command.

Figure 81 `show spanning-tree rstp port statistics` command output



```
Port: 1
-----------
Number of  Fwd Transitions:   0
Rx RST BPDUs Count:           0
Rx Config BPDUs Count:        0
Rx TCN BPDUs Count:           0
Tx RST BPDUs Count:           0
Tx Config BPDUs Count:        0
Tx TCN BPDUs Count:           0
Invalid RST BPDUs Rx Count:   0
Invalid Config BPDUs Rx Count:0
Invalid TCN BPDUs Rx Count:   0
Protocol Migration Count:     0
```

show spanning-tree rstp port status command

The `show spanning-tree rstp port status` command displays the Rapid Spanning Tree Protocol (RSTP) related status information for the selected port. The syntax for the `show spanning-tree rstp port status` command is:

```
show spanning-tree rstp port status [<portlist>]
```

The `show spanning-tree rstp port status` command is in the privExec command mode.

Figure 82 displays sample output from the `show spanning-tree rstp port status` command.

Figure 82 `show spanning-tree rstp port status` command output

```
Port: 1
---------
Port Designated Root:  40:00:00:E0:7B:3D:CA:38
Port Designated Cost:  200020
Port Designated Bridge:80:00:00:04:3B:D5:82:C0
Port Designated Port:  80:02
```

spanning-tree rstp command

The `spanning-tree rstp` command sets the RSTP parameters which includes forward delay, hello time, maximum age time, default pathcost version, bridge priority, transmit holdcount, and version for the bridge. The syntax for the `spanning- tree rstp` command is:

```
spanning- tree rstp[forward-time<4 - 30>]
[hello-time <1 - 10>][max-age <6 - 40>]
[pathcost-type{ bits16 | bits32}]
[priority{0000|10000|20000| …| F0000}]
[tx-holdcount<1 - 10>]
[veraciousness-compatible|rstp}]
```

The `spanning- tree rstp` command is in the CLI Global configuration mode.

Table 205 describes the parameters and variables for the `spanning- tree rstp` command.

Table 205 `spanning- tree rstp` command parameters and variables

Parameters and variables	Description
`forward-time<4-30>`	Sets the RSTP forward delay for the bridge in seconds; default is 15.
`hello-time<1- 10>`	Sets the RSTP hello time delay for the bridge in seconds; default is 2
`max-age <6 - 40>`	Sets the RSTP maximum age time for the bridge in seconds; default is 20
`pathcost-type {bits16 | bits32}`	Sets the RSTP default pathcost version; default is bits32

Table 205 `spanning- tree rstp` command parameters and variables

Parameters and variables	Description
`priority {0000 | 1000 | … | F000}`	Sets the RSTP bridge priority (in hex); default is 8000
`tx-hold count`	Sets the RSTP Transmit Hold Count; default is 3
`version {stp-compatible | rstp}`	Sets the RSTP version; default is rstp

spanning- tree rstp port role command

The `spanning- tree rstp port role` command sets the RSTP parameters which includes pathcost, edge-port indicator, learning mode, point-to-point indicator, priority, and protocol migration indicator on the single or multiple port.

The syntax for the `spanning- tree rstp port role` command is:

```
spanning- tree rstp [port <portlist>] [cost <1 -
200000000>] [edge-port {false | true}]
[learning {disable | enable}]
[p2p {auto | force-false | force-true}]
[priority {00 | 10 | … | F0}]
[protocol-migration {false | true}]
```

The `spanning- tree rstp port role` command is in the CLI Interface configuration mode.

Table 206 describes the parameters and variables for the `spanning- tree rstp port` command.

Table 206 `spanning- tree rstp port role` command parameters

Parameters and variables	Description
`port <portlist>`	Filter on list of ports.
`cost <1 - 200000000>`	Sets the RSTP pathcost on the single or multiple port; default is 200000

Table 206 `spanning- tree rstp port role` command parameters (Continued)

Parameters and variables	Description
`edge-port {false | true}`	Indicates whether the single or multiple port should be assumed to be edge port or not. This parameter sets the Admin value of edge port status; default is false
`learning {disable | enable}`	Enables or disables RSTP on the single or multiple port; default is enable
`p2p {auto | force-false | force-true}`	Indicates whether the single or multiple port should be treated as a point-to-point link or not. This command sets the Admin value of P2P Status; default is force-true
`priority {00 | 10 |... | F0}`	Sets the RSTP port priority on the single or multiple port; default is 80
`protocol-migration {false | true}`	Forces the single or multiple port to transmit RSTP BPDUs when set true, while operating in RSTP mode; default is false

show spanning-tree mstp config command

The `show spanning-tree mstp config` command displays the Multi Spanning Tree Protocol (MSTP) related bridge-level, VLAN and region information.The syntax for the `show spanning-tree mstp config` command is:

```
show spanning-tree mstp config
```

The `show spanning-tree mstp config` command is in the privExec command mode.

Figure 83 displays sample output from the `show spanning-tree mstp config` command.

Figure 83 `show spanning-tree mstp config` command output

```
Maximum Mst Instance Number:7
Number of Msti Supported:0
Cist Bridge Priority:8000
Stp Version:  Mstp Mode
Cist Bridge Max Age:20 seconds
Cist Bridge Forward Delay:15 seconds
Tx Hold Count:3
PathCost Default Type:32-bit
Max Hop Count:2000
```

show spanning-tree mstp statistics command

The `show spanning-tree mstp statistics` command displays the Multi Spanning Tree Protocol (MSTP) related bridge-level statistics.The syntax for the `show spanning-tree mstp statistics` command is:

```
show spanning-tree mstp statistics
```

The `show spanning-tree mstp statistics` command is in the privExec command mode.

Figure 84 displays sample output from the `show spanning-tree mstp statistics` command.

Figure 84 `show spanning-tree mstp statistics` command output

```
Region Config Change Count:1
Time since Topology change:1327 seconds
Topology Change Count:2
Count of Root Bridge Changes:0
```

show spanning-tree mstp status command

The `show spanning-tree mstp status` command displays the Multi Spanning Tree Protocol (MSTP) related status information known by the selected bridge. The syntax for the `show spanning-tree mstp status` command is:

```
show spanning-tree mstp status
```

The `show spanning-tree mstp status` command is in the privExec command mode.

Figure 85 displays sample output from the `show spanning-tree mstp status` command.

Figure 85 `show spanning-tree mstp status` command output

```
Bridge Address:00:04:38:D5:82:C0
Cist Root:40:00:00:E0:7B:3D:CA:38
Cist Regional Root:80:00:00:04:38:D5:82:C0
Cist Root Port:37
Cist Root Cost200020
Cist Regional Root Cost:0
Cist Max Age:20 seconds
Cist Forward Delay:15 seconds
```

show spanning-tree mstp port config command

The `show spanning-tree mstp port config` command displays the Multi Spanning Tree Protocol (MSTP) Cist Port information maintained by every port of the Common Spanning Tree. The syntax for the `show spanning-tree mstp port config` command is:

```
show spanning-tree mstp port config [<portlist>]
```

The `show spanning-tree mstp port config` command is in the privExec command mode.

Table 207 describes the parameter and variable for the `show spanning-tree mstp port config` command.

Table 207 `show spanning-tree mstp port config` parameters

Parameters and variables	Description
`<portlist>`	Enter a list or range of port numbers.

Figure 86 displays sample output from the `show spanning-tree mstp port config` command.

Figure 86 `show spanning-tree mstp port config` command output

```
Port: 1
-----------
Cist Port Priority:80
Cist Port PathCost:20000
Cist Port Designated Root:80:00:00:04:38:D5:82:C0
Cist Port Designated Cost:20000
Cist Port Designated Bridge: 80:00:AB:04:38:D5:82:C0
Cist Port Designated Port:32
Cist Port Regional Root:80:00:00:04:38:D5:82:CF
Cist Port Regional PathCost:20000
Cist Port Protocol Migration:False
Cist Port Admin Edge Status:False
Cist Port Oper Edge Status:False
Cist Port Admin P2P Status:True
Cist Port Oper P2P Status:True
Cist Port Hello Time:2 seconds
Cist Port Oper Protocol Version:Mstp
```

show spanning-tree mstp port statistics command

The `show spanning-tree mstp port statistics` command displays the Multi Spanning Tree Protocol (MSTP) Cist Port statistics maintained by every port. The syntax for the `show spanning-tree mstp port statistics` command is:

```
show spanning-tree mstp port statistics [<portlist>]
```

The `show spanning-tree mstp port statistics` command is in the privExec command mode.

Table 208 describes the parameter and variable for the `show spanning-tree mstp port statistics` command.

Table 208 `show spanning-tree mstp port statistics` parameters

Parameters and variables	Description
`<portlist>`	Enter a list or range of port numbers.

Figure 87 displays sample output from the `show spanning-tree mstp port statistics` command.

Figure 87 `show spanning-tree mstp port statistics` command output

```
Port: 1
-----------
Cist Port Fwd Transitions:0
Cist Port Rx MST BPDUs Count:0
Cist Port Rx RST BPDUs Count:0
Cist Port Rx Config BPDUs Count:0
Cist Port Rx TCN BPDUs Count:0
Cist Port Tx MST BPDUs Count:0
Cist Port Tx RST BPDUs Count:0
Cist Port Tx Config BPDUs Count:0
Cist Port Tx TCN BPDUs Count:0
Cist Port Invalid MST BPDUs Rx:0
Cist Port Invalid RST BPDUs Rx:0
Cist Port Invalid Config BPDUs Rx:0
Cist Port Invalid TCN BPDUs Rx:0
Cist Port Protocol Migration Count:0
```

show spanning-tree mstp-msti config command

The `show spanning-tree mstp-msti config` command displays the Multi Spanning Tree Protocol (MSTP) instance-specific bridge and VLAN information. The syntax for the `show spanning-tree mstp-msti config` command is:

```
show spanning-tree mstp-msti config <1 - 7>
```

The `show spanning-tree mstp-msti config` command is in the privExec command mode.

Table 209 describes the parameter and variable for the `show spanning-tree mstp-msti config` command.

Table 209 `show spanning-tree mstp-msti config` parameters

Parameters and variables	Description
`<1 - 7>`	Filter on MSTP instance.

Figure 88 displays sample output from the `show spanning-tree mstp-msti config` command.

Figure 88 `show spanning-tree mstp-msti config` command output

```
Instance Id:  1
Msti Bridge Regional Root:00:00:00:04:38:D5:82:C0
Msti Bridge Priority:0
Msti Root Cost:0
Msti Root Port:0
```

show spanning-tree mstp msti statistics command

The `show spanning-tree mstp msti statistics` command displays the Multi Spanning Tree Protocol (MSTP) instance-specific bridge statistics.The syntax for the `show spanning-tree mstp msti statistics` command is:

```
show spanning-tree mstp msti statistics <1 - 7>
```

The `show spanning-tree mstp msti statistics` command is in the privExec command mode.

Table 210 describes the parameter and variable for the `show spanning-tree mstp msti statistics` command.

Table 210 `show spanning-tree mstp msti statistics` parameters

Parameters and variables	Description
`<1 - 7>`	Filter on MSTP instance.

Figure 89 displays sample output from the `show spanning-tree mstp msti statistics` command.

Figure 89 `show spanning-tree mstp msti statistics` command output

```
Instance Id:  1
Time since Topology change:5238 seconds
Topology Change Count:0
Count of Root Bridge Changes:0
Instance UP Count:1
Instance DOWN Count:
```

Show spanning-tree mstp msti port config command

The `show spanning-tree mstp msti port config` command displays the Multi Spanning Tree Protocol (MSTP) instance-specific to port information. The syntax for the `show spanning-tree mstp msti port config` command is:

```
show spanning-tree mstp msti port config <1 - 7>
[<portlist>]
```

The `show spanning-tree mstp msti port config` command is in the privExec command mode.

Table 211 describes the parameter and variable for the `show spanning-tree mstp msti port config` command.

Table 211 `show spanning-tree mstp msti port config` parameters

Parameters and variables	Description
`<1 - 7>`	Filter on MSTP instance.
[<portlist>]	Enter a list or range of port numbers.

Figure 90 displays sample output from the `show spanning-tree mstp msti port config` command.

Figure 90 `show spanning-tree mstp msti port config` command output

```
Instance Id: 1
Port: 1
------------------
Msti Port Priority:80
Msti Port PathCost:20000
Msti Port Designated Root:80:00:00:04:38:D5:82:C0
Msti Port Designated Cost:20000
Msti Port Designated Bridge: 80:00:AB:04:38:D5:82:C0
Msti Port Designated Port:32
```

show spanning-tree mstp msti port statistics command

The `show spanning-tree mstp msti port statistics` command displays the Multi Spanning Tree Protocol (MSTP) instance-specific to port statistics.The syntax for the `show spanning-tree mstp msti port statistics` command is:

```
show spanning-tree mstp msti port statistics <1 - 7>
[<portlist>]
```

The `show spanning-tree mstp msti port statistics` command is in the privExec command mode.

Table 212 describes the parameter and variable for the `show spanning-tree mstp msti port statistics` command.

Table 212 `show spanning-tree mstp msti port statistics`

Parameters and variables	Description
`<1 - 7>`	Filter on MSTP instance.
[<portlist>]	Enter a list or range of port numbers.

Figure 91 displays sample output from the `show spanning-tree mstp msti port statistics` command.

Figure 91 `show spanning-tree mstp msti port statistics` command output

```
Instance Id: 1
Port: 1
------------------
Msti Port Fwd Transitions:0
Msti Port Received BPDUs:0
Msti Port Transmitted BPDUs:0
Msti Port Invalid BPDUs Rcvd:0
```

spanning-tree mstp command

The `spanning-tree mstp` command sets the MSTP parameters which includes maximum hop count, maximum number of instances allowed, forward delay time, hello time, maximum age time, default pathcost version, priority, transmit hold count, and version for the Cist Bridge.The syntax for the `spanning- tree mstp` command is:

```
spanning- tree mstp [max-hop <600 - 4000>]
[forward-time <4 - 30>]
[max-age <6 - 40>]
[pathcost-type {bits16 | bits32}]
[priority {0000 | 10000 | 20000 | … | F0000}]
[tx-hold count <1 - 10>]
[version {stp-compatible | rstp| mstp}]
```

The `spanning- tree mstp` command is in the CLI Global configuration mode.

Table 213 describes the parameters and variables for the `spanning- tree mstp` command.

Table 213 `spanning- tree mstp` command parameters and variables

Parameters and variables	Description
`max-hop <600 - 4000>`	Sets the MSTP maximum hop count; default is 2000.
forward-time <4 - 30>	Sets the MSTP forward delay for the Cist Bridge in seconds; default is 15.

Table 213 `spanning- tree mstp` command parameters and variables

Parameters and variables	Description
`max-age <6 - 40>`	Sets the MSTP maximum age time for the Cist Bridge in seconds; default is 20
`pathcost-type {bits16 | bits32}`	Sets the MSTP default pathcost version; default is bits32
`priority {0000 | 10000|20000 … | F000}`	Sets the MSTP bridge priority for the Cist Bridge; default is 8000
`tx-holdcount<1 - 10>`	Sets the MSTP Transmit Hold Count; default is 3
`version {stp-compatible | rstp | mstp}`	Sets the MSTP version for the Cist Bridge; default is mstp

spanning- tree mstp port role command

The `spanning- tree mstp port role` command sets the MSTP parameters which includes pathcost, hello time, edge-port indicator, learning mode, point-to-point indicator, priority, and protocol migration indicator on the single or multiple port for the Common Spanning Tree.

The syntax for the `spanning- tree mstp port role` command is:

```
spanning- tree mstp [port <portlist>] [cost <1 -
200000000>][edge-port {false | true}][hello-time <1 - 10>]
[learning {disable | enable}][p2p {auto | force-false |
force-true}][priority {00 | 10 | … | F0}]
[protocol-migration {false | true}]
```

The `spanning- tree mstp port role` command is in the CLI Interface configuration mode.

Table 214 describes the parameters and variables for the `spanning- tree mstp port role` command.

Table 214 `spanning- tree mstp port role` command parameters

Parameters and variables	Description
`port <portlist>`	Enter a list or range of port numbers.
`cost <1 - 200000000>`	Sets the MSTP pathcost on the single or multiple port; default is 200000
hello-time <1 - 10>	Sets the MSTP hello time on the single or multiple port for the Common Spanning Tree; default is 2
`edge-port {false | true}`	Indicates whether the single or multiple port should be assumed to be edge port or not. This parameter sets the Admin value of edge port status; default is false
`learning {disable | enable}`	Enables or disables MSTP on the single or multiple port; default is enable
`p2p {auto | force-false | force-true}`	Indicates whether the single or multiple port should be treated as a point-to-point link or not. This command sets the Admin value of P2P Status; default is force-true
`priority {00 | 10 |... | F0}`	Sets the MSTP port priority on the single or multiple port; default is 80
`protocol-migration {false | true}`	Forces the single or multiple port to transmit MSTP Buds when set true, while operating in MSTP mode; default is false

spanning-tree mstp region command

The `spanning-tree mstp region` command sets the MSTP parameters which includes config ID selector, region name, and region version. The syntax for the `spanning- tree mstp region` command is:

```
spanning- tree mstp region [config-id-sell <0 - 255>]
[region-name <1 - 32 chars>][region-version <0 - 65535>]
```

The `spanning- tree mstp region` command is in the CLI Global configuration mode.

Table 215 describes the parameters and variables for the `spanning- tree mstp region` command.

Table 215 `spanning- tree mstp region` **command parameters**

Parameters and variables	Description
`[config-id-sell <0 - 255>]`	Sets the MSTP config ID selector; default is 0.
[region-name <1 - 32 chars>]	Sets the MSTP region name, default is 0
[region-version <0 - 65535>]	Sets the MSTP region version; default is 0.

spanning-tree mstp msti command

The `spanning-tree mstp msti` command sets the MSTP parameters which includes forward delay time, hello-time, max hop count, priority, and VLAN mapping for the bridge instance.The syntax for the `spanning- tree mstp msti` command is:

```
spanning-tree mstp msti<1 - 7>[priority{0000|1000|…|F000}]
[add-vlan <vid>]
[remove-vlan <vid>]
[enable]
```

The `spanning- tree mstp msti` command is in the CLI global configuration mode.

Table 216 describes the parameters and variables for the `spanning- tree mstp msti` command.

Table 216 `spanning- tree mstp msti` **command parameters**

Parameters and variables	Description
`<1 - 7>`	Filter on MSTP instance.
`priority {0000	1000 |...	F000}`	Sets the MSTP priority for the bridge instance; default is 8000

Table 216 `spanning- tree mstp msti` command parameters

Parameters and variables	Description
`add-vlan <1 - 4094>`	Maps the specified Vlan and MSTP bridge instance
`remove-vlan <1 - 4094>`	Unmaps the specified Vlan and MSTP bridge instance
`enable`	Enables the MSTP bridge instances

Show spanning-tree mstp msti port role command

The `spanning-tree mstp msti port role` command sets the MSTP parameters which includes MSTP port pathcost, learning mode, and priority on the single or multiple port for the bridge instance.The syntax for the `spanning-tree mstp msti port role` command is:

```
spanning-tree mstp msti <1 - 7> [port <portlist>] [cost <1 -
200000000>][learning {disable | enable}][priority {00 | 10 |
… | F0}]
```

The `spanning-tree mstp msti port role` command is in the CLI Global configuration mode.

Table 217 describes the parameters and variables for the `spanning-tree mstp msti port role` command.

Table 217 `spanning-tree mstp msti port role` command parameters

Parameters and variables	Description
`<1 - 7>`	Filter on MSTP instance.
port <portlist>	Enter a list or range of port numbers.
`cost <1 - 200000000>`	Sets the MSTP port pathcost on the single or multiple port for the bridge instance; default is 200000
`learning {disable | enable}`	Enables or disables MSTP on the single or multiple port for the bridge instance; default is enable
`priority {00 | 10 |... | F0}`	Sets the MSTP port priority on the single or multiple port for the bridge instance; default is 80

No spanning-tree mstp msti command

This command deletes a MSTP bridge-instance.

This command can be executed in the configuration mode, and the syntax is:

```
no spanning-tree mstp msti <1 - 7> [port <portlist>]
```

Spanning-tree mstp msti enable

This command enables a MSTP bridge-instance.

This command can be executed in the configuration mode, and the syntax is:

```
no spanning-tree mstp msti <1 - 7> [port <portlist>]enable
```

No spanning-tree mstp msti enable

This command disables a MSTP bridge-instance.

This command can be executed in the configuration mode, and the syntax is:

```
spanning-tree mstp msti <1 - 7> [port <portlist>]disable
```

Chapter 9
Configuring QoS

This chapter describes how to configure DiffServ and Quality of Service (QoS) parameters for policy-enabled networks. This chapter covers the following topics:

- "Displaying QoS parameters ", next
- "Resetting" on page 342
- "Configuring COPS" on page 343
- "Configuring QoS interface groups" on page 350
- "Configuring DSCP and 802.1p and queue associations" on page 353
- "Configuring QoS filters and filter groups" on page 356
- "Configuring QoS actions" on page 361
- "Configuring QoS meters" on page 363
- "Configuring QoS shapers" on page 364
- "Configuring QoS policies" on page 367
- "Reordering packets" on page 369
- "Interface Class Restrictions" on page 370
- "User-based policies" on page 370

Refer to the *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches* for more information on policy-enable networks, Differentiated Services, and QoS. Refer to Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches for information on configuring these features using the Web-based management system, and refer to Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches for configuration information for the DM.

Note: When you use the `ignore` value in QoS, the system matches all values for that parameter.

Displaying QoS parameters

You can display QoS parameters using the CLI show qos command

The show qos command displays the current QoS policy configuration The syntax for the show qos command is:

```
show qos [interface-groups|interface-assignments|
if-assign-list|egressmap|ingressmap|
ip-filters|ip-filter-sets|
l2-filters|l2-filter-sets|
actions|meters|shapers|policies|
queue-sets|queue-set-assignments|
agent|statistics]
```

The show qos command is in the privExec command mode.

Table 218 describes the parameters and variables for the show qos command.

Table 218 show qos command parameters and variables

Parameters and variables	Description
interface-groups	Displays configured interface groups.
interface-assignments	Displays interface-to-interface group assignments.
if-assign-list	Displays interface-to-interface group assignments.
egressmap	Displays DSCP-to-802.1p priority and loss-sensitivity mapping.
ingressmap	Displays 802.1p priority-to-DSCP mapping.
ip-filters	Displays defined IP filters.
ip-filter-sets	Displays defined IP filter sets.
l2-filters	Displays defined Layer 2 filters.
l2-filter-sets	Displays defined Layer 2 filter sets.
actions	Displays defined QoS action entries.
meters	Displays defined traffic metering entries.
shapers	Displays defined traffic shaping entries.
policies	Displays configured QoS policies.
queue-sets	Displays current queue set information.

Table 218 `show qos` command parameters and variables (Continued)

Parameters and variables	Description
`queue-set-assignments`	Displays 802.1p priority-to-queue assignments by queue set.
`agent`	Displays QoS agent configuration parameters.
`statistics`	Displays QoS policy statistics.

Figure 92 displays sample output from the `show qos interface-groups` command.

Figure 92 `show qos interface-groups` command output

```
BS470_24#show qos interface-groups
     Role          Interface               Capabilities                  Storage
  Combination        Class                                                Type
_______________ ____________ ____________________________________ ___________
allBPSIfcs      Untrusted    Input 802, Input IP                  Read Only
```

Figure 93 displays sample output from the `show qos interface-assignments` command.

Figure 93 `show qos interface-assignments` command output

```
BS470_24#show qos interface-assignments
Unit Port IfIndex Role Combination

____ ____ _______ _________________
1    1          1   allBPSIfcs
1    2          2   Webbrowsing
1    3          3   Test1
1    4          4   allBPSIfcs
1    5          5   allBPSIfcs
1    6          6   allBPSIfcs
1    7          7   Test1
1    8          8   allBPSIfcs
1    9          9   allBPSIfcs
1    10         10  allBPSIfcs
1    11         11  Webbrowsing
1    12         12  allBPSIfcs
1    13         13  allBPSIfcs
1    14         14  allBPSIfcs
1    15         15  Test1
1    16         16  allBPSIfcs
1    17         17  Webbrowsing
1    18         18  allBPSIfcs
1    19         19  allBPSIfcs
1    20         20  allBPSIfcs
1    21         21  allBPSIfcs
1    22         22  allBPSIfcs
1    23         23  allBPSIfcs
1    24         24  allBPSIfcs
```

Figure 94 displays sample output from the `show qos if-assign-list` command.

Figure 94 `show qos if-assign-list` command output

```
BS470_24#show qos interface-assignments
Unit Port IfIndex Role Combination

____ ____ _______ _________________
1    1      1      allBPSIfcs
1    2      2      Webbrowsing
1    3      3      Test1
1    4      4      allBPSIfcs
1    5      5      allBPSIfcs
1    6      6      allBPSIfcs
1    7      7      Test1
1    8      8      allBPSIfcs
1    9      9      allBPSIfcs
1    10     10     allBPSIfcs
1    11     11     Webbrowsing
1    12     12     allBPSIfcs
1    13     13     allBPSIfcs
1    14     14     allBPSIfcs
1    15     15     Test1
1    16     16     allBPSIfcs
1    17     17     Webbrowsing
1    18     18     allBPSIfcs
1    19     19     allBPSIfcs
1    20     20     allBPSIfcs
1    21     21     allBPSIfcs
1    22     22     allBPSIfcs
1    23     23     allBPSIfcs
1    24     24     allBPSIfcs
```

Figure 95 displays sample output from the `show qos egressmap` command.

Figure 95 `show qos egressmap` command output

```
DSCP 802.1p Priority  Drop Precedence

____ _______________ __________________
0    0                Not Loss Sensitive
1    0                Not Loss Sensitive
2    0                Not Loss Sensitive
3    0                Not Loss Sensitive
4    0                Not Loss Sensitive
5    0                Not Loss Sensitive
6    0                Not Loss Sensitive
7    0                Not Loss Sensitive
8    2                Not Loss Sensitive
9    0                Not Loss Sensitive
10   2                Loss Sensitive
11   0                Not Loss Sensitive
12   2                Not Loss Sensitive
13   0                Not Loss Sensitive
14   2                Not Loss Sensitive
15   0                Not Loss Sensitive
16   3                Not Loss Sensitive
17   0                Not Loss Sensitive
18   3                Loss Sensitive
19   0                Not Loss Sensitive
```

Figure 96 displays sample output from the `show qos ingressmap` command.

Figure 96 `show qos ingressmap` command output

```
BS470_24#show qos ingressmap
802.1p Priority DSCP

_______________ ____
0               0
1               0
2               10
3               18
4               26
5               34
6               46
7               48
```

Figure 97 displays sample output from the `show qos ip-filters` command.

Figure 97 `show qos ip-filters` command output

```
BS470_24#show qos ip-filters
Id    Destination       Source       DSCP  Protocol  Dest     Src
      Addr / Mask     Addr / Mask                   L4 Port L4 Port

___ _______________ _______________ ______ ________ _______ _______
1   Ignore          Ignore          Ignore Ignore   0       0
    Ignore          Ignore
2   10.10.1.102     Ignore          Ignore Ignore   0       0
    255.255.255.255 Ignore
```

Figure 98 displays sample output from the `show qos ip-filter-sets` command.

Figure 98 `show qos ip-filter-sets` command output

```
BS470_24#show qos ip-filter-sets
IP Filter Sets

Id        Name       Acl Id Ace Id Ace Order

___ ________________ ______ ______ _________
2   G1-ip            1      2      2
```

Figure 99 displays sample output from the `show qos l2-filters` command.

Figure 99 `show qos l2-filters` command output

```
BS470_24#show qos l2-filters
Id  VLAN  VLAN Tag Ether   802.1p   DSCP  Protocol    Dest IP       Src IP
                   Type   Priority                    L4 Port       L4 Port
                                                     Min   Max     Min   Max

__ ______ ________ ______ ________ ______ ________ ______ ______ ______ ______
1  Ignore Ignore   Ignore          Ignore Ignore   Ignore Ignore Ignore Ignore
2  Ignore Ignore   0x800  Ignore   63     Ignore   Ignore Ignore Ignore Ignore
3  Ignore Ignore   Ignore          Ignore Ignore   Ignore Ignore Ignore Ignore
4  Ignore Ignore   Ignore 0,1,2,3, Ignore Ignore   Ignore Ignore Ignore Ignore
5  Ignore Ignore   0x800           1      Ignore   Ignore Ignore Ignore Ignore
BS470_24#
```

Figure 100 displays sample output from the `show qos l2-filter-sets` command.

Figure 100 `show qos l2-filter-sets` command output

```
BS470_24#show qos l2-filter-sets
Layer2 Filter Sets

Id        Name       Acl Id Ace Id Ace Order
___ ________________ ______ ______ _________
1   fGrp1            1      1      1
2   fGrp2            2      1      1
```

Figure 101 displays sample output from the `show qos actions` command. Each service class has a default action that uses default mappings.

Figure 101 `show qos actions` command output

```
BS470_24#show qos actions
 Id         Name       Drop  Update      Set Drop      802.1p Priority
                              DSCP      Precedence

_____ ________________ _____ ______ __________________ _______________
65526 Drop_Traffic     True  Ignore Ignore             Ignore
65527 Standard_Service False 0x0    Not Loss Sensitive Priority 0
65528 Bronze_Service   False 0xA    Loss Sensitive     Priority 2
65529 Silver_Service   False 0x12   Loss Sensitive     Priority 3
65530 Gold_Service     False 0x1A   Loss Sensitive     Priority 4
65531 Platinum_Service False 0x22   Loss Sensitive     Priority 5
65532 Premium_Service  False 0x2E   Loss Sensitive     Priority 6
65533 Network_Service  False 0x30   Loss Sensitive     Priority 7
65534 Trusted_IP        False Ignore Use Egress Map     Use Egress Map
65535 Trusted_NonIP    False Ignore Ignore             Ignore
```

Figure 102 displays sample output from the `show qos meters` command. Each service class has a default meter that uses default actions and mappings.

Figure 102 `show qos meters` command output

```
BS470_48#show qos meters
 Id       Name         Data    Commit  Commit   In-Profile Out-Profile
                       Spec     Rate    Burst   Action         Action
                               (Kbps)  (Bytes)

_____ ________________ _____________________________________________
65526 Drop_Traffic     No Meter 0        0      Drop_Traffic
65527 Standard_Service No Meter 0        0      Standard_Servi
65528 Bronze_Service   No Meter 0        0      Bronze_Service
65529 Silver_Service   No Meter 0        0      Silver_Service
65530 Gold_Service     No Meter 0        0      Gold_Service
65531 Platinum_Service No Meter 0        0      Platinum_Servi
65532 Premium_Service  No Meter 0        0      Premium_Servic
65533 Network_Service  No Meter 0        0      Network_Servic
65534 Trusted_IP       No Meter 0        0      Trusted_IP
65535 Trusted_NonIP    No Meter 0        0      Trusted_NonIP
```

Figure 103 displays sample output from the `show qos shapers` command.

Figure 103 `show qos shapers` command output

```
BS470_24#show qos shapers
Id        Name                Rate          Burst         Queue
                                            Size           Size
                             (Kbps)        (Bytes)        (Packets)

___ ___________________________ ___________ _______________
1         shaper1            64000          5555             2
```

Figure 104 displays sample output from the `show qos policies` command.

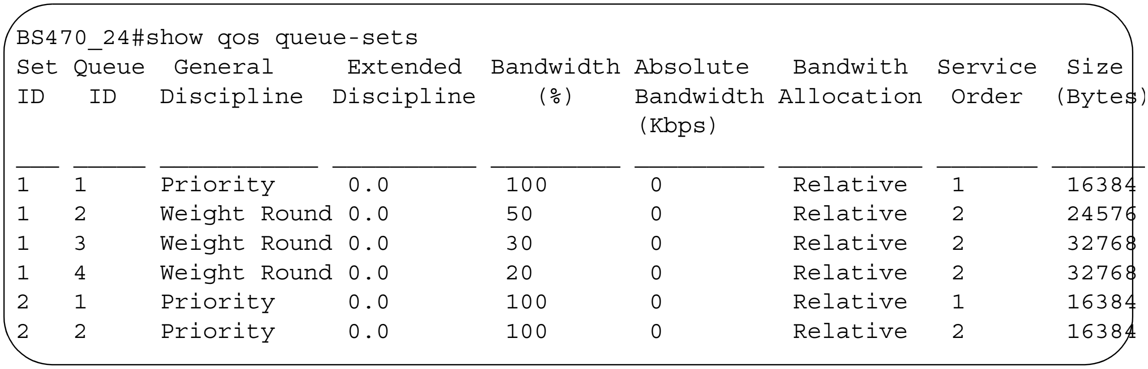
Figure 104 `show qos policies` command output

```
BS470_24#show qos policies
Id    Name       Filter Set    Filter      Role         Order Type   Combination

___ ___________ _______________ ______ ______
1   wizardIP     wizardIP_FLTR    IP     allBPSIfcs     1
2   wizardL2     wizardL2_FLTR    L2     allBPSIfcs       2
Id Meter In-Profile   Out-of-Profile  Shaper Shaper  User Group
```

Figure 105 displays sample output from the `show qos queue-sets` command.

Figure 105 `show qos queue-sets` command output



```
BS470_24#show qos queue-sets
Set Queue  General      Extended  Bandwidth Absolute   Bandwith  Service  Size
ID   ID   Discipline   Discipline    (%)    Bandwidth Allocation  Order  (Bytes)
                                            (Kbps)

___ _____ ___________ __________ _________ _________ __________ _______ ______
1   1     Priority      0.0        100       0          Relative   1        16384
1   2     Weight Round 0.0         50        0          Relative   2        24576
1   3     Weight Round 0.0         30        0          Relative   2        32768
1   4     Weight Round 0.0         20        0          Relative   2        32768
2   1     Priority      0.0        100       0          Relative   1        16384
2   2     Priority      0.0        100       0          Relative   2        16384
```

Figure 106 displays sample output from the `show qos queue-set-assignments` command.

Figure 106 `show qos queue-set-assignments` command output

```
BS470_24#show qos queue-set-assignment
Queue Set 1

802.1p Priority Queue
_______________ _____
0               4
1               4
2               3
3               3
4               2
5               2
6               1
7               1
Queue Set 2

802.1p Priority Queue
_______________ _____
0               2
1               2
2               2
3               2
4               2
5               2
6               1
7               1
```

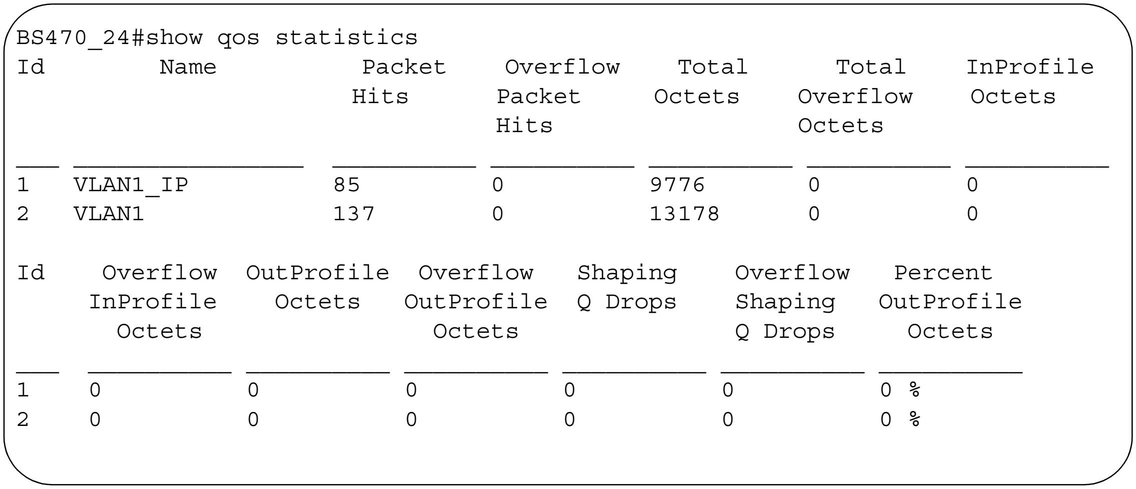
Figure 107 displays sample output from the `show qos agent` command.

Figure 107 `show qos agent` command output

```
BS470_24#show qos agent
QoS Policy Server Control: Enabled
QoS Policy Agent Retry Timer: 5 seconds
Allow Packet Reordering: Enabled
Maintain Policing Statistics: Enabled
Interface Class Restrictions: Allow All Classes
```

Figure 108 displays sample output from the `show qos statistics` command.

Figure 108 `show qos statistics` command output



```
BS470_24#show qos statistics
Id        Name          Packet     Overflow    Total      Total    InProfile
                       Hits      Packet     Octets    Overflow    Octets
                                 Hits                 Octets

___ ________________  __________ __________ __________ __________ __________
1   VLAN1_IP          85         0          9776       0          0
2   VLAN1             137        0          13178      0          0

Id    Overflow  OutProfile  Overflow   Shaping    Overflow   Percent
     InProfile    Octets   OutProfile  Q Drops    Shaping   OutProfile
       Octets                Octets               Q Drops     Octets
___  __________ __________ __________ __________ __________ __________
1    0          0          0          0          0          0 %
2    0          0          0          0          0          0 %
```

Resetting

You can reset the system to the factory defaults.

qosagent reset-default command

The `qosagent reset-default` command deletes all installed states and resets the system to factory default values. The syntax for the `qosagent reset-default` command is:

```
qosagent reset-default
```

The `qosagent reset-default` command is in the config mode.

The `qosagent reset-default` command has no parameters or variables.

Configuring COPS

Note: COPS is not supported in this release of the BayStack 460-24T-PWR switch.

You can enable COPS-PR, the dynamic management system, using the CLI. This section covers:

- "qosagent server-control command ", next
- "show cops retry command" on page 344
- "show cops server command" on page 344
- "show cops stats command" on page 345
- "cops retry command" on page 348
- "cops server command" on page 348
- "default cops retry command" on page 349
- "no cops server command" on page 350

qosagent server-control command

The `qosagent server-control` command enables COPS. The syntax for the `qosagent server-control` command is:

```
qosagent server-control {enable|disable} [retry-timer
<no-retry|1-86400>]
```

The `qosagent server-control` command is in the config mode.

Table 219 describes the parameters and variables for the `qosagent server-control` command.

Table 219 `qosagent server-control` command parameters and variables

Parameters and variables	Description
`enable|disable`	Enables COPS.

`retry-timer`
`<no-retry|1-86400>`
	Sets the value for the retry timer:
	• no retry—connection retry not attempted after a failed attempt
	• 1-86400—specifies the seconds between receipt of a connection termination/rejection notification and initiation of a new connection request

show cops retry command

The `show cops retry` command displays COPS TCP retry settings. The syntax for the `show cops retry` command is:

```
show cops retry
```

The `show cops retry` command is in the privExec mode.

The `show cops retry` command has no variables or parameters.

Figure 109 displays sample output from the `show cops retry` command.

Figure 109 `show cops retry` command output

```
BS470_24#show cops retry
Retry Algorithm:  Sequential
Retry Count    :  1
Retry Interval :  100 seconds
```

show cops server command

The `show cops server` command displays configured COPS servers. The syntax for the `show cops server` command is:

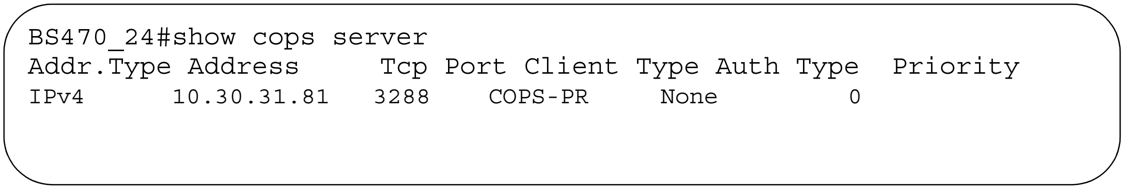
```
show cops server
```

The `show cops server` command is in the privExec mode.

The `show cops server` command has no variables or parameters.

Figure 110 displays sample output from the `show cops server` command.

Figure 110 `show cops server` command output



```
BS470_24#show cops server
Addr.Type Address      Tcp Port Client Type Auth Type   Priority
IPv4      10.30.31.81    3288     COPS-PR     None          0
```

show cops stats command

The `show cops stats` command displays COPS statistics. The syntax for the `show cops stats` command is:

```
show cops stats
```

The `show cops stats` command is in the privExec mode.

The `show cops stats` command has no variables or parameters.

Figure 111 and Figure 112 display sample output from the `show cops stats` command.

Figure 111 `show cops stats` command output (1 of 2)

```
BS470_24#show cops stats
---------------------------------------------
PDP IPv4 Address:             47.130.100.42
    TCP Port:                 3288
    Configuration Source:     Static
    Authentication Type:      None
    Last Connection Attempt:  5745
    TCP Connect Attempts:     12
    TCP Connect Failures:     12
    Connection State:            Invalid
    Keep-Alive Time:             0
    Accounting Time:             0
    Messages Received:           0
    Messages Sent:               0
    Messages Syntax Errors:      0
    Last Protocol Error:         <unknown>
    Open Attempts:               0
    Open Failures:               0
    Unsupported Client Types:    0
    Unsupported Versions:        0
    Length Mismatches:           0
    Unknown Opcodes:             0
    Unknown C-NUMs:              0
    Bad C-TYPEs:                 0
    Bad Sends:                   0
    Wrong Objects:               0
    Wrong Opcodes:               0
    Client Keep-Alive Timeouts:  0
    Authentication Failures:     0
    Authentication Missings:     0
---------------------------------------------
PDP IPv4 Address:             47.130.101.81
    TCP Port:                 3288
    Configuration Source:     Static
    Authentication Type:      None
    Last Connection Attempt:  6343
TCP Connect Attempts:     12
    TCP Connect Failures:     11
    Connection State:            Connected
    Keep-Alive Time:             120
    Accounting Time:             0
```

Figure 112 `show cops stats` command output (2 of 2)

```
Accounting Time:             0
   Messages Received:           21
   Messages Sent:               3
   Messages Syntax Errors:      0
   Last Protocol Error:         <unknown>
   Open Attempts:               0
   Open Failures:               0
   Unsupported Client Types:    0
   Unsupported Versions:        0
   Length Mismatches:           0
   Unknown Opcodes:             0
   Unknown C-NUMs:              0
   Bad C-TYPEs:                 0
   Bad Sends:                   0
   Wrong Objects:               0
   Wrong Opcodes:               0
   Client Keep-Alive Timeouts:  0
   Authentication Failures:     0
   Authentication Missings:     0
                Client Type:  COPS-PR
                        Connection State:            Accepted
                        Keep-Alive Time:             120
                        Accounting Time:             0
                        Messages Received:           15
                        Messages Sent:               16
                        Messages Syntax Errors:      0
                        Last Protocol Error:         <unknown>
                        Open Attempts:               1
                        Open Failures:               0
                        Unsupported Client Types:    0
                        Unsupported Versions:        0
                        Length Mismatches:           0
                        Unknown Opcodes:             0
                        Unknown C-NUMs:              0
                        Bad C-TYPEs:                 0
                        Bad Sends:                   0
                        Wrong Objects:               0
                        Wrong Opcodes:               0
                        Client Keep-Alive Timeouts:  0
                        Authentication Failures:     0
                        Authentication Missings:     0
```

cops retry command

The `cops retry` command sets the COPS TCP retry settings. The syntax for the `cops retry` command is:

```
cops retry <0-32> <1-600>
```

The `cops retry` command is in the config command mode.

Table 220 describes the parameters and variables for the `cops retry` command.

Table 220 `cops retry` command parameters and variables

Parameters and variables	Description
`retry <0-32> <1-500>`	Enter the number of retries and the retry interval (in seconds). Default is 10 seconds.

cops server command

The `cops server` command creates or modifies a COPS server configuration. The syntax for the `cops server` command is:

```
cops server <A.B.C.D> [tcp-port <0-65535>] [priority
<0-65535>]
```

The `cops server` command is in the config command mode.

Table 221 describes the parameters and variables for the `cops server` command.

Table 221 `cops server` command parameters and variables

Parameters and variables	Description
`<A.B.C.D>`	Enter the IP address of the COPS server you want to use.
`tcp-port <0-65535>`	Enter the number of the TCP port you want to use. The default port is 3288.
`priority <0-65535>`	Enter the priority you want this server to have. The default priority is 0.

default cops retry command

The `default cops retry` command restores the default COPS TCP retry settings. The syntax for the `default cops retry` command is:

```
default cops retry
```

The `default cops retry` command is in the config command mode.

The `default cops retry` command has no variables or parameters.

default cops server command

The `default cops server` command restores COPS TCP port and priority settings for a COPS server configuration. The syntax for the `default cops server` command is:

```
default cops server <A.B.C.D> [tcp-port] [priority]
```

The `default cops server` command is in the config command mode.

Table 222 describes the parameters and variables for the `default cops server` command.

Table 222 `default cops server` command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of the COPS server you want to use.
tcp-port	Restores the default TCP port. The default TCP port is 3288
priority *<0-65535>*	Restores the default priority. The default priority is 0.

no cops server command

The `no cops server` command removes a COPS server configuration. The syntax for the `no cops server` command is:

```
no cops server <A.B.C.D>
```

The `no cops server` command is in the config command mode.

Table 223 describes the parameters and variables for the `no cops server` command.

Table 223 `no cops server` command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of the COPS server you want to clear. Omitting this variable will clear the entire COPS server table.

Configuring QoS interface groups

You can add or delete ports to or from an interface group, or add or delete the interface groups themselves. This section covers:

- "qos if-assign command ", next
- "qos if-group command" on page 351

- “qos if-assign-list command” on page 352

qos if-assign command

The `qos if-assign` command adds or deletes ports to or from a defined interface group. The syntax for the `qos if-assign` command is:

```
qos if-assign {del [portlist <portlist>]|add [port
<portlist>] name <tag>}
```

The `qos if-assign` command is in the config-if command mode.

Table 224 describes the parameters and variables for the `qos if-assign` command.

qos if-group command

Table 224 `qos if-assign` command parameters and variables

Parameters and variables	Description
`add|del`	Adds or deletes the port to or from the interface group.
`port <portlist>`	Enter the port(s) the port to add or delete to interface group. Note: If you omit this parameter, the system uses the port number specified when you issued the `interface` command.
`name <tag>`	Enter the name of the defined interface group.

The `qos if-group` command adds or deletes interface groups. The syntax for the `qos if-group` command is:

```
qos if-group name <tag> {create class <ifclass>|delete}
```

The `qos if-group` command is in the config command mode.

Table 225 describes the parameters and variables for the `qos if-group` command.

Table 225 `qos if-group` command parameters and variables

Parameters and variables	Description
`name <tag>`	Enter the name of the interface group you are working with; maximum of 32 alphanumeric characters.
`create class <ifclass>`	Defines a new interface group and specifies the class of traffic received on interfaces associated with this interface group: • `trusted` • `untrusted` • `unrestricted`
`delete`	Deletes an existing interface group.

qos if-assign-list command

The `qos if-assign-list` command adds or deletes a list of ports to or from a defined interface group. The syntax for the `qos if-assign-list` command is:

```
qos if-assign-list {del portlist <portlist>|add portlist
<portlist> name <tag>}
```

The `qos if-assign-list` command is in the config-if command mode.

Table 226 describes the parameters and variables for the `qos if-assign-list` command.

Table 226 `qos if-assign-list` command parameters and variables

Parameters and variables	Description
`add|del`	Adds or deletes the port to or from the interface group.
`portlist <portlist>`	Enter the list of ports to add or delete to interface group. Note: If you omit this parameter, the system uses the port number specified when you issued the `interface` command.
`name <tag>`	Enter the name of the defined interface group.

Note: Before adding an interface to an interface group, you must delete the interface from its current interface group.

Note: You cannot delete interface groups that are referenced by an installed policy or associated with device interfaces.

qosagent class-restrictions command

The `qosagent class-restrictions` command restricts interfaces classes to all classes, trusted and unrestricted, or unrestricted-only. The syntax for the `qosagent class-restrictions` command is:

```
qosagent class-restrictions
{all-classes|trusted-and-unrestricted|unrestricted-only}
```

The `qosagent class-restrictions` command is in the config mode.

Table 227 describes the parameters and variables for the `qosagent class-restrictions` command.

Table 227 `qosagent class-restrictions` command parameters and variables

Parameters and variables	Description
<all-classes|trusted-and-unrestricted|unrestricted-only>	Sets the allowed interface class or classes.

Configuring DSCP and 802.1p and queue associations

You can configure the DSCP, IEEE 802.1p priority, and queue set association using the CLI. This section covers:

- "qos egressmap command "," next
- "qos ingressmap command" on page 354
- "qos queue-set-assignment command" on page 355

qos egressmap command

The `qos egressmap` command configures DSCP-to-802.1p priority and drop precedence associations that are used for assigning these values at packet egress, based on the DSCP in the received packet. The syntax for the `qos egressmap` command is:

```
qos egressmap ds <dscp> 1p <ieee1p> dp <dropprec>
```

The `qos egressmap` command is in the config command mode.

Table 228 describes the parameters and variables for the `qos egressmap` command.

Table 228 `qos egressmap` command parameters and variables

Parameters and variables	Description
`ds <dscp>`	Enter the DSCP value used as a lookup key for 802.1p priority and drop precedence at egress when appropriate; range is between 0 and 63.
`1p <ieee1p>`	Enter the 802.1p priority value associated with the DSCP; range is between 0 and 7.
`dp <dropprec>`	Enter the drop precedence values associated with the DSCP: • loss-sensitive • not-loss-sensitive

qos ingressmap command

The `qos ingressmap` command configures 802.1p priority-to-DSCP associations that are used for assigning default values at packet ingress, based on the 802.1p priority value in the received packet. The syntax for the `qos ingressmap` command is:

```
qos ingressmap 1p <ieee1p> ds <dscp>
```

The `qos ingressmap` command is in the config command mode.

Table 229 describes the parameters and variables for the `qos ingressmap` command.

Table 229 `qos ingressmap` command parameters and variables

Parameters and variables	Description
`1p <ieee1p>`	Enter the 802.1p priority value used as a lookup key for DSCP assignment at ingress when appropriate; range is between 0 and 7.
`ds <dscp>`	Enter the DSCP value associated with the 802.1p priority value; range is between 0 and 63.

qos queue-set-assignment command

The `qos queue-set-assignment` command associates the 802.1p priority values with a specific queue **within** a specific queue set. This association determines the egress scheduling treatment that traffic with a specific 802.1p priority value receives. The syntax for the `qos queue-set-assignment` command is:

```
qos queue-set-assignment queue-set <setid> 1p <ieee1p>
queue <qid>
```

The `qos queue-set-assignment` command is in the config command mode.

Table 230 describes the parameters and variables for the `qos queue-set-assignment` command.

Table 230 `qos queue-set-assignment` command parameters and variables

Parameters and variables	Description
`queue-set <setid>`	Enter the queue set ID.
`1p <ieee1p>`	Enter the 802.1p priority value for which the queue association is being modified; range is between 0 and 7.
`queue <qid>`	Enter the queue **within** the identified queue set to assign the 802.1p priority traffic at egress.

Configuring QoS filters and filter groups

You can configure filters and filter sets using the CLI. This section covers:

- "qos ip-filter command ", next
- "qos ip-filter-set command" on page 357
- "qos l2-filter command" on page 358
- "qos l2-filter-set command" on page 360

qos ip-filter command

The `qos ip-filter` command adds or deletes IP filters. The syntax for the `qos ip-filter` command is:

```
qos ip-filter <fid> {create [src-ip <src-ip-info>] [dst-ip
<dst-ip-info>] [ds-field <dscp>] [protocol <protocoltype>]
[src-port <port>] [dst-port <port>]|delete}
```

The `qos ip-filter` command is in the config command mode.

Table 231 describes the parameters and variables for the `qos ip-filter` command.

Table 231 `qos ip-filter` command parameters and variables

Parameters and variables	Description
<fid>	Enter an integer to specify the filter ID.
create	Defines a new IP filter with the specified filter ID.
src-ip <*src-ip-info*>	Enter the source IP address and mask in the form of a.b.c.d/x or a.b.c.d x.x.x.x. Default is 0.0.0.0.
dst-ip <*dst-ip-info*>	Enter the destination IP address and mask in the form of a.b.c.d/x or a.b.c.d x.x.x.x. Default is 0.0.0.0.
ds-field <*dscp*>	Enter 6-bit DSCP value; range is 0 to 63. Default is ignore.

Table 231 `qos ip-filter` command parameters and variables

Parameters and variables	Description
`protocol <protocoltype>`	Enter the protocol type: • ignore • icmp • tcp • udp Default is ignore.
`src-port <port>`	Enter TCP/UDP source port value. Default is ignore.
`dst-port <port>`	Enter TCP/UDP destination port value. Default is ignore.
`delete`	Deletes the IP filter with the specified filter ID.

Note: If you omit any parameter, the default value is used..

qos ip-filter-set command

The `qos ip-filter-set` command adds or deletes currently defined IP filters into an IP filter set. The syntax for the `qos ip-filter-set` command is:

```
qos ip-filter-set <fgid> {create set <setid> [name
<setname>] filter <fid> filter-prec <prec>|delete}
```

The `qos ip-filter-set` command is in the config command mode.

Table 232 describes the parameters and variables for the `qos ip-filter-set` command.

Table 232 `qos ip-filter-set` command parameters and variables

Parameters and variables	Description
<fgid>	Enter an integer to specify the filter group ID; range is 1 to 65535.
create set *<setid>*	Initiates creation of an IP filter set with the designated filter set ID. Enter the IP filter set ID; range is 1 to 65535
name *<setname>*	Assigns a name to the designated filter set ID. Enter the name for the filter set; maximum is 16 alphanumeric characters
filter *<fid>*	Adds an IP filter to the filter set; range is 1 to 65535.
filter-prec *<prec>*	Specifies the precedence, or filter evaluation order, within the set. Enter the precedence value you want for this filter; range is 1 to 65535.
delete	Deletes the IP filter set.

Note: You must define the filter before adding it to a filter set. You cannot delete an IP filter set that is referenced in an installed policy. You cannot delete the last IP filter in an IP filter set that is referenced in an installed policy.

qos l2-filter command

The `qos l2-filter` command adds and deletes layer 2 (L2) filters. The syntax for the `qos l2-filter` command is:

```
qos l2-filter <fid> {create [ethertype <etype>]
[vlan <vidlist>] [vlan-tag <vtag>] [priority <ieee1p-seq>]
[ds-field <dscp>] [protocol <protocoltype>] [src-port-min
<port> src-port-max <port>] [dst-port-min <port>
dst-port-max <port>]|delete}
```

The `qos l2-filter` command is in the config mode.

Table 233 describes the parameters and variables for the `qos l2-filter` command.

Table 233 `qos l2-filter` command parameters and variables

Parameters and variables	**Description**
<*fid*>	Enter an integer to specify the filter ID; range is 1 to 65535.
`create`	Defines a new L2 filter with the specified filter ID.
`ethertype` <*etype*>	Enter the Ethernet type in the form of 0xXXXX, for example, 0x0801. Default is ignore.
`vlan` <*vidlist*>	Enter the number of the VLAN IDs, separated by commas. (Format: VLAN x-x, x, x) Default is ignore.
`vlan-tag` <*vtag*>	Enter the type of VLAN tagging filter you want: • tagged • untagged • ignore Default is ignore.
`priority` <*ieee1p-seq*>	Enter the 802.1p priority values; range from 0 to 7. Enter in the form of [a(,b)*(c-d)*], for example, 0, 3-4, 7. Default is ignore.
`ds-field` <*dscp*>	Enter a 6-bit value for the DS field; range is from 0 to 63. Default is ignore.
`protocol` <*protocoltype*>	Enter the protocol type: • ignore • icmp • tcp • udp Default is ignore.
`src-port-min` <*port*>	Enter the TCP/UDP minimum source port value; range is 0 to 65535. Default is 0 = ignore.
`src-port-max` <*port*>	Enter the TCP/UDP maximum source port value; range is 0 to 65535. Default is 65535 = ignore.
`dst-port-min` <*port*>	Enter the TCP/UDP minimum destination port value; range is 0 to 65535. Default is 0 = ignore.

Table 233 `qos l2-filter` command parameters and variables (Continued)

Parameters and variables	Description
`dst-port-max <port>`	Enter the TCP/UDP maximum destination port value; range is 0 to 65535. Default is 65535 = ignore.
`delete <fid>`	Enter the filter ID you want to delete.

Note: If you omit any parameter, the default value is used. You cannot delete a filter that is referenced by an L2 filter set.

qos l2-filter-set command

The `qos l2-filter-set` command adds and deletes Layer 2 filters into an L2 filter set. The syntax for the `qos l2-filter-set` command is:

```
qos l2-filter-set <fgid> {create set <setid> [name
<setname>] filter <fid> filter-prec <prec>|delete}
```

The `qos l2-filter-set` command is in the config command mode.

Table 234 describes the parameters and variables for the `qos l2-filter-set` command.

Table 234 `qos l2-filter-set` command parameters and variables

Parameters and variables	Description
`<fgid>`	Enter an integer to specify the filter group ID you want to work with; range is 1 to 65535.
`create set <setid>`	Initiates creation of an L2 filter set with the designated filter set ID. Enter the IP filter set ID; range is 1 to 65535.
`name <setname>`	Assigns a name to the designated filter set ID. Enter the name for the filter set; maximum is 16 alphanumeric characters.
`filter <fid>`	Adds an L2 filter to the filter set; range is 1 to 65535.

Table 234 `qos l2-filter-set` command parameters and variables (Continued)

Parameters and variables	Description
`filter-prec <prec>`	Specifies the precedence, or filter evaluation order, within the set. Enter the precedence value you want for this filter; range is 1 to 65535.
`delete`	Deletes the L2 filter set.

> ➡ You must define the filter before adding it to a filter set. You cannot delete an L2 filter set that is referenced in an installed policy. You cannot delete the last L2 filter in an L2 filter set that is referenced in an installed policy.

Layer-2 restricted QoS meters

With restricted meters, you are allowed a maximum of 23 Layer-2 metered policies. All 23 metered policies may have a different in-profile-action, but they will all share the same out-of-profile action. The first policy created will consume two filters; one filter is consumed for the in-profile action, and another filter is consumed for the out-of-profile action. Subsequent restricted Layer-2 metered policies will only use one filter for the in-profile-action and they will share the out-of-profile action defined by the first filter. Since only one filter is used for each policy, statistics will only count in-profile traffic.

Restricted meters can only be used when the Interface Class Restriction is set to Unrestricted Only.

Configuring QoS actions

You can configure QoS actions, which directs the BayStack 470-24T to take specific action on each packet, using the CLI.

qos action command

The `qos action` command creates or deletes a QoS action. The syntax for the `qos action` command is:

```
qos action <actid> [name <actname>] [drop-action
{enable|disable}] [update-dscp <dscp>] [update-1p
{<ieee1p>|default|use-egress-map}] [set-drop-prec
{loss-sensitive|not-loss-sensitive|default|use-egress-map}]
```

The `qos action` command is in the config mode.

Table 235 describes the parameters and variables for the `qos action` command.

Table 235 `qos action` command parameters and variables

Parameters and variables	Description
`<actid>`	Enter an integer to specify the QoS action; range is 1 to 65535.
`name <actname>`	Assigns a name to a QoS action with the designated action ID. Enter the name for the action; maximum is 16 alphanumeric characters
`drop-action {enable|disable}`	Specifies whether packets should be dropped or not; the drop action equals enable. Default is disable.
`update-dscp <dscp>`	Specifies whether DSCP value should be updated or left unchanged; unchanged equals ignore. Enter the 6-bit DSCP value you want; range is 0 to 63. Default is ignore.
`update-1p`	Specifies whether 802.1p priority value should be updated or left unchanged; unchanged equals ignore: • ieee1p—enter the value you want; range is 0 to 7 • default—allows the value to be derived based on assignment of other action parameters • use-egress-map—uses the egress map to assign value Default is ignore.
`set-drop-prec {loss-sensitive|not-loss-sensitive|default|use-egress-map}`	Enter the loss-sensitivity value you want: • loss-sensitive • not-loss-sensitive • default • use-egress-map Default is ignore.

Note: Certain options may be restricted based on the policy associated with the specific action.
You cannot delete an action that is referenced in an installed policy.

Configuring QoS meters

Using the CLI, you set meters. If you want to meter, or police, the traffic, configure the committed rate, burst rate, and burst duration. If you are not metering data, skip this page.

qos meter command

The `qos meter` command creates or deletes a QoS meter. The syntax for the `qos meter` command is:

```
qos meter <metid> {create [name <metname>] committed-rate
<rate> max-burst-rate <burstrate> [max-burst-duration
<burstdur>]|delete}
```

The `qos meter` command is in the config command mode.

Table 236 describes the parameters and variables for the `qos meter` command.

Table 236 `qos meter` command parameters and variables

Parameters and variables	Description
`<metid>`	Enter an integer to specify the QoS meter; range is 1 to 65535.
`name <metname>`	Assigns a name to the QoS meter with the designated meter ID. Enter name for meter; maximum is 16 alphanumeric characters.
`committed-rate <rate>`	Specifies rate that traffic must not exceed for extended periods to be considered in-profile. Enter the rate in Kb/s for in-profile traffic; range is 1 to 65535 Kb/s.
`max-burst-rate <burstrate>`	Specifies the largest burst of traffic that can be received a given time for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst rate in Kb/s for in-profile traffic; range is 1 to 65535 Kb/s

Table 236 `qos meter` command parameters and variables (Continued)

Parameters and variables	Description
`max-burst-duration <burstdur>`	Specifies the amount of time that the largest burst of traffic that can be received for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst duration in ms for in-profile traffic; range is 1 to 65535 ms.
`delete`	Deletes the specified meter.

The formula for the Committed Burst Size (in bytes) is:

Committed Burst Size = (max-burst-duration * (max-burst-rate - committed rate))/ 8

Where:

Committed Burst Size is rounded up to one of the following values:

2047, 4095, 8191, 16383, 32767, 65535, 131071

➡ **Note:** You cannot delete a meter that is referenced in an installed policy.

Configuring QoS shapers

➡ **Note:** You must be using the BayStack 470-24T GBIC in order to implement the QoS shaping features.

Using the CLI, you set shapers. If you want to shape traffic at the egress point, configure the committed rate, burst rate, burst duration, and queue depth for each shaper.

qos shaper command

The `qos shaper` command creates or deletes a QoS shaper. The syntax for the `qos shaper` command is:

```
qos shaper <shapeid> {create [name <shapername>] shape-rate
<rate> max-burst-rate <burstrate> [max-burst-duration
<burstdur>] queue-size <1|2|4|8|16>|delete}
```

The `qos shaper` command is in the config command mode.

Table 237 describes the parameters and variables for the `qos shaper` command.

Table 237 `qos shaper` command parameters and variables

Parameters and variables	Description
`<shapeid>`	Enter an integer to specify the QoS shaper; range is 1 to 65535.
`name <shapername>`	Assigns a name to the QoS shaper with the designated shaper ID. Enter name for shaper; maximum is 16 alphanumeric characters.
`shape-rate <rate>`	Specifies maximum rate that traffic will be transmitted over a given duration Enter the rate in Kbps; range is 1 to 42949672955 Kbps. Note**:** You must specify a value that is a multiple of 64 Kbps; O is invalid.
`max-burst-rate <burstrate>`	Specifies the largest burst of traffic that can be transmitted without a shaping delay. Used in calculating the committed burst size. Enter the burst rate in klbs; range is 0 to 42949672955 kbps.
`max-burst-duration <burstdur>`	Specifies the amount of time that the largest burst of traffic can be transmitted without a shaping delay. Enter the burst duration in ms; range is 0 to 42949672955 ms.
`queue-size <1|2|4|8|16>`	Specifies the number of packets that can exceed the largest burst of traffic allowed and still be queued for transmission.
`delete`	Deletes the specified shaper.

The formula for the Committed Burst Size (in bytes) is:

Committed Burst Size = (max-burst-duration * (max-burst-rate - shape rate))/8

Where:

Committed Burst Size is rounded up to one of the following values:

2047, 4095, 8191, 16383, 32767, 65535

➡ You cannot delete a shaper that is referenced in an installed policy.

Gathering QoS statistics

You can gather statistics on QoS, such as the number of in-profile octets and out-of-profile octets. These statistics can serve as an important method to evaluate the effectiveness of the installed policies. However, tracking these statistics requires additional system resources, which limits the number of filters for classification.

qosagent police-statistics command

The `qosagent police-statistics` command for BayStack 460-24T-PWR switches gathers traffic policing, or metering, statistics. The syntax for the `qosagent police-statistics` command is:

```
qosagent police-statistics {enable|disable}
```

The `qosagent police-statistics` command is in the config command mode.

Table 238 describes the parameters and variables for the `qosagent police-statistics` command.

Table 238 `qosagent police-statistics` command parameters and variables

Parameters and variables	**Description**
`enable|disable`	Set policing statistics to: • Enable—statistics are tracked by default for all policies defined after this command is issued • Disable—disables tracking statistics for policies defined after this command is issued

Configuring QoS policies

You configure QoS policies using the CLI.

qos policy command

The `qos policy` command creates or deletes a QoS policy. The syntax for the `qos policy` command is:

```
qos policy <polid> {create [name <polname>]
if-group <ifgroup> filter-set-type {ip|l2}
{filter-set <setid>|filter-set-name <setname>}
{{in-profile-action <actid>|in-profile-action-name
<actname>}|
{{meter <metid>|meter-name <metname>}
{in-profile-action <actid>|in-profile-action-name <actname>}
{out-profile-action <actid>|out-profile-action-name
<actname>}}}
[shaper <shapeid>|shaper-name <shapename>]
[shaper-group <shapegroup>]
order <order>|delete|enable|disable}
```

The `qos policy` command is in the config command mode.

Table 239 describes the parameters and variables for the `qos policy` command.

Table 239 `qos policy` command parameters and variables

Parameters and variables	Description
`<polid>`	Enter an integer to specify the QoS policy; range is 1 to 65535.
`create`	Creates the QoS policy.
`name <polname>`	Assigns a name to the QoS policy with the designated policy ID. Enter the name for the policy; maximum is 16 alphanumeric characters.
`if-group <ifgroup>`	Enter the interface group name to which this policy applies.
`filter-set-type {ip|l2}`	Enter the type of filter set associated with this policy: • ip—specifies IP filter set • l2—specifies Layer 2 filter set
`filter-set <setid>`	Enter the filter set ID associated with this policy; range is 1 to 65535.

Table 239 `qos policy` command parameters and variables (Continued)

Parameters and variables	Description
`filter-set-name <setname>`	Enter the name of the filter set associated with this policy.
`in-profile-action <actid>`	Enter the action ID for in-profile traffic; range is 1 to 65535.
`in-profile-action-name <actname>`	Enter the action name for in-profile traffic; maximum is 16 alphanumeric characters.
`meter <metid>`	Enter meter ID associated with this policy; range is 1 to 65535.
`meter-name <metname>`	Enter the meter name associated with this policy; maximum of 16 alphanumeric characters.
`in-profile-action <actid>`	Enter the action ID for in-profile traffic; range is 1 to 65535.
`in-profile-action-name <actname>`	Enter the action name for in-profile traffic; maximum is 16 alphanumeric characters.
`out-profile-action <actid>`	Enter the action ID for out-of-profile traffic; range is 1 to 65535.
`out-profile-action -name <actname>`	Enter the action name for in-profile traffic; maximum is 16 alphanumeric characters.
`shaper <shapeid>`	Enter shaper ID associated with this policy; range is 1 to 65535.
`shaper-name <shapername>`	Enter the shaper name associated with this policy; maximum of 16 alphanumeric characters.
`shaper-group <shapegroup>`	Enter shaper group ID associated with this policy; range is 2 to 63.
`order <order>`	Specifies the evaluation order of this policy in relation to other policies associated with the same interface group. Enter order number; range is 1 to 65535. Note: Policies with a lower order value are evaluated before policies with a higher order number. Evaluation goes from lowest value to highest.
`delete`	Deletes the specified QoS policy.
`enable|disable`	Enables or disables the specified QoS policy.

➡ You must define all components associated with a policy, including the interface group, filter set, meter, and shaper before referencing those components with a policy.

Reordering packets

Support for certain per-hop behaviors (PHBs) requires packets within a flow be reordered upon transmission. Using the CLI, you can assign packets to specified egress queues.

qosagent packet-reordering command

The `qosagent packet-reordering` command allows you to reorder packets for transmission. The syntax for the `qosagent packet-reordering` command is:

```
qosagent packet-reordering {enable|disable}
```

The `qosagent packet-reordering` command is in the config command mode.

Table 240 describes the parameters and variables for the `qosagent packet-reordering` command.

Table 240 `qosagent packet-reordering` command parameters and variables

Parameters and variables	**Description**
`enable|disable`	Set packet-reordering to: • Enable—allows full flexibility in terms of the egress queue to which a packet is assigned. • Disable—the system verifies that in-profile and out-of-profile actions associated with a flow will not cause packets from the same flow to be assigned to different egress queues.

Interface Class Restrictions

qosagent class restrictions command

The `qosagent class restrictions` command allows you to set restrictions for each type of qosagent. The syntax for the `qosagent class restrictions` command is:

```
qosagent class-restrictions {all
classes|trusted-and-untrusted| unrestricted only}
```

User-based policies

This feature allows user-specific QoS policy information to be manipulated based on the presence, or lack thereof, of a specific network user. User information is retrieved from the RADIUS Server during EAP authentication and passed to the QoS Agent. The QoS Agent, in turn, notifies OPS of the user's presence if the policy server is currently in-charge of policy configuration. OPS may then download policy components to the device that is associated with the user. The User Based Policies (UBP) components will automatically be deleted when the user logs off or is no longer authenticated.

This feature adds an ON/OFF attribute to the console interface to enable/disable UBP support. For SNMP support, an Enterprise-specific MIB is added. CLI support is similar to other EAP configuration. This attribute is presently not supported from the Web interface.

In a mixed stack including the 450, this attribute defaults to disabled and cannot be changed (i.e, this feature is disabled).

eapol user-based-policies enable command

The `eapol user-based-policies enable` command enables user-based-policies. RADIUS must be configured prior to enabling user-based-policies. The syntax for user-based-policies is:

```
eapol user-based-policies enable
```

no eapol user-based-policies enable command

The `no eapol user-based-policies enable` command disables user-based-policies. The syntax for no eapol user-based-policies enable is:

```
no eapol user-based-policies enable
```

default eapol user-based-policies enable command

The `default eapol user-based-policies enable` command sets user-based-policies to the default setting. The default setting for user-based-policies is disabled. The syntax for the default `eapol user-based-policies enable` command is:

```
default eapol user-based-policies enable
```

show eapol command

The `show eapol` command shows whether user-based-policies are enabled or disabled. The syntax for `show eapol` is:

```
show eapol
```

The `show eapol` command is in the privExec mode.

The `show eapol` command has no variables or parameters.

Figure 113 displays sample output from the `show eapol` command.

Figure 113 `show eapol` command output

```
BS460_24T_PWR#show eapol
EAPOL Administrative State:  Disabled
EAPOL User-Based Policies :  Disabled
     Admin         Admin Oper ReAuth ReAuth Quiet  Xmit   Supplic Server  Max
Port Status   Auth Dir   Dir  Enable Period Period Period Timeout Timeout Req
---- -------- ---- ----- ---- ------ ------ ------ ------ ------- ------- ---
1    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
2    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
3    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
4    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
5    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
6    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
7    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
8    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
9    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
10   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
11   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
12   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
13   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
14   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
15   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
16   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
17   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
----More ----
```

Chapter 10
IGMP and IGAP

This chapter describes how to configure IGMP and IGAP snooping parameters. This chapter covers the following topics:

- "Using IGMP snooping ", next
- "Using IGAP snooping" on page 377

Refer to the *Application Guide for BoSS Release 3.5 for BayStack 460 and 470 Switches* for more information IGMP snooping as well as configuration directions using the console interface (CI) menus. Refer to Using Web-based Management for BoSS Release 3.5 for BayStack 460 and 470 Switches for information on configuring these features using the Web-based management system, and refer to Reference for Switch Management Software for BoSS Release 3.5 for BayStack 460 and 470 Switches for configuration information for the DM.

Note: The standalone or stack of switches must be operating in Pure Stack mode. Refer to "Configuring the stack operational mode" on page 72.

Using IGMP snooping

You can configure and display IGMP snooping parameters using the CLI. This section covers:

- "show vlan igmp command ", next
- "vlan igmp command" on page 375
- "vlan igmp unknown-mcast-no-flood" on page 376
- "default vlan igmp command" on page 376

show vlan igmp command

The `show vlan igmp` command displays the IGMP snooping configuration. The syntax for the `show vlan igmp` command is:

```
show vlan igmp {<1-4094> |unknown-mcast-no-flood}
```

The `show vlan igmp` command is in the privExec mode.

Table 241 describes the parameters and variables for the `show vlan igmp` command.

Table 241 `show igmp` command parameters and variables

Parameters and variables	**Description**
<1-4094>	Specifies the VLAN to display IGMP snooping configuration.
`unknown-mcast-no-flood`	Displays the setting for flooding packets with unknown multicast addresses.

Figure 114 displays sample output from the `show vlan igmp` command.

Figure 114 `show vlan igmp` command output

```
BS470_24#show vlan igmp 1
Snooping:  Enabled
Proxy:  Enabled
Robust Value:  2
Query Time:  125 seconds
IGMPv1 Static Router Ports:
IGMPv2 Static Router Ports:
```

vlan igmp command

The `vlan igmp` command configures IGMP snooping parameters. The syntax for the `vlan igmp` command is:

```
vlan igmp {<1-4094> [snooping {enable|disable}]
[proxy {enable|disable}] [robust-value <value>]
[query-interval <time>] [v1-members <portlist>] [v2-members
<portlist>] | unknown-mcast-no-flood {disable |enable }}
```

The `vlan igmp` command is in the config mode.

Table 242 describes the parameters and variables for the `vlan igmp` command.

Table 242 `vlan igmp` command parameters and variables

Parameters and variables	Description
`<1-4094>`	Enter the VLAN to configure for IGMP.
`snooping {enable|disable}`	Enables or disables the VLAN for IGMP snooping.
`proxy {enable|disable}`	Enables or disables the VLAN for IGMP proxy.
`robust-value <value>`	Enter the robust value you want for IGMP.
`query-interval <time>`	Enter the number of seconds you want for the query interval of IGMP.
`v1-members <portlist>`	Enter the list of ports for port membership for IGMP v1.

Table 242 `vlan igmp` command parameters and variables (Continued)

Parameters and variables	Description
`v2-members <portlist>`	Enter the list of ports for port membership for IGMP v2.
`unknown-mcast-no-flood`	Enables or disables the flooding packets with unknown multicast addresses.

vlan igmp unknown-mcast-no-flood

The `vlan igmp unknown-mcast-no-flood` command allows the user to block flooding of packets with unknown multicast address. Instead, the unknown multicast traffic will be sent only to IGMP static router ports. The syntax for the `vlan igmp unknown-mcast-no-flood` command is:

```
vlan igmp unknown-mcast-no-flood
```

The `vlan igmp unknown-mcast-no-flood` command is in the config command mode.

Table 243 describes the parameters and variables for the `vlan igmp unknown-mcast-no-flood` command.

Table 243 `vlan igmp unknown-mcast-no-flood` command parameters and variables

Parameters and variables	Description
`enable`	Enables flooding of packets with unknown multicast addresses. **Note:** The default parameter is enabled.
`disable`	Disables flooding of packets with unknown multicast addresses.

default vlan igmp command

The `default vlan igmp` command sets all IGMP snooping parameters to the factory default settings. The syntax for the `default vlan igmp` command is:

```
default vlan igmp <1-4094> | unknown-mcast-no-flood
```

The `default vlan igmp` command is in the config mode.

Table 244 describes the parameters and variables for the `default vlan igmp` command.

Table 244 `default vlan igmp` **command parameters and variables**

Parameters and variables	Description
<1-4094>	Enter the VLAN to default IGMP settings to factory default.
`unknown-mcast-no-flood`	Sets the flooding packets with unknown multicast addresses to factory default - disabled.

Using IGAP snooping

IGAP is an authentication and accounting protocol for clients receiving multicast streams. IGAP extends the functionality of the Internet Group Management Protocol (IGMPv2) by giving providers more control over their networks. With IGAP, service providers and enterprises can authenticate users before granting access to their networks and track how long users receive multicast traffic.

You can configure and display IGAP snooping parameters using the CLI. This section covers:

- "Config ip igmp interface ", next
- "Config vlan command" on page 378
- "Clearing IGAP counters" on page 379
- "Setting vendor-specific attributes" on page 380
- "Config radius igap-timeout-log-fsize command" on page 381
- "Config radius server create command" on page 382
- "Config radius server delete command" on page 383
- "Config radius server set command" on page 383
- "Show ip igmp igap command" on page 384
- "Show ip igmp igap-group command" on page 385
- "Troubleshooting IGAP network connectivity" on page 387

Config ip igmp interface

The `config ip igmp interface` command configures IGAP on a specific interface. The syntax for the `config ip igmp interface` command is:

```
config ip igmp interface <ipaddr> igap
```

where:
ipaddr indicates the IP address of the selected interface.

Table 245 describes the parameters and variables for the `config ip igmp interface` command.

Table 245 `config ip igmp interface` command parameters and variables

Parameters and variables	Description
`info`	Displays information about the IGAP interface.
enable	Enables IGAP on this interface.
disable	Disables IGAP on this interface.
authentication <enable|disable>	Enables or disables authentication on the specified interface. The default is enable.
accounting <enable|disable>	Enables or disables accounting on the specified interface. The default is enable.
clear-counters	Clears the IGAP counters for this interface.

Config vlan command

`The config vlan` command configures IGAP on a VLAN. The syntax for `config vlan` command is:

```
config vlan <vid> ip igmp igap
```

where:
vid is a VLAN ID from 1 to 4092.

Table 246 describes the parameters and variables for the `config vlan` command.

Table 246 `config ip igmp interface` command parameters and variables

Parameters and variables	Description
`info`	Displays IGAP settings on the VLAN.
enable	Enables IGAP on this VLAN.
disable	Disables IGAP on this VLAN.
authentication <enable|disable>	Enables or disables authentication on this VLAN.
accounting <enable|disable>	Enables or disables accounting on this VLAN.
clear-counters	Clears the IGAP counters for this VLAN.

Clearing IGAP counters

IGAP counters provide information that is used to monitor and troubleshoot IGAP interfaces. See "Troubleshooting IGAP network connectivity" on page 387. To help you isolate a problem, you may want to clear one or all of the counters to observe traffic behavior.

There are three commands that you use to clear counters

- To clear all counters, use the following command:

```
config ip igmp igap clear-counters
```

- To clear counters on a specific interface, use the following command:

```
config ip igmp interface <ipaddr> igap clear-counters
```

- To clear counters on a specific VLAN, use the following command:

```
config vlan <vid> ip igmp igap clear-counters
```

Configuring IGAP with RADIUS

IGAP uses RADIUS servers to authenticate users and account for how long they use the multicast services. This section describes the IGAP-specific RADIUS commands. For information about the complete set of RADIUS parameters, refer to the publication, *Configuring and Managing Security.*

Setting vendor-specific attributes

The following two sections describe the RADIUS commands that set vendor-specific attributes (VSAs) for IGAP.

Config radius mcast-addr-attr-value command

The `config radius mcast-addr-attr-value` command allows you to set the vendor-specific attribute for the multicast address on an IGAP-enabled RADIUS server.

The syntax for the `config radius mcast-addr-attr-value` command is:

```
config radius mcast-addr-attr-value <value>
```

Table 247 describes the parameters and variables for the `config radius mcast-addr-attr-value` command.

Table 247 `config radius mcast-addr-attr-value` command parameters

Parameters and variables	Description
<value>	This indicates an integer assigned to this vendor-specific attribute, which must be in the range from 0 to 255. The default is 90.

Config radius auth-info-attr-value command

The `config radius auth-info-attr-value` command allows you to set the vendor-specific attribute for the authentication information on an IGAP-enabled RADIUS server.

The syntax for the `config radius auth-info-attr-value` command is:

```
config radius auth-info-attr-value <value>
```

Table 248 describes the parameters and variables for the `config radius auth-info-attr-value` command.

Table 248 `config radius auth-info-attr-value` command parameters

Parameters and variables	Description
<value>	This indicates an integer assigned to this vendor-specific attribute, which must be in the range from 0 to 255. The default is 91.

Config radius igap-timeout-log-fsize command

The Passport 8600 captures authentication and accounting information in an IGAP timeout log for each session. The timeout log records information such as when the Passport 8600 sent an accounting start request to the RADIUS server, what the server's response was and when accounting started.

The `config radius igap-timeout-log-fsize` command allows you to set the maximum size of the RADIUS timeout log file. The syntax for the `config radius igap-timeout-log-fsize` command is:

```
config radius igap-timeout-log-fsize <value>
```

Table 249 describes the parameters and variables for the `config radius igap-timeout-log-fsize` command.

Table 249 `config radius igap-timeout-log-fsize` command

Parameters and variables	Description
<value>	This indicates an integer (in KB), which must be in the range from 50 to 8192. The default is 512.

Config radius server create command

The `config radius server create` command allows you to add an IGAP-enabled RADIUS server. The syntax for `config radius server create` command is:

```
config radius server create <ipaddr> secret <value> usedby
igap
```

The RADIUS server uses the password to validate the IGAP client.

Table 250 describes the parameters and variables for the `config radius server create` command.

Table 250 `config radius server create` **command parameters**

Parameters and variables	**Description**
<ipaddr>	Indicates the IP address of the selected interface.
<value>	specifies the secret key, which is a string of up to 20 characters.

Note: The `usedby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`igap` - configures the server for IGAP authentication.
`snmp` - configures the server for SNMP authentication.

The other parameters that you can use with this command are:

```
[port <value>] [priority <value>] [retry <value>]
[timeout <value>] [enable <value>] [acct-port <value>]
[acct-enable <value>]
```

Config radius server delete command

The `config radius server delete` command allows you to delete an IGAP-enabled RADIUS server. The syntax for the `config radius server delete` command is:

```
config radius server delete <ipaddr> usedby igap
```

Table 251 describes the parameters and variables for the `config radius server delete` command.

Table 251 `config radius server delete` command parameters

Parameters and variables	Description
<ipaddr>	Indicates the IP address of the selected interface.

Note: The `usedby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`igap` - configures the server for IGAP authentication.
`snmp` - configures the server for SNMP authentication.

Config radius server set command

The `config radius server set` command allows you to set IGAP-enabled RADIUS server parameters. The syntax for `config radius server set` command is:

```
config radius server set <ipaddr> usedby igap
```

Table 252 describes the parameters and variables for the `config radius server set` command.

Table 252 `config radius server set` **command parameters**

Parameters and variables	Description
<ipaddr>	Indicates the IP address of the selected interface.

Note: The `usedby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`igap` - configures the server for IGAP authentication.
`snmp` - configures the server for SNMP authentication.

The other parameters that you can set with this command are:

```
[secret <value>] [port <value>] [priority <value>]
[retry <value>] [timeout <value>] [enable <value>]
[acct-port <value>] [acct-enable <value>]
```

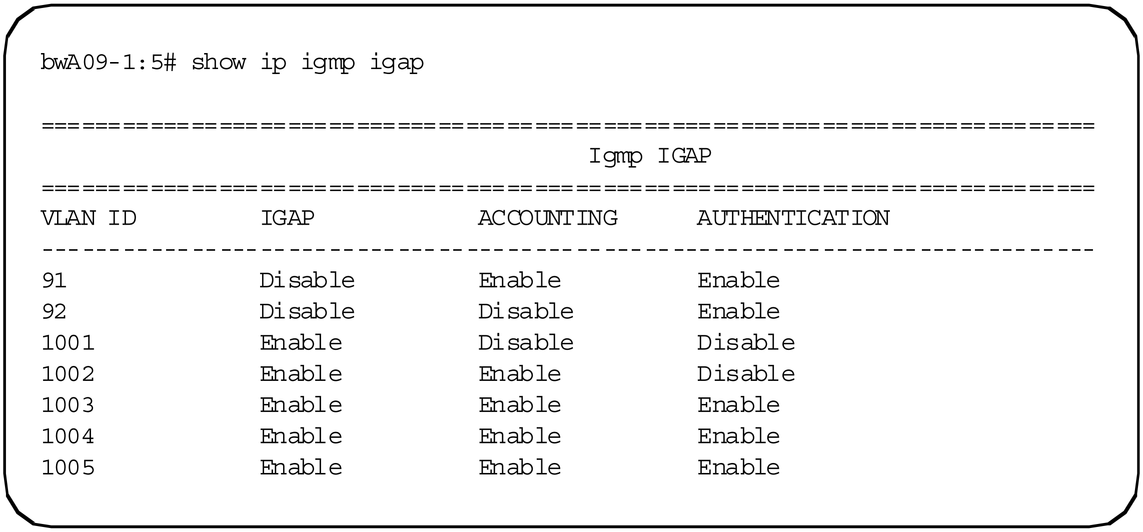
Show ip igmp igap command

The `show ip igmp igap` command displays the information on IGAP-enabled interfaces. The syntax for `show ip igmp igap` command is:

```
show ip igmp igap
```

Figure 115 displays sample output from the `show ip igmp igap` command.

Figure 115 `show ip igmp igap` command output



```
bwA09-1:5# show ip igmp igap

==============================================================================
                                         Igmp IGAP
==============================================================================
VLAN ID         IGAP            ACCOUNTING      AUTHENTICATION
------------------------------------------------------------------------------
91              Disable         Enable          Enable
92              Disable         Disable         Enable
1001            Enable          Disable         Disable
1002            Enable          Enable          Disable
1003            Enable          Enable          Enable
1004            Enable          Enable          Enable
1005            Enable          Enable          Enable
```

Show ip igmp igap-group command

The `show ip igmp igap-group` command displays information on IGAP groups. The syntax for the `show ip igmp igap-group` command is:

```
show ip igmp igap-group [count] [memb-subnet <value>] [grp <value>]
```

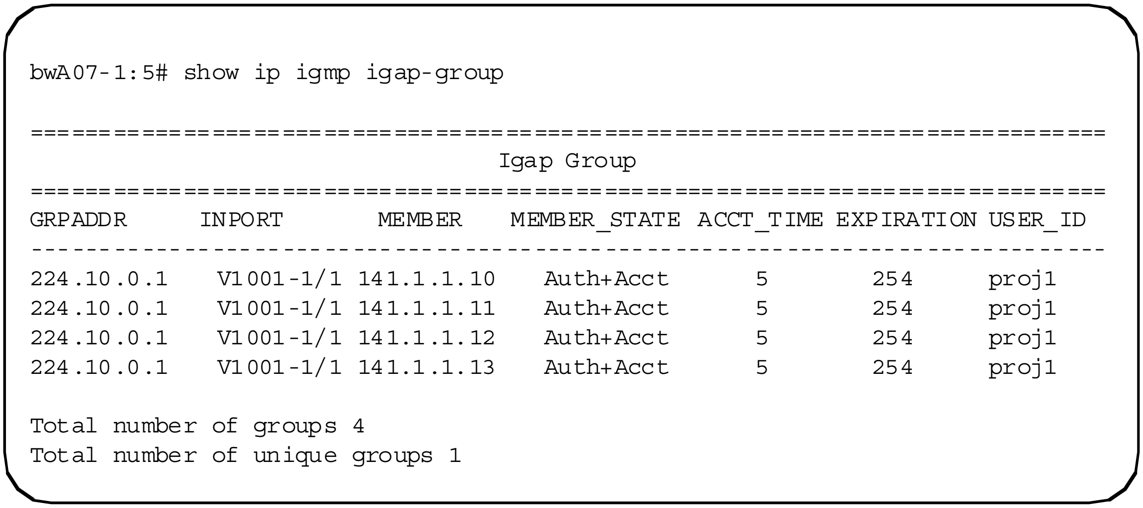
Table 253 describes the parameters and variables for the `show ip igmp igap-group` command.

Table 253 `show ip igmp igap-group` command parameters and variables

Parameters and variables	Description
`[count]`	Indicates the number of entries.
`[memb-subnet <value>]`	specific IP address and network mask.
`[grp <value>]`	IP address of a specific group.

Figure 116 displays sample output from the `show ip igmp igap-group` command.

Figure 116 `show ip igmp igap-group` command output



```
bwA07-1:5# show ip igmp igap-group

=============================================================================
                                  Igap Group
=============================================================================
GRPADDR     INPORT       MEMBER   MEMBER_STATE ACCT_TIME EXPIRATION USER_ID
-----------------------------------------------------------------------------
224.10.0.1   V1001-1/1 141.1.1.10   Auth+Acct      5        254      proj1
224.10.0.1   V1001-1/1 141.1.1.11   Auth+Acct      5        254      proj1
224.10.0.1   V1001-1/1 141.1.1.12   Auth+Acct      5        254      proj1
224.10.0.1   V1001-1/1 141.1.1.13   Auth+Acct      5        254      proj1

Total number of groups 4
Total number of unique groups 1
```

Table 254 describes the parameters and variables for the `show ip igmp igap-group` command.

Table 254 IGAP group parameters

Parameters and variables	**Description**
GRPADDR	Indicates the IP address of this IGAP group.
INPORT	Displays the ingress port and VLAN of the IGAP report.
MEMBER	Indicates the IP address of this IGAP group member.
MEMBER_STATE	Displays the state of this IGAP group member. • **Auth** indicates that the member was authenticated by a RADIUS server. • **Acct** indicates that a RADIUS server successfully started accounting for this member's session.
ACCT_TIME	Displays the accounting time (in seconds) for the duration of the multicast session for this IGAP group member.
EXPIRATION	Specifies how much time is left (in seconds) before the Group Report for this interface expires. This timer is restarted when the RADIUS server receives a new group report.
USER_ID	Displays the User ID for this IGAP member.

Troubleshooting IGAP network connectivity

IGAP counters provide network connectivity information that you can use to monitor and troubleshoot IGAP interfaces. To display the counter information, use the following command:

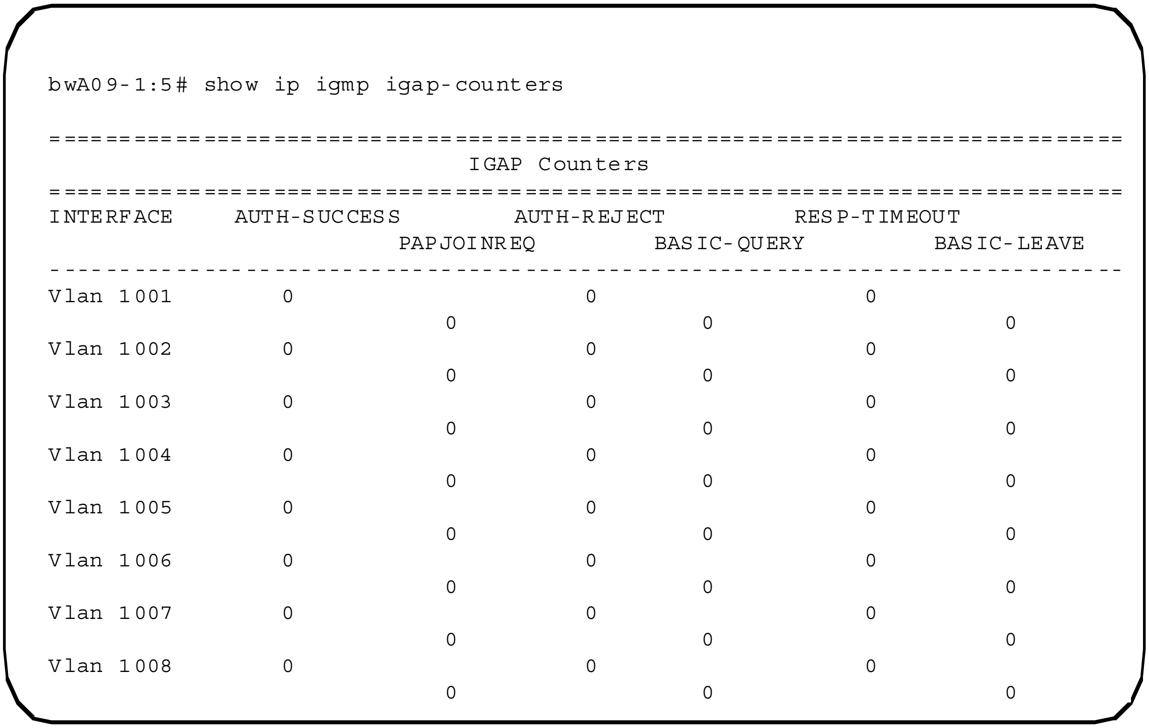
```
show ip igmp igap-counters [vlan <value>]
```

where:

`vlan <value>` indicates the ID number of the VLAN you want to show.

Figure 117 displays sample output from the `show ip igmp igap-counters` command.

Figure 117 `show IGAP counters` command output



```
bwA09-1:5# show ip igmp igap-counters

==============================================================================
                               IGAP Counters
==============================================================================
INTERFACE     AUTH-SUCCESS        AUTH-REJECT         RESP-TIMEOUT
                          PAPJOINREQ        BASIC-QUERY         BASIC-LEAVE
------------------------------------------------------------------------------
Vlan 1001        0                     0                    0
                             0                  0                     0
Vlan 1002        0                     0                    0
                             0                  0                     0
Vlan 1003        0                     0                    0
                             0                  0                     0
Vlan 1004        0                     0                    0
                             0                  0                     0
Vlan 1005        0                     0                    0
                             0                  0                     0
Vlan 1006        0                     0                    0
                             0                  0                     0
Vlan 1007        0                     0                    0
                             0                  0                     0
Vlan 1008        0                     0                    0
                             0                  0                     0
```

Table 255 describes the parameters and variables for the `show ip igmp igap-counters` command.

Table 255 IGAP counter parameters

Parameters and variables	**Description**
INTERFACE	Indicates the VLAN ID of this IGAP interface.
AUTH-SUCCESS	Displays the number of authentication success messages received from the RADIUS server on this interface.
AUTH-REJECT	Displays the number of authentication fail messages received from the RADIUS server on this interface.
RESP-TIMEOUT	Displays the number of times that the Authentication Timer timed out. This timer controls the waiting time from sending an Authentication request to receiving an Authentication response.
PAPJOINREQ	Displays the number of Password Authentication Protocol (PAP) Join requests received for members of this interface.
BASIC-QUERY	Displays the number of Basic Query messages sent by the Passport 8600 on an IGAP-enabled interface.
BASIC-LEAVE	Displays the number of Basic Leave messages received by this interface.

Appendix A
Command List

This appendix provides the complete CLI command list in alphabetical order, with approximate page references for the beginning pages of further explanations.

Note: This information is presented for reference only and should not be considered to be an exact representation.

Table 256 CLI command list

Command	Page No.
`auto-negotiation-advertisements [port <portlist>] [10-full] [10-half] [100-full] [100-half] [1000-full] [1000-half] [asymm-pause-frame] [pause-frame]`	page 236
`auto-pvid`	page 273
`autotopology`	page 157
`boot [default] [unit <unitno>]`	page 102
`clear logging [nv]`	page 126
`clear-stats [port<portlist>]`	page 133

`cli-password {switch|stack} {ro|rw} <WORD> <WORD>`
`cli-password {switch|stack} {serial|telnet} {none|local|radius}`
	page 162

`config radius auth-info-attr-value <value>`	page 380
`config ip igmp igap clear-counters`	page 379
`config ip igmp interface <ipaddr> igap`	page 378
`config radius igap-timeout-log-fsize <value>`	page 381
`config radius mcast-addr-attr-value <value>`	page 380
`config radius server create <ipaddr> secret <value> usedby igap`	page 382

Table 256 CLI command list (Continued)

Command	Page No.
config radius server delete <*ipaddr*> usedby igap	page 383
config radius server set <*ipaddr*> usedby igap	page 383
config switch mode <l2|traffic-separation>	page 147
configure {terminal|network|memory}	page 53
configure network [load-on-boot {disable|use-bootp|use-config}] configure network [filename <*WORD*>] configure network [address <*XXX.XXX.XXX.XXX*>]	page 82
configure network [address <A.B.C.D>] [filename <WORD>]	page 86
configure network load-on-boot {disable|use-bootp|use-config} [address <A.B.C.D>] filename <WORD>	page 89
config vlan <*vid*> ip igmp igap	page 378
cops retry	page 348
cops server	page 348
copy config nvram	page 149
copy config tftp [address <*XXX.XXX.XXX.XXX*>] filename <*WORD*>	page 106
copy running-config tftp [address <A.B.C.D>] filename <WORD>	page 86
copy tftp config [address <*XXX.XXX.XXX.XXX*>] filename <*WORD*>	page 106
copy tftp config unit <unit #>	page 150
default auto-negotiation-advertisements [port <portlist>]	page 238
default autotopology	page 158
default cops retry	page 349
default cops server	page 349
default duplex [port <*portlist*>]	page 226
default flowcontrol [port <*portlist*>]	page 229
default ip address unit <*1-8*>	page 72
default ip bootp server	page 104
default lacp aggregation [port <portlist>] enable	page 285
default lacp mode [port <portlist>]	page 284

Table 256 CLI command list (Continued)

Command	Page No.
default lacp priority [port <portlist>]	page 287
default lacp timeout-time [port <portlist>]	page 288
default lacp system-priority	page 283
default logging	page 126
default logging remote level	page 147
default mac-address-table aging-time	page 271
default name [port <*portlist*>]	page 222
default rate-limit [port <*portlist*>]	page 233
default set logging	page 125
default snmp trap link-status [port <*portlist*>]	page 113
default snmp-server authentication-trap	page 187
default snmp-server community [ro|rw]	page 190
default snmp-server contact	page 191
default snmp-server host	page 195
default snmp-server location <text>	page 196
default snmp-server name <text>	page 197
default spanning-tree [stp <*1-8*>] [forward-time] [hello-time] [max-age] [priority] [tagged-bpdu]	page 303
default spanning-tree [port <*portlist*>] [stp <*1-8*>] [learning] [cost] [priority]	page 307
default speed [port <*portlist*>]	page 224
default ssh [dsa-auth|dsa-key|max-sessions|pass-auth|port|timeout]	page 181
default telnet-access	page 173
default terminal {speed|length|width}	page 97
default vlan igmp {<*1-4094*> | unknown-mcast-no-flood}	page 376
default vlan mgmt <*1-4094*>	page 262
disable	page 54
download [address <*ip*>] {image <*image-name*> | image-if-newer <*image name*> | bs450-image <image-name> | diag <*filename*>}	page 90

Table 256 CLI command list (Continued)

Command	Page No.
duplex [port <*portlist*>] {full|half|auto}	page 225
eapol [{enable|disable}] [port <*portlist*>] [init] [status authorized|unauthorized|auto] [traffic-control in-out|in] [re-authentication enable|disable] [re-authentication-interval <*num*>] [re-authenticate] [quiet-interval <*num*>] [transmit-interval <*num*>] [supplicant-timeout <*num*>] [server-timeout <*num*>] [max-request <*num*>]	page 216
enable	page 53
end	page 55
exit	page 55
flowcontrol [port <*portlist*>] {asymmetric|symmetrid|auto|disable}	page 227
help	page 51
interface FastEthernet {<*portlist*>}	page 54
ip address[stack|switch] <*XXX.XXX.XXX.XXX*> [netmask <*XXX.XXX.XXX.XXX*>]	page 66
ip address unit <*1-8*> A.B.C.D	page 70
ip bootp server {last|needed|disable|always}	page 102
ip default-gateway <*XXX.XXX.XXX.XXX*>	page 68
ipmgr list {telnet|snmp|http}	page 166
ipmgr list {source-ip <1-10> <*XXX.XXX.XXX.XXX*> [mask <*XXX.XXX.XXX.XXX*>]}	page 167
lacp aggregation [port <portlist>] enable	page 284
lacp key [port <portlist>] <1-4095>	page 286
lacp mlt <mlt-id> [learning {disable | fast | normal}] <portlist>	page 294
lacp mode [port <portlist>] {off | passive | active}	page 283
lacp priority [port <portlist>] <0-255>	page 286
lacp system-priority [0-65535]	page 282
lacp timeout-time [port <portlist>] {short | long}	page 287
logging remote address <A.B.C.D>	page 145

Table 256 CLI command list (Continued)

Command	Page No.
logging remote level {critical|informational|serious}	page 146
logout	page 53
mac-address-table aging-time <*time*>	page 270
mac-security [disable|enable] [filtering {enable|disable}] [intrusion-detect {enable|disable|forever}] [intrusion-timer <1-65535>] [learning-ports <*portlist*>] [learning {enable|disable}] [snmp-lock {enable|disable}] [snmp-trap {enable|disable}]	page 209
mac-security [port <*portlist*>] {disable|enable|learning}	page 213
mac-security mac-address-table address <*H.H.H.*> {port <*portlist*>|security-list <*1-32*>}	page 210
mac-security security-list <*1-32*> mac-security security-list <*portlist*>	page 211
mac-security mac-da-filter	page 214
mlt <*id*> [name <*trunkname*>] [enable|disable] [member <*portlist*>] [learning {disable | fast | normal}]	page 280
name [port <*portlist*>] <*LINE*>	page 221
no auto-negotiation-advertisements [port <portlist>]	page 237
no auto-pvid	page 274
no autotopology	page 158
no cops server	page 350
no flowcontrol [port <*portlist*>]	page 228
no ip address {stack|switch}	page 67
no ip address unit <*1-8*>	page 71
no ip bootp server	page 103
no ip default-gateway	page 68
no ipmgr {telnet|snmp|http}	page 166
no ipmgr {source IP [<*1-10*>]}	page 168
no lacp aggregation [port <portlist>] enable	page 285
no lacp mlt <mlt-id>	page 294
no logging remote address	page 145

Table 256 CLI command list (Continued)

Command	Page No.
no logging remote level	page 146
no mac-security	page 211
no mac-security mac-address-table {address <*H.H.H*>| port <*portlist*>|security-list <*1-32*>]	page 212
no mac-security security-list <*1-32*>	page 212
no mlt [<*id*>]	page 281
no name [port <*portlist*>]	page 222
no port-mirroring	page 157
no radius-server	page 206
no rate-limit [port <*portlist*>]	page 232
no remote logging enable	page 144
no rmon alarm [*1...65535*]	page 118
no rmon event [*1...65535*]	page 119
no rmon history [*1...65535*]	page 120
no rmon stats [*1...65535*]	page 122
no set logging	page 125
no shutdown [port <*portlist*>]	page 220
no snmp server [authentication-trap|community [ro|rw] contact|host [<*host-ip*> <community-string>] [location|name]	page 111
no snmp trap link-status [port <*portlist*>]	page 112
no sntp enable	page 139
no sntp server <primary|secondary>	page 140
no ssh [dsa-auth|dsa-key|pass-auth]	page 179
no spanning-tree [port <*portlist*>] [stp <*1-8*>]	page 308
no telnet-access [source-ip [<*1-10*>]]	page 172
no tftp-server	page 106
no vlan <*1-4094*> no vlan mac-address <*1-4094*> address <*H.H.H.*>	page 261 page 267
no web-server	page 183
ping <*XXX.XXX.XXX.XXX*>	page 77

Table 256 CLI command list (Continued)

Command	Page No.
poe poe-dc-source-conf [unit <*1-8*>] {powersharing|rpsu|ups}	page 247
poe poe-dc-source-type [unit <*1-8*>] {baystack10|nes}>	page 246
poe poe-pd-detect-type [unit <*1-8*>] {802dot3af|802dot3af_and_legacy}	page 248
poe poe-limit [unit <*1-8*>] <*3-20*>	page 255
poe poe-power-pairs [unit <*1-8*>] {spare|signal}	page 249
poe poe-power-usage-threshold [unit <*1-8*>] <*1-99*>	page 251
poe poe-priority [port <*portlist*>] {low|high|critical}	page 254
poe poe-shutdown [port <*portlist*>]	page 253
poe poe-trap [unit <*1-8*>]	page 251
port-mirroring mode disable port-mirroring mode Xrx monitor-port <*portlist*> mirror-port X <*portlist*> port-mirroring mode XrxOrXtx monitor-port <*portlist*> mirror-port X <*portlist*> mirror-port-Y <*portlist*> port-mirroring mode XrxOrYtx monitor-port <*portlist*> mirror-port X <*portlist*> mirror-port-Y <*portlist*> port-mirroring mode XrxYtx monitor-port <*portlist*> mirror-port X <*portlist*> mirror-port-Y <*portlist*> port-mirroring mode XrxYtxOrYrxXtx monitor-port <*portlist*> mirror-port X <*portlist*> mirror-port-Y <*portlist*> port-mirroring mode Asrc monitor-port <*portlist*> mirror-MAC-A <*macaddr*> port-mirroring mode Adst monitor-port <*portlist*> mirror-MAC-A <*macaddr*> port-mirroring mode AsrcOrAdst monitor-port <*portlist*> mirror-MAC-A <*macaddr*> port-mirroring mode AsrcBdst monitor-port <*portlist*> mirror-MAC-A <*macaddr*> mirror-MAC-B <*macaddr*> port-mirroring mode AsrcBdstOrBsrcAdst monitor-port <*portlist*> mirror-MAC-A <*macaddr*> mirror-MAC-B <*macaddr*>	page 155

Table 256 CLI command list (Continued)

Command	Page No.

qos action <*actid*> name <*actname*>
qos action <*actid*> drop-action {enable|disable}
qos action <*actid*> update-dscsp <*dscp*>
qos action <*actid*> update-1p {<*ieee1p*>|default|use-egress-map}
qos action <*actid*> set-drop-prec {loss-sensitive|not-loss-sensitive|default|use-egress-map}
	page 362

qos egressmap	page 354
qos if-assign	page 351
qos if-assign-list	page 352
qos if-assign-list name <*tag*> {add|del} [portlist <*portlist*>]	page 352
qos if-assign name <*tag*> {add|del} [port <*portlist*>]	page 351
qos if-group	page 351
qos if-group name <*tag*> {create <*ifclass*>|delete}	page 351
qos ingressmap	page 354
qos ingressmap 1p <*ieee1p*> ds <*dscp*>	page 354

qos ip-filter <*fid*> {create src-ip <*src-ip-info*>}
qos ip-filter <*fid*> {create dst-ip <*dst-ip-info*>}
qos ip-filter <*fid*> {create ds-field <*dscp*>}
qos ip-filter <*fid*> {create protocol <*protocoltype*>}
qos ip-filter <*fid*> {create src-port <*port*>}
qos ip-filter <*fid*> {create dst-port <*port*>}
qos ip-filter <*fid*> {delete}
	page 356

qos ip-filter-set <*fgid*> {create set <*setid*> [name <*setname*>] filter-id <*fid*> filter-prec <*prec*>}
qos ip-filter-set <*fgid*> {delete}
	page 357

Table 256 CLI command list (Continued)

Command	Page No.

qos l2-filter <*fid*> {create ethertype <*etype*>}
qos l2-filter <*fid*> {create vlan <*vidlist*>}
qos l2-filter <*fid*> {create vlantag <*vtag*>}
qos l2-filter <*fid*> {create priority<ieee1p-seq>}
qos l2-filter <*fid*> {create dsfield <*dscp*>}
qos l2-filter <*fid*> {create protocol <*protocoltype*>}
qos l2-filter <*fid*> {create src-port <*min*> src-port <*max*>}
qos l2-filter <*fid*> {create dst-port <*min*> dst-port <*max*>}
qos l2-filter <*fid*> {delete}
	page 358

qos l2-filter-set <*fgid*> {create set <*setid*> [name <*setname*>] filter-id <*fid*> filter-prec <*prec*>}
qos l2-filter-set <*fgid*> {delete}
	page 360

qos meter <*metid*> {create [name <*metname*>] committed-rate <*rate*> max-burst-rate <*burstrate*> [max-burst-duration <*burstdur*>] |delete}	page 363
qos policy	page 367
qos queue-set	page 355
qos shaper	page 365
qosagent class-restrictions	page 370
qosagent packet-reordering	page 369
qosagent police-statistics {enable|disable}	page 366
qosagent reset-default	page 342
qosagent server-control	page 343
radius-server host <*address*> [secondary-host <*address*>] port <*num*> key <*string*>	page 205
rate-limit [port <*portlist*>] {multicast <*pct*>| broadcast <*pct*>|both <*pct*>}	page 231
remote logging enable	page 144
renumber unit	page 75
rmon alarm <*1-65535*> <*WORD*> <*1-2147483647*> [absolute|delta] rising-threshold <*-2147483647-2147483648*> [<*1-65535*>] falling-threshold <*-2147483647-2147483648*> [<*1-65535*>] [owner <*LINE*>]	page 117

Table 256 CLI command list (Continued)

Command	Page No.
`rmon event <1-65535> [log] [trap] [description <LINE>] [owner <LINE>]`	page 119
`rmon history <1-65535> <LINE> <1-65535> <1-3600> [owner <LINE>]`	page 120
`rmon stats <1-65535> <LINE> [owner <LINE>]`	page 121

`set logging [enable|disable]`
`[level critical|serious|informational]`
`[nv-level critical|serious|informational|none]`
	page 124

`show arp-table command`	page 127
`show auto-negotiation-advertisements [port <portlist>]`	page 234
`show auto-negotiation-capabilities [port <portlist>]`	page 235
`show autotopology settings`	page 158
`show autotopology nmm-table`	page 159
`show config-network`	page 83
`show cops`	page 345
`show cops retry`	page 344
`show cops server`	page 344
`show cops stats`	page 345
`show eapol`	page 215
`show interfaces [names] [<portlist>]`	page 128
`show ip [bootp] [default-gateway] [address [stack|switch]]`	page 69
`show ipmgr`	page 164
`show ip igmp igap`	page 384
`show ip igmp igap-counters [vlan <value>]`	page 387
`show ip igmp igap-group [count] [memb-subnet <value>] [grp <value>]`	page 385
`show lacp debug member [portlist]`	page 291
`show lacp mlt`	page 289
`show lacp mlt <mlt-id>`	page 289
`show lacp port [<portlist>]`	page 290

Table 256 CLI command list (Continued)

Command	Page No.
`show lacp stats [port <portlist>]`	page 293
`show lacp system`	page 288

`show logging [critical]`
`show logging [serious]`
`show logging [informational]`
	page 122 and page 142

`show mac-address-table [aging-time]`
`show mac-address-table [vid <1-4094>] [address <H.H.H.>]`
	page 269

`show mac-security {config|mac-address-table [addr <macaddr>]|port|security-lists}`	page 207
`show mac-security mac-da-filter`	page 208
`show mlt [utilization <1-6>]`	page 280
`show poe-main-status [unit <1-8>]`	page 238
`show poe-port-status [ports <portlist>]`	page 240
`show poe-power-measurement [ports <portlist>]`	page 241
`show port-mirroring`	page 154
`show port-statistics [port <portlist>]`	page 131

Table 256 CLI command list (Continued)

Command	Page No.
show qos if-assign-list show qos interface-assignments show qos interface-groups show qos egressmap show qos ingressmap show qos ip-filters show qos ip-filter-sets show qos l2-filters show qos l2-filter-sets show qos actions show qos meters show qos shapers show qos policies show qos queue-sets show qos queue-set-assignments show qos agent show qos statistics	page 332
show radius-server	page 205
show rate-limit	page 230
show rmon alarm	page 114
show rmon event	page 114
show rmon history	page 115
show rmon stats	page 116
show running-configuration	page 85
show sntp	page 137
show spanning-tree {stp <*1-8*>] {config|port}	page 297
show spanning-tree rstp info	page 310
show spanning-tree rstp statistics	page 311
show spanning-tree rstp status	page 311
show spanning-tree rstp port info	page 312
show spanning-tree rstp port statistics	page 313

Table 256 CLI command list (Continued)

Command	Page No.
show spanning-tree rstp port status	page 314
show spanning-tree mstp info	page 317
show spanning-tree mstp region	page 318
show spanning-tree mstp statist	page 318
show spanning-tree mstp statu	page 318
show spanning-tree mstp port info [<portlist>]	page 319
show spanning-tree mstp port statistics [<portlist>]	page 320
show spanning-tree mstp msti info <1 -	page 321
show spanning-tree mstp msti statistics <1 - 7>	page 322
show spanning-tree mstp msti port info <1 - 7> [<portlist>]	page 323
show spanning-tree mstp msti port statistics <1 - 7> [<portlist>]	page 324
show ssh global	page 174
show ssh session	page 175
show ssh download-auth-key	page 176
show-stack-info	page 74
show stack-oper-mode	page 73
show sys-info	page 59 and page 137
show telnet-access	page 171
show terminal	page 96
show tftp-server	page 105
show vlan igmp *<1-4094>* | unknown-mcast-no-flood	page 374
show vlan interface info [*<portlist>*]	page 264
show vlan interface vids [*<portlist>*]	page 265
show vlan mac-address *<1-4094>* [*<H.H.H.>*]	page 277
show vlan multicast membership *<1-4094>*	page 277
shutdown [port *<portlist>*]	page 220
snmp trap link-status [port *<portlist>*]	page 111

Table 256 CLI command list (Continued)

Command	Page No.
snmp-server {{enable|disable}|authentication-trap|community <community-string> [ro|rw] contact <*text*>|host <*host-ip*> <*community-string*>| location <*text*> | name <*text*>}	page 110
sntp enable	page 138
sntp server primary address <A.B.C.D>	page 139
sntp server secondary address <A.B.C.D>	page 140
spanning-tree [stp <*1-8*>] [forward-time <*4-30*>] [hello-time <*1-10*>] [max-age <*6-40*>] [priority <*0000|1000|2000|...|F000*>] [tagged-bpdu {enable|disable}] [tagged-bpdu-vid <*1-4094*>] [multicast-address <*H.H.H.*>]	page 302
sntp sync-interval <0-168>	page 141
sntp sync-now	page 141
spanning- tree mstp [max-hop <600 - 4000>] [max-instance <1 - 65>] [forward-time <4 - 30>] [hello-time <1 - 10>] * not available in software [max-age <6 - 40>] [pathcost-type { bits16 | bits32 }] [priority { 0000 | 10000 | 20000 | … | F0000 }] [tx-holdcount <1 - 10>] [version { stp-compatible | rstp| mstp }]	page 325
spanning- tree mstp [port <portlist>] [cost <1 - 200000000>] [edge-port { false | true }] [hello-time <1 - 10>] [learning { disable | enable }] [p2p { auto | force-false | force-true }] [priority { 00 | 10 | … | F0 }] [protocol-migration { false | true }]	page 326

Table 256 CLI command list (Continued)

Command	Page No.
spanning- tree mstp region [config-id-sel <0 - 255>] [region-name <1 - 32 chars>] [region-version <0 - 65535>]	page 327
spanning- tree mstp msti<1 - 7>[forward-time <4 - 30>] * not available in software [hello-time <1 - 10>] * not available in software [max-hop <600 - 4000>] * not available in software [priority { 0000 | 1000 | … | F000 }] [add-vlan <vid>] [remove-vlan <vid>]	page 328
spanning- tree mstp msti <1 - 7> [port <portlist>] [cost <1 - 200000000>] [learning { disable | enable }] [priority { 00 | 10 | … | F0 }]	page 329
spanning-tree [port <portlist>] [stp <*1-8*>] [learning {disable|normal|fast}] [cost <*1-65535*>] [priority <*00|10|20|...|F0*>]	page 306
spanning-tree [stp <*1-8*>] [forward-time <*4-30*>] [hello-time <*1-10*>] [max-age <*6-40*>] [priority <*0-65535*>] [tagged-bpdu {enable|disable}] [tagged-bpdu-vid <*1-4094*>]	page 302
spanning-tree [port <*portlist*>] [stp <*1-8*>] [learning {disable|normal|fast}] [cost <*1-65535*>] [priority <*0-255*>]	page 307
spanning- tree rstp [forward-time <4 - 30>] [hello-time <1 - 10>] [max-age <6 - 40>] [pathcost-type { bits16 | bits32 }] [priority { 0000 | 10000 | 20000 | … | F0000 }] [tx-holdcount <1 - 10>] [version { stp-compatible | rstp }]	page 315

Table 256 CLI command list (Continued)

Command	Page No.

`spanning- tree rstp [port <portlist>] [ cost <1 - 200000000> ]`
`[ edge-port { false | true } ]`
`[ learning { disable | enable } ]`
`[ p2p { auto | force-false | force-true } ]`
`[ priority { 00 | 10 | … | F0 } ]`
`[ protocol-migration { false | true } ]`
	page 316

`spanning-tree [stp <1-8>] remove-vlan <1-4094>`	page 305
`spanning-tree stp <2-8> create`	page 299
`spanning-tree stp <2-8> delete`	page 300
`spanning-tree stp <2-8> disable`	page 301
`spanning-tree stp <2-8> enable`	page 300
`speed [port <portlist>] {10|100|1000|auto}`	page 223
`ssh`	page 177
`ssh download-auth-key [address <XXX.XXX.XXX.XXX>] [key-name <file>]`	page 181
`ssh dsa-auth`	page 176
`ssh dsa-key [<512-1024>]`	page 176
`ssh max-sessions <0-2>`	page 178
`ssh pass-auth`	page 180
`ssh port <1-65535>`	page 180
`ssh secure`	page 178
`ssh timeout <1-120>`	page 179
`stack bootp-mac-addr-type {base-unit|stack}`	page 103
`stack oper-mode {hybrid |BS470}`	page 73
`stack replace unit <1-8>`	page 151

`telnet-access [enable|disable] [login-timeout <1-10>] [retry <1-100>] [inactive-timeout <0-60>]`
`[logging {none|access|failures|all}]`
`[source-ip <1-10> <XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]]`
	page 171

Table 256 CLI command list (Continued)

Command	Page No.
`terminal {2400|4800|9600|19200|38400} | length <1-132> | width <1-132>`	page 97
`tftp-server <XXX.XXX.XXX.XXX>`	page 105

`vlan create <1-4094> type macsa`
`vlan create <1-4094> type port`
`vlan create <1-4094> type protocol-ApltkEther2Snap`
`vlan create <1-4094> type protocol-decEther2`
`vlan create <1-4094> type protocol-decOtherEther2`
`vlan create <1-4094> type protocol-ipEther2`
`vlan create <1-4094> type protocol-ipv6Ether2`
`vlan create <1-4094> type protocol-ipx802.2`
`vlan create <1-4094> type protocol-ipx802.3`
`vlan create <1-4094> type protocol-ipxEther2`
`vlan create <1-4094> type protocol-ipxSnap`
`vlan create <1-4094> type protocol-Netbios`
`vlan create <1-4094> type protocol-RarpEther2`
`vlan create <1-4094> type protocol-sna802.2`
`vlan create <1-4094> type protocol-snaEther2`
`vlan create <1-4094> type protocol-Userdef <4096-65534>`
`vlan create <1-4094> type protocol-vinesEther2`
`vlan create <1-4094> type protocol-xnsEther2`
	page 258

Table 256 CLI command list (Continued)

Command	Page No.
`vlan create <1-4094> name <line> type macsa`	page 258
`vlan create <1-4094> name <line> type port`	
`vlan create <1-4094> name <line> type protocol-ApltkEther2Snap`	
`vlan create <1-4094> name <line> type protocol-decEther2`	
`vlan create <1-4094> name <line> type protocol-decOtherEther2`	
`vlan create <1-4094> name <line> type protocol-ipEther2`	
`vlan create <1-4094> name <line> type protocol-ipv6Ether2`	
`vlan create <1-4094> name <line> type protocol-ipx802.2`	
`vlan create <1-4094> name <line> type protocol-ipx802.3`	
`vlan create <1-4094> name <line> type protocol-ipxEther2`	
`vlan create <1-4094> name <line> type protocol-ipxSnap`	
`vlan create <1-4094> name <line> type protocol-Netbios`	
`vlan create <1-4094> name <line> type protocol-RarpEther2`	
`vlan create <1-4094> name <line> type protocol-sna802.2`	
`vlan create <1-4094> name <line> type protocol-snaEther2`	
`vlan create <1-4094> name <line> type protocol-Userdef <1-4094>`	
`vlan create <1-4094> name <line> type protocol-vinesEther2`	
`vlan create <1-4094> name <line> type protocol-xnsEther2`	

Table 256 CLI command list (Continued)

Command	Page No.
vlan create *<1-4094>* type macsa learning IVL	page 258
vlan create *<1-4094>* type port learning IVL	
vlan create *<1-4094>* type protocol-ApltkEther2Snap learning IVL	
vlan create *<1-4094>* type protocol-decEther2 learning IVL	
vlan create *<1-4094>* type protocol-decOtherEther2 learning IVL	
vlan create *<1-4094>* type protocol-ipEther2 learning IVL	
vlan create *<1-4094>* type protocol-ipv6Ether2 learning IVL	
vlan create *<1-4094>* type protocol-ipx802.2 learning IVL	
vlan create *<1-4094>* type protocol-ipx802.3 learning IVL	
vlan create *<1-4094>* type protocol-ipxEther2 learning IVL	
vlan create *<1-4094>* type protocol-ipxSnap learning IVL	
vlan create *<1-4094>* type protocol-Netbios learning IVL	
vlan create *<1-4094>* type protocol-RarpEther2 learning IVL	
vlan create *<1-4094>* type protocol-sna802.2 learning IVL	
vlan create *<1-4094>* type protocol-snaEther2 learning IVL	
vlan create *<1-4094>* type protocol-Userdef *<4096-65534>* learning IVL	
vlan create *<1-4094>* type protocol-vinesEther2 learning IVL	
vlan create *<1-4094>* type protocol-xnsEther2 learning IVL	

Table 256 CLI command list (Continued)

Command	Page No.
`vlan create <1-4094> type macsa learning SVL`	page 258
`vlan create <1-4094> type port learning SVL`	
`vlan create <1-4094> type protocol-ApltkEther2Snap learning SVL`	
`vlan create <1-4094> type protocol-decEther2 learning SVL`	
`vlan create <1-4094> type protocol-decOtherEther2 learning SVL`	
`vlan create <1-4094> type protocol-ipEther2 learning SVL`	
`vlan create <1-4094> type protocol-ipv6Ether2 learning SVL`	
`vlan create <1-4094> type protocol-ipx802.2 learning SVL`	
`vlan create <1-4094> type protocol-ipx802.3 learning SVL`	
`vlan create <1-4094> type protocol-ipxEther2 learning SVL`	
`vlan create <1-4094> type protocol-ipxSnap learning SVL`	
`vlan create <1-4094> type protocol-Netbios learning SVL`	
`vlan create <1-4094> type protocol-RarpEther2 learning SVL`	
`vlan create <1-4094> type protocol-sna802.2 learning SVL`	
`vlan create <1-4094> type protocol-snaEther2 learning SVL`	
`vlan create <1-4094> type protocol-Userdef <4096-65534> learning SVL`	
`vlan create <1-4094> type protocol-vinesEther2 learning SVL`	
`vlan create <1-4094> type protocol-xnsEther2 learning SVL`	

Table 256 CLI command list (Continued)

Command	Page No.
vlan create <*1-4094*> name <*line*> type macsa learning IVL	page 258
vlan create <*1-4094*> name <*line*> type port learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-ApltkEther2Snap learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-decEther2 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-decOtherEther2 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-ipEther2 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-ipv6Ether2 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-ipx802.2 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-ipx802.3 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-ipxEther2 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-ipxSnap learning IVL	
vlan create <1-4094> name <*line*> type protocol-Netbios learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-RarpEther2 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-sna802.2 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-snaEther2 learning IVL	
vlan create <1-4094> name <*line*> type protocol-Userdef <4096-65534> learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-vinesEther2 learning IVL	
vlan create <*1-4094*> name <*line*> type protocol-xnsEther2 learning IVL	

Table 256 CLI command list (Continued)

Command	Page No.

`vlan create <1-4094> name <line> type macsa learning SVL`
`vlan create <1-4094> name <line> type port learning SVL`
`vlan create <1-4094> name <line> type protocol-ApltkEther2Snap learning SVL`
`vlan create <1-4094> name <line> type protocol-decEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-decOtherEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipv6Ether2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipx802.2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipx802.3 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipxEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipxSnap learning SVL`
`vlan create <1-4094> name <line> type protocol-Netbios learning SVL`
`vlan create <1-4094> name <line> type protocol-RarpEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-sna802.2 learning SVL`
`vlan create <1-4094> name <line> type protocol-snaEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-Userdef <1-4094> learning SVL`
`vlan create <1-4094> name <line> type protocol-vinesEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-xnsEther2 learning SVL`
	page 258

`vlan delete <1-4094>`	page 261

Table 256 CLI command list (Continued)

Command	Page No.
vlan igmp <*1-4094*> [snooping {enable|disable}] [proxy {enable|disable}] [robust-value <*value*>] [query-interval <time>] [v1-members <*portlist*>] [v2-members <*portlist*>] [unknown-mcast-no-flood {enable|disable }]	page 375
vlan mac-address <*1-4094*> address <*H.H.H.*>	page 266
vlan members <*1-4094*> <*portlist*> vlan members add <*1-4094*> <*portlist*> vlan members remove <*1-4094*> <*portlist*>	page 275
vlan mgmt <*1-4094*>	page 258
vlan name <*1-4094*> <*line*>	page 263
vlan ports [<*portlist*>] [tagging {enable|disable}] [pvid <*1-4094*>] [filter-tagged-frame {enable|disable}] [filter-untagged-frame {enable|disable}] [filter-unregistered-frames {enable|disable}] [priority <*0-7*>] [name <*line*>]	page 274
web-server {enable|disable}	page 182

Index