Part No. 213296-A
December 2002

4655 Great America Parkway
Santa Clara, CA 95054

Reference for the BayStack 460-24T-PWR Switch NNCLI Command Line Interface

NORTEL NETWORKS™

Copyright © 2002 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 Communications Manager, Nortel Networks, the Nortel Networks logo, Optivity, Optivity Policy Services, and Preside are trademarks of Nortel Networks.

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

Intergy is a trademark of Invensys Energy Systems.

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).

USA requirements only

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the 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.

European requirements only

EN 55 022 statement

This is to certify that the Nortel Networks BayStack 460-24T-PWR Switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

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

Achtung: Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

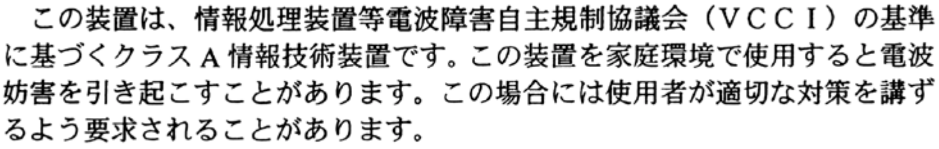
Attention: Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l’utilisateur de prendre les mesures spécifiques appropriées.

AEC Declaration of Conformity

This product conforms (or these products conform) to the provisions of the R&TTE Directive 1999/5/EC.

Japan/Nippon requirements only

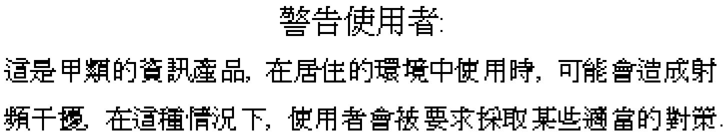
Voluntary Control Council for Interference (VCCI) statement



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。

Taiwan requirements

Bureau of Standards, Metrology and Inspection (BSMI) Statement



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.

Canada requirements only

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (BayStack 460-24T-PWR Switch) does 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

Cent appareil numérique (BayStack 460-24T-PWR Switch) 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.

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.

Contents

Figures

Tables

Preface

The BayStack* 460-24T-PWR Switch Nortel Networks* Command Line Interface (NNCLI) is one tool used to configure and manage a BayStack 460-24T-PWR switch. The NNCLI allows you to set up, configure, and manage your BayStack 460-24T-PWR switch.

You can also use the Java* Device Manager graphical user interface (GUI), the Web-based management system GUI, and the console interface (CI) menus to configure and manage the switch. For more information on these management systems, refer to *Reference for the BayStack 460-24T-PWR Switch Management Software, Using Web-based Management for the BayStack 460-24T-PWR Switch,* and *Using the BayStack 460-24T-PWR Switch*.

For general information on using and configuring the BayStack 460-24T-PWR switch, refer to *Using the BayStack 460-24T-PWR Switch.*

About this guide

This guide provides information about using the features and capabilities of the CLI to manage switching operations in the BayStack 460-24T-PWR switch, as well as a complete list of CLI commands.

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 460-24T-PWR 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 BayStack 460-24T-PWR Switch, refer to the following publications:

- *Release Notes for the BayStack 460-24T-PWR Switch* (part number 213297-A)

  Documents important changes about the software and hardware that are not covered in other related publications.

- *BayStack 460-24T-PWR Switch Installation Instructions* (part number 213318-A)

  Describes how to install the BayStack 460-24T-PWR switch.

- *Using the BayStack 460-24T-PWR Switch* (part number 213293-A)

  Describes how the physical switch and its functionality.

- *Reference for the BayStack 460-24T-PWR Switch Management Software* (part number 213295-A)

  Describes how to use the Java-based device-level software management application.

- *Using Web-based Management for the BayStack 460-24T-PWR Switch* (part number 213294-A)

  Describes how to use the Web-based management tool to configure switch features.

- *Installing Media Dependent Adapters (MDAs)* (part number 302403-H)

  Describes how to install optional MDAs in your BayStack 460-24T-PWR switch.

- *Installing Gigabit Interface Converters, SFPs, and CWDM SFP Gigabit Interface Converters* (part number 312865-C)

  Describes how to install optional GBICs, SFP GBICs, and CWDM SFP GBICs into the optional MDA in your BayStack 460-24T-PWR switch.

- *Installing the BayStack 400-ST1 Cascade Module (*part number 304433-B)

  Describes how to connect up to eight switches into a stack configuration by installing optional BayStack 400-ST1 Cascade Modules.

- *BayStack 10 Power Supply Unit Installation Instructions* (part number 208558-B)

  Describes installation, power-up, power-down and fan replacement procedures.

- *Release Notes for the BayStack 10 Power Supply Unit* (part number 208560-B)

  Documents important changes about the RPSU/UPS that are not covered in other related publications.

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 460-24T-PWR switch 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.

You can purchase printed books and documentation sets from Vervante. To order printed documentation, go to Vervante at the www.vervante.com/nortel URL.

How to get help

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 BayStack 460-24T-PWR 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 the BayStack 460-24T-PWR Switch Management Software*. For more information on using the Web-based management system, refer to *Using Web-based Management for the BayStack 460-24T-PWR Switch*. For more information on using the CI menus, refer to *Using the BayStack 460-24T-PWR Switch*.

The BayStack 460-24T-PWR switch Nortel Networks Command Line Interface (NNCLI) 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 NNCLI commands, refer to Appendix A.

You can use the NNCLI interactively, or you can load and execute NNCLI "scripts." NNCLI 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

This chapter discusses the following CLI topics:

- "Stacking compatibility," next
- "MDA compatibility" on page 33
- "CLI command modes" on page 34
- "Port numbering" on page 37
- "IP notation" on page 40

- “Accessing the CLI” on page 41
- “Setting the CLI password” on page 43
- “Getting help” on page 44
- “Basic navigation” on page 45
- “Managing basic system information” on page 51
- “Managing MAC address forwarding database table” on page 54
- “Displaying and setting stack operational mode” on page 56

Stacking compatibility

You can stack the BayStack 460-24T-PWR switch up to 8 units high. There are two types of stacks:

- Pure BayStack 460-24T-PWR switch—This stack has *only* BayStack 460-24T-PWR switches. It is sometimes referred to as a pure stack. The stack operational mode for this type of stack is Pure BPS/460 Mode.
- Hybrid—This stack has a combination of BayStack 460-24T-PWR switch switches *and* other BayStack or Business Policy 2000 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 BayStack 460-24T-PWR switch.You can only stack BayStack 460-24T-PWR switches in this release.

When you work with the BayStack 460-24T-PWR switch in standalone mode, you should ensure that the stack operational mode shows Pure BPs/460 Mode, and does not show Hybrid Mode.

All BayStack 460-24T-PWR switch switches in the stack must be running the identical version of software, and all the BayStack switches 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 the other BayStack and Business Policy 2000 switches must have the same ISVN as the BayStack 460-24T-PWR switch. If the ISVNs are not the same, the stack does not operate.

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

- Pure BayStack 460-24T-PWR 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 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.

Refer to Appendix B of *Using the BayStack 460-24T-PWR Switch* for complete information on interoperability and compatibility between the BayStack 460-24T-PWR switch and BayStack switches.

MDA compatibility

Note: The MDA ports do not supply power.

The BayStack 460-24T-PWR switch provides support for many Nortel Networks MDAs that use a variety of media, including Gigabit Interface Converters (GBICs) and CWDM.

Note: If you are using the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA, ensure that you are using version 03 of this product. (The 03 version number appears on the MDA itself; as well as on the shipping box.)

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.

CLI command modes

Most CLI commands are available only under a certain command mode. The BayStack 460-24T-PWR 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 BayStack 460-24T-PWR 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 but 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 BayStack 460-24T-PWR switch. The Privileged EXEC mode is also referred to as privExec mode.

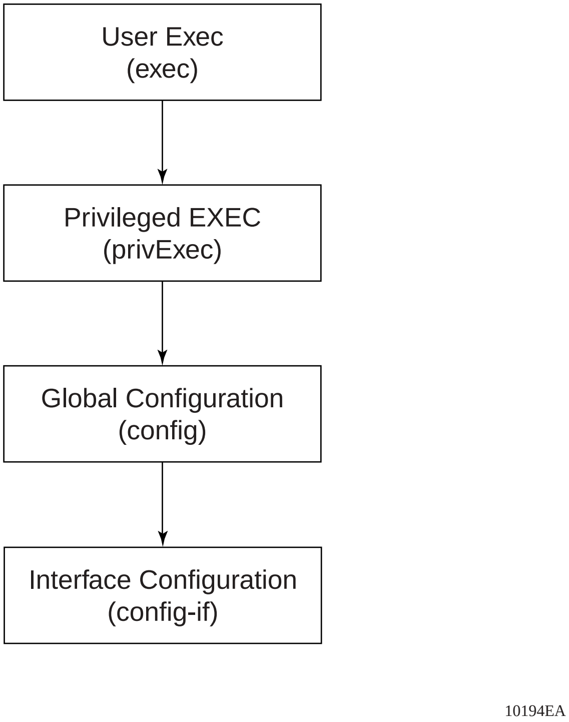
The last two command modes allow you to change the configuration of the BayStack 460-24T-PWR switch. Changes made in these command modes are immediately applied to the switch configuration and saved to NVRAM.

The Global Configuration commands allow you to set and display general configurations for the switch, such as the IP address, SNMP parameters, the 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 1 provides an illustration of the hierarchy of BayStack 460-24T-PWR switch CLI command modes.

Figure 1 CLI command mode hierarchy



You see a specific value for each command mode at the prompt line, and you use specific commands to enter or exit each command mode (Table 1). Additionally, you can only enter command modes from specific modes and only exit to specific command modes.

Table 1 Command mode prompts and entrance/exit commands

Command mode	**Prompt**	**Enter/exit command**
User EXEC (exec)	`460-24T-PWR>`	• Default mode, automatically enter • `logout` or `exit` to quit CLI
Privileged EXEC (privExec)	`460-24T-PWR#`	• `enable` to enter from User EXEC mode • `logout` or `exit` to quit CLI
Global Configuration (config)	`460-24T-PWR(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)#`	• `interface Fast Ethernet {<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`, and the current CLI command mode:

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

Refer to Appendix A 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 logged into the BayStack 460-24T-PWR 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 logged 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 logged 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.

Port numbering

The BayStack 460-24T-PWR switch operates either in standalone mode or in stack mode. The BayStack 460-24T-PWR switch has 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 ports do not supply power. You configure Power over Ethernet (PoE) parameters *only* on ports 1 to 24 for each BayStack 460-24T-PWR switch.

In stack mode, the BayStack 460-24T-PWR switch operates either in Pure BPS/460 Stack mode or in Hybrid Stack mode. The Hybrid Stack mode is when you are working with a combination of other BayStack and Business Policy 2000 switches and BayStack 460-24T-PWR switch switches in one stack.

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

When you are working with a standalone BayStack 460-24T-PWR switch, ensure that the operational mode is set for Pure BPS/460 Stack. (Refer to "show stack-oper-mode command" on page 57 and "stack oper-mode command" on page 58 for information on operational mode commands.)

Note: The variable *portlist* replaces the use the variable *portnum*, or *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 BayStack 460-24T-PWR switch or with a stack (either Pure BPS/460 Stack or Hybrid Stack).

Port numbering in standalone mode

Ensure that the operational mode is set for the Pure BPS/460 Stack mode when you are working with a standalone BayStack 460-24T-PWR switch.

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

- A single port number—an integer between 1 through 28
  - Example: `7` means port 7
- A range of port numbers—a pair of port numbers between 1 and 28 separated by a dash
  - Example: `1-3` means ports 1, 2, and 3
  - Example: `5-27` means all ports from port 5 through port 27
- 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 BPS 2000, including any MDA ports (not case-sensitive)

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

Port numbering in stacked mode

In stacked mode, either Pure BPS/460 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 will always be integers between 1 and 8, and the port numbers will always be integers between 1 and 28. 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 28 separated by a dash
  - — Example: `1/1-3` means unit 1, ports 1, 2, and 3
  - — Example: `3/5-27` means unit 3, port 5 through port 27
- 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, issue the `show stack-info` command ("show stack-info command" on page 53). You must be in the Privileged EXEC (privExec) mode to issue this command.

Refer to *Using the BayStack 460-24T-PWR Switch* guide, for more information on numbering units within the stack.

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.

Or, when you are specifying both an IP address and a netmask, you may alternatively enter XXX.XXX.XXX.XXX/0-32, where XXX.XXX.XXX.XXX is the IP address in dotted-decimal notation and the value 0-32 specifies the number of bits starting from the left in the mask (for example, a value of 8 is 255.0.0.0).

Accessing the CLI

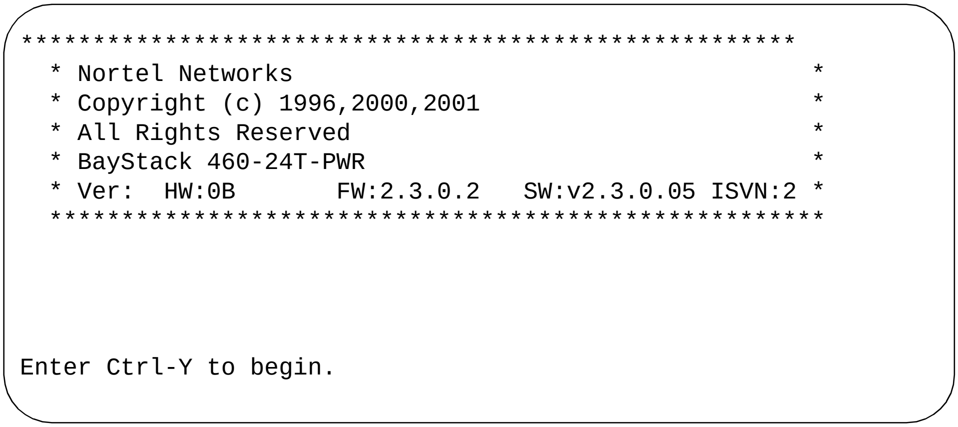
You access the CI menus using Telnet or a a direct connection to the switch from a terminal or personal computer (PC). You can use any terminal or PC with a terminal emulator as the CLI command station. Be sure the terminal has the following features:

- 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 BayStack 460-24T-PWR 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 BayStack 460-24T-PWR switch, the banner appears (Figure 2).

Figure 2 BayStack 460-24T-PWR switch banner



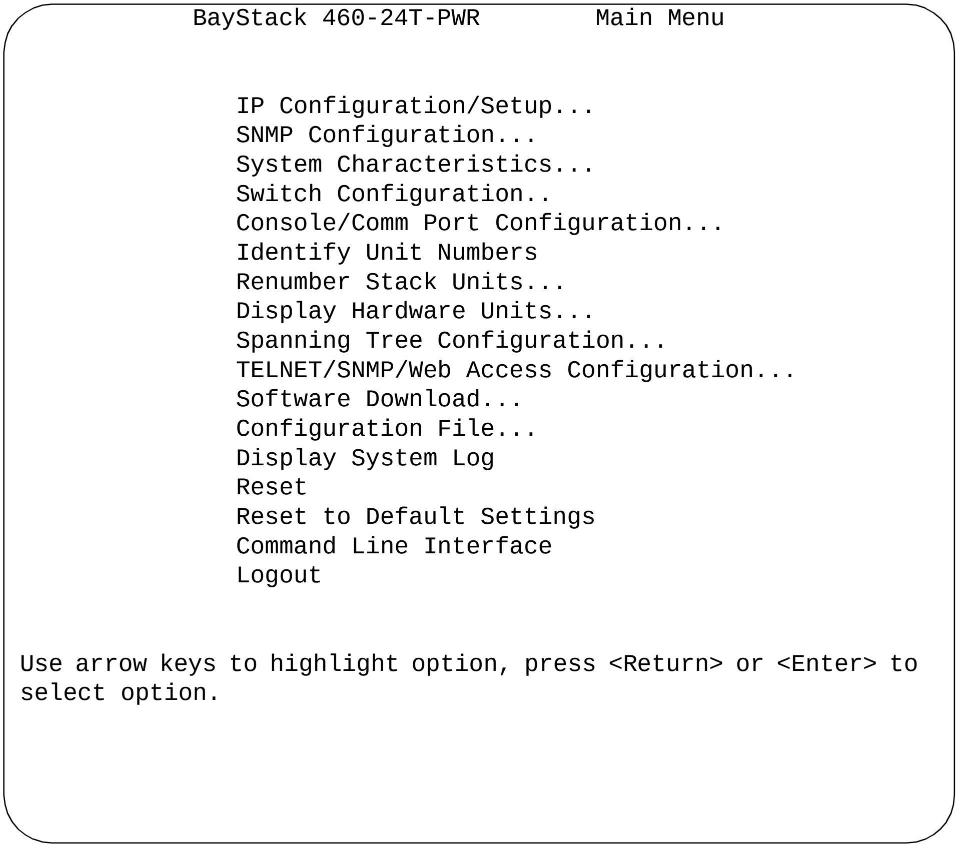
```
******************************************************
  * Nortel Networks                                    *
  * Copyright (c) 1996,2000,2001                       *
  * All Rights Reserved                                *
  * BayStack 460-24T-PWR                               *
  * Ver:  HW:0B       FW:2.3.0.2   SW:v2.3.0.05 ISVN:2 *
  ******************************************************




Enter Ctrl-Y to begin.
```

2 Press [Ctrl]+Y, and the Main Menu appears on the console screen (Figure 3) with the top line highlighted.

Figure 3 Main Menu for BayStack 460-24T-PWR switch console interface



```
             BayStack 460-24T-PWR        Main Menu


                IP Configuration/Setup...
                SNMP Configuration...
                System Characteristics...
                Switch Configuration..
                Console/Comm Port Configuration...
                Identify Unit Numbers
                Renumber Stack Units...
                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:

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

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” on page 34, to select the command mode you want to use (and are authorized to use).

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 Chapter 3. For more information on using RADIUS security with the CLI, refer to Chapter 3.

cli password command

The `cli password` is in two forms and performs the following functions for either the switch of 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 2 describes the parameters and variables for the `cli password` command.

Table 2 cli password command parameters and variables

Parameters and variables	Description
switch|stack	Specifies you are modifying the settings on the switch or on the 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

Getting 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 47 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 46
- "help command" on page 47
- "no command" on page 48
- "default command" on page 48
- "logout command" on page 48
- "enable command" on page 49
- "configure command" on page 49
- "interface command" on page 50
- "disable command" on page 50
- "end command" on page 50
- "exit command" on page 51

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 47 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. Refer to Appendix A 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 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 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
[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

Table 3 Keystroke navigation (continued)

Key combination	Function
[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 4 shows the output from the `help` command.

Figure 4 help command output in privExec mode

```
460-24T-PWR#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 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 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 3). 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 BayStack 460-24T-PWR switch switch to be able 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 BayStack 460-24T-PWR 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 BayStack 460-24T-PWR 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.

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 topics are covered:

- "show sys-info command," next
- "show stack-info command" on page 53
- "renumber unit command" on page 53

Refer to *Using the BayStack 460-24T-PWR Switch*, 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. 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 5 displays sample output from the `show sys-info` command.

Figure 5 show sys-info command output

```
460-24T-PWR#show sys-info
Operation Mode:   Stack, Unit # 1
Size Of Stack:    2
Base Unit:        1
MAC Address:      00-03-4B-FF-F1-9F
Reset Count:      33
Last Reset Type:  Software Download
Power Status:     Primary Power
Local MDA Type:   None
sysDescr:         BayStack 460-24T-PWR
                  HW:0C   FW:2.3.0.2 SW:v2.3.0.05 ISVN:2
sysObjectID:      1.3.6.1.4.1.45.3.40.1
sysUpTime:        5 days, 08:31:54
sysServices:      3
sysContact:
sysName:
sysLocation:
```

To change the system contact, name, or location, refer to the `snmp-server` command in Chapter 2.

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
```

renumber unit command

The `renumber unit` command changes the unit number of each switch in the stack. 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.

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 55
- "default mac-address-table aging-time command" on page 56

show mac-address-table command

The `show mac-address-table` command displays the current contents of the MAC address forwarding database table. The syntax for the `show mac-address-table` command is:

```
show mac-address-table [vid <1-4094>] [aging-time] [address
<H.H.H>]
```

The `show mac-address-table` command is in the privExec command mode.

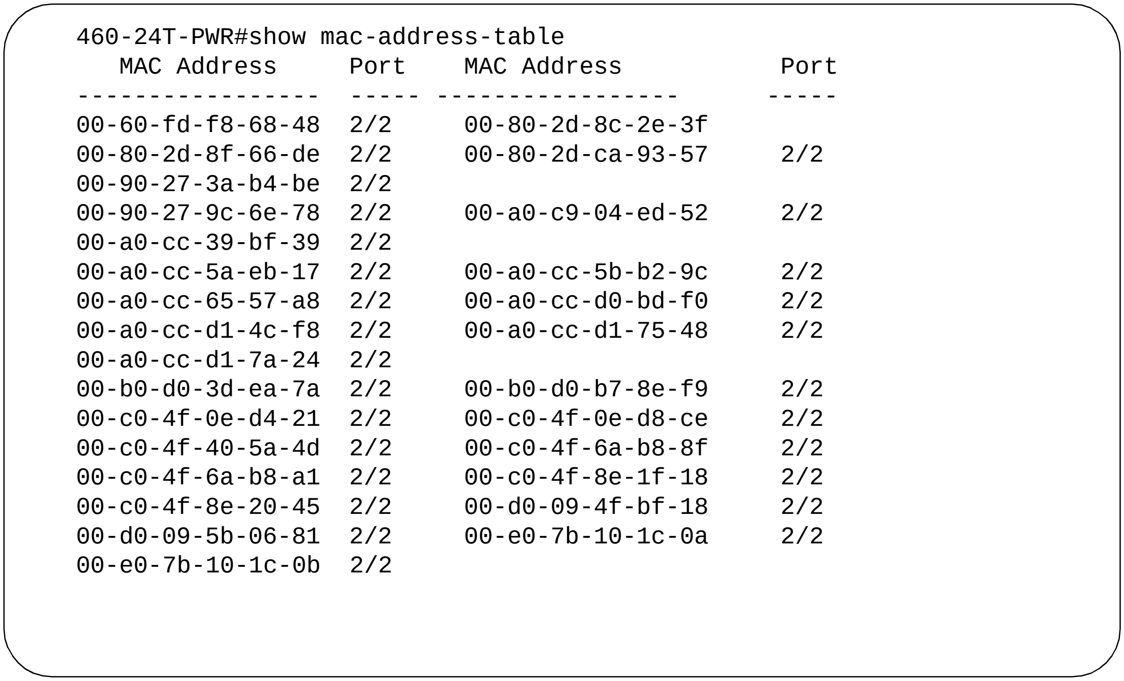
Table 6 describes the parameters and variables for the `show mac-address-table` command.

Table 6 show mac-address-table command parameters and variables

Parameters and variables	Description
vid <1-4094>	Enter the number of the VLAN you want to display the forwarding database of. 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 7 displays sample output from the `show mac-address-table` command.

Figure 7 show mac-address-table command output



```
460-24T-PWR#show mac-address-table
   MAC Address      Port     MAC Address           Port
-----------------  ----- -----------------      -----
00-60-fd-f8-68-48  2/2     00-80-2d-8c-2e-3f
00-80-2d-8f-66-de  2/2     00-80-2d-ca-93-57     2/2
00-90-27-3a-b4-be  2/2
00-90-27-9c-6e-78  2/2     00-a0-c9-04-ed-52     2/2
00-a0-cc-39-bf-39  2/2
00-a0-cc-5a-eb-17  2/2     00-a0-cc-5b-b2-9c     2/2
00-a0-cc-65-57-a8  2/2     00-a0-cc-d0-bd-f0     2/2
00-a0-cc-d1-4c-f8  2/2     00-a0-cc-d1-75-48     2/2
00-a0-cc-d1-7a-24  2/2
00-b0-d0-3d-ea-7a  2/2     00-b0-d0-b7-8e-f9     2/2
00-c0-4f-0e-d4-21  2/2     00-c0-4f-0e-d8-ce     2/2
00-c0-4f-40-5a-4d  2/2     00-c0-4f-6a-b8-8f     2/2
00-c0-4f-6a-b8-a1  2/2     00-c0-4f-8e-1f-18     2/2
00-c0-4f-8e-20-45  2/2     00-d0-09-4f-bf-18     2/2
00-d0-09-5b-06-81  2/2     00-e0-7b-10-1c-0a     2/2
00-e0-7b-10-1c-0b  2/2
```

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 <time>
```

The `mac-address-table aging-time` command is in the config command mode.

Table 7 describes the parameters and variables for the `mac-address-table aging-time` command.

Table 7 mac-address-table aging-time command parameters and variables

Parameters and variables	Description
time	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.

Displaying and setting 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 58

Refer to *Using the BayStack 460-24T-PWR Switch* for more information on the stack operation, including features requiring 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 BPS/460 Stack

or

- Hybrid Stack

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

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

```
Current Operational Mode:  Pure BPS/460 Stack
Next Boot Operational Mode:  Pure BPS/460 Stack
Stack BootP MAC Address Type:  Stack MAC Address
```

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 {bps460|hybrid}
```

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

Table 8 describes the parameters and variables for the `stack oper-mode` command.

Table 8 stack oper-mode command parameters and variables

Parameters and variables	**Description**
bps/460|hybrid	Sets the stack operational mode for the next boot: • bps2000—Pure BPS/460 Stack mode. This means *only* BayStack 460-24T-PWR switch switches either standalone or in a stack. • hybrid—Hybrid Stack mode. This means a mixture of BayStack 460-24T-PWR switch and BayStack 450 or 410 switches in a stack. Note: Hybrid Stack mode is not supported in this release of the BayStack 460-24T-PWR switch.

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

Chapter 2
General CLI commands

In the BayStack 460-24T-PWR switch, the Command Line Interface (CLI) commands allows you to display and modify the switch configuration while the switch is operating.

This chapter includes information about general switch maintenance, such as setting up access parameters, upgrading the software, and setting the speed. This chapter covers the following topics:

- "Setting the terminal," next
- "Pinging" on page 62
- "Assigning and clearing IP addresses" on page 66
- "Assigning and clearing IP addresses for specific units" on page 70
- "Setting Telnet access" on page 73
- "Setting server for Web-based management" on page 77
- "Setting boot parameters" on page 78
- "Setting TFTP parameters" on page 81
- "Upgrading software" on page 84
- "Displaying interfaces" on page 89
- "Setting SNMP parameters" on page 91
- "Setting the system event log" on page 95
- "Displaying port statistics" on page 99
- "Enabling or disabling a port" on page 101
- "Naming ports" on page 103
- "Setting port speed" on page 105
- "Enabling Autopology" on page 109
- "Enabling flow control" on page 110
- "Enabling rate-limiting" on page 112
- "Saving the configuration to NVRAM" on page 118

Setting the terminal

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

- "show terminal command," next
- "default terminal command" on page 61
- "terminal command" on page 61

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:

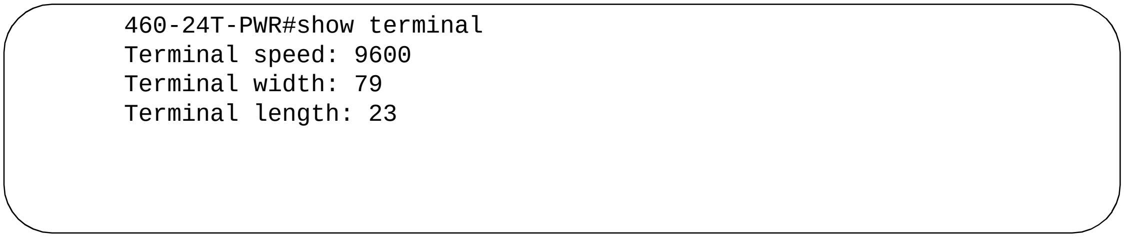
```
show terminal
```

The show terminal command is in the exec command mode.

The show terminal command has no parameters or variables.

Figure 9 displays the output from the show terminal command.

Figure 9 show terminal command output



```
460-24T-PWR#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 9 describes the parameters and variables for the `default terminal` command.

Table 9 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 10 describes the parameters and variables for the `terminal` command.

Table 10 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 displaying characters; default 79.

Pinging

To ensure that the BayStack 460-24T-PWR switch has connectivity to the network, ping a device you know is connected to this network.

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.

➡ **Note:** Refer to “Assigning and clearing IP addresses” on page 66 for information on setting IP addresses.

The syntax for the `ping` command is:

```
ping <XXX.XXX.XXX.XXX>
```

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

Table 11 describes the parameters and variables for the `ping` command.

Table 11 ping command parameters and variables

Parameters and variables	Description
XXX.XXX.XXX.XXX	Specify the IP address of the target device in dotted-decimal notation.

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 10 displays sample `ping` responses.

Figure 10 ping command responses

```
460-24T-PWR#ping 10.10.40.29
Host is reachable
BPS2000#ping 10.10.41.29
Host is not reachable
```

Automatically loading 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 65

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 `configure network` with no parameters, the system prompts you for the script file name and TFTP server address and then downloads the script.

Table 12 describes the parameters and variables for the `configure network` command.

Table 12 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.

Table 12 configure network command parameters and variables

Parameters and variables	Description
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 will be 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:

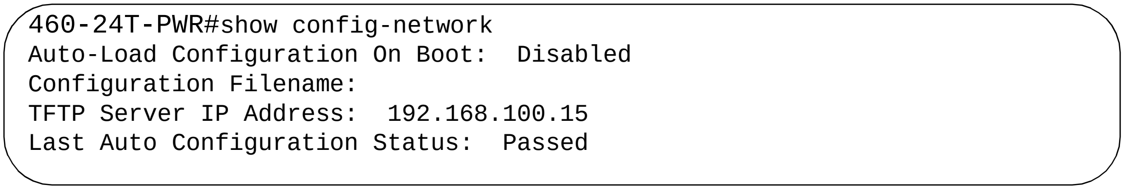
```
show config-network
```

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

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

The output for the `show config-network` command is shown in Figure 11,

Figure 11 show config-network command



```
460-24T-PWR#show config-network
Auto-Load Configuration On Boot:  Disabled
Configuration Filename:
TFTP Server IP Address:  192.168.100.15
Last Auto Configuration Status:  Passed
```

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 [stack|switch] <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 13 describes the parameters and variables for the `ip address` command.

Table 13 ip address command parameters and variables

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

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 or a stack to all zeros (0). The syntax for the no ip address command is:

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

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

Table 14 describes the parameters and variables for the no ip address command.

Table 14 no ip address command parameters and variables

Parameters and variables	Description
stack|switch	Zeroes out the stack IP address and subnet mask for the switch IP address and subnet mask.

➡ **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 15 describes the parameters and variables for the `ip default-gateway` command.

Table 15 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 these 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 [stack|switch]]
```

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.

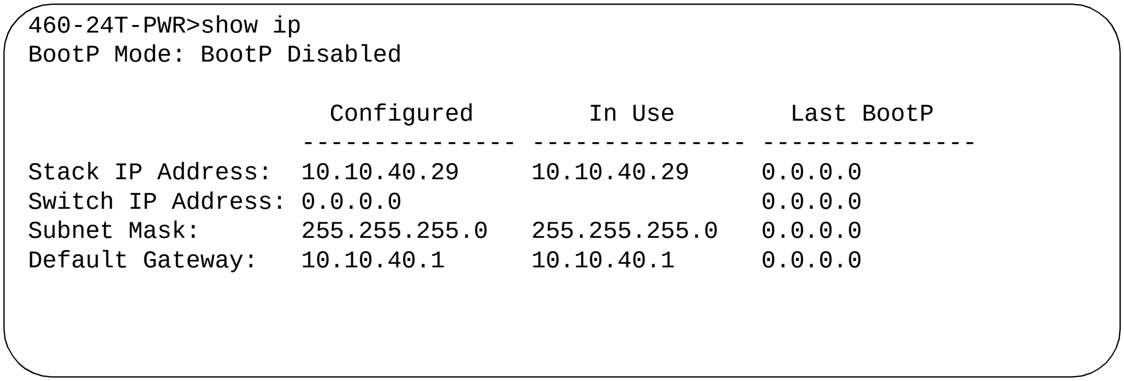
Table 16 describes the parameters and variables for the show ip command.

Table 16 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.
stack|switch	Specifies current IP address of the stack or the switch.

Figure 12 displays a sample output of the show ip command.

Figure 12 show ip command output



```
460-24T-PWR>show ip
BootP Mode: BootP Disabled

                     Configured        In Use        Last BootP
                   --------------- --------------- ---------------
Stack IP Address:  10.10.40.29     10.10.40.29     0.0.0.0
Switch IP Address: 0.0.0.0                         0.0.0.0
Subnet Mask:       255.255.255.0   255.255.255.0   0.0.0.0
Default Gateway:   10.10.40.1      10.10.40.1      0.0.0.0
```

Assigning and clearing IP addresses for specific units

You can assign IP addresses for 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 unit in the 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 17 describes the parameters and variables for the `ip address unit` command.

Table 17 ip address unit command parameters and variables

Parameters and variables	Description
unit <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 in a stack 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 18 describes the parameters and variables for the `no ip address unit` command.

Table 18 no ip address command parameters and variables

Parameters and variables	Description
unit <1-8>	Zeroes 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 in a stack 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 19 describes the parameters and variables for the `default ip address unit` command.

Table 19 default ip address unit command parameters and variables

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

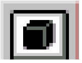
➡ **Note:** When you change the IP gateway, you may lose connection to Telnet and the Web.

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 BayStack 460-24T-PWR switch.

To open a Telnet session from Device Manager, click on the Telnet icon on the toolbar (Figure 13) or click Action > Telnet on the Device Manager toolbar.

Figure 13 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 total of 12 users on the stack. 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 75
- "no telnet-access command" on page 76
- "default telnet-access command" on page 76

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:

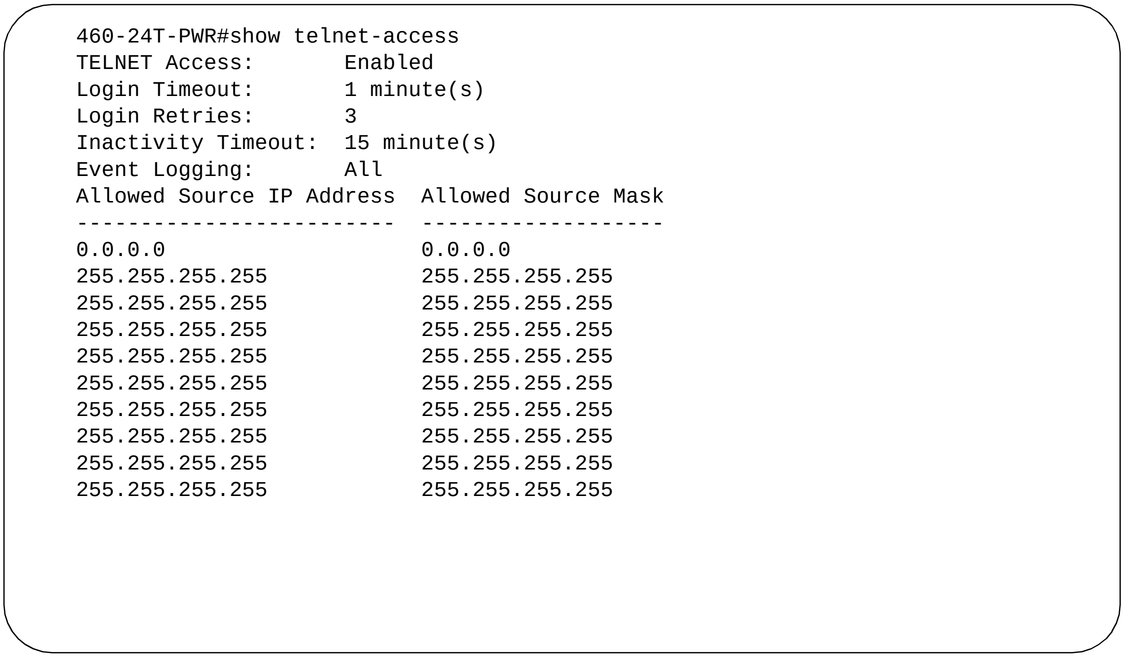
```
show telnet-access
```

The `show telnet-access` command is in the privExec command mode.

The `show telnet-access` command has no parameters or variables.

Figure 14 displays sample output from the `show telnet-access` command.

Figure 14 show telnet-access command output



```
460-24T-PWR#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 20 describes the parameters and variables for the `telnet-access` command.

Table 20 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 you want 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 from which connections are allowed. Enter the IP address either as an integer or in dotted-decimal notation. Specifies the subnet mask from which connections are allowed; 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, refer to Chapter 3.

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 21 describes the parameters and variables for the `no telnet-access` command.

Table 21 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, refer to Chapter 3.

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 values.

Setting server for Web-based management

You can enable or disable the Web server to use for the Web-based management system. Refer to *Using Web-based Management for the BayStack 460-24T-PWR Switch* for information on the Web-based management system. This section discusses the following commands:

- "web-server," next
- "no web-server" on page 77

web-server

The `web-server` command enables or disables the Web server that you 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 22 describes the parameters and variables for the `web-server` command.

Table 22 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 values.

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 79
- "stack bootp-mac-addr-type command" on page 79
- "no ip bootp server command" on page 80
- "default ip bootp server command" on page 80

boot command

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

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

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

Table 23 describes the parameters and variables for the `boot` command.

Table 23 boot command parameters and variables

Parameters and variables	Description
default	Restores switch or stack to factory-default settings after rebooting.
unit <unitno>	Specifies which unit of the stack will 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 or stack retains the stack operational mode, last reset count, and reason for last reset; these three parameters are not defaulted to factory defaults.

ip bootp server command

The `ip bootp server` command configures BootP on the current instance of the switch or server. 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 24 describes the parameters and variables for the `ip bootp server` command.

Table 24 ip bootp server command parameters and variables

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

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 460-24T-PWR switch that is set for stack operational mode of Pure BPS/460 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 25 describes the parameters and variables for the `stack boot-mac-addr-type` command.

Table 25 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 values.

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 values.

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 82
- "no tftp-server command" on page 82
- "copy config tftp command" on page 82
- "copy tftp config command" on page 83

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:

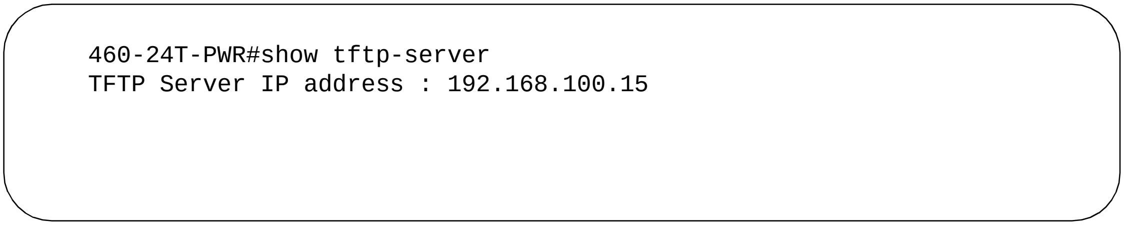
```
show tftp-server
```

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

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

Figure 15 displays a sample output of the `show tftp-server` command.

Figure 15 show tftp-server command output



```
460-24T-PWR#show tftp-server
TFTP Server IP address : 192.168.100.15
```

tftp-server command

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

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

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

Table 26 describes the parameters and variables for the tftp-server command.

Table 26 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 values.

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

Table 27 copy config tftp command parameters and variables

Parameters and variables	Description
address	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.

copy tftp config command

The `copy tftp config` command retrieves the system configuration file from the TFTP server and uses the retrieved information as the current configuration on the system.The syntax for the `copy tftp config` command is:

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

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

Table 28 describes the parameters and variables for the `copy tftp config` command.

Table 28 copy tftp config 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>	Enter the name of the configuration file you want to copy from the TFTP server.

Upgrading software

You can download the BayStack 460-24T-PWR switch software image that is located in non-volatile flash memory. To download the BayStack 460-24T-PWR switch software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the switch must have an IP address. To learn how to configure the switch or stack 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 86
- "Upgrading software images" on page 87

download command

The `download` command upgrades the software for the BayStack 460-24T-PWR 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 will be upgraded, and the new image is loaded onto every unit of the stack.

Note: The system resets after downloading a new image.

The syntax for the `download` command is:

```
download [[address <ip>] {image <filename>|diag
<filename>|image-if-newer <filename>|poe_module_image
<filename>}]
```

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

Note: You can use the `download` command without parameters. The system displays the most recently used TFTP serve IP address and file name; if you still want to use these, press `[Enter]` You can also change these.

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

Table 29 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 <filename>	Enter the name of the BayStack 460-24T-PWR switch software image you want to download.
diag <filename>	Enter the name of the BayStack 460-24T-PWR switch diagnostics image you want to download.
image-if-newer <filename>	Enter the name of the BayStack 460-24T-PWR switch image you are currently running. The system automatically downloads a newer image, if a newer image is present.
poe_module_image <filename>	Enter the name of the BayStack 460-24T-PWR switch PoE image you want to download. Note: You need not download this image; the power comes when you issue the `image <filename>` command.

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 and the new software image initiates a self-test. The system returns a message after successfully downloading a new image. Figure 16 displays a sample output of the download command.

Figure 16 download message

```
Download Image [/]

Saving Image [-]

Finishing Upgrading Image
```

During the download process, the BayStack 460-24T-PWR switch is not operational. You can monitor the progress of the download process by observing the LED indications.

Observing LED indications

Table 30 describes the LED indications during the software download process.

Note: When you upgrade the software in a mixed stack, or Hybrid Stack operational mode, all the BU LEDs on all BayStack 460-24T-PWR 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 switch.

Table 30 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 switch's flash memory are being erased. When LEDs 1 to 12 are all on, the switch's 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 switch's flash memory. When LEDs 1 to 8 are all on, the new software image has been programmed successfully into the switch's 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.

Upgrading software images

You follow a different procedure depending if you are using a Pure BPS/460 stack or a Hybrid stack.

The stacking software compatibility requirements are as follows:

- Pure BPS/460 stack—All units must be running the same software version.
- Hybrid stack—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.

This section discusses the following topics:

- "Upgrading software in a Pure BPS/460 stack," next
- "Upgrading software in a Hybrid stack" on page 88

Upgrading software in a Pure BPS/460 stack

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

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

   The system resets and opens to the BayStack 460-24T-PWR switch banner. Refer to "Accessing the CLI" on page 41 to return to the CLI.

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

   The system resets and opens to the BayStack 460-24T-PWR switch banner. Refer to "Accessing the CLI" on page 41 to return to the CLI.

Upgrading software in a Hybrid stack

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

The physical order of the units and the unit numbering in the Hybrid stack does not affect the upgrading process at all. In addition, the cabling order regarding upstream/downstream neighbors does not affect the process.

Before you attempt to download new software (or upgrade software) to a Hybrid (mixed) stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the other BayStack and Business Policy 200 switches must have the same ISVN as the BayStack 460-24T-PWR switch. If the ISVNs are not the same, the stack does not operate. The ISVNs and the accompanying software release are:

- ISVN 1
  - BayStack 410 or Bay Stack 450—version 3.1
  - BPS 2000—versions 1.0 and 1.0.1
- ISVN 2
  - BayStack 410 or BayStack 450—versions 4.0 and 4.1
  - BPS 2000—versions 1.1, 1.1.1, 1.2, and 2.0

Displaying interfaces

You can view the status of all interfaces on the switch or stack, 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.

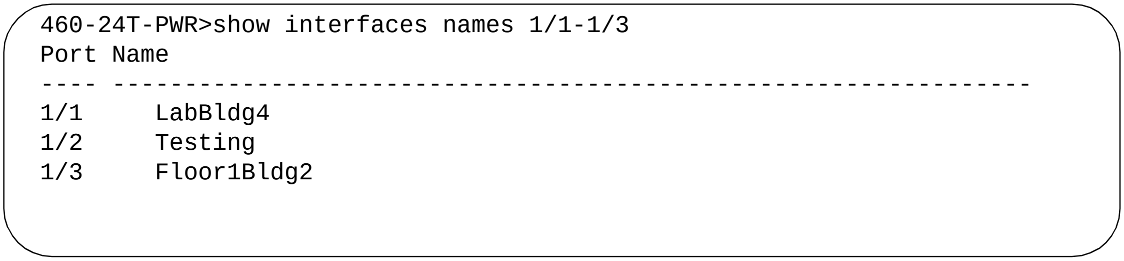
Table 31 describes the parameters and variables for the `show interfaces` command.

Table 31   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 17 displays a sample output of the `show interfaces names` command.

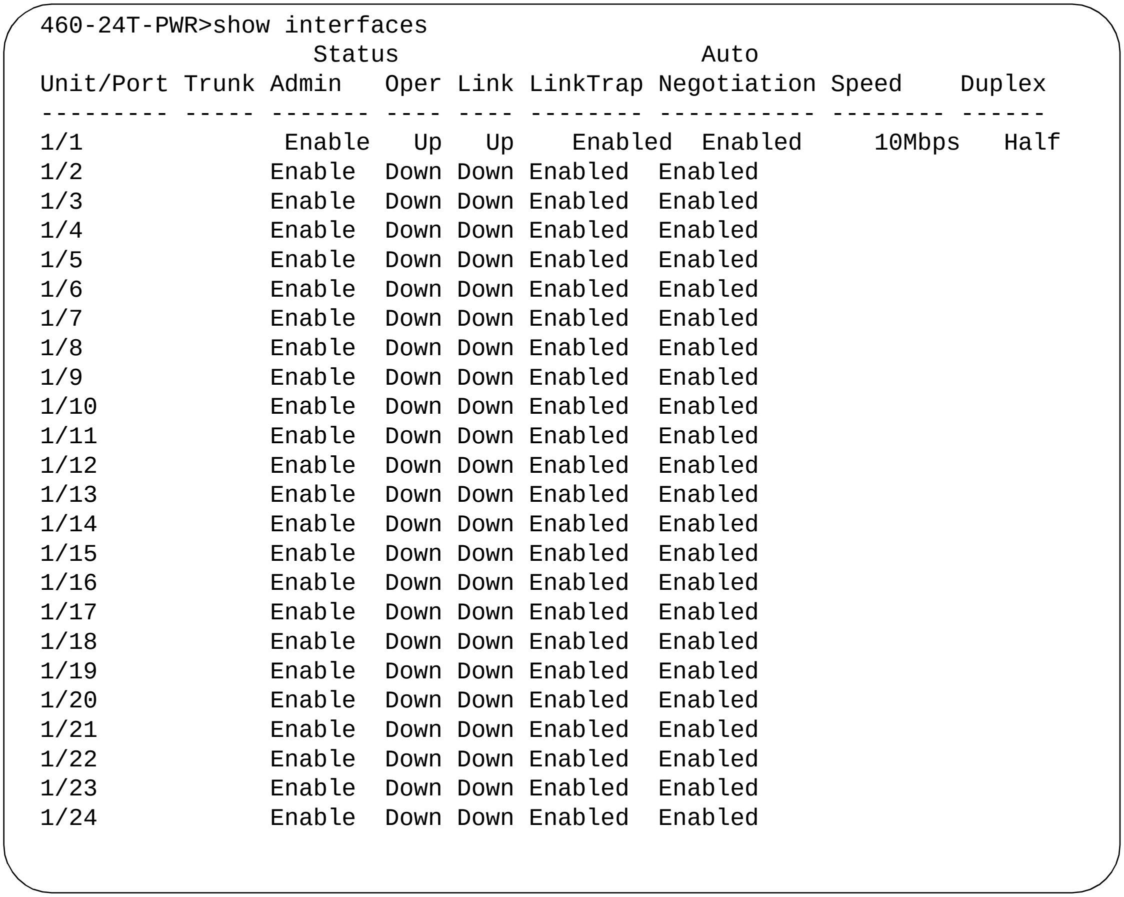
Figure 17   show interfaces names command output



```
460-24T-PWR>show interfaces names 1/1-1/3
Port Name
---- ----------------------------------------------------------------
1/1     LabBldg4
1/2     Testing
1/3     Floor1Bldg2
```

Figure 18 displays a sample output of the `show interfaces` command without the names variable.

Figure 18 show interfaces command output



```
460-24T-PWR>show interfaces
                   Status                     Auto
Unit/Port Trunk Admin   Oper Link LinkTrap Negotiation Speed    Duplex
--------- ----- ------- ---- ---- -------- ----------- -------- ------
1/1              Enable   Up   Up    Enabled  Enabled     10Mbps   Half
1/2             Enable  Down Down Enabled  Enabled
1/3             Enable  Down Down Enabled  Enabled
1/4             Enable  Down Down Enabled  Enabled
1/5             Enable  Down Down Enabled  Enabled
1/6             Enable  Down Down Enabled  Enabled
1/7             Enable  Down Down Enabled  Enabled
1/8             Enable  Down Down Enabled  Enabled
1/9             Enable  Down Down Enabled  Enabled
1/10            Enable  Down Down Enabled  Enabled
1/11            Enable  Down Down Enabled  Enabled
1/12            Enable  Down Down Enabled  Enabled
1/13            Enable  Down Down Enabled  Enabled
1/14            Enable  Down Down Enabled  Enabled
1/15            Enable  Down Down Enabled  Enabled
1/16            Enable  Down Down Enabled  Enabled
1/17            Enable  Down Down Enabled  Enabled
1/18            Enable  Down Down Enabled  Enabled
1/19            Enable  Down Down Enabled  Enabled
1/20            Enable  Down Down Enabled  Enabled
1/21            Enable  Down Down Enabled  Enabled
1/22            Enable  Down Down Enabled  Enabled
1/23            Enable  Down Down Enabled  Enabled
1/24            Enable  Down Down Enabled  Enabled
```

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 92
- "snmp trap link-status command" on page 93
- "no snmp trap link-status command" on page 94
- "default snmp trap link-status command" on page 95

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

Table 32 snmp-server command parameters and variables

Parameters and variables	Description
authentication-trap	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.

Table 32 snmp-server command parameters and variables (continued)

Parameters and variables	Description
host <host-ip> <community-string>	Configures an SNMP trap destination: • 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
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 33 describes the parameters and variables for the `snmp-server` command.

Table 33 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 will also lock you out of the DM 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 34 describes the parameters and variables for the snmp trap link-status command.

Table 34 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 you specified in 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 35 describes the parameters and variables for the no snmp trap link-status command.

Table 35 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 you specified in 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 36 describes the parameters and variables for the default `snmp trap link-status` command.

Table 36 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 you specified in the `interface` command.

Setting the system event log

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

- "show logging," next
- "set logging" on page 97
- "no set logging" on page 97
- "default set logging" on page 98
- "clear logging command" on page 98

show logging

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

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

The show logging command is in the privExec command mode.

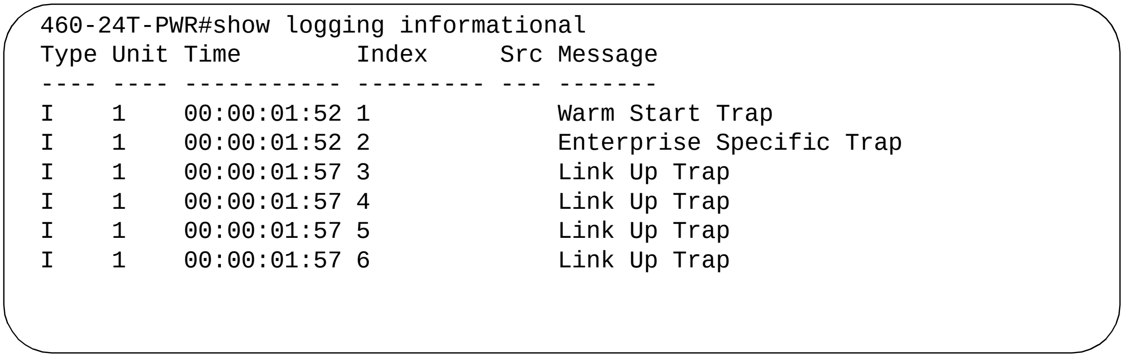
Table 37 describes the parameters and variables for the show logging command.

Table 37 show logging command parameters and variables

Parameters and variables	Description
critical	Displays critical log messages.
serious	Displays serious log messages.
informational	Displays informational log messages.

Figure 19 shows the output of the show logging informational command.

Figure 19 show logging command output



```
460-24T-PWR#show logging informational
Type Unit Time        Index     Src Message
---- ---- ----------- --------- --- -------
I    1    00:00:01:52 1             Warm Start Trap
I    1    00:00:01:52 2             Enterprise Specific Trap
I    1    00:00:01:57 3             Link Up Trap
I    1    00:00:01:57 4             Link Up Trap
I    1    00:00:01:57 5             Link Up Trap
I    1    00:00:01:57 6             Link Up Trap
```

set logging

The `set logging` command configures the system settings for the system event log. 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 38 describes the parameters and variables for the `set logging` command.

Table 38 set logging command parameters and values

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 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 values.

default set logging

The `default set logging` command configures the system settings as the factory default settings for the 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 values.

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 39 shows the parameters and values for the `clear logging` command.

Table 39 clear logging command parameters and values

Parameters and values	Description
nv	Clears all log messages in both DRAM and NVRAM.

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 101

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

Table 40 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 you specified in the `interface` command.

Figure 20 displays sample output from the `show port-statistics` command.

Figure 20 show port-statistics command output

```
460-24T-PWR(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 41 describes the parameters and variables for the clear-stats command.

Table 41 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 you specified in the interface command.

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 102

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 42 describes the parameters and variables for the `shutdown` command.

Table 42 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 you specified in 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 43 describes the parameters and variables for the `no shutdown` command.

Table 43 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 disable. Note: If you omit this parameter, the system uses the port number you specified in 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 104
- "default name command" on page 104

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 44 describes the parameters and variables for the name command.

Table 44 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 45 describes the parameters and variables for the no name command.

Table 45 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 you specified in 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 46 describes the parameters and variables for the default name command.

Table 46 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 you specified in 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 106
- "duplex command" on page 107
- "default duplex command" on page 108

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. You cannot *disable* autonegotiation on the BPS2000 1-GT and BPS2000 2-GT MDA ports.

Table 47 describes the parameters and variables for the `speed` command.

Table 47 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 you specified in 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 48 describes the parameters and variables for the `default speed` command.

Table 48 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 you specified in 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. You cannot *disable* autonegotiation on the BPS2000 1-GT and BPS2000 2-GT MDA ports.

Table 49 describes the parameters and variables for the `duplex` command.

Table 49 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 you specified in 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 50 describes the parameters and variables for the `default duplex` command.

Table 50 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 you specified in the `interface` command.

Note: You cannot *enable* autonegotiation on fiber optic ports. You cannot *disable* autonegotiation on the BPS2000 1-GT and BPS2000 2-GT MDA ports.

Enabling Autopology

You can enable the Optivity* Autopology* protocol using the CLI. Refer to the www.nortelnetworks.com/documentation URL for information on Autopology. (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 109
- "default autotopology command" on page 110

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 values.

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 values.

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 values.

Enabling flow control

If you use a Gigabit Ethernet MDA with the BayStack 460-24T-PWR 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 111
- "default flowcontrol command" on page 112

flowcontrol command

The `flowcontrol` command is used only on Gigabit Ethernet 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 51 describes the parameters and variables for the `flowcontrol` command.

Table 51 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 you specified in 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 52 describes the parameters and variables for the `no flowcontrol` command.

Table 52 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 you specified in 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 53 describes the parameters and variables for the `default flowcontrol` command.

Table 53 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 you specified in 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 *Using the BayStack 460-24T-PWR Switch*.

This section covers:

- "show rate-limit command," next
- "rate-limit command" on page 114
- "no rate-limit command" on page 115
- "default rate-limit command" on page 116

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:

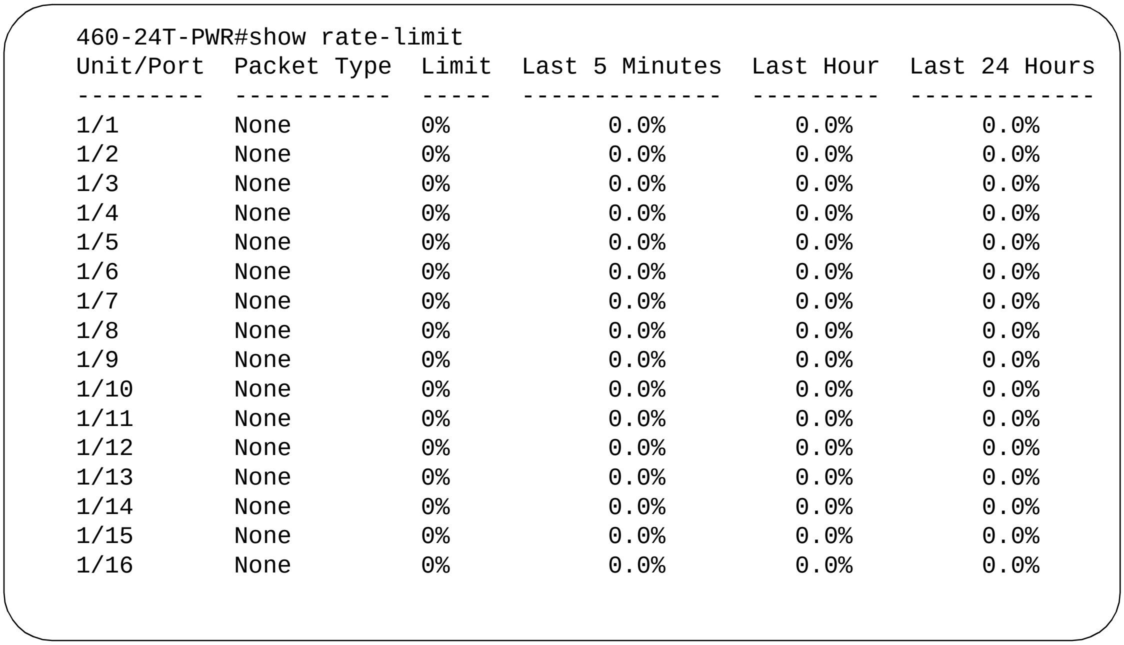
```
show rate-limit
```

The `show rate-limit` command is in the privExec command mode.

The `show rate-limit` command has no parameters or variables.

Figure 21 displays sample output from the `show rate-limit` command.

Figure 21 show rate-limit command output



```
460-24T-PWR#show rate-limit
Unit/Port  Packet Type  Limit  Last 5 Minutes  Last Hour  Last 24 Hours
---------  -----------  -----  --------------  ---------  -------------
1/1        None         0%           0.0%         0.0%         0.0%
1/2        None         0%           0.0%         0.0%         0.0%
1/3        None         0%           0.0%         0.0%         0.0%
1/4        None         0%           0.0%         0.0%         0.0%
1/5        None         0%           0.0%         0.0%         0.0%
1/6        None         0%           0.0%         0.0%         0.0%
1/7        None         0%           0.0%         0.0%         0.0%
1/8        None         0%           0.0%         0.0%         0.0%
1/9        None         0%           0.0%         0.0%         0.0%
1/10       None         0%           0.0%         0.0%         0.0%
1/11       None         0%           0.0%         0.0%         0.0%
1/12       None         0%           0.0%         0.0%         0.0%
1/13       None         0%           0.0%         0.0%         0.0%
1/14       None         0%           0.0%         0.0%         0.0%
1/15       None         0%           0.0%         0.0%         0.0%
1/16       None         0%           0.0%         0.0%         0.0%
```

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 54 describes the parameters and variables for the `rate-limit` command.

Table 54 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 you specified in 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 55 describes the parameters and variables for the no rate-limit command.

Table 55 no rate-limit command parameters and variables

Parameters and variables	Description
port <portlist>	Specifies the port numbers to disable for 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 56 describes the parameters and variables for the `default rate-limit` command.

Table 56 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 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 57 describes the parameters and variables for the `default rate-limit` command.

Table 57 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 you specified in the `interface` command.

Saving the configuration to NVRAM

You can save your configuration parameters to 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.

Chapter 3
Power over Ethernet

This chapter describes how to display and configure Power over Ethernet (PoE) parameters. This chapter covers the following topics:

- "Displaying PoE configuration," next
- "Configuring power parameters on the switch" on page 125
- "Configuring power parameters on the ports" on page 133

Refer to the *Using the BayStack 460-24T-PWR Switch* for more information on the PoE feature on the switch. Refer to *Using Web-based Management for the BayStack 460-24T-PWR Switch* for information on configuring these features using the Web-based management system, and refer to *Reference for the BayStack 460-24T-PWR Switch Management Software Operations* for configuration information for the DM.

➡ **Note:** For information on downloading the PoE image, refer to "download command" on page 84.

Displaying PoE configuration

You display the status for the PoE configuration on the BayStack 460-24T-PWR switch using the NNCLI, using the following commands:

- "show poe-main-status command," next
- "show poe-port-status command" on page 121
- "show poe-power-measurement command" on page 123

show poe-main-status command

The `show poe-main-status` command displays the current PoE configuration of the BayStack 460-24T-PWR switch, as well as per port 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.

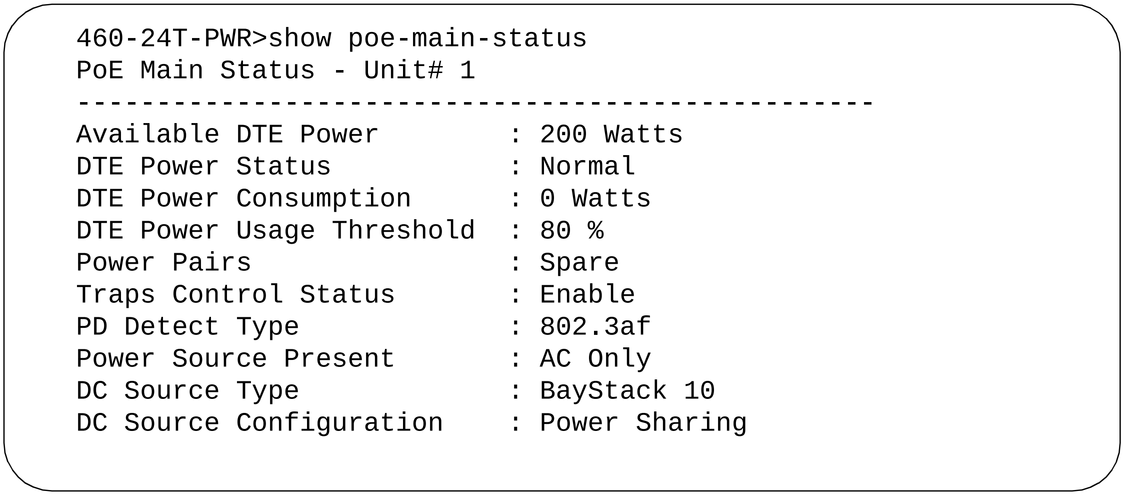
Table 58 describes the parameters and variables for the `poe poe-main-status` command.

Table 58 show poe-main-status command parameters and variables

Parameters and variables	Description
unit <1-8>	Enter the unit number for which you wan to display the power statistics. Note: If you omit this parameter, the system displays the unit you are connected to using the console port; if you telnet to the switch, the system displays the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.

Figure 22 displays sample output from the `show poe-main-status` command.

Figure 22 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 *Using the BayStack 460-24T-PWR Switch* 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 59 describes the parameters and variables for the `show poe-port-status` command.

Table 59 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 23 displays sample output from the `show poe-port-status` command.

Figure 23 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 60 shows the variables and parameters for the show poe-power-measurement command.

Table 60 show poe-power-measurement command parameters and variables

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 24 displays sample output from the `show poe-power-measurement` command.

Figure 24 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
1/10       0.0      0             0.000
1/11       0.0      0             0.000
1/12       0.0      0             0.000
1/13       0.0      0             0.000
1/14       0.0      0             0.000
1/15       0.0      0             0.000
1/16       0.0      0             0.000
1/17       0.0      0             0.000
1/18       0.0      0             0.000
1/19       0.0      0             0.000
1/20       0.0      0             0.000
1/21       0.0      0             0.000
1/22       0.0      0             0.000
1/23       0.0      0             0.000
1/24       0.0      0             0.000
--More--
```

Configuring power parameters on the switch

You configure power parameters for each BayStack 460-24T-PWR switch 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 127
- "poe poe-pd-detect-type command" on page 128
- "poe poe-power-pairs command" on page 129
- "poe poe-power-usage-threshold command" on page 130
- "poe poe-trap command" on page 131
- "no poe-trap command" on page 132

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 61 describes the parameters and variables for the `poe poe-dc-source-type` command.

Table 61 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 will set the unit you are connected to. If you omit this parameter and you are working through Telnet, this command will set 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. Refer to *Using the BayStack 460-24T-PWR Switch* for more information on power sharing, RPSU, and UPS DC source type options.

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 460-24T-PWR switch. 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 62 describes the parameters and variables for the `poe poe-dc-source-conf` command.

Table 62 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 will set the unit you are connected to. If you omit this parameter and you are working through Telnet, this command will set 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 460-24T-PWR switch: • 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. Refer to *Using the BayStack 460-24T-PWR Switch* for more information on power sharing, RPSU, and UPS DC source configuration options.

poe poe-pd-detect-type command

The `poe poe-pd-detect-type` command sets the method the BayStack 460-24T-PWR switch 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 63 describes the parameters and variables for the `poe poe-pd-detect-type` command.

Table 63 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 will set the unit you are connected to. If you omit this parameter and you are working through Telnet, this command will set 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 460-24T-PWR switch matches that used by the IP devices you are powering. Refer to *Using the BayStack 460-24T-PWR Switch* 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 64 describes the parameters and variables for the `poe poe-power-pairs` command.

Table 64 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 will set the unit you are connected to. If you omit this parameter and you are working through Telnet, this command will set 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 BayStack 460-24T-PWR Switch* for complete information on power pairs. Note: Ensure that the power pair you choose for the BayStack 460-24T-PWR switch 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 460-24T-PWR switch. 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 65 describes the parameters and variables for the poe poe-power-usage-threshold command.

Table 65 poe poe-power-usage-threshold command parameters and variables

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 will set the unit you are connected to. If you omit this parameter and you are working through Telnet, this command will set 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 460-24T-PWR switch. 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 66 describes the parameters and variables for the `poe poe-trap` command.

Table 66 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 will set the unit you are connected to. If you omit this parameter and you are working through Telnet, this command will set 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 460-24T-PWR switch. 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 67 describes the parameters and variables for the `no poe-trap p` command.

Table 67 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 will set the unit you are connected to. If you omit this parameter and you are working through Telnet, this command will set 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 configure power parameters for each port on the BayStack 460-24T-PWR switch 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 134
- “poe poe-priority command” on page 135
- “poe poe-limit command” on page 136

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 68 describes the parameters and variables for the `no poe-shutdown` command.

Table 68 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 you entered in 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 69 describes the parameters and variables for the `poe poe-shutdown` command.

Table 69 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 you entered in 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 70 describes the parameters and variables for the `poe poe-priority` command.

Table 70 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 you entered in 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 will be shut down first.) For more information on port priority and overall power balancing, refer to *Using the BayStack 460-24T-PWR-Switch*.

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 71 describes the parameters and variables for the `poe poe-limit` command.

Table 71 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 you entered in the `interface FastEthernet` command.

Chapter 4
Security

This chapter describes the security commands available with the CLI. There are four types of security available on the BayStack 460-24T-PWR switch:

- "Using the IP manager list," next
- "Using MAC address security" on page 142
- "Using EAPOL-based security" on page 151
- "Using RADIUS authentication" on page 154

Refer to *Using the BayStack 460-24T-PWR Switch* for more information on these security features, as well as using the console interface (CI) menus. Refer to *Using Web-based Management for the BayStack 460-24T-PWR Switch* for information on configuring these features using the Web-based management system, and refer to *Reference for the BayStack 460-24T-PWR Switch Management Software for* information on configuring with the DM.

Using the IP manager list

When enabled, the IP manager list determines which source IP addresses are allowed access to the BayStack 460-24T-PWR 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 139
- "no ipmgr command for management system" on page 140
- "ipmgr command for source IP address" on page 141
- "no ipmgr command for source IP address" on page 142

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 25 displays sample output from the `show ipmgr` command.

Figure 25 show ipmgr command output

```
460-24T-PWR#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 Web access. The syntax for the `ipmgr` command for the management systems is:

```
ipmgr {telnet|snmp|web}
```

The `ipmgr` command for the management systems is in the config mode.

Table 72 describes the parameters and variables for the `ipmgr` command.

Table 72 ipmgr command for system management parameters and variables

Parameters and variables	Description
telnet|snmp|web	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 DM • web—provides list access using the Web-based management system

no ipmgr command for management system

The `no ipmgr` command disables the IP manager list for Telnet, SNMP, or Web access. The syntax for the `no ipmgr` command for the management systems is:

```
no ipmgr {telnet|snmp|web}
```

The `no ipmgr` command is in the config mode.

Table 73 describes the parameters and variables for the `no ipmgr` command.

Table 73 no ipmgr command for management system parameters and variables

Parameters and variables	**Description**
telnet|snmp|web	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 DM • web—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 74 describes the parameters and variables for the `ipmgr` command for the source IP addresses.

Table 74 ipmgr command for source IP addresses parameters and variables

Parameters and variables	Description
source-ip <1-10> <XXX.XXX.XXX.XXX>[mask <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. 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 the 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 75 describes the parameters and variables for the no `ipmgr` command for the source IP addresses.

Table 75 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.

Using MAC address 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 144
- "mac-security command" on page 145
- "mac-security mac-address-table address command" on page 146
- "mac-security security-list command" on page 147
- "no mac-security command" on page 147
- "no mac-security mac-address-table command" on page 147
- "no mac-security security-list command" on page 148
- "mac-security command for specific ports" on page 149
- "mac-security mac-da-filter command" on page 150

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 76 describes the parameters and variables for the show mac-security command.

Table 76 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 26 displays sample output from the show mac-security config command.

Figure 26 show mac-security command output

```
460-24T-PWR#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: NONE
```

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 27 displays sample output from the show mac-security mac-da-filter command.

Figure 27 show mac-security mac-da-filter command output

```
460-24T-PWR#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 77 describes the parameters and variables for the `mac-security` command.

Table 77 mac-security command parameters and values

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
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 78 describes the parameters and variables for the `mac-security mac-address-table address` command.

Table 78 mac-security mac-address-table address command parameters and values

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 79 describes the parameters and variables for the mac-security security-list command.

Table 79 mac-security security-list command parameters and values

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 80 describes the parameters and variables for the no `mac-security mac-address-table` command.

Table 80 no mac-security mac-address-table command parameters and values

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 81 describes the parameters and variables for the no `mac-security security-list` command.

Table 81 no mac-security security-list command parameters and values

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 82 describes the parameters and variables for the `mac-security` command for specific ports.

Table 82 mac-security command for a single port parameters and variables

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 83 describes the parameters and variables for the `mac-security mac-da-filter` command.

Table 83 mac-security mac-da-filter command parameters and values

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.

Using 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 151
- "eapol command for modifying parameters" on page 152

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
```

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

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

The `show eapol` command displays the current status of the EAPOL parameters.

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 84 describes the parameters and variables for the `eapol` command.

Table 84 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 85 describes the parameters and variables for the `eapol` command for modifying parameters

Table 85 eapol command for modifying parameters and variables

Parameters and variables	**Description**
port <portllist>	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-outlin	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
re-authentication enable|disable	Enables or disables re-authentication.

Table 85 eapol command for modifying parameters and variables (continued)

Parameters and variables	Description
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.

Using RADIUS authentication

Using a the RADIUS protocol and a server, you can configure the BayStack 460-24T-PWR switch for authentication. With the CLI system, you use the following commands:

- "show radius-server command," next
- "radius-server command" on page 155
- "no radius-server command" on page 155

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 28 displays sample output from the `show radius-server` command.

Figure 28 show radius-server command output

```
460-24T-PWR#show radius-server
host: 0.0.0.0
Secondary-host: 0.0.0.0
port: 1645
key:
```

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 86 describes the parameters and variables for the radius-server command.

Table 86 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.

Chapter 5
Spanning Tree, MLT, and Port-Mirroring

This chapter describes how to configure the Spanning Tree Protocol, spanning tree groups, Multi-Link Trunking (MLT), and port-mirroring. This chapter covers the following topics:

- "Using spanning tree," next
- "Using MLT" on page 170
- "Using port-mirroring" on page 173

Refer to the *Using the BayStack 460-24T-PWR Switch*for more information on multiple spanning tree groups, spanning tree, MLT, and port-mirroring, as well as configuration directions using the console interface (CI) menus. Refer to *Using Web-based Management for the BayStack 460-24T-PWR Switch* for information on configuring these features using the Web-based management system, and refer to *Reference for the BayStack 460-24T-PWR Switch Management Software* for configuration information for the DM.

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*.

With the BayStack 460-24T-PWR 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 BPS/460 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 161
- "spanning-tree stp delete command by STG" on page 162
- "spanning-tree stp enable command by STG" on page 162
- "spanning-tree stp disable command by STG" on page 163
- "spanning-tree command by STG" on page 164
- "default spanning-tree command by STG" on page 165
- "spanning-tree add-vlan command" on page 166
- "spanning-tree remove-vlan command" on page 167
- "spanning-tree command by port" on page 168
- "default spanning-tree command by port" on page 169
- "no spanning-tree command by port" on page 170

➡ **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>] {config|port}
```

The show spanning-tree command is in the privExec command mode,

Table 87 describes the parameters and variables for the show spanning-tree command.

Table 87 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.
config|port	Displays spanning tree configuration for: • config—the specified (or default) spanning tree group • port—the ports within the spanning tree group

Figure 29 displays sample output from the show spanning-tree command for the default spanning tree group (STP1). Figure 30 shows the spanning tree parameters by port.

Figure 29 show spanning-tree command output by port

```
460-24T-PWR#show spanning-tree stp 1 port
Unit Port Trunk   Participation   Priority  Path Cost    State
---- ---- -----  ---------------  --------  ---------  ----------
1    1           Normal Learning  128       10         Forwarding
1    2           Normal Learning  128       10         Forwarding
1    3           Normal Learning  128       10         Forwarding
1    4           Normal Learning  128       10         Forwarding
1    5           Normal Learning  128       10         Forwarding
1    6           Normal Learning  128       10         Forwarding
1    7           Normal Learning  128       10         Forwarding
1    8           Normal Learning  128       10         Forwarding
1    9           Normal Learning  128       10         Forwarding
1    10          Normal Learning  128       10         Forwarding
1    11          Normal Learning  128       10         Forwarding
1    12          Normal Learning  128       10         Forwarding
1    13          Normal Learning  128       10         Forwarding
1    14          Normal Learning  128       10         Forwarding
1    15          Normal Learning  128       10         Forwarding
1    16          Normal Learning  128       10         Forwarding
1    17          Normal Learning  128       10         Forwarding
1    18          Normal Learning  128       10         Forwarding
1    19          Normal Learning  128       10         Forwarding
1    20          Normal Learning  128       10         Forwarding
1    21          Normal Learning  128       10         Forwarding
1    22          Normal Learning  128       10         Forwarding
1    23          Normal Learning  128       10         Forwarding
1    24          Normal Learning  128       10         Forwarding
```

Figure 30 show spanning-tree command output for spanning tree group

```
460-24T-PWR#show spanning-tree config
Bridge Priority:            8000
Designated Root:            8000000081c6a801
Root Port:                  1/1
Root Path Cost:             124
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
```

spanning-tree stp create command by STG

Note: For guidelines for configuring STGs, VLANs, and MLTs, refer to Chapter 1 of the *Using the BayStack 460-24T-PWR Switch*.

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 88 describes the parameters and variables for the `spanning-tree stp create` command.

Table 88 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 89 describes the parameters and variables for the `spanning-tree stp delete` command.

Table 89 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 90 describes the parameters and variables for the `spanning-tree stp enable` command.

Table 90 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 91 describes the parameters and variables for the `spanning-tree stp disable` command.

Table 91 spanning-tree stp disable command parameters and variables

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 92 describes the parameters and variables for the `spanning-tree` command by STG.

Table 92 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.

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]
```

The `default spanning-tree` command by STG is in the config command mode.

Table 93 describes the parameters and variables for the `default spanning-tree` command by STG.

Table 93 default spanning-tree command by STG parameters and variables

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.

spanning-tree add-vlan command

➡ **Note:** You use the `spanning-tree add-vlan` command to move and VLAN from one spanning tree group to another 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 94 describes the parameters and variables for the `spanning-tree add-vlan` command.

Table 94 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 95 describes the parameters and variables for the `spanning-tree remove-vlan` command.

Table 95 spanning-tree remove-vlan command parameters and variables

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 for configuring STGs, VLANs, and MLTs, refer to Chapter 1 of the *Using the BayStack 460-24T-PWR Switch*.

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 <0-255>]
```

The `spanning-tree` command by port is in the config-if command mode.

Table 96 describes the parameters and variables for the `spanning-tree` command by port.

Table 96 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 you specified when you issued the `interface` command.
stp <1-8>	Specifies the spanning tree group you want; enter the STG ID.
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 <0-255>	Enter the priority value of the spanning tree; range is 0-255.

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 97 describes the parameters and variables for the `default spanning-tree` command by port.

Table 97 default 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 set to factory spanning tree default values. Note: If you omit this parameter, the system uses the port number you specified when you issued 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 0x8000.

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 98 describes the parameters and variables for the `no spanning-tree` command by port.

Table 98 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 MLT

Note: For guidelines for configuring STGs, VLANs, and MLTs, refer to Chapter 1 of the *Using the BayStack 460-24T-PWR Switch*.

You configure Multi-Link Trunking (MLT) using the following commands:

- "show mlt command," next
- "mlt command" on page 172
- "no mlt command" on page 173

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.

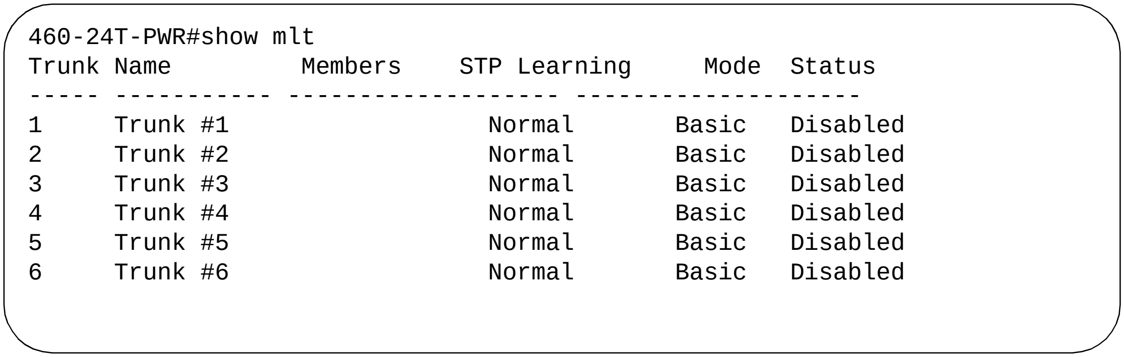
Table 99 describes the parameters and variables for the `show mlt` command.

Table 99 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 31 displays sample output from the `show mlt` command.

Figure 31 show mlt command output



```
460-24T-PWR#show mlt
Trunk Name         Members    STP Learning     Mode  Status
----- ----------- ------------------- --------------------
1     Trunk #1                  Normal       Basic   Disabled
2     Trunk #2                  Normal       Basic   Disabled
3     Trunk #3                  Normal       Basic   Disabled
4     Trunk #4                  Normal       Basic   Disabled
5     Trunk #5                  Normal       Basic   Disabled
6     Trunk #6                  Normal       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>]
```

The mlt command is in the config command mode.

Table 100 describes the parameters and variables for the mlt command.

Table 100 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.

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 101 describes the parameters and variables for the no `mlt` command.

Table 101 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 port-mirroring

You use port-mirroring to monitor traffic. Refer to *Using the BayStack 460-24T-PWR Switch* for configuration guidelines for port-mirroring. This section covers the following commands:

- "show port-mirroring command," next
- "port-mirroring command" on page 174
- "no port-mirroring command" on page 176

show port-mirroring command

The `show port-mirroring` command displays the port-mirroring configuration. The syntax for the `show port-mirroring` command is:

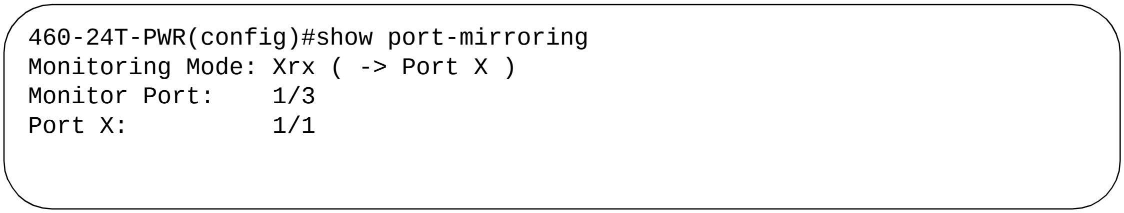
```
show port-mirroring
```

The `show port-mirroring` command is in the privExec command mode.

The `show port-mirroring` command has no parameters or variables.

Figure 32 displays sample output from the `show port-mirroring` command.

Figure 32 show port-mirroring command output



```
460-24T-PWR(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 102 describes the parameters and variables for the `port-mirroring` command.

Table 102 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.

Chapter 6
VLANs and IGMP

This chapter describes how to configure virtual LANs and IGMP snooping parameters. This chapter covers the following topics:

- "Increased VLAN support," next
- "Configuring and displaying VLANs" on page 179
- "Displaying multicast membership" on page 193
- "Using IGMP snooping" on page 194

Refer to the *Using the BayStack 460-24T-PWR Switch* for more information on VLANs, IGMP snooping, and multicast groups, as well as configuration directions using the console interface (CI) menus. Refer to *Using Web-based Management for the BayStack 460-24T-PWR Switch* for information on configuring these features using the Web-based management system, and refer to *Reference for the BayStack 460-24T-PWR Switch Management Software* for configuration information for the DM.

Increased VLAN support

The BayStack 460-24T-PWR switch supports up to 256 VLANs. You can configure as many as 255 protocol-based VLANs, with up to 14 different protocols. To find out which version of the BayStack 460-24T-PWR switch software is running, use the `show sys-info` command in the privExec command mode The software currently running is displayed in the sysDescr field.

You can use 256 port-, protocol-, and MAC SA-based VLANs for the stack with a Pure BPS/460 stack. (The maximum number of MAC SA-based VLANs available is 48). If you are working with a mixed, or hybrid, stack, you can use 64 VLANs for the entire stack. When you change from a Pure BPS/460 Stack mode to a Hybrid Stack mode:

- If you have up to 64 VLANs on the Pure BPS/460 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS/460 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

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

Also, a mixed, or hybrid, stack does not support multiple Spanning Tree Groups (STG). You have a single instance of STG when working with a mixed stack.

Note: Ensure that stack operational mode is set to Pure BPS/460 stack mode, and not Hybrid. The standalone or stack of BayStack 460-24T-PWR switches must be operating in Pure BPS/460 Stack mode. Refer to Chapter 1 for information on displaying and setting the stack operational mode.

Configuring and displaying VLANs

You 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 section covers the following topics:

- "show vlan interface info command," next
- "show vlan interface vids command" on page 182
- "vlan mgmt command" on page 183
- "default vlan mgmt command" on page 183
- "vlan create command" on page 184
- "vlan delete command" on page 186
- "no vlan command" on page 187v
- "vlan name command" on page 187
- "auto-pvid command" on page 188
- "no auto-pvid command" on page 188
- "vlan ports command" on page 189
- "vlan members command" on page 190
- "show vlan mac-address command" on page 191
- "vlan mac-address command" on page 192
- "no vlan mac-address command" on page 192

Refer to Appendix A for an alphabetical list of the VLAN commands.

Note: For guidelines for configuring VLANs, spanning tree groups, and MLTs, refer to Chapter 1 of the *Using the BayStack 460-24T-PWR Switch*.

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.

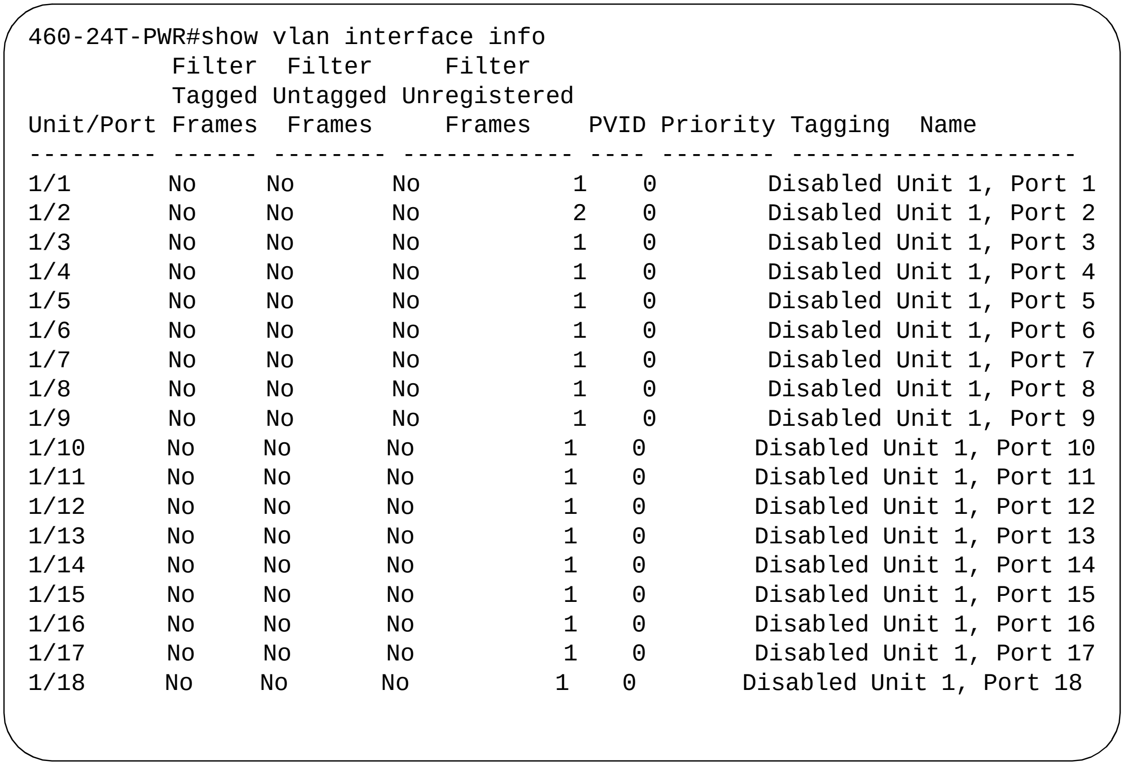
Table 103 describes the parameters and variables for the show vlan interface info command.

Table 103 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 33 displays sample output from the `show vlan interface info` command.

Figure 33 show vlan interface info output



```
460-24T-PWR#show vlan interface info
          Filter  Filter     Filter
          Tagged Untagged Unregistered
Unit/Port Frames  Frames     Frames    PVID Priority Tagging  Name
--------- ------ -------- ------------ ---- -------- --------------------
1/1       No     No      No           1    0        Disabled Unit 1, Port 1
1/2       No     No      No           2    0        Disabled Unit 1, Port 2
1/3       No     No      No           1    0        Disabled Unit 1, Port 3
1/4       No     No      No           1    0        Disabled Unit 1, Port 4
1/5       No     No      No           1    0        Disabled Unit 1, Port 5
1/6       No     No      No           1    0        Disabled Unit 1, Port 6
1/7       No     No      No           1    0        Disabled Unit 1, Port 7
1/8       No     No      No           1    0        Disabled Unit 1, Port 8
1/9       No     No      No           1    0        Disabled Unit 1, Port 9
1/10      No     No      No          1    0        Disabled Unit 1, Port 10
1/11      No     No      No          1    0        Disabled Unit 1, Port 11
1/12      No     No      No          1    0        Disabled Unit 1, Port 12
1/13      No     No      No          1    0        Disabled Unit 1, Port 13
1/14      No     No      No          1    0        Disabled Unit 1, Port 14
1/15      No     No      No          1    0        Disabled Unit 1, Port 15
1/16      No     No      No          1    0        Disabled Unit 1, Port 16
1/17      No     No      No          1    0        Disabled Unit 1, Port 17
1/18     No     No      No          1    0        Disabled Unit 1, Port 18
```

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.

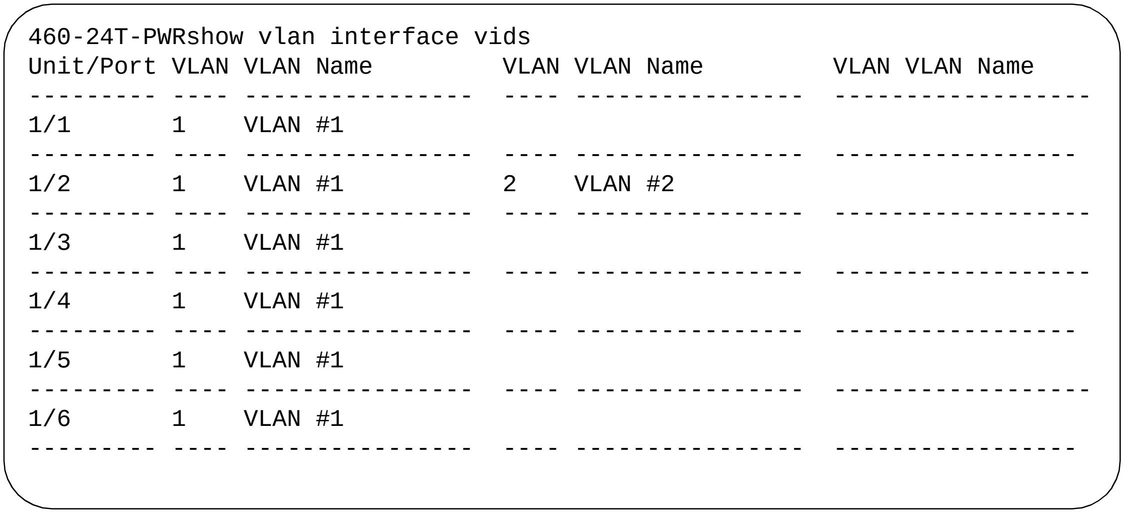
Table 104 describes the parameters and variables for the `show vlan interface vids` command.

Table 104 show vlan command interface vids 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 34 displays sample output from the `show vlan interface vids` command.

Figure 34 show vlan interface vids output



```
460-24T-PWRshow vlan interface vids
Unit/Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
--------- ---- ----------------  ---- ----------------  ------------------
1/1       1    VLAN #1
--------- ---- ----------------  ---- ----------------  -----------------
1/2       1    VLAN #1           2    VLAN #2
--------- ---- ----------------  ---- ----------------  ------------------
1/3       1    VLAN #1
--------- ---- ----------------  ---- ----------------  ------------------
1/4       1    VLAN #1
--------- ---- ----------------  ---- ----------------  -----------------
1/5       1    VLAN #1
--------- ---- ----------------  ---- ----------------  ------------------
1/6       1    VLAN #1
--------- ---- ----------------  ---- ----------------  -----------------
```

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 105 describes the parameters and variables for the `vlan mgmt` command.

Table 105 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.

vlan create command

Note: For guidelines for configuring STGs, VLANs, and MLTs, refer to Chapter 1 of the *Using the BayStack 460-24T-PWR Switch*.

The `vlan create` command allows you to create a VLAN. You create a VLAN by setting the state of a previously non-existent VLAN.

Note: You can configure as many as 255 protocol-based VLANs, with up to 14 different protocols.

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 106 describes the parameters and variables for the `vlan create` command.

Table 106 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.
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 BPS/460 stack mode. The Hybrid stack mode is not supported on this release of the BayStack 460-24T-PWR switch.

Note: This command fails if the VLAN already exists.

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 107 describes the parameters and variables for the `vlan delete` command.

Table 107 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 <2-4094>
```

The no vlan command is in the config command mode.

Table 108 describes the parameters and variables for the no vlan command.

Table 108 no vlan command parameters and variables

Parameters and variables	Description
<2-4094>	Enter the number of the VLAN to delete.

➡ **Note:** You cannot delete VLAN 1, which is the default management VLAN.

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 109 describes the parameters and variables for the vlan name command.

Table 109 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.

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 *Using the BayStack 460-24T-PWR Switch*.

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 *Using the BayStack 460-24T-PWR Switch*.

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}]
[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 110 describes the parameters and variables for the `vlan ports` command.

Table 110 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}	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 111 describes the parameters and variables for the `vlan members` command.

Table 111 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.

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.

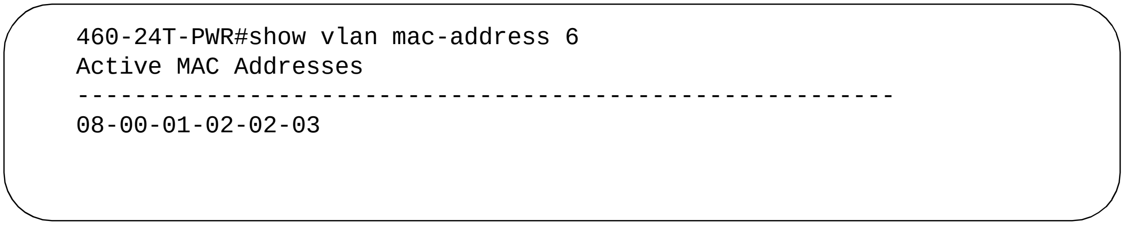
Table 112 describes the parameters and variables for the show vlan mac-address command.

Table 112 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 35 displays sample output from the show vlan mac-address command.

Figure 35 show vlan mac-address command output



```
460-24T-PWR#show vlan mac-address 6
Active MAC Addresses
---------------------------------------------------------
08-00-01-02-02-03
```

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 113 describes the parameters and variables for the `vlan mac-address` command.

Table 113 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 114 describes the parameters and variables for the `no vlan mac-address` command.

Table 114 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.

Displaying multicast membership

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 115 describes the parameters and variables for the `show vlan multicast membership` command.

Table 115 show vlan multicast membership command parameters and variables

Parameters and variables	**Description**
<1-4094>	Specifies the VLAN to display IP multicast sessions.

Figure 36 displays sample output from the `show vlan multicast membership` command.

Figure 36 show vlan multicast membership command output

```
460-24T-PWR#show vlan 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
```

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 195
- "default vlan igmp command" on page 196
- "vlan igmp unknown-mcast-no-flood command" on page 196
- "default vlan igmp unknown-mcast-no-flood command" on page 197

show vlan igmp command

The `show vlan igmp` command displays the IGMP snooping configuration and whether flooding of packets with unknown multicast addresses is enabled or disabled. The syntax for the `show vlan igmp` command is:

```
show vlan igmp {unknown-mcast-no-flood|<1-4094>}
```

The `show vlan igmp` command is in the privExec mode.

Table 116 describes the parameters and variables for the `show vlan igmp` command.

Table 116 show igmp command parameters and variables

Parameters and variables	**Description**
unknown-mcast-no-flood	Displays whether flooding of packets with unknown multicast addresses is enabled or disabled.
<1-4094>	Specifies IGMP setting for specified VLAN.

Figure 37 displays sample output from the `show vlan igmp` command.

Figure 37 show vlan igmp command output

```
460-24T-PWR#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>]
```

The `vlan igmp` command is in the config mode.

Table 117 describes the parameters and variables for the `vlan igmp` command.

Table 117 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.
v2-members <portlist>	Enter the list of ports for port membership for IGMP v2.

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>
```

The `default vlan igmp` command is in the config mode.

Table 118 describes the parameters and variables for the `default vlan igmp` command.

Table 118 default vlan igmp command parameters and variables

Parameters and variables	Description
<1-4094>	Enter the VLAN to default IGMP settings to factory default.

vlan igmp unknown-mcast-no-flood command

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 {enable|disable}
```

The `vlan igmp unknown-mcast-no-flood` command is in the config command mode.

Table 119 describes the parameters and variables for the `vlan igmp unknown-mcast-no-flood` command.

Table 119 vlan igmp unknown-mcast-no-flood command parameters and variables

Parameters and variables	Description
enable|disable	Enter whether you want to enable or disable the flooding of packets with unknown multicast addresses. Note**:** The default parameter is enabled.

default vlan igmp unknown-mcast-no-flood command

The `default vlan igmp unknown-mcast-no-flood` command enables flooding of packets with unknown multicast address. The syntax for the `default vlan igmp unknown-mcast-no-flood` command is:

```
default vlan igmp unknown-mcast-no-flood
```

The `default vlan igmp unknown-mcast-no-flood` command is in the privExec command mode.

The `default vlan igmp unknown-mcast-no-flood` command has no parameters or variables.

Chapter 7
RMON

This chapter describes how to display and configure RMON settings. This chapter covers the following topics:

- "Displaying RMON settings," next
- "Setting RMON parameters" on page 203

Displaying RMON settings

You the RMON settings using the NNCLI. This section covers the following topics:

- "show rmon alarm," next
- "show rmon event" on page 200
- "show rmon history" on page 201
- "show rmon stats" on page 202

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

Figure 38 show rmon alarm command output

```
460-24T-PWR#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 39 displays a sample output of the `show rmon event` command.

Figure 39 show rmon event command output

```
460-24T-PWR#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:

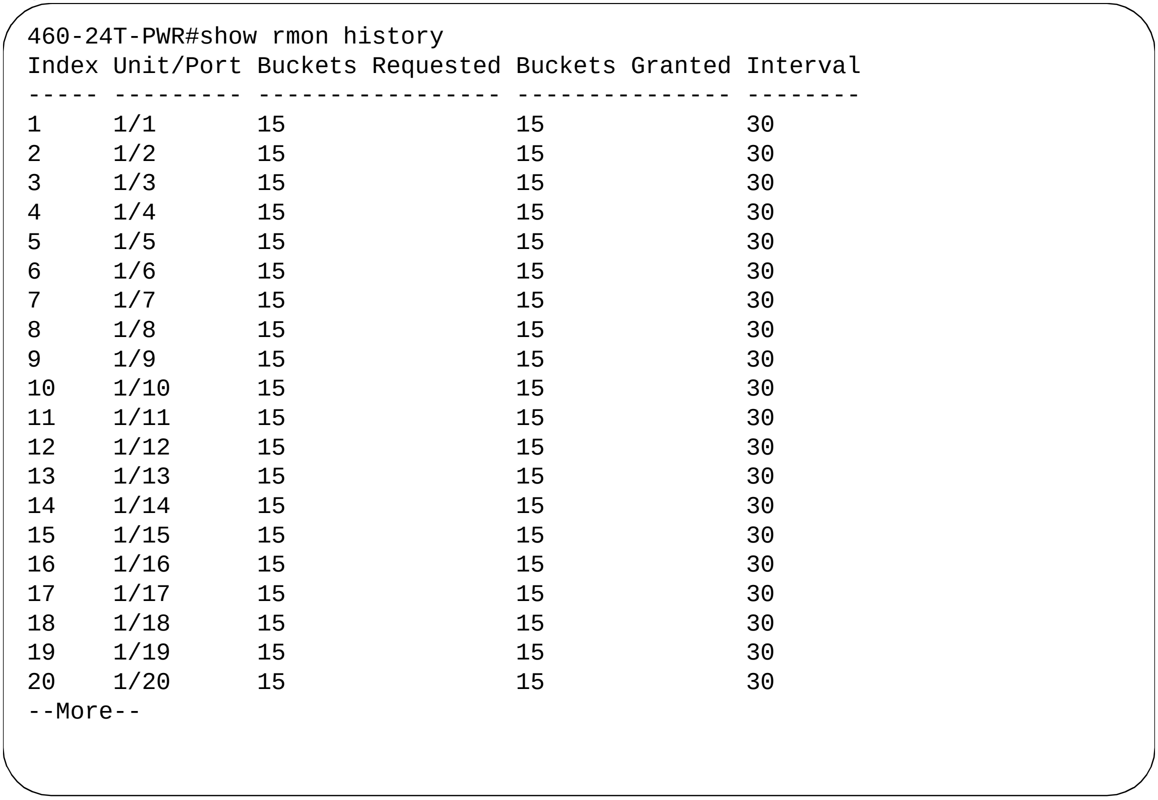
```
show rmon history
```

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

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

Figure 40 displays a sample output of the `show rmon history` command.

Figure 40 show rmon history command output



```
460-24T-PWR#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 41 displays a sample output of the show rmon stats command.

Figure 41 show rmon stats command output

```
460-24T-PWR#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--
```

Setting RMON parameters

You set the RMON parameters for alarms, events, history, and statistics using the NNCLI. This section covers the following topics:

- "rmon alarm," next
- "no rmon alarm" on page 204
- "rmon event" on page 205
- "no rmon event" on page 205
- "rmon history" on page 206
- "no rmon history" on page 206
- "rmon stats" on page 207
- "no rmon stats" on page 207

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 120 describes the parameters and variables for the `rmon alarm` command.

Table 120 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.

Table 120 rmon alarm command parameters and variables (continued)

Parameters and variables	Description
absolute|delta	Enter the comparison you want: • absolute— value of the MIB object compared directly with thresholds • delta—change in the value of the MIB object between samples 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 will be 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 will be triggered.
owner <LINE]	Specify an owner string to identify the alarm entry.

no rmon alarm

The `no rmon alarm` command turns off the RMON alarms. 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 121 describes the parameters and variables for the `no rmon alarm` command.

Table 121 no rmon alarm command parameters and variables

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

rmon event

The `rmon event` 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 122 describes the parameters and variables for the `rmon event` command.

Table 122 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` turns off RMON event log and trap settings. 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 123 describes the parameters and variables for the `no rmon event` command.

Table 123 no rmon event command parameters and variables

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

rmon history

The `rmon history` 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 124 describes the parameters and variables for the `rmon history` command.

Table 124 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` turns off RMON history. 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 125 describes the parameters and variables for the `no rmon history` command.

Table 125 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 statistics 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 126 describes the parameters and variables for the `rmon stats` command.

Table 126 rmon stats command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the stats entry.
<port>	Specify a port for the stats.
owner <LINE>	Specify 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 entries in the table 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 127 describes the parameters and variables for the `no rmon stats` command.

Table 127 no rmon stats command parameters and variables

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

Chapter 8
Policy-enabled networks and QoS

This chapter describes how to configure Quality of Service (QoS) parameters for policy-enabled networks. This chapter covers the following topics:

- "Displaying QoS parameters," next
- "Resetting" on page 221
- "Configuring COPS" on page 221
- "Configuring QoS interface groups" on page 226
- "Configuring DSCP and 802.1p and queue associations" on page 229
- "Configuring QoS filters and filter groups" on page 231
- "Configuring QoS actions" on page 237
- "Configuring QoS meters" on page 238
- "Configuring QoS shapers" on page 239
- "Gathering QoS statistics" on page 241
- "Configuring QoS policies" on page 242
- "Reordering packets" on page 244

Refer to the *Using the BayStack 460-24T-PWR Switch* for more information on policy-enable networks, Differentiated Services, and QoS. Refer to *Using Web-based Management for the BayStack 460-24T-PWR Switch* for information on configuring these features using the Web-based management system, and refer to *Reference for the BayStack 460-24T-PWR Switch Management Software* 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 128 describes the parameters and variables for the show qos command.

Table 128 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.
queue-set-assignments	Displays 802.1p priority-to-queue assignments by queue set.

Table 128 show qos command parameters and variables (continued)

Parameters and variables	Description
agent	Displays QoS agent configuration parameters.
statistics	Displays QoS policy statistics.

Figure 42 displays sample output from the `show qos interface-groups` command.

Figure 42 show qos interface-groups command output

```
460-24T-PWR#show qos interface-groups
     Role         Interface              Capabilities                Storage
  Combination       Class                                              Type
_______________ ____________ ____________________________________ ___________
allBPSIfcs      Untrusted    Input 802, Input IP                  Read Only
```

Figure 43 displays sample output from the `show qos interface-assignments` command.

Figure 43 show qos interface-assignments command output

```
460-24T-PWR#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 44 displays sample output from the `show qos if-assign-list` command.

Figure 44 show qos if-assign-list command output

```
400-24T-PWR#show qos if-assign-list
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 45 displays sample output from the `show qos egressmap` command.

Figure 45 show qos egressmap command output

```
460-24T-PWR#show qos egressmap
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 46 displays sample output from the `show qos ingressmap` command.

Figure 46 show qos ingressmap command output

```
460-24T-PWR#show qos ingressmap
802.1p Priority DSCP

_______________ ____
0               0
1               0
2               10
3               18
4               26
5               34
6               46
7               48
```

Figure 47 displays sample output from the `show qos ip-filters` command.

Figure 47 show qos ip-filters command output

```
460-24T-PWR#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 48 displays sample output from the `show qos ip-filter-sets` command.

Figure 48 show qos ip-filter-sets command output

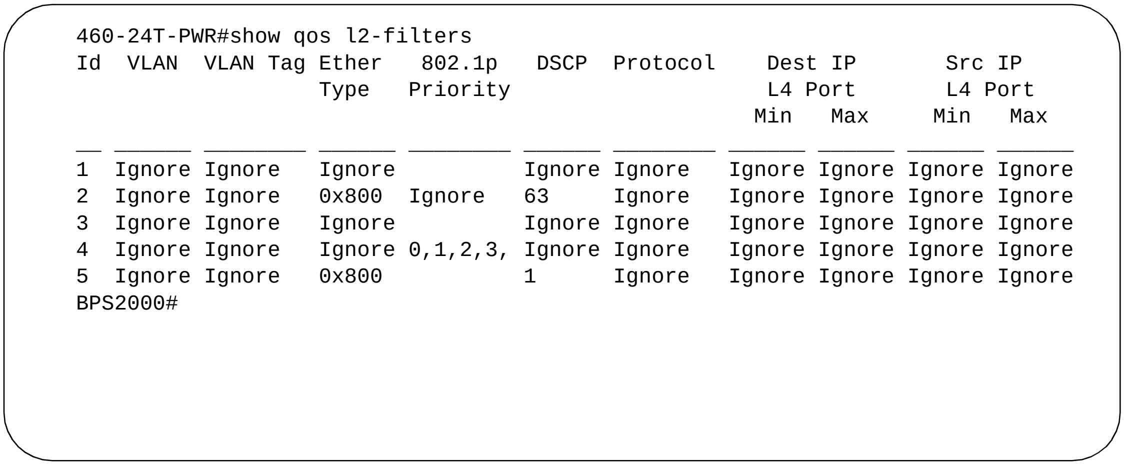
```
460-24T-PWR#show qos ip-filter-sets
IP Filter Sets

Id         Name        Acl Id Ace Id Ace Order

___ ________________ ______ ______ _________
2   G1-ip            1      2      2
```

Figure 49 displays sample output from the `show qos l2-filters` command.

Figure 49 show qos l2-filters command output

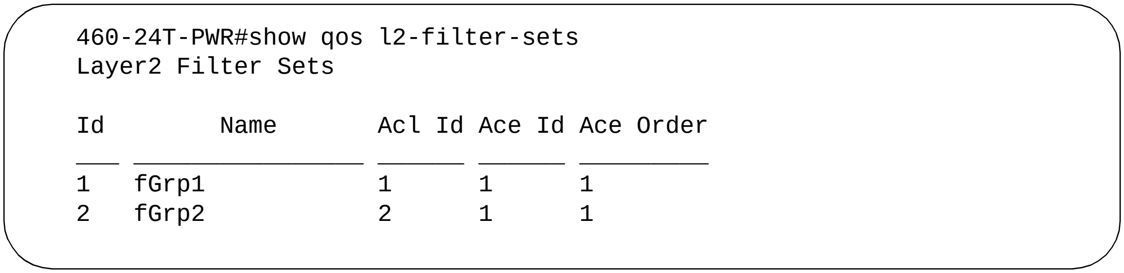


```
460-24T-PWR#show qos l2-filters
Id  VLAN  VLAN Tag Ether   802.1p   DSCP  Protocol    Dest IP       Src IP
                   Type   Priority                    L4 Port       L4 Port
                                                     Min   Max     Min   Max

__ ______ ________ ______ ________ ______ ________ ______ ______ ______ ______
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
BPS2000#
```

Figure 50 displays sample output from the `show qos l2-filter-sets` command.

Figure 50 show qos l2-filter-sets command output



```
460-24T-PWR#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 51 displays sample output from the `show qos actions` command. Each service class has a default action that uses default mappings.

Figure 51 show qos actions command output

```
460-24T-PWR#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 52 displays sample output from the `show qos meters` command. Each service class has a default meter that uses default actions and mappings.

Figure 52 show qos meters command output

```
460-24T-PWR#show qos meters
 Id         Name         Data   Commit Commit  In-Profile Out-Profile
                              Spec    Rate   Burst      Action           Action
                             (Kbps)(Bytes)

_____ ________________ ________ ______ __  ________________ ____
1     practice         Metered  3000 2047
65526 Drop_Traffic     No Meter 0     0    Drop_Traffic
65527 Standard_Service No Meter 0     0    Standard_Servic
65529 Bronze_Service   No Meter 0     0    Bronze_Service
65530 Silver_Service   No Meter 0     0    Silver_Service
65531 Gold_Service     No Meter 0     0    Gold_Service
65532 Platinum_Service No Meter 0     0    Platinum_Servic
65533 Premium_Service  No Meter 0     0    Premium_Service
65534 Network_Service  No Meter 0     0    Network_Service
```

Figure 53 displays sample output from the `show qos shapers` command.

Figure 53 show qos shapers command output

```
460-24T-PWR#show qos shapers
Id         Name              Rate          Burst          Queue
                                           Size            Size
                            (Kbps)        (Bytes)         (Packets)

___ ___________________________ ___________ ________________ _________________
1          shaper1           64000         5555              2
```

Figure 54 displays sample output from the `show qos policies` command.

Figure 54 show qos policies command output

```
460-24T-PWR#show qos policies

Id     Name    State     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  Track
                Action         Action                 Group   Stats

___ _________  ____________  ______________ ________  _____   ____
1              Standard_Servi                          0
2              Standard_Servi                          0
```

Figure 55 displays sample output from the `show qos queue-sets` command.

Figure 55 show qos queue-sets command output

```
460-24T-PWR#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 56 displays sample output from the `show qos queue-set-assignments` command.

Figure 56 show qos queue-set-assignments command output

```
460-24T-PWR#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 57 displays sample output from the `show qos agent` command.

Figure 57 show qos agent command output

```
460-24T-PWR#show qos agent
QoS Policy Server Control: Enabled
QoS Policy Agent Retry Timer: 5 seconds
Allow Packet Reordering: Enabled
Maintain Policing Statistics: Enabled
```

Figure 58 displays sample output from the `show qos statistics` command.

Figure 58 show qos statistics command output

```
460-24T-PWR#show qos statistics

Id  Name      Packet    Overflow    Total      Total    InProfile
           Hits      Packet     Octets    Overflow    Octets
                      Hits                Octets

___ _________ ______ __________ __________ __________ __________
1   wizardIP   0          0          0          0          0
2   wizardL2   0          0          0          0          0

Id Name    Overflow  OutProfile  Overflow   Shaping    Overflow
          InProfile    Octets   OutProfile  Q Drops    Shaping
           Octets                 Octets               Q Drops

_________ __________ __________ __________ __________ __________
1 wizardIP   0          0          0          0          0
2 wizardL2   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 222
- "show cops server command" on page 223
- "show cops stats command" on page 223
- "cops retry command" on page 223
- "cops server command" on page 224
- "default cops retry command" on page 224
- "no cops server command" on page 225

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 129 describes the parameters and variables for the `qosagent server-control` command.

Table 129 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.

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.

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.

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 130 describes the parameters and variables for the cops retry command.

Table 130 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 131 describes the parameters and variables for the `cops server` command.

Table 131 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 132 describes the parameters and variables for the `default cops server` command.

Table 132 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 133 describes the parameters and variables for the `no cops server` command.

Table 133 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.

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 227
- "qos if-assign-list command" on page 228

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 name <tag> {add|del} [port <portlist>]
```

The `qos if-assign` command is in the config-if command mode.

Table 134 describes the parameters and variables for the `qos if-assign` command.

Table 134 qos if-assign command parameters and variables

Parameters and variables	**Description**
name <tag>	Enter the name of the defined interface group.
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.

qos if-group command

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 135 describes the parameters and variables for the `qos if-group` command.

Table 135 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 name <tag> {add|del} [portlist
<portlist>]
```

The `qos if-assign-list` command is in the config-if command mode.

Table 136 describes the parameters and variables for the `qos if-assign-list` command.

Table 136 qos if-assign-list command parameters and variables

Parameters and variables	Description
name <tag>	Enter the name of the defined interface group.
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.

Note: You cannot delete interface groups that are referenced by an installed policy or associated with device interfaces.

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 230
- "qos queue-set-assignment command" on page 230

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 137 describes the parameters and variables for the `qos egressmap` command.

Table 137 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 138 describes the parameters and variables for the qos ingressmap command.

Table 138 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 139 describes the parameters and variables for the `qos queue-set-assignment` command.

Table 139 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 233
- "qos l2-filter command" on page 234
- "qos l2-filter-set command" on page 236

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 140 describes the parameters and variables for the `qos ip-filter` command.

Table 140 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.
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.
You cannot delete an IP filter that is referenced by an IP filter set.

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 141 describes the parameters and variables for the `qos ip-filter-set` command.

Table 141 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.

Note: You can reference up to 32 VLANs with a single layer 2 filter.

Table 142 describes the parameters and variables for the `qos l2-filter` command.

Table 142 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.

Table 142 qos l2-filter command parameters and variables (continued)

Parameters and variables	**Description**
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.
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 143 describes the parameters and variables for the `qos l2-filter-set` command.

Table 143 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.
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.

Note: 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.

Configuring QoS actions

You can configure QoS actions, which directs the BayStack 460-24T-PWR switch 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 144 describes the parameters and variables for the `qos action` command.

Table 144 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 default.
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 use default.

➡ **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 145 describes the parameters and variables for the `qos meter` command.

Table 145 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 size in Kb/s for in-profile traffic; range is 1 to 65535 Kb/s

Table 145 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.

➡ You cannot delete a meter that is referenced in an installed policy.

Configuring QoS shapers

➡ **Note:** You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA 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 146 describes the parameters and variables for the `qos shaper` command.

Table 146 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 size in bytes; range is 0 to 42949672955 bytes.
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.

➡ 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 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 147 describes the parameters and variables for the `qosagent police-statistics` command.

Table 147 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>]
[track-statistics {enable|disable}]order <order>|
delete|enable|disable}
```

The `qos policy` command is in the config command mode.

Table 148 describes the parameters and variables for the `qos policy` command.

Table 148 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 148 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.
track-statistics {enable|disable}	Enables maintaining policing statistics on the specified flow. Default is based on value of setting of `qosagent police-statistics` command.
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 149 describes the parameters and variables for the `qosagent packet-reordering` command.

Table 149 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.

Appendix A
Command List

This appendix provides the complete NNCLI 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 150 CLI command list

Command	**Page No.**
auto-pvid	page 188
autotopology	page 109
boot [default] [unit <unitno>]	page 78
clear logging [nv]	page 98
clear-stats [port<portlist>]	page 101
cli-password {switch|stack} {ro|rw} <WORD> <WORD> cli-password {switch|stack} {serial|telnet} {none|local|radius}	page 43
configure {terminal|network|memory}	page 49
configure network [load-on-boot {disable|use-bootp|use-config}] configure network [filename <WORD>] configure network [address <XXX.XXX.XXX.XXX>]	page 64
cops retry	page 223
cops server	page 224
copy config nvram	page 118
copy config tftp [address <XXX.XXX.XXX.XXX>] filename <WORD>	page 82
copy tftp config [address <XXX.XXX.XXX.XXX>] filename <WORD>	page 83
default autotopology	page 110
default cops retry	page 224

Table 150 CLI command list (continued)

Command	Page No.
default cops server	page 225
default duplex [port <portlist>]	page 108
default flowcontrol [port <portlist>]	page 112
default ip address unit <1-8>	page 72
default ip bootp server	page 80
default mac-address-table aging-time	page 56
default name [port <port.ist>]	page 104
default rate-limit [port <portlist>]	page 116
default set logging	page 98
default snmp trap link-status [port <portlist>]	page 95
default spanning-tree [stp <1-8>] [forward-time] [hello-time] [max-age] [priority] [tagged-bpdu]	page 165
default spanning-tree [port <portlist>] [stp <1-8>] [learning] [cost] [priority]	page 169
default speed [port <portlist>]	page 106
default telnet-access	page 76
default terminal {speed|length|width}	page 61
default vlan igmp <1-4094>	page 196
default vlan igmp unknown-mcast-no-flood	page 197
default vlan mgmt <1-4094>	page 183
disable	page 50
download [[address <ip>] {image <filename>|diag <filename>|image-if-newer <filename> |poe_module_image <filename>}]	page 84
duplex [port <portlist>] {full|half|auto}	page 107
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 151
enable	page 49
end	page 50
exit	page 51
flowcontrol [port <portlist>] {asymmetric|symmetrid|auto|disable}	page 110
help	page 47
interface FastEthernet {<portlist>}	page 50

Table 150 CLI command list (continued)

Command	Page No.
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 79
ip default-gateway <XXX.XXX.XXX.XXX>	page 68
ipmgr list {telnet|snmp|http}	page 140
ipmgr list {source-ip <1-10> <XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]}	page 141
logout	page 48
mac-address-table aging-time <time>	page 55
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 145
mac-security [port <portlist>] {disable|enable|learning}	page 149
mac-security mac-address-table address <H.H.H.> {port <portlist>|security-list <1-32>}	page 146
mac-security security-list <1-32> mac-security security-list <portlist>	page 147
mac-security mac-da-filter	page 150
mlt <id> [name <trunkname>] [enable|disable] [member <portlist>]	page 172
name [port <portlist>] <LINE>	page 103
no auto-pvid	page 188
no autotopology	page 109
no cops server	page 225
no flowcontrol [port <portlist>]	page 111
no ip address {stack|switch}	page 67
no ip address unit <1-8>	page 71
no ip bootp server	page 80
no ip default-gateway	page 68
no ipmgr {telnet|snmp|http}	page 140
no ipmgr {source IP [<1-10>]}	page 142
no mac-security	page 147
no mac-security mac-address-table {address <H.H.H>|port <portlist>|security-list <1-32>]	page 147
no mac-security security-list <1-32>	page 148

Table 150 CLI command list (continued)

Command	Page No.
no mlt [<id>]	page 173
no name [port <portlist>]	page 104
no port-mirroring	page 176
no poe-shutdown [port <portlist>]	page 133
no poe-trap [unit <1-8>	page 132
no radius-server	page 155
no rate-limit [port <portlist>]	page 115
no rmon alarm [<1-65535>]	page 204
no rmon event [<1-65535>]	page 205
no rmon history [<1-65535>]	page 206
no rmon stats [<1-65535>]	page 207
no set logging	page 97
no shutdown [port <portlist>]	page 102
no snmp server [authentication-trap|community [ro|rw] contact|host [<host-ip> <community-string>] [location|name]	page 92
no snmp trap link-status [port <portlist>]	page 94
no spanning-tree [port <portlist>] [stp <1-8>]	page 170
no telnet-access [source-ip [<1-10>]]	page 76
no tftp-server	page 82
no vlan <2-4094> no vlan mac-address <1-4094> address <H.H.H.>	page 187 page 192
no web-server	page 77
ping <XXX.XXX.XXX.XXX>	page 62
poe poe-dc-source-conf [unit <1-8>] {powersharing|rpsu|ups}	page 127
poe poe-dc-source-type [unit <1-8>] {baystack10|nes}>	page 125
poe poe-pd-detect-type [unit <1-8>] {802dot3af|802dot3af_and_legacy}	page 128
poe poe-limit [unit <1-8>] <3-20>	page 136
poe poe-power-pairs [unit <1-8>] {spare|signal}	page 129
poe poe-power-usage-threshold [unit <1-8>] <1-99>	page 130
poe poe-priority [port <portlist>] {low|high|critical}	page 135
poe poe-shutdown [port <portlist>]	page 134

Table 150 CLI command list (continued)

Command	Page No.
poe poe-trap [unit <1-8>]	page 131
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 174

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 237

qos egress map ds <dscp> 1p <ieee1p> dp <dropprec>	page 229
qos if-assign name <tag> {add|del} [port <portlist>]	page 226
qos if-assign-list name <tag> {add|del} [portlist <portlist>]	page 228
qos if-group name <tag> {create <ifclass>|delete}	page 227
qos ingress map 1p <ieee1p> ds <dscp>	page 230

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 231

qos ip-filter-set <fgid> {create set <setid> [name <setname>] filter-id <fid> filter-prec <prec>}
qos ip-filter-set <fgid> {delete}
	page 233

Table 150 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 234

qos l2-filter-set <fgid> {create set <setid> [name <setname>] filter-id <fid> filter-prec <prec>}
qos l2-filter-set <fgid> {delete}
	page 236

qos meter <metid> {create [name <metname>] committed-rate <rate> max-burst-rate <burstrate> [max-burst-duration <burstdur>] |delete}	page 238

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 <shhapeid>|shaper-name <shapename>] [shaper-group <shapegroup>] [track-statistics {enable|disable} order <order>}
qos policy <polid> {delete}
	page 242

qos queue-set-assignment queue-set <setid> 1p <ieee1p> queue <qid>	page 230
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}	page 239
qosagent packet-reordering {enable|disable}	page 244
qosagent police-statistics {enable|disable}	page 241
qosagent reset-default	page 221
qosagent server-control {enable|disable| [retry-timer <no-retry|1-86400>]	page 222
radius-server host <address> [secondary-host <address>] port <num> key <string>	page 155
rate-limit [port <portlist>] {multicast <pct>|broadcast <pct>|both <pct>}	page 114
renumber unit	page 53
rmon alarm <1-65535> <WORD> <1-2147483647> [absolute|delta] rising-threshold <-2147483647-2147483648> [<1-65535>] falling-threshold <-2147483647-2147483648> [<1-65535>] [owner <LINE>]	page 203
rmon event <1-65535> [log] [trap] [description <LINE>] [owner <LINE>]	page 205
rmon history <1-65535> <LINE> <1-65535> <1-3600> [owner <LINE>]	page 206

Table 150 CLI command list (continued)

Command	**Page No.**
rmon stats <1-65535> <LINE> [owner <LINE>]	page 207
set logging [enable|disable] [level critical|serious|informational] [nv-level critical|serious|informational|none]	page 97
show config-network	page 65
show cops retry	page 222
show cops server	page 223
show cops stats	page 223
show eapol	page 151
show interfaces [names] [<portlist>]	page 89
show ip [bootp] [default-gateway] [address [stack|switch]]	page 69
show ipmgr	page 138
show logging [critical] show logging [serious] show logging [informational]	page 96
show mac-address-table [aging-time] show mac-address-table [vid <1-4094>] [address <H.H.H.>]	page 54
show mac-security {config|mac-address-table [addr <macaddr>]|port|security-lists}	page 143
show mac-security mac-da-filter	page 144
show mlt [utilization <1-6>]	page 171
show poe-main-status [unit <1-8>]	page 120
show poe-port-status [ports <portlist>]	page 121
show poe-power-measurement [ports <portlist>]	page 123
show port-statistics [port <portlist>]	page 99

Table 150 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 210
show radius-server	page 154
show rate-limit	page 113
show rmon alarm	page 199
show rmon event	page 200
show rmon history	page 201
show rmon stats	page 202
show spanning-tree {stp <1-8>] {config|port}	page 159
show-stack-info	page 53
show stack-oper-mode	page 57
show sys-info	page 52
show telnet-access	page 74
show terminal	page 60
show tftp-server	page 81
show vlan igmp {unknown-mcast-no-flood|<1-4094>}	page 194
show vlan interface info [<portlist>]	page 180
show vlan interface vids [<portlist>]	page 182
show vlan mac-address <1-4094> [<H.H.H>]	page 191
show vlan multicast membership <1-4094>	page 191

Table 150 CLI command list (continued)

Command	**Page No.**
shutdown [port <portlist>]	page 101
snmp trap link-status [port <portlist>]	page 93
snmp-server {{enable|disable}|authentication-trap|community <community-string> [ro|rw] contact <text>|host <host-ip> <community-string>|location >text>|name <text>}	page 91
spanning-tree [stp <1-8>] add-vlan <1-4094>	page 166
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>]	page 164
spanning-tree [port <portlist>] [stp <1-8>] [learning {disable|normal|fast}] [cost <1-65535>] [priority <0-255>]	page 168
spanning-tree [stp <1-8>] remove-vlan <1-4094>	page 167
spanning-tree stp <2-8> create	page 161
spanning-tree stp <2-8> delete	page 162
spanning-tree stp <2-8> disable	page 163
spanning-tree stp <2-8> enable	page 162
speed [port <portlist>] {10|100|1000|auto}	page 105
stack bootp-mac-addr-type {base-unit|stack}	page 79
stack oper-mode {bps2000|hybrid}	page 58
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 75
terminal {2400|4800|9600|19200|38400}|length <1-132>|width <1-132>	page 61
tftp-server <XXX.XXX.XXX.XXX>	page 82

Table 150 CLI command list (continued)

Command	Page No.
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 184
vlan create <1-4094> name <line> type macsa 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 <4096-65534> vlan create <1-4094> name <line> type protocol-vinesEther2 vlan create <1-4094> name <line> type protocol-xnsEther2	page 184

Table 150 CLI command list (continued)

Command	Page No.
vlan create <1-4094> type macsa learning IVL 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	page 184
vlan create <1-4094> type macsa learning SVL 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	page 184

Table 150 CLI command list (continued)

Command	Page No.
vlan create <1-4094> name <line> type macsa learning IVL 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	page 184
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 <4096-65534> 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 184
vlan delete <1-4094>	page 186

Table 150 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>]	page 195
vlan igmp unknown-mcast-no-flood {enable|disable}	page 196
vlan mac-address <1-4094> address <H.H.H>	page 192
vlan members <1-4094> <portlist> vlan members add <1-4094> <portlist> vlan members remove <1-4094> <portlist>	page 190
vlan mgmt <1-4094>	page 183
vlan name <1-4094> <line>	page 187
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 189
web-server{enable|disable}	page 77

Index