Part No. 216339-A
December 2003

4655 Great America Parkway
Santa Clara, CA 95054

Reference for the BayStack 380-24T and 24F Command Line Interface, Software Version 3.0

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

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

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

Trademarks

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

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

Java is a trademark of Sun Microsystems, Inc.

Acrobat and Adobe are trademarks of Adobe Systems, Inc.

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

Restricted rights legend

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

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

Statement of conditions

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

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

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

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

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

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 380-24T 10/100/1000 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 380 10/100/1000 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 380 10/100/1000 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 Nortel Networks* BayStack 380 10/100/1000 Switch* command line interface (CLI) is one tool used to configure and manage a BayStack 380 Switch. The CLI allows you to set up, configure, and manage your BayStack 380.

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 380 10/100/1000 Switch Management Software Version 3.0, Using Web-based Management for the BayStack 380 10/100/1000 Switch Software Version 3.0,* and *Using the BayStack 380 10/100/1000 Switch Software Version 3.0*.

For general information on using and configuring the BS 380, refer to *Using the BayStack 380 10/100/1000 Switch Software Version 3.0.*

About this guide

This guide provides information about using the features and capabilities of the CLI to manage switching operations in the BayStack 380, 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 380 10/100/1000 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 380 Switch, refer to the following publications:

- *Release Notes for the BayStack 380 10/100/1000 Switch Software Version 3.0* (part number 212864-C)
- *Installing the BayStack 380-24T 10/100/1000 Switch* (part number 212794-A)
- *Using the BayStack 380 10/100/1000 Switch Software Version 3.0* (part number 212791-C)
- *Getting Started with the BayStack 380 10/100/1000 Switch Management Software Operations* (part number 213909-A)
- *Reference for the BayStack 380 10/100/1000 Switch Management Software Version 3.0* (part number 212789-C)
- *Using Web-based Management for the BayStack 380 10/100/1000 Switch Software Version 3.0* (part number 212792-C)
- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (part number 312865-B)

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. (The product family for the BayStack 380 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.

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 380 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 380 10/100/1000 Switch Management Software Version 3.0*. For more information on using the Web-based management system, refer to *Using Web-based Management for the BayStack 380-24T 10/100/1000 Switch Software Version 3.0*. For more information on using the CI menus, refer to *Using the BayStack 380 10/100/1000 Switch Software Version 3.0*.

The BayStack 380 command line interface (CLI) is a management tool that provides methods for configuring, managing, and monitoring the operational functions of the switch. You access the CLI through a direct connection to the switch console port, or remotely using Telnet. For a complete, alphabetical list of CLI commands, refer to Appendix A.

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

- By downloading a CLI script file from a tftp server.
- By pasting a series of CLI commands into the terminal emulator window.

This chapter discusses the following CLI topics:

- "Basic navigation" on page 33
- "Managing basic system information" on page 40
- "Managing MAC address forwarding database table" on page 41

CLI command modes

Most CLI commands are available only under a certain command mode. The BayStack 380 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 380. 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 not to the User EXEC mode. The commands in this mode allow you to perform basic switch-level management tasks, such as downloading the software image and booting the BayStack 380. The Privileged EXEC mode is also referred to as privExec mode.

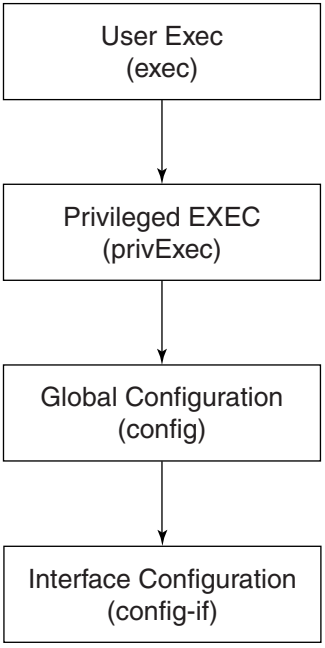
The last two command modes, Global Configuration and Interface Configuration, allow you to change the configuration of the BayStack 380. Changes made in these command modes are immediately applied to the switch configuration and saved to non-volatile memory.

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 and duplex mode. The Interface Configuration mode is also referred to as config-if mode.

Figure 1 provides an illustration of the hierarchy of BayStack 380 CLI command modes.

Figure 1 CLI command mode hierarchy



10194EA

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)	`BS380>`	• Default mode, automatically enter • `logout` or `exit` to quit CLI
Privileged EXEC (privExec)	`BS380#`	• `enable` to enter from User EXEC mode • `logout` or `exit` to quit CLI
Global Configuration (config)	`BS380(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)	`BS380(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, `BayStack 380`, and the current CLI command mode:

- User EXEC—`BS380>`
- Privileged EXEC—`BS380#`
- Global Configuration—`BS380(config)#`
- Interface Configuration—`BS380(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 380 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 380 operates in standalone mode. The BayStack 380 has 24 10/100/1000 Mb/s or 24 1000 Mb/s ports on the front. Thus, you have a maximum of 24 ports on one BayStack 380.

The CLI uses the variable `<portlist>` when a command specifies one or more ports for the command.

Port numbering in standalone mode

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

- A single port number—an integer between 1 through 24
  - Example: `7` means port 7
- A range of port numbers—a pair of port numbers between 1 and 24 separated by a dash
  - Example: `1-3` means ports 1, 2, and 3
  - Example: `5-24` means all ports from port 5 through port 24
- A list of port numbers and/or port ranges, separated by commas
  - Example: `1,3,7` means ports 1, 3, and 7
  - Example: `1-3,9-11` means ports 1, 2, 3, 9, 10, and 11
  - Example: `1,3-5,9-11,15` means ports 1, 3, 4, 5, 9, 10, 11, and 15
- `none` means no ports (not case-sensitive)
- `all` means all the ports on the standalone BayStack 380 (not case-sensitive)

IP notation

You enter IP addresses and subnet masks in dotted decimal notation (XXX.XXX.XXX.XXX), specifying both the IP address and the subnet mask in dotted-decimal notation.

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 380 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 380, the banner appears (Figure 2).

Figure 2 BayStack 380 banner

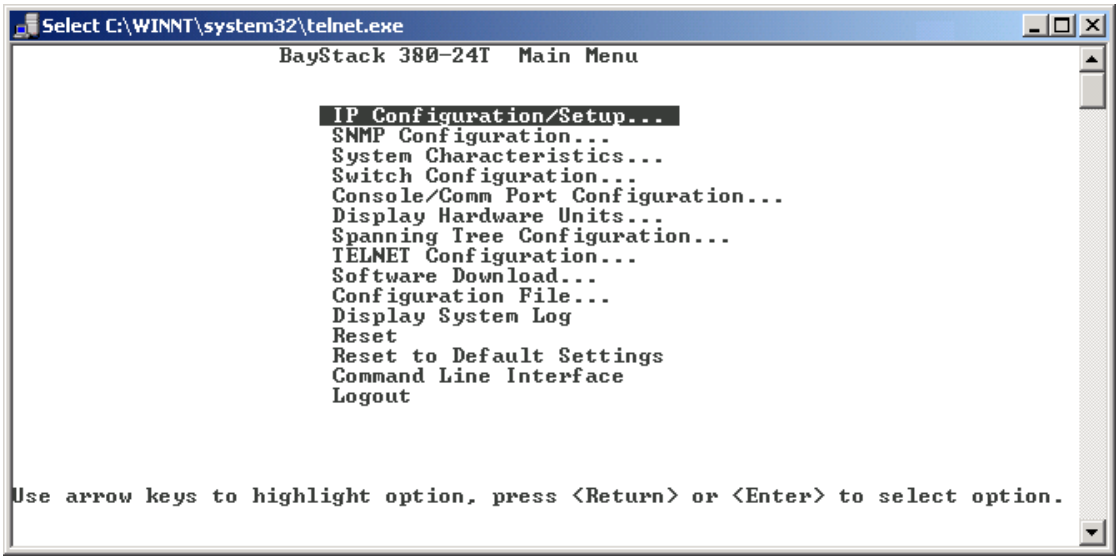
```
******************************************************
* Nortel Networks
* Copyright (c) 1996 - 2003
* All Rights Reserved
* BayStack 38024T 10/100/1000 Switch
* Ver: HW:Rev X    FW:3.0.0.5    SW:v3.0.0.28
************************************************************



Enter Ctrl-Y to begin.
```

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

Figure 3 Main Menu for BayStack 380 console interface



3 Using the Down Arrow key, scroll down to Command Line Interface, and press [Enter]. The CLI cursor appears:

```
BS380>
```

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 26, to select the command mode you want to use (and are authorized to use).

Setting the CLI password

You can set passwords for access through the serial console port or telnet access using the `cli password` command for selected types of access using the local 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 the switch:

- 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 {ro|rw} <WORD> <WORD>

cli password {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
ro|rw	Specifies you are modifying the read-only (ro) password or the read-write (rw) password.
<username> <password>	Enter your username for the first variable, and your password for the second variable. The username is not used, but it must be present.
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 35 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

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 35 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. 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

Table 3 Keystroke navigation

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

help command

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

```
help
```

The `help` command has no parameters or variables.

Figure 4 shows the output from the `help` command.

Figure 4 help command output in privExec mode

```
BS380#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.

Note: You must have read-write access to the BayStack 380 switch to be able to use the `enable` command.

configure command

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

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

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	Specifies the source for the configuration commands for the BayStack 380: • 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

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.

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. The following topic is covered:

- "show sys-info command," next

show sys-info command

The `show sys-info` command displays the current system characteristics. The syntax for the `show sys-info` command is:

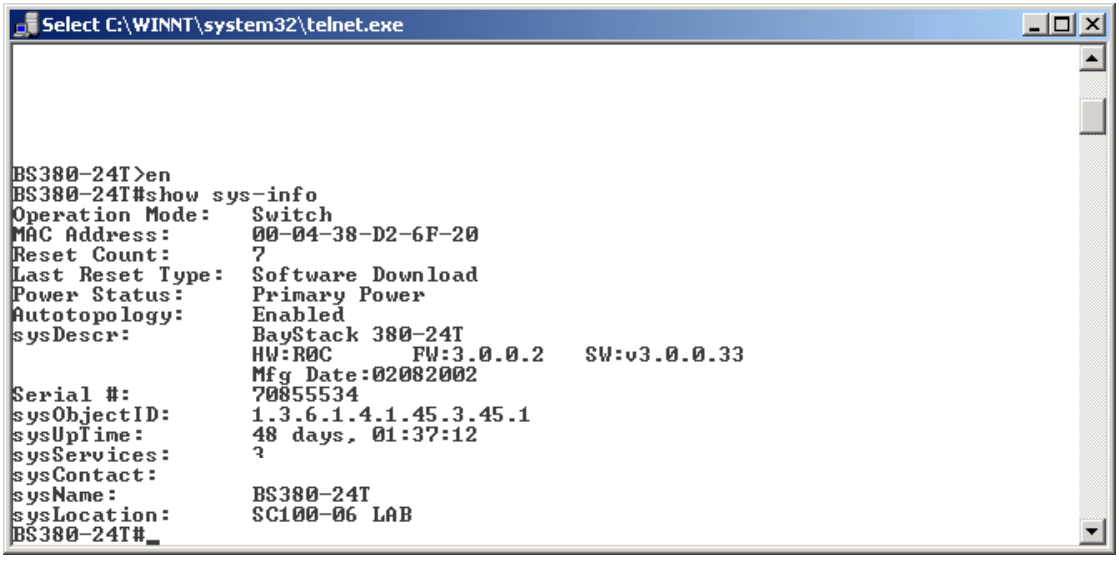
```
show sys-info
```

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



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

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 43
- "default mac-address-table aging-time command" on page 44

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 6 displays sample output from the `show mac-address-table` command.

Figure 6 show mac-address-table command output

```
BayStack 380 3.0#show mac-address-table
Mac Address Table Aging Time: 300
Number of addresses: 61

   MAC Address      Port            MAC Address      Port
-----------------  -----        -----------------  -----
00-00-81-bc-ea-81  14           00-00-81-c1-9b-81  14
00-00-81-c1-f6-81  14           00-00-a2-8d-7b-9b  14
00-00-a2-f8-4d-c0  14           00-03-4b-40-6b-f4  14
00-04-dc-72-c3-f4  14           00-04-dc-72-cf-f4  14
00-04-dc-72-db-f4  14           00-04-dc-74-33-f4  14
00-08-c7-20-29-8e  14           00-60-f3-20-15-9b  14
00-80-2d-06-e5-39  14           00-80-2d-06-f3-1c  14
00-80-2d-0a-03-f4  14           00-80-2d-22-0c-40  14
00-80-2d-22-0e-00  14           00-80-2d-22-23-f4  14
00-80-2d-22-4f-f6  14           00-80-2d-22-87-f4  14
00-80-2d-22-93-f6  14           00-80-2d-39-7b-f4  14
00-80-2d-39-f0-c7  14           00-80-2d-39-f2-01  14
00-80-2d-39-f7-f4  14           00-80-2d-3a-7b-f4  14
00-80-2d-3f-b3-f4  14           00-80-2d-8c-48-c0  14
00-80-2d-ac-db-f4  14           00-80-2d-ad-9b-f4  14
```

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 (10-1000000) 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.

Setting the default management system

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

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

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

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

Chapter 2
General CLI commands

In the BayStack 380 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:

- "SNMPv3 Commands" on page 105

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
- "terminal command" on page 47

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 7 displays the output from the `show terminal` command.

Figure 7 show terminal command output

```
BS380_24#show terminal
Terminal speed: 9600
Terminal width: 79
Terminal length: 23
BS380_24#
```

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 8 describes the parameters and variables for the `terminal` command.

Table 8 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 <1-132>	Sets the length of the terminal display in characters; default is 24.
width <1-132>	Sets the width of the terminal displaying characters; default 79.

Pinging

To ensure that the BayStack 380 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 52 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 9 describes the parameters and variables for the `ping` command.

Table 9 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 8 displays sample `ping` responses.

Figure 8 ping command responses

```
BS380_24#ping 10.10.40.29
Host is reachable
BS380_24#ping 10.10.41.29
Host is not reachable
```

show cli

The `show cli` command displays the CLI command modes and the type of password required for each mode. The syntax for the `show cli command` is:

```
show cli [info] [password [type]]
```

The show cli command is in the config command mode.

The `show cli` command has the following parameters.

Table 10 describes the parameters and variables for the `show cli` command.

Table 10 show cli command parameters and variables

Parameters and variables	Description
info	Displays general CLI settings.
password (type)	Displays CLI user names, passwords, and password types.

show gbic-info

The `show gbic-info` command displays the type of GBIC used in the GBIC port. The syntax for the show gbic-info is:

```
show gbic-info
```

The `show gbic-info` command is in the config command mode.

There are no parameters or variables for the `show gbic-info` command.

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

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. 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 11 describes the parameters and variables for the `configure network` command.

Table 11 configure network command parameters and variables

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

Note: When you specify the file name or address, these parameters will be used 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:

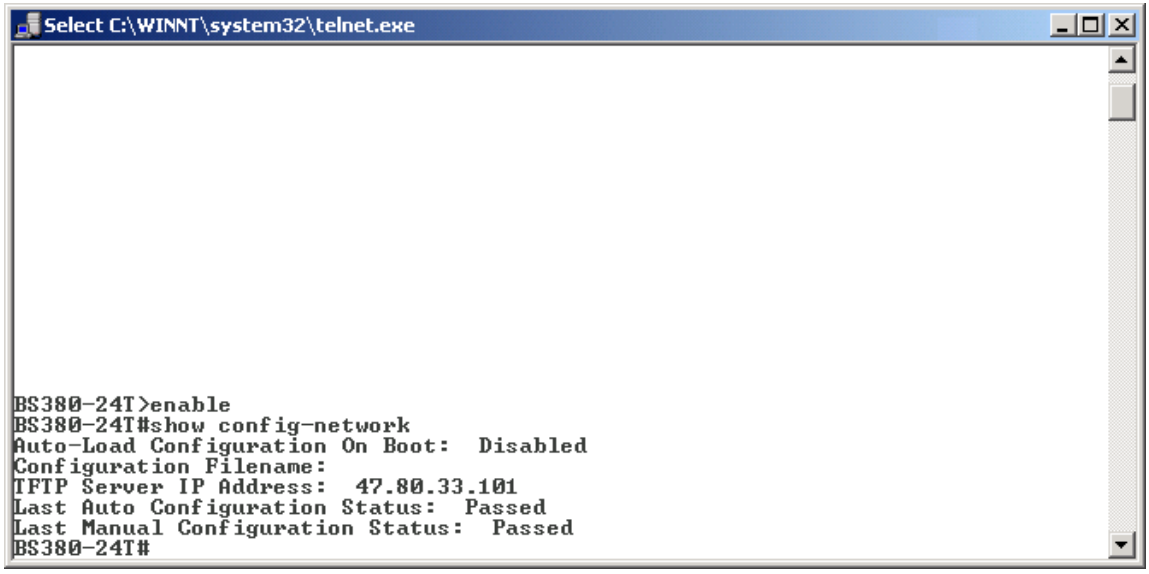
```
show config-network
```

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 9,

Figure 9 show config-network command



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

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

```
ip address <XXX.XXX.XXX.XXX> [netmask <XXX.XXX.XXX.XXX>]
```

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

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

Table 12 ip address command parameters and variables

Parameters and variables	Description
<XXX.XXX.XXX.XXX>	Enter IP address in dotted decimal notation; netmask is optional.
netmask	Set the IP subnet mask for the 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 to all zeros (0). The syntax for the `no ip address` command is:

```
no ip address {switch}
```

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

Table 13 describes the parameters and variables for the `no ip address` command.

Table 13 no ip address command parameters and variables

Parameters and variables	Description
switch	Prompts you with “Are you sure you want to delete the switch IP address and subnet mask Y/N?” If you enter Y, this command zeroes out the IP address and subnet mask for the switch.

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

Table 14 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, 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]
```

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 15 describes the parameters and variables for the `show ip` command.

Table 15 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.

Figure 10 displays a sample output of the `show ip` command.

Figure 10 show ip command output

```
BS380_24#show ip
BootP Mode: BootP Disabled

                    Configured        In Use        Last BootP
                   --------------- --------------- ---------------
Switch IP Address: 10.30.31.200                    0.0.0.0
Subnet Mask:       255.255.255.0   255.255.255.0   0.0.0.0
Default Gateway:   10.20.30.1      10.20.30.1      0.0.0.0
BS380_24#
```

Assigning and clearing IP addresses for specific units

You can assign IP addresses for a specific unit. This section covers the topic:

- “default ip address command” on page 57

default ip address command

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

```
default ip address
```

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

There are no parameters and variables for the `default ip address` command.

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 380.

Note: Multiple users can access the CLI system simultaneously, through the serial port, Telnet, and modems. The maximum number of users is 5. 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

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

Figure 11 show telnet-access command output

```
BS380_24#show telnet-access
TELNET Access:       Enabled
Login Timeout:       1 minute(s)
Login Retries:       3
Inactivity Timeout:  15 minute(s)
Event Logging:       All
Allowed Source IP Address  Allowed Source Mask
-------------------------  ------------------
0.0.0.0                    0.0.0.0
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
255.255.255.255            255.255.255.255
BS380_24#
```

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 16 describes the parameters and variables for the `telnet-access` command.

Table 16 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 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 17 describes the parameters and variables for the `no telnet-access` command.

Table 17 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 boot parameters

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

- "boot command," next
- "ip bootp server command" on page 61

boot command

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

```
boot [default]
```

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

Table 18 describes the parameters and variables for the `boot` command.

Table 18 boot command parameters and variables

Parameters and variables	Description
default	Restores switch to factory-default settings after rebooting.

Note: When you reset to factory defaults, the switch retains the last reset count, and reason for last reset; these 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 19 describes the parameters and variables for the `ip bootp server` command.

Table 19 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

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

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

Figure 12 show tftp-server command output

```
BS380_24#show tftp-server
TFTP Server IP address : 192.168.100.15
BS380_24#
```

tftp-server command

The `tftp-server` command assigns the address for the 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 20 describes the parameters and variables for the `tftp-server` command.

Table 20 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 specifies a default address for the switch to use for TFTP services. The syntax of the `no tftp-server` command is:

```
no tftp-server
```

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

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

default tftp-server command

The `default tftp server` command restores the table to defaults (0.0.0.0). The syntax for the `default tftp server` is:

```
default tftp server
```

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

There are no parameters or variables for the `default tftp server` command.

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

Table 21 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 22 describes the parameters and variables for the `copy tftp config` command.

Table 22 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 380 software image that is located in non-volatile flash memory. To download the BayStack 380 software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch IP address, refer to "Assigning and clearing IP addresses" on page 52.

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

This section covers the following topics:

download command

The `download` command upgrades the software for the BayStack 380. You can upgrade both the software image and the diagnostics image.

Note: The system resets after downloading a new image.

The syntax for the `download` command is:

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

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

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

Table 23 download command parameters and variables

Parameters and variables	Description
address <ip>	Specifies the TFTP server you want to use. Note: If this parameter is omitted, the system goes to the server specified by the `tftp-server` command.
image <image-name>	Enter the name of the BS 380 software image you want to download.
image-if-newer <image-name>	Enter the name of the BS 380 software image that you want to download if it is newer than the current running image.
diag <filename>	Enter the name of the BS 380 diagnostics image you want to download.

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 13 displays a sample output of the download command.

Figure 13 download message

```
Download Image [/]

Saving Image [-]

Finishing Upgrading Image
```

During the download process, the BayStack 380-24T Switch is not operational. You can monitor the progress of the download process by observing the LED indications.

Observing LED indications

Table 24 describes the LED indications during the software download process.

Table 24 LED Indications during the software download process

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

Upgrading software images

To download, or upgrade, software in a BayStack 380 switch:

1 Enter `download [address <ip>] image BS380_24.img.`

The system resets and opens to the 380 banner. Refer to "Accessing the CLI" on page 30 to return to the CLI.

2 Enter `download [address <ip>] diag BS380_24diags.bin.`

The system resets and opens to the 380 banner. Refer to "Accessing the CLI" on page 30 to return to the CLI.

Displaying interfaces

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

show interfaces command

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

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

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

Table 25 describes the parameters and variables for the `show interfaces` command.

Table 25 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 14 displays a sample output of the `show interfaces names` command.

Figure 14 show interfaces names command output

```
BS380_24 SW 3.0 in SC2-02 LAB>show interfaces names 1-3
Port Name
---- ------------------------------------------------------------------
1     LabBldg4
2     Testing
3     Floor1Bldg2
```

Figure 15 displays a sample output of the `show interfaces` command without the names variable.

Figure 15 show interfaces command output

```
BayStack 380 3.0#show interfaces
             Status                    Auto
Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation Speed
Duplex Control
---- ----- ------- ---- ---- -------- ----------- --------
------ -------
1          Enable  Down Down Enabled  Enabled
2          Enable  Down Down Enabled  Enabled
3          Enable  Down Down Enabled  Enabled
4          Enable  Down Down Enabled  Enabled
5          Enable  Down Down Enabled  Enabled
6          Enable  Down Down Enabled  Enabled
7          Enable  Down Down Enabled  Enabled
8          Enable  Down Down Enabled  Enabled
9          Enable  Down Down Enabled  Enabled
10         Enable  Down Down Enabled  Enabled
11         Enable  Down Down Enabled  Enabled
12         Enable  Down Down Enabled  Enabled
13         Enable  Down Down Enabled  Enabled
14         Enable  Up   Up   Enabled  Enabled     10M
15         Enable  Down Down Enabled  Enabled
16         Enable  Down Down Enabled  Enabled
17         Enable  Down Down Enabled  Enabled
18         Enable  Down Down Enabled  Enabled
19         Enable  Down Down Enabled  Enabled
--More--
```

Setting SNMP parameters

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

snmp-server command

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

```
snmp-server {authentication-trap|community
<community-string> contact <text>|host <host-ip>
<community-string>|location <text>|name <text>}
```

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

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

Table 26 snmp-server command parameters and variables

Parameters and variables	Description
authentication-trap	Enables or disables generation of SNMP authentication failure trap.
bootstrap	Generates the SNMP bootstrap parameters.
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.
contact <text>	Specifies the SNMP sysContact value; enter an alphanumeric string.
host <host-ip> <community-string>	Configures an SNMP trap destination: • host-ip—enter a dotted-decimal IP address of a host that 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.
user	Creates an SNMPv3 user
view	Creates or changes an SNMP access view.

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|contact|host
[<host-ip> <community-string>]|location |name]
```

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

Table 27 describes the parameters and variables for the `snmp-server` command.

Table 27 no snmp-server command parameters and variables

Parameters and variables	Description
authentication-trap	Disables authentication failure traps.
community	Disables the community string.
contact <text>	Clears the SNMP sysContact value.
sysContact value	Specifies the SNMP sysContact value; enter an alphanumeric string.
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.

default snmp-server command

The `default snmp-server` command specifies using the default SNMP configuration parameter. The default parameter is 0.0.0.0. The syntax for the `default snmp-server` is:

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

The `default snmp-server` command is in the global configuration command mode.

Table 28 describes the parameters and variables for the `snmp-server` command.

Table 28 default 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.
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

show snmp-server

The show `snmp-server` command displays the defaults for the snmp-server command. The syntax for the `show snmp-server` is:

show `snmp-server`

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

Table 29 describes the parameters and variables for the `snmp-server` command.

Table 29 show snmp-server parameters and variable

Parameters and variables	Description
community	Displays SNMP community strings.
host	Displays SNMP trap destinations.
user	Displays SNMP users.
view	Displays SNMP views

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 enable|disable [port <portlist>]
```

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

Table 30 describes the parameters and variables for the `snmp trap link-status` command.

Table 30 snmp trap link-status command parameters and variables

Parameters and variables	Description
disable	Disables generation of linkUp/Down traps.
enable	Enables generation of linkUp/Down traps.
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 31 describes the parameters and variables for the `no snmp trap link-status` command.

Table 31 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 default values are 0.0.0.0. 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 32 describes the parameters and variables for the default `snmp trap link-status` command.

Table 32 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.

Configuring remote network monitoring (RMON)

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

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

Figure 16 show rmon alarm command output

```
BS380_24#show rmon alarm
                                          Sample      Rising          Falling
Index Interval Variable                    Type  Threshold Event Threshold Event
----- -------- ------------------------- ------ --------- ----- --------- -----
1     30       ifInOctets.1              delta 500       1     10        1
```

show rmon event

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

```
show rmon event
```

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

The `show rmon event` command has no parameters or variables. Figure 17 displays a sample output of the `show rmon event` command.

Figure 17 show rmon event command output

```
BS380_24#show rmon event
Index Log Trap Description
----- --- ---- -----------------------------------------------------
1     Yes Yes  'Rising or Falling alarm on received octets'
```

show rmon history

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

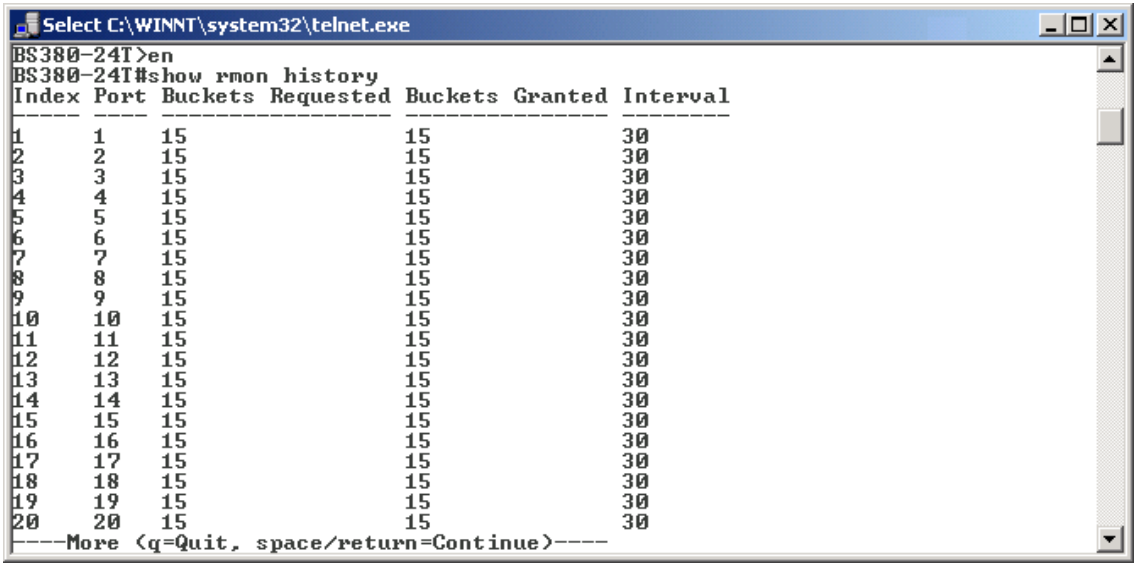
```
show rmon history
```

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

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

Figure 18 displays a sample output of the `show rmon history` command.

Figure 18 show rmon history command output



show rmon stats

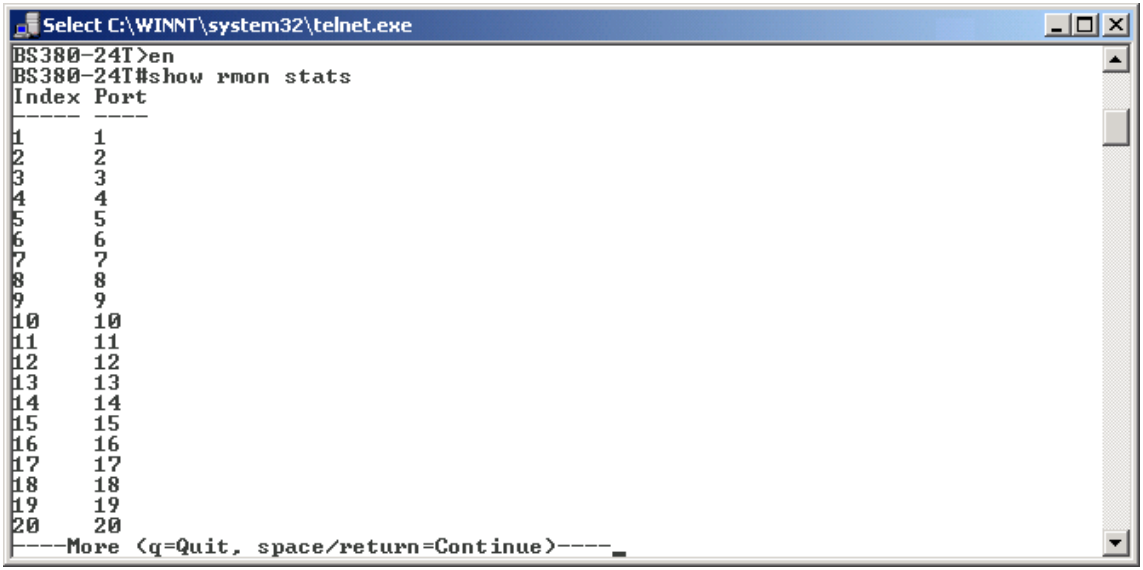
The `show rmon stats` command displays information regarding the configuration of RMON statistics. The syntax for the `show rmon stats` command is:

```
show rmon stats
```

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

The `show rmon stats` command has no parameters or variables. Figure 19 displays a sample output of the `show rmon stats` command.

Figure 19 show rmon stats command output



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

Table 33 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.

Table 33 rmon alarm command parameters and variables

Parameters and variables	Description
<1-2147483647>	The sampling interval, in seconds.
absolute	Use absolute values (value of the MIB object is compared directly with thresholds).
delta	Use delta values (change in the value of the MIB object between samples is compared with thresholds).
rising-threshold <-2147483648-2147483647> [<1-65535>]	The first integer value is the rising threshold value. The optional second integer specifies the event entry to be triggered when the rising threshold is crossed. If omitted, or if an invalid event entry is referenced, no event 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.

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 34 describes the parameters and variables for the `rmon event` command.

Table 34 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.

Table 34 rmon event command parameters and variables

Parameters and variables	Description
[description *<LINE>*]	Specify a textual description for the event.
[owner *<LINE>*]	Specify an owner string to identify 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> <port> <1-65535> <1-3600>`* `[owner` *`<LINE>`*`]`

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

Table 35 describes the parameters and variables for the `rmon history` command.

Table 35 rmon history command parameters and variables

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

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> <LINE>`* `[owner` *`<LINE>`*`]`

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

Table 36 describes the parameters and variables for the `rmon stats` command.

Table 36 rmon stats command parameters and variables

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

Setting the system event log

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

show logging

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

```
show logging config

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

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

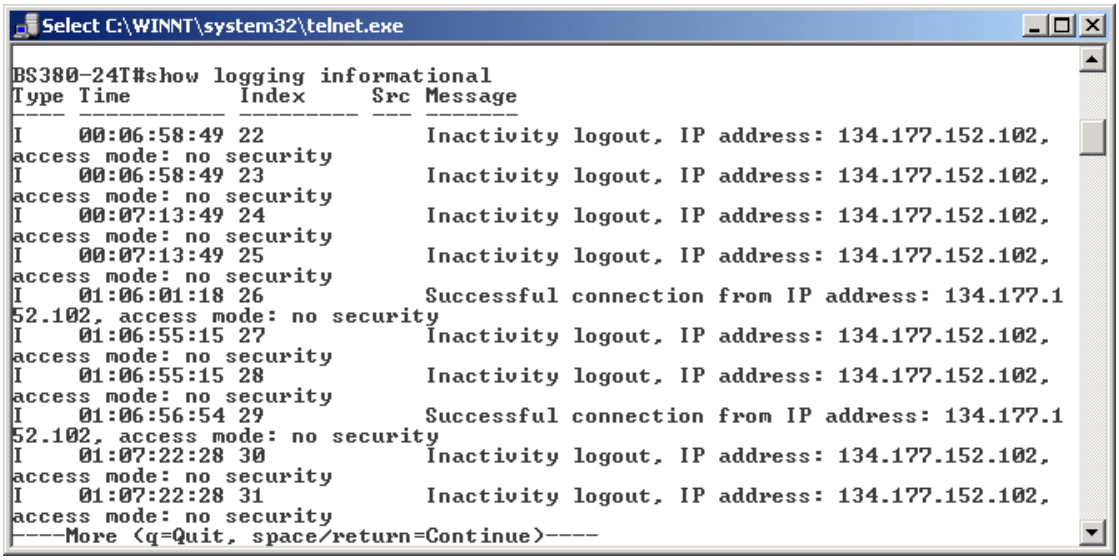
Table 37 describes the parameters and variables for the `show logging` command.

Table 37 show logging command parameters and variables

Parameters and variables	Description
config	Displays the current logging settings.
critical	Displays critical log messages.
serious	Displays serious log messages.
informational	Displays informational log messages.

Figure 20 shows the output of the `show logging informational` command.

Figure 20 show logging informational command output



logging

The `logging` command configures the system settings for the system event log. The syntax for the `logging` command is:

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

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

Table 38 describes the parameters and variables for the `logging` command.

Table 38 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|none	Specifies the level of logging stored in non-volatile memory.

no logging

The `no logging` command disables the system event log. The syntax for the `no logging` command is:

```
no logging
```

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

The `no logging` command has no parameters or values.

default logging

The `default logging` command configures the system settings as the factory default settings for the system event log. The syntax for the `default logging` command is:

```
default logging
```

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

The `default logging` command has no parameters or 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 non-volatile memory.

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 90

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

Figure 21 show port-statistics command output

```
BS380_24(config-if)#show port-statistics
Received
  Packets:              1117620
  Multicasts:           112524
  Broadcasts:           996989
  Total Octets:         75698837
  Packets 64 bytes:     1106427
      65-127 bytes:   2143
      128-255 bytes:  1731
      256-511 bytes:  2977
      512-1023 bytes: 3662
      1024-1518 bytes: 680
  Jumbo  1519-9216 bytes: 0
  Control Packets:      0
  FCS Errors:           0
  Undersized Packets:   0
  Oversized Packets:    0
  Filtered Packets:     0
  Flooded Packets:      1004751
Transmitted
  Packets:              32451
  Multicasts:           31643
  Broadcasts:           0
  Total Octets:         2183060
  Packets 64 bytes:     32030
      65-127 bytes:   161
      128-255 bytes:  107
      256-511 bytes:  62
      512-1023 bytes: 85
      1024-1518 bytes: 6
  Jumbo  1519-9216 bytes: 0
  Control Packets:      0
  Collisions:           0
  Single Collisions:    0
  Multiple Collisions:  0
  Excessive Collisions: 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 91

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 enable. Note: If you omit this parameter, the system uses the port number you specified in the `interface` command.

default shutdown command

The `default shutdown` command specifies shutdown of a port or ports based on the default configuration. The syntax for the `default shutdown` is:

```
default shutdown [port <portlist>]
```

The `default shutdown` command is in the interface configuration command mode.

Table 44 describes the parameters and variables for the `default shutdown` command.

Table 44 default 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.

Naming ports

You can name a port using the CLI. This section covers the following commands:

- "name command," next
- "no name command" on page 93
- "default name command" on page 94

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 45 describes the parameters and variables for the `name` command.

Table 45 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 46 describes the parameters and variables for the `no name` command.

Table 46 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 47 describes the parameters and variables for the `default name` command.

Table 47 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 95
- "duplex command" on page 96
- "default duplex command" on page 97

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: Fiber optic ports can only be set to 1000.

Table 48 describes the parameters and variables for the `speed` command.

Table 48 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 49 describes the parameters and variables for the `default speed` command.

Table 49 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: Fiber optic ports can only be set to 1000.

Table 50 describes the parameters and variables for the `duplex` command.

Table 50 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, and that duplex matches on both sides: full or half.

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 51 describes the parameters and variables for the `default duplex` command.

Table 51 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.

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 99
- "default autotopology command" on page 99

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.

show autotopology

The `show autotopology` command displays the default autopology values. The syntax for the show autotopology is:

```
show autotopology
```

The `show autotopology` command is in the config command mode.

There are no parameters or variables for the `show autotopology` command.

Enabling flow control

If you use a Gigabit Interface Connector (GBIC) with the BayStack 380, you control traffic on this port using the `flowcontrol` command. This section covers the following commands:

flowcontrol command

The `flowcontrol` command is used only on Gigabit Interface Connector ports and controls the traffic rates during congestion. The syntax for the `flowcontrol` command is:

```
flowcontrol [port <portlist>]
{asymmetric|symmetric|auto|disable}
```

The `flowcontrol` command is in the config-if mode.

Table 52 describes the parameters and variables for the `flowcontrol` command.

Table 52 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 on the remote end and allows the remote end to perform flow control at the local end • 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 53 describes the parameters and variables for the `no flowcontrol` command.

Table 53 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 54 describes the parameters and variables for the `default flowcontrol` command.

Table 54 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.

Single fiber fault detection

When a partial fiber break occurs, data is lost on one side of a link. Single Fiber Fault Detection (SFFD) detects this error condition, and causes the port that is losing data to go down. This stops the loss of data.

The Single Fiber Fault Detection feature is enabled on a port by port basis for the BPS 2000 2GE MDA, and BayStack 380 and BayStack 470-48T and 470-24T GBIC ports. At present, you can access this feature through the NNCLI.

Single Fiber Fault Detection (SFFD) has the following requirements and limitations:

- SFFD must be implemented on both sides of a link. For example:

  Passport 8600 and BoSS 3.0
- SFFD must be enabled on a per-port basis
- By default, SFFD is disabled on all ports
- SFFD takes about 50 seconds to detect a fault
- Once a link is repaired, the link recovers automatically

Far End Fault Indication (FEFI)

When a fiber optic transmission link to a remote device fails, the remote device indicates the failure and the port is disabled. To use FEFI, the user must enable autonegotiation on the port.

CLI commands for SFFD

This section lists the CLI commands that will be used on the BayStack products to support the SFFD feature.

show sffd

This command shows the SFFD configuration information for all ports where the SFFD feature is applicable. The output shows if the SFFD feature is enabled or disabled.

The command works in ALL of the NNCLI modes (e.g., User EXEC, Privileged EXEC, Global Configuration, and Interface Configuration).

sffd [port <portlist>] enable

This command enables the SFFD feature on specified ports, and is only available in the NNCLI using interface configuration mode.

The argument `port <portlist>` specifies the port number(s) to enable the SFFD feature. If not specified, the system will use the port number specified in the interface command.

no sffd [port <portlist>] enable

This command disables the SFFD feature on specified ports, and is only available in the NNCLI interface configuration mode.

The argument `port <portlist>` specifies the port number(s) to disable the SFFD feature. If not specified, the system will use port number specified in the interface command.

default sffd [port <portlist>] enable

This command changes the SFFD setting for the specified ports to the factory setting. The factory default setting is disabled.

The argument `port <portlist>` specifies the port number(s) to default the SFFD feature setting. If not specified, the system will use port number specified in the interface command.

SNMPv3 Commands

BayStack 380 provides the following CLI commands for SNMPv3:

show snmp-server command

The `show snmp-server` command displays SNMP configuration. The syntax for the `show snmp-server` command is:

```
show snmp-server {community|host|user|views}
```

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

Table 55 describes the parameters and variables for the `show snmp-server` command.

Table 55 show snmp-server command parameters and variables

Parameters and variables	Description
community|host|user |view	Displays SNMPv3 configuration information: • community strings as configured in SNMPv3 MIBs • trap receivers as configured in SNMPv3 MIBs • SNMPv3 users, including views accessible to each user • SNMPv3 views
view/views	Displays SNMPv3 views.

snmp-server authentication-trap command

The `snmp-server authentication-trap` command enables or disables the generation of SNMP authentication failure traps. The syntax for the `snmp-server authentication-trap` command is:

```
snmp-server authentication-trap {enable|disable}
```

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

Table 56 describes the parameters and variables for the snmp-server authentication-trap command.

Table 56 snmp-server authentication-trap command parameters and variables

Parameters and variables	Description
enable|disable	Enables or disables the generation of authentication failure traps.

no snmp-server authentication-trap command

The `no snmp-server authentication-trap` command disables generation of SNMP authentication failure traps. The syntax for the `no snmp-server authentication-trap` command is:

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

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

There are no parameters or variables for the `no snmp-server authentication-trap` command.

default snmp-server authentication-trap command

The `default snmp-server authentication-trap` command restores SNMP authentication trap configuration to the default settings. The syntax for the `default snmp-server authentication-trap` command is:

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

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

There are no parameters for the `default snmp-server authentication-trap` command.

snmp-server community for read/write command

The `snmp-server community` command for read/write modifies the community strings for SNMP v1 and SNMPv2c access. The syntax for the `snmp-server community` for read/write command is:

```
snmp-server community <community-string> [ro|rw]
```

The `snmp-server community` for read/write command is in the config command mode.

This command configures a single read-only or a single read-write community. A community configured using this command does not have access to any of the SNMPv3 MIBs. The community strings created by this command are controlled by the SNMP Configuration screen in the console interface.

This command affects community strings that were created prior to BoSS 3.0. These community strings will have a fixed MIB view.

Table 57 describes the parameters and variables for the `snmp-server community` for read/write command.

Table 57 snmp-server community for read/write command parameters and variables

Parameters and variables	Description
community-string	Changes community strings for SNMP v1 and SNMPv2c access. Enter a community string that works as a password and permits access to the SNMP protocol. If you set the value to 'NONE' it will be disabled.
ro|rw	Specifies read-only or read-write access. Stations with ro access can only retrieve MIB objects, and stations with rw access can retrieve and modify MIB objects. **Note**: If neither ro nor rw is specified, ro is assumed (default).

snmp-server community command

The `snmp-server community` command allows you to create community strings with varying levels of read, write, and notification acess based on SNMPv3 views. These community strings are separate from those created using the `snmp-server community` for read/write command.

This command affects community strings stored in the SNMPv3 snmpCommunityTable, which allows several community strings to be created. These community strings may have any MIB view.

The syntax for the `snmp-server community` command is:

```
snmp-server community <community-string> {read-view
<view-name>|write-view <view-name>|notify-view <view-name>}
```

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

Table 58 describes the parameters and variables for the `snmp-server community` command.

Table 58 snmp-server community command parameters and variables

Parameters and variables	Description
community-string	Enter a community string to be created with access to the specified views.
read-view <view-name>	Changes the read view used by the new community string for different types of SNMP operations. • view-name—specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.

Table 58 snmp-server community command parameters and variables (continued)

Parameters and variables	Description
write-view <view-name>	Changes the write view used by the new community string for different types of SNMP operations. • view-name—specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.
notify-view <view-name>	Changes the notify view settings used by the new community string for different types of SNMP operations. • view-name—specifies the name of the view which is a set of MIB objects/instances that can be accessed; enter an alphanumeric string.

no snmp-server community command

The `no snmp-server community` command clears the snmp-server community configuration. The syntax for the `no snmp-server community` command is:

```
no snmp-server community [ro|rw|<community-string>]
```

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

If you do not specify a read-only or read-write community parameter, all community strings are removed, including all communities controlled by the `snmp-server community` command and the `snmp-server community` for read-write command.

If you specify read-only or read-write, then just the read-only or read-write community is removed. If you specify the name of a community string, then the community string with that name is removed.

Table 59 describes the parameters and variables for the `no snmp-server community` command.

Table 59 no snmp-server community command parameters and variables

Parameters and variables	Description
ro|rw|<community-string>	Changes the settings for SNMP: • ro|rw—sets the specified old-style community string's value to 'NONE', thereby disabling it. • community-string—deletes the specified community string from the SNMPv3 MIBs (that is, from the new-style configuration).

default snmp-server community command

The `default snmp-server community` command restores the community string configuration to the default settings. The syntax for the `default snmp-server community` command is:

```
default snmp-server community [ro|rw]
```

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

If the read-only or read-write parameter is omitted from the command, then all communities are restored to their default settings. The read-only community is set to Public, the read-write community is set to Private, and all other communities are deleted.

Table 60 describes the parameters and variables for the `default snmp-server community` command.

Table 60 default snmp-server community command parameters and variables

Parameters and variables	Description
ro|rw	Restores the read-only community to 'public', or the read-write community to 'private'.

snmp-server contact command

The `snmp-server contact` command configures the SNMP sysContact value. The syntax for the `snmp-server contact` command is:

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

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

Table 61 describes the parameters and variables for the `snmp-server contact` command.

Table 61 snmp-server contact command parameters and variables

Parameters and variables	Description
text	Specifies the SNMP sysContact value; enter an alphanumeric string.

no snmp-server contact command

The `no snmp-server contact` command clears the sysContact value. The syntax for the `no snmp-server contact` command is:

```
no snmp-server contact
```

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

There are no parameters or variables for the `no snmp-server contact` command.

default snmp-server contact command

The `default snmp-server contact` command clears sysContact. The syntax for the `default snmp-server contact` command is:

```
default snmp-server contact
```

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

There are no parameters or variables for the `default snmp-server contact` command.

snmp-server command

The `snmp-server` command enables or disables the SNMP server. The syntax for the `snmp-server` command is:

```
snmp-server {enable|disable}
```

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

Table 62 describes the parameters and variables for the `snmp-server` command.

Table 62 snmp-server command parameters and variables

Parameters and variables	Description
enable|disable	Enables or disables the SNMP server.

no snmp-server command

The `no snmp-server` command disables SNMP access. The syntax for the `no snmp-server` command is:

```
no snmp-server
```

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

There are no parameters or variables for the `no snmp-server` command.

Note: If you disable SNMP access to the switch, you will not be able to use Device Manager for the switch.

snmp-server host for old-style table command

The `snmp-server host` for old-style table command adds a trap receiver to the old-style trap-receiver table The table has a maximum of four entries, and the entries can generate only SNMPv1 traps. This command controls the contents of the s5AGTrpRcvrTable which is the set of trap destinations contolled by the SNMP Configuration screen in the console interface.

The syntax for the `snmp-server host` for old-style table command is:

```
snmp-server host <host-ip> <community-string>
```

The `snmp-server host` for old-style table command is in the config command mode.

Table 63 describes the parameters and variables for the `snmp-server host` for old-style table command.

Table 63 snmp-server host for old-style table command parameters and variables

Parameters and variables	Description
<host-ip>	Enter a dotted-decimal IP address of a host that will be the trap destination.
<community-string>	Enter a community string that works as a password and permits access to the SNMP protocol.

snmp-server host for new-style table command

The `snmp-server host` for new-style table command adds a trap receiver to the new-style configuration (that is, to the SNMPv3 tables) You can create several entries in this table, and each can generate v1, v2c, or v3 traps. Note that you must have previously configured the community string or user that is specified, with a notify-view. The syntax for the `snmp-server host` for new-style table command is:

```
snmp-server host <host-ip> {v1 <community-string>|v2c
<community-string>|v3 {auth|no-auth|auth-priv}<username>}
```

The `snmp-server host` for new-style table command is in the config command mode.

Table 64 describes the parameters and variables for the `snmp-server host` for new-style table command.

Table 64 snmp-server host for new-style table command parameters and variables

Parameters and variables	Description
<host-ip>	Enter a dotted-decimal IP address of a host that will be the trap destination.
v1 <community-string>	Using v1 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels may be created.
v2c <community-string>	Using v2c creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels may be created.
v3 {auth|no-auth|auth-priv}	Using v3 creates trap receivers in the SNMPv3 MIBs. Multiple trap receivers with varying access levels may be created: Enter the following variables: • auth|no-auth—specifies whether SNMPv3 traps should be authenticated • auth-priv—this parameter is only available if the image has full SHA/DES support.
<username>	Specifies the SNMPv3 username for trap destination; enter an alphanumeric string.

no snmp-server host for old-style table command

The `no snmp-server host` for old-style table command deletes trap receivers from the old-style table. The syntax for the `no snmp-server host` for old-style table command is:

```
no snmp-server host <host-ip> <community-string>
```

The `no snmp-server host` for old-style table command is in the config command mode.

Table 65 describes the parameters and variables for the `no snmp-server host` for old-style table command.

Table 65 no snmp-server host for old-style table command parameters and variables

Parameters and variables	Description
<host-ip> <community-string>	Enter the following variables: • host-ip—the IP address of a trap destination host. • community-string—the community string that works as a password and permits access to the SNMP protocol.

no snmp-server host for new-style table command

The `no snmp-server` for new-style table command deletes trap receivers from the new-style table (SNMPv3 MIB). Any trap receiver matching the IP address and SNMP version will be deleted. The syntax for the `no snmp-server host` for new-style table command is:

```
no snmp-server host <host-ip> {v1|v2c|v3}
```

The `no snmp-server host` for new-style table command is in the config command mode.

Table 66 describes the parameters and variables for the `no snmp-server host` for new-style table command.

Table 66 no snmp-server host for new-style command parameters and variables

Parameters and variables	Description
<host-ip>	Enter the IP address of a trap destination host.
v1|v2c|v3	Specifies trap receivers in the SNMPv3 MIBs.

default snmp-server host command

The `default snmp-server host` command restores the old-style table to defaults (that is, it clears the table). The syntax for the `default snmp-server host` is:

```
default snmp-server host
```

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

There are no parameters or variables for the `default snmp-server host` command.

snmp-server location command

The `snmp-server location` command configures the SNMP sysLocation value. The syntax for the `snmp-server location` command is:

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

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

Table 67 describes the parameters and variables for the `snmp-server location` command.

Table 67 snmp-server location command parameters and variables

Parameters and variables	Description
<text>	Specify the SNMP sysLocation value; enter an alphanumeric string of up to 255 characters.

no snmp-server location command

The `no snmp-server location` command clears the SNMP sysLocation value. The syntax for the `no snmp-server location` command is:

```
no snmp-server location
```

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

There are no parameters or variables for the `no snmp-server location` command.

default snmp-server location command

The `default snmp-server location` command restores sysLocation to the default value. The syntax for the `default snmp-server location` command is:

```
default snmp-server location
```

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

snmp-server name command

The `snmp-server name` command configures the SNMP sysName value. The syntax for the `snmp-server name` command is:

```
snmp-server name <text>
```

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

Table 68 describes the parameters and variables for the `snmp-server name` command.

Table 68 snmp-server name command parameters and variables

Parameters and variables	Description
<text>	Specify the SNMP sysName value; enter an alphanumeric string of up to 255 characters..

no snmp-server name command

The `no snmp-server name` command clears the SNMP sysName value. The syntax for the `no snmp-server name` command is:

```
no snmp-server name
```

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

There are no parameters or variables for the `no snmp-server name` command.

default snmp-server name command

The `default snmp-server name` command restores sysName to the default value. The syntax for the `default snmp-server name` command is:

```
default snmp-server name
```

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

snmp-server user command

The `snmp-server user` command creates an SNMPv3 user. The syntax for the `snmp-server user` command is:

```
snmp-server user <username> [read-view view-name>]
[write-view <view-name>][notify-view <view-name>] [{md5|sha}
<password>[read-view <view-name>] [write-view <view-name>]
[notify-view <view-name>] [des <password> [read-view
<view-name>][write-view <view-name>][notify-view
<view-name>]]]
```

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

The `sha` and `des` parameters are only available if the switch image has full SHA/DES support.

There are three sets of read/write/notify views shown in the command. The first set specifies unauthenticated access. The second set specifies authenticated access. The third set specifies authenticated and encrypted access.

You can only specify authenticated access if the md5 or sha parameter is included. Likewise, and you can only specify authenticated and encrypted access if if the des parameter is included.

If you omit the authenticated view parameters, authenticated access uses the views specified for unauthenticated access. If you omit all of the authenticated and encrypted view parameters, the authenticated and encrypted access uses the same views used for authenticated access. These will be the unauthenticated views if all the authenticated ones were also omitted.

Table 69 describes the parameters and variables for the `snmp-server user` command.

Table 69 snmp-server user command parameters and variables

Parameters and variables	Description
<username>	Specifies the user name; enter an alphanumeric string of up to 255 characters.
md5 <password>	Specifies the use of an md5 password. <password> specifies the new user md5 password; enter an alphanumeric string. If this parameter is omitted, the user will be created with only unauthenticated access rights.

Table 69 snmp-server user command parameters and variables

Parameters and variables	Description
read-view <view-name>	Specifies the read view to which the new user has access: • view-name—specifies the viewname; enter an alphanumeric stringof up to 255 characters.
write-view <view-name>	Specifies the write view to which the new user has access: • view-name—specifies the viewname; enter an alphanumeric stringof up to 255 characters.
notify-view <view-name>	Specifies the notify view to which the new user has access: • view-name—specifies the viewname; enter an alphanumeric stringof up to 255 characters.
SHA	Specifies SHA authentication or DES privacy encryption..
DES	Specifies DES privacy encryption..

no snmp-server user command

The `no snmp-server user` command deletes the specified user. The syntax for the `no snmp-server user` command is:

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

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

Table 70 describes the parameters and variables for the `no snmp-server user` command.

Table 70 no snmp-server user command parameters and variables

Parameters and variables	Description
<username>	Specifies the user to be removed.

snmp-server view command

The `snmp-server view` command creates an SNMPv3 view The view is a set of MIB object instances which may be accessed. The syntax for the `snmp-server view` command is:

```
snmp-server view <view-name> <OID> [<OID> [<OID> [<OID>
[<OID> [<OID> [<OID> [<OID> [<OID> [<OID>]]]]]]]]]
```

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

Table 71 describes the parameters and variables for the `snmp-server view` command.

Table 71 snmp-server view command parameters and variables

Parameters and variables	Description
<viewname>	Specifies the name of the new view; enter an alphanumeric string.
<OID>	Specifies Object identifier. OID may be entered as a MIB object English descriptor, a dotted form OID, or a mix of the two. Each OID should be preceded by a '+' or '-' sign (if this is omitted, a '+' sign is implied). For the dotted form, a sub-identifier can be a '*' indicating a wildcard. Here are some examples of valid OID parameters: • sysName • +sysName • -sysName • +sysName.0 • +ifIndex.1 • -ifEntry.*.1 (this matches all objects in the ifTable with an instance of 1, i.e., the entry for interface #1) • 1.3.6.1.2.1.1.1.0 (the dotted form of sysDescr) The '+' or '-' indicates whether the specified OID is included in or excluded from, respectively, the set of MIB objects that are accessible using this view. For example, if you create a view like this: • snmp-server view myview +system -sysDescr And you use that view for the read-view of a user, then the user can read only the system group except for sysDescr.

no snmp-server view command

The `no snmp-server view` command deletes the specified view. The syntax for the `no snmp-server view` is:

```
no snmp-server view <viewname>
```

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

Table 72 describes the parameters and variables for the `no snmp-server view` command.

Table 72 no snmp-server view command parameters and variables

Parameters and variables	Description
<viewname>	Specifies the name of the view to be removed. If no view is specified, all views are removed.

snmp trap link-status command

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

```
snmp trap link-status {enable|disable} [port <portlist>]
```

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

Table 73 describes the parameters and variables for the `snmp trap link-status` command.

Table 73 snmp trap link-status command parameters and variables

Parameters and variables	Description
enable|disable	Enables or disables SNMP link-status.
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 74 describes the parameters and variables for the `no snmp trap link-status` command.

Table 74 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 75 describes the parameters and variables for the default `snmp trap link-status` command.

Table 75 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.

snmp-server bootstrap command

The `snmp-server bootstrap` command allows you to specify how you wish to secure SNMP communications, as described in the SNMPv3 standards. It creates an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (in RFC 3414 and 3415). It consists of a set of initial users, groups, and views. This command deletes ALL existing SNMP configurations, so it should be used with care.

The syntax for the `snmp-server bootstrap` command is:

```
snmp-server bootstrap <minimum-secure> | <semi-secure>
|<very-secure>
```

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

Table 76 describes the parameters and variables for the `snmp-server bootstrap` command.

Table 76 snmp-server bootstrap command parameters and variables

Parameters and variables	Description
<minimum-secure>	Specifies a minumum security configuration that allows read access to everything via noAuthNoPriv, and write access to everything via authNoPriv.
<semi-secure>	Specifes a partial security configuration that allows read access to a small subset of system information using noAuthNoPriv, and read and write access to everything using authNoPriv.
<very-secure>	Specifies a maximum security configuration that allows no access.

show running-config

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

```
show running-config
```

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

There are no parameters or variables for the show running-config command.

Setting Class of Service

The BayStack 380 may prioritize traffic based on the Class of Service/Diffserv Code Point (CoS/DSCP) of IP packets. It allows you to map all 64 possible DSCP values in the IPv4 frame to any of four (4) priority queues. The IPv4 frames will be forwarded according to the COS queue priorities.

This section covers:

show cos-dscp

The `show cos-dscp` command displays the current class of service mapping. The syntax for the `show cos-dscp` command is:

```
show cos-dscp config
```

The `show cos-dscp` command is in the config command mode.

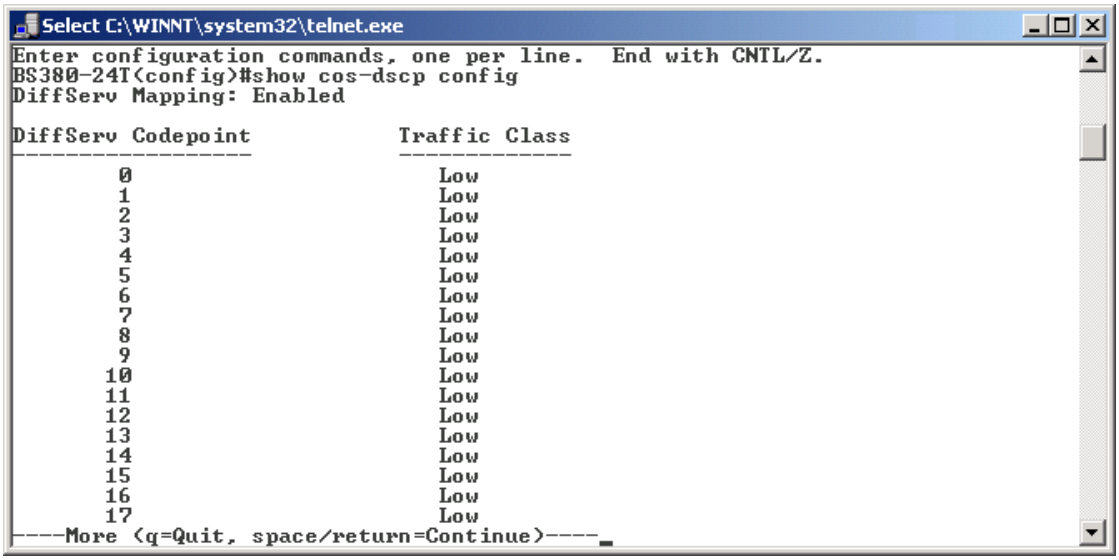
Table 77 describes the parameters and variables for the `show cos-dscp` command.

Table 77 show cos-dscp command parameters and variables

Parameters and variables	Description
config	Displays the current cos-dscp settings.

Figure 22 shows the output of the `show cos-dscp` command.

Figure 22 show cos-dscp config command output



cos-dscp

The `cos-dscp` command configures the system settings for the system event log. The syntax for the `cos-dscp` command is:

```
cos-dscp [enable|disable] [map-set]
```

The `cos-dscp` command is in the config command mode.

Table 38 describes the parameters and variables for the `cos-dscp` command.

Table 78 cos-dscp command parameters and values

Parameters and variables	Description
enable|disable	Enables or disables cos-dscp mapping.
map-set	Specifies the mapping values for cos-dscp

no cos-dscp

The `no cos-dscp` command disables class of service mapping. The syntax for the `no cos-dscp` command is:

```
no cos-dscp
```

The `no cos-dscp` command is in the config command mode.

The `no cos-dscp` command has no parameters or values.

default cos-dscp

The `default cos-dscp` command configures the system settings as the factory default settings for class of service. The syntax for the `default cos-dscp` command is:

```
default cos-dscp
```

The `default cos-dscp` command is in the config command mode.

The `default cos-dscp` command has no parameters or values.

Chapter 3
Security

This chapter describes the security commands available with the CLI.

Refer to *Using the BayStack 380 10/100/1000 Switch Software Version 3.0* for more information on the security features, as well as using the console interface (CI) menus. Refer to *Using Web-based Management for the BayStack 380 10/100/1000 Switch Software Version 3.0* for information on configuring these features using the Web-based management system, and refer to *Reference for the BayStack 380 10/100/1000 Switch Management Software Version 3.0* for information on configuring with the Device Manager.

Using MAC address security

You configure the BaySecure* application using MAC addresses with the following commands:

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}
```

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

Table 79 describes the parameters and variables for the `show mac-security` command.

Table 79 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.

Figure 23 displays sample output from the `show mac-security` command.

Figure 23 show mac-security command output

```
BS380_24#show mac-security config
MAC Address Security: Disabled
MAC Address Security SNMP-Locked: Disabled
Current Learning Mode: Disabled
Learn by Ports:
```

mac-security command

The `mac-security` command modifies the BaySecure configuration. The syntax for the `mac-security` command is:

```
mac-security [disable|enable][learning-ports <portlist>]
[learning {enable|disable}] [snmp-lock {enable|disable}]
```

The `mac-security` command is in the config command mode.

Table 80 describes the parameters and variables for the `mac-security` command.

Table 80 mac-security command parameters and values

Parameters and variables	Description
disable|enable	Disables or enables MAC address-based security.
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.

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>}
```

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

Table 81 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.

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.

default mac-security command

The default mac-security command specifies the use of the default BaySecure configuration by a specific port or list of ports. The syntax for the default mac-security is:

```
default mac-security [port <portlist>]
```

The default mac-security command is in the secure interface configuration mode.

Table 82 describes the parameters and variables for the mac-security command.

Table 82 default mac-security

Parameters and variables	Description
port <portlist>	Specifies the port or the list of ports using the default BaySecure configuration.

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>
```

The no mac-security mac-address-table command is in the config command mode.

Table 83 describes the parameters and variables for the no mac-security mac-address-table command.

Table 83 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.

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

Table 84 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

Using RADIUS authentication

Using a the RADIUS protocol and a server, you can configure the BayStack 380 for authentication. With the CLI system, you use the following commands:

- "show radius-server command," next
- "radius-server command" on page 138
- "no radius-server command" on page 139

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

Figure 24 show radius-server command output

```
BS380_24#show radius-server
host: 0.0.0.0
Secondary-host: 0.0.0.0
port: 1645
key:
BS380_24#
```

radius-server command

The `radius-server` command changes the RADIUS server settings. The syntax for the `radius-server` command is:

```
radius-server host <address> [secondary-host <address>] port
<num> key <string>
```

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

Table 85 describes the parameters and variables for the `radius-server` command.

Table 85 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.

default radius-server command

The `default radius-server` command specifies the use of the default RADIUS server setting. The syntax for the `default radius-server` is:

```
default radius-server
```

The `default radius-server` command is in the config command mode.

There are no parameters or variables for the `default radius-server` command.

Chapter 4
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:

Refer to the *Using the BayStack 380 10/100/1000 Switch Software Version 3.0* for more information on a 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 380 10/100/1000 Switch Software Version 3.0* for information on configuring these features using the Web-based management system, and refer to *Reference for the BayStack 380 10/100/1000 Switch Management Software Version 3.0* for configuration information for the Device Manager.

Using spanning tree

Note: For detailed information on spanning tree parameters, spanning tree groups, and configuration guidelines, refer to *Using the BayStack 380 10/100/1000 Switch Software Version 3.0.*

With the BayStack 380 with software version 3.0, you can configure a spanning tree group (STG). The CLI allows you to configure a spanning tree group, to add or remove VLANs to the spanning tree group, and to configure the usual spanning tree parameters and FastLearn. This section covers the following topics:

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 {config|port}
```

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

Table 86 describes the parameters and variables for the `show spanning-tree` command.

Table 86 show spanning-tree command parameters and variables

Parameters and variables	Description
config|port	Displays spanning tree configuration for: • config—the specified (or default) spanning tree group • port—the ports within the spanning tree group

Figure 25 shows the spanning tree parameters by port. Figure 26 displays sample output from the `show spanning-tree` command for the spanning tree group (STP1).

Figure 25 show spanning-tree command output by port

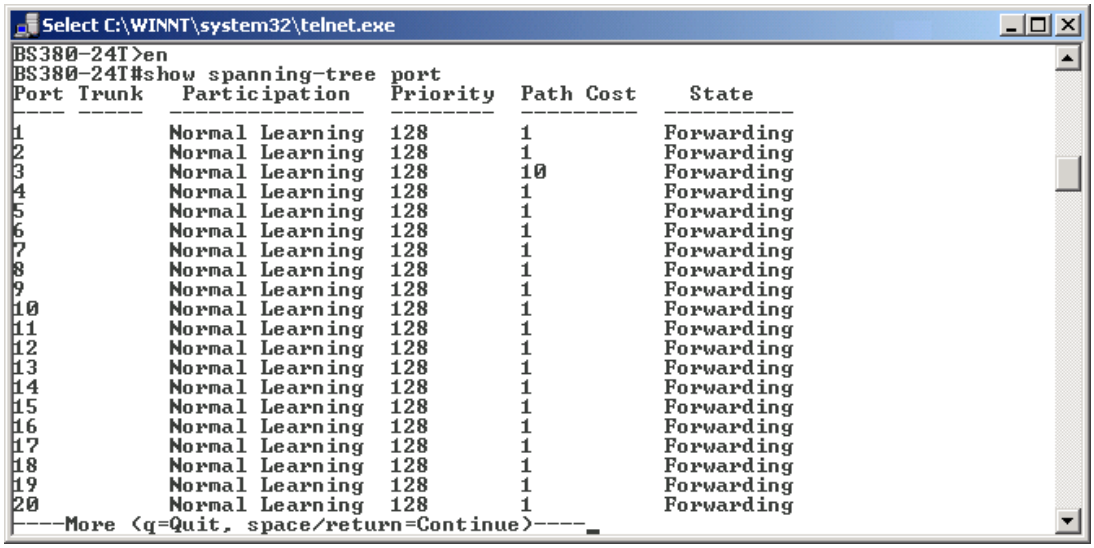
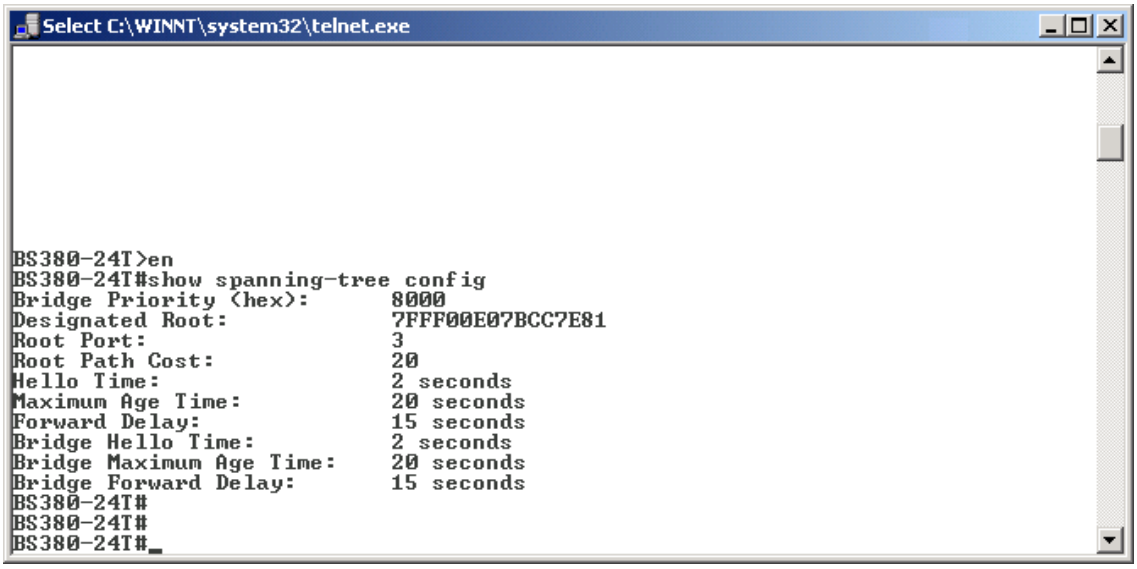


Figure 26 show spanning-tree command output for spanning tree config



spanning-tree command

The `spanning-tree` command sets STP values. The syntax for the `spanning-tree` command is:

```
spanning-tree [forward-time <4-30>] [hello-time <1-10>]
[max-age <6-40>] [priority <0-65535>] [
```

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

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

Table 87 spanning-tree command parameters and variables

Parameters and variables	Description
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.

default spanning-tree command

The `default spanning-tree` command restores the default spanning tree values for the spanning tree group. The syntax for the `default spanning-tree` command is:

```
default spanning-tree [forward-time] [hello-time] [max-age]
[priority]
```

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

Table 88 describes the parameters and variables for the `default spanning-tree` command.

Table 88 default spanning-tree command parameters and variables

Parameters and variables	Description
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.

spanning-tree command by port

Note: For guidelines for configuring STGs, VLANs, and MLTs, refer to Chapter 1 of the *Using the BayStack 380 10/100/1000 Switch, Software Version 3.0*.

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>][learning
{disable|normal|fast}] [cost <1-65535>] [priority
<00|10|20|...|F0>]
```

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

Table 89 describes the parameters and variables for the `spanning-tree` command by port.

Table 89 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.
learning {disable|normal|fast}	Specifies the STP learning mode: • disable—disables FastLearn mode • normal—changes to normal learning mode • fast—enables FastLearn mode

Table 89 spanning-tree command by port parameters and variables

Parameters and variables	Description
cost <1-65535>	Enter the path cost of the spanning tree; range is 1-.65535.
priority <00|10|20|...|F0>	Enter the priority value of the port; range is 00|10|20|...|F0.

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>] [learning] [cost]
[priority]
```

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

Table 90 describes the parameters and variables for the `default spanning-tree` command by port.

Table 90 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.
learning	Sets the spanning tree learning mode to factory default value. Default value for learning is normal mode.

Table 90 default spanning-tree command by port parameters and variables

Parameters and variables	Description
cost	Sets the path cost to factory default value. Default value for path cost depends on the type of port.
priority	Sets the priority to factory default value. Default value for the priority is 0x80.

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>]
```

The `no spanning-tree` command by port is in the config-if command mode.

Table 91 describes the parameters and variables for the `no spanning-tree` command by port.

Table 91 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.

Using MLT

Note: For guidelines for configuring STGs, VLANs, and MLTs, refer to Chapter 1 of the *Using the BayStack 380 10/100/1000 Switch Software Version 3.0*.

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

- "show mlt command," next
- "mlt command" on page 150
- "no mlt command" on page 151

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 92 describes the parameters and variables for the `show mlt` command.

Table 92 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 27 displays sample output from the `show mlt` command.

Figure 27 show mlt command output

```
BS380_24#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
BS380_24#
```

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 93 describes the parameters and variables for the `mlt` command.

Table 93 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 94 describes the parameters and variables for the `no mlt` command.

Table 94 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 380 10/100/1000 Switch Software Version 3.0* for configuration guidelines for port-mirroring. This section covers the following commands:

- "show port-mirroring command," next
- "port-mirroring command" on page 152
- "no port-mirroring command" on page 153

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

Figure 28 show port-mirroring command output

```
BayStack 380 (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 <port#> mirror-port-X <port#>|
Xtx monitor-port <port#> mirror-port-X <port#>
```

Note: In this command, `portlist` must specify only a single port

The `port-mirroring` command is in the config command mode.

Table 95 describes the parameters and variables for the `port-mirroring` command.

Table 95 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.
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.

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 5
VLANs and IGMP

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

Refer to the *Using the BayStack 380 10/100/1000 Switch Software Version 3.0* 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 380 10/100/1000 Switch Software Version 3.0* for information on configuring these features using the Web-based management system, and refer to *Reference for the BayStack 380 10/100/1000 Switch Management Software Version 3.0* for configuration information for the DM.

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:

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

Note: For guidelines for configuring VLANs, spanning tree, and MLTs, refer to Chapter 1 of the *Using the BayStack 380 10/100/1000 Switch Software Version 3.0*.

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.

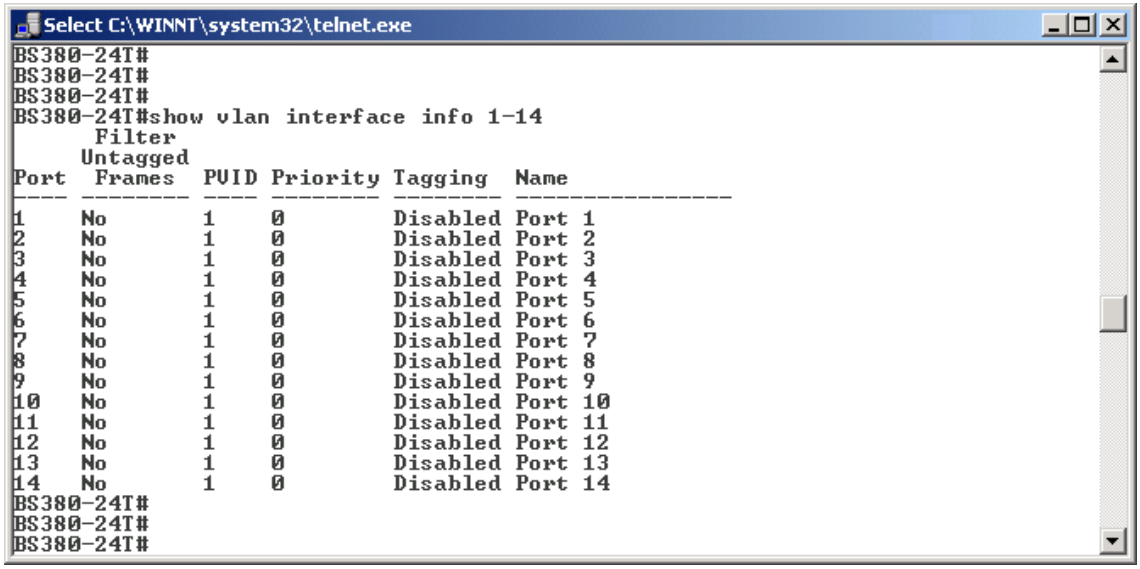
Table 96 describes the parameters and variables for the `show vlan interface info` command.

Table 96 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 29 displays sample output from the `show vlan interface info` command.

Figure 29 show vlan interface info output



show vlan interface vids command

The `show vlan interface vids` command displays the VLANs assigned to ports. 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.

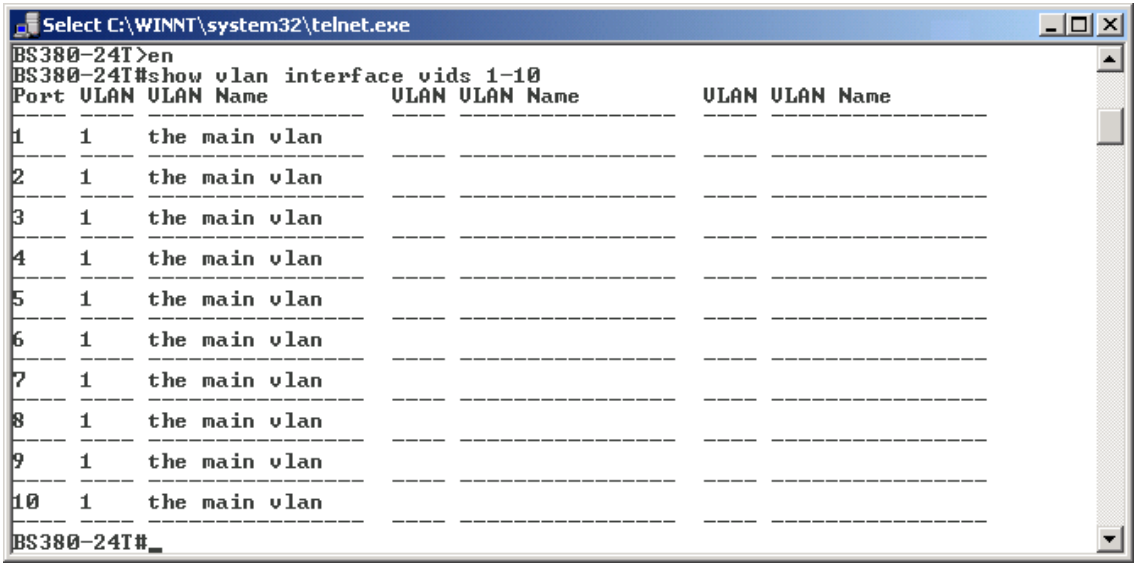
Table 96 describes the parameters and variables for the `show vlan interface vids` command.

Table 97 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 30 displays sample output from the `show vlan interface vids` command.

Figure 30 show vlan interface vids output



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

Table 98 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 VLANs and MLTs, refer to Chapter 1 of the *Using the BayStack 380 10/100/1000 Switch Software Version 3.0*.

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

The syntax for the `vlan create` command is:

```
vlan create <2-4094>] [name <line>] type {port]
```

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

Table 99 describes the parameters and variables for the `vlan create` command.

Table 99 vlan create command parameters and variables

Parameters and variables	Description
<2-4094>	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: • port—port-based

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 <2-4094>
```

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

Table 99 describes the parameters and variables for the `vlan delete` command.

Table 100 vlan delete command parameters and variables

Parameters and variables	Description
<2-4094>	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 99 describes the parameters and variables for the `no vlan` command.

Table 101 no vlan command parameters and variables

Parameters and variables	Description
<1-4094>2	Enter the number of the VLAN to delete.

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 99 describes the parameters and variables for the `vlan name` command.

Table 102 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 380 10/100/1000 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 380 10/100/1000 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-untagged-frame {enable|disable}]
[priority <0-7>] [name <line>]
```

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

Table 103 describes the parameters and variables for the `vlan ports` command.

Table 103 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>	Sets the PVID for the port list.
filter-untagged-frame {enable|disable}	Enables or disables the port to filter received untagged packets.
priority <0-7>	Sets the priority for the switch to use when it forwards packets received on the ports in <portlist>.
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] <2-4094> <portlist>
```

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

Table 104 describes the parameters and variables for the `vlan members` command.

Table 104 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.
<2-4094>	Specifies the target VLAN.
portlist	Enter the list of port(s) you are adding, removing, or assigning to the VLAN.

show vlan command

The `show vlan` command displays the configured VLANs. The syntax for the `show vlan` command is:

```
show vlan
```

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

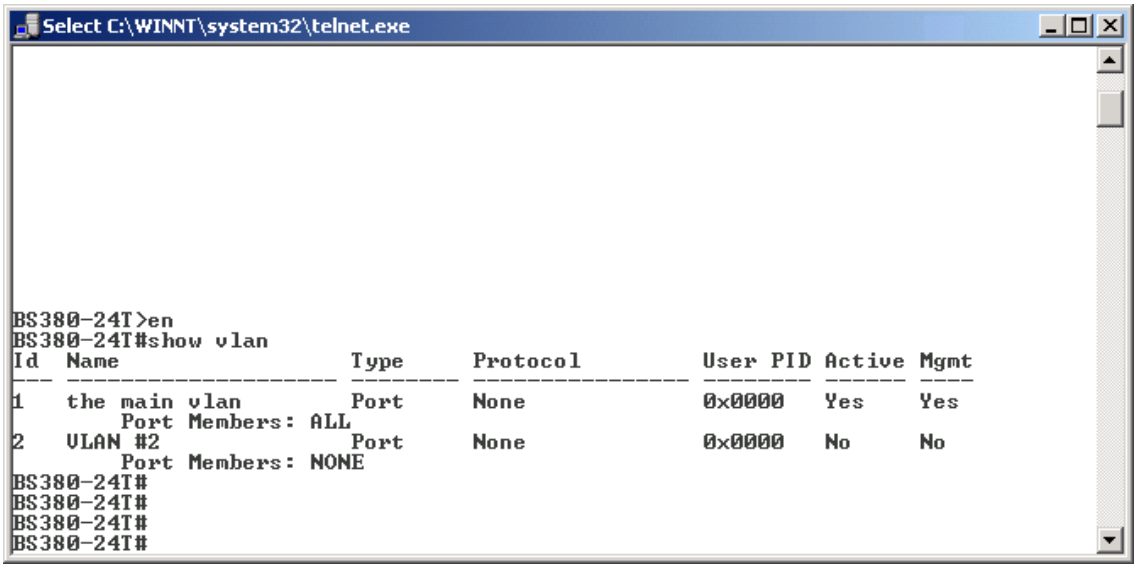
Table 105 describes the parameters and variables for the `show vlan` command.

Table 105 show vlan command parameters and variables

Parameters and variables	Description
<2-4094>	Enter the number of the VLAN you want to display MAC source addresses for.

Figure 31 displays sample output from the `show vlan` command.

Figure 31 show vlan command output



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

Table 106 show vlan multicast membership command parameters and variables

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

Figure 32 displays sample output from the `show vlan multicast membership` command.

Figure 32 show vlan multicast membership command output

```
BS380(config)#sh vlan multicast membership 1
Multicast Group Address Port
----------------------- ----
225.0.0.192             23
225.0.0.183             22
225.0.0.174             21
225.0.0.93              12
225.0.0.84              11
225.0.0.75              10
225.0.0.165             20
225.0.0.156             19
225.0.0.66              9
225.0.0.57              8
225.0.0.147             18
225.0.0.138             17
225.0.0.48              7
225.0.0.94              12
```

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 168
- "default vlan igmp command" on page 169

show vlan igmp command

The `show vlan igmp` command displays the IGMP snooping configuration. The syntax for the `show vlan igmp` command is:

```
show vlan igmp <1-4094>
```

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

Table 107 describes the parameters and variables for the `show vlan igmp` command.

Table 107 show vlan igmp command parameters and variables

Parameters and variables	Description
<1-4094>	Specifies the VLAN to display IGMP snooping configuration.

Figure 33 displays sample output from the `show vlan igmp` command.

Figure 33 show vlan igmp command output

```
BS380_24#show vlan igmp 1
Snooping:  Enabled
Proxy:  Enabled
Robust Value:  2
Query Time:  125 seconds
IGMPv1 Static Router Ports:
IGMPv2 Static Router Ports:
```

vlan igmp command

The `vlan igmp` command configures IGMP snooping parameters. The syntax for the `vlan igmp` command is:

```
vlan igmp {<1-4094> [snooping {enable|disable}]
[proxy {enable|disable}] [query-interval <time>] }
```

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

Table 108 describes the parameters and variables for the `vlan igmp` command.

Table 108 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.
query-interval <time>	Enter the number of seconds you want for the query interval of IGMP.

Table 108 vlan igmp command parameters and variables

Parameters and variables	Description
v2-members <portlist>	Enter the list of ports for port membership for IGMP v2.
unknown-mcast-no-flood	Enables or disables the flooding of packets with unknown multicast addresses.

default vlan igmp command

The `default vlan igmp` command sets all IGMP snooping parameters to the factory default settings. The syntax for the `default vlan igmp` command is:

```
default vlan igmp <1-4094>
```

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

Table 108 describes the parameters and variables for the `default vlan igmp` command.

Table 109 default vlan igmp command parameters and variables

Parameters and variables	Description
<1-4094>	Enter the VLAN to configure for IGMP.

Appendix A
Command List

This appendix provides the complete CLI command list in alphabetical order, with approximate page references for the beginning pages of further explanations.

Note: This information is presented for reference only and should not be considered to be an exact representation.

Table 110 CLI command list

Command	Page No.
auto-pvid	page 162
autotopology	page 98
boot [default]	page 61
clear logging [nv]	page 86
clear-stats [port<portlist>]	page 90
cli-password {ro|rw} <WORD> <WORD> cli-password {serial|telnet} {none|local|radius}	page 32
configure {terminal|network|memory}	page 38
configure network [load-on-boot {disable|use-bootp|use-config}] configure network [filename <WORD>] configure network [address <XXX.XXX.XXX.XXX>]	page 50
copy config tftp [address <XXX.XXX.XXX.XXX>] filename <WORD>	page 65
copy tftp config [address <XXX.XXX.XXX.XXX>] filename <WORD>	page 65
default autotopology	page 99
default duplex [port <portlist>]	page 97
default flowcontrol [port <portlist>]	page 102
default ip address	page 57
default ip bootp server	page 62

Table 110 CLI command list (continued)

Command	Page No.
default mac-address-table aging-time	page 44
default name [port <port.ist>]	page 94
default logging	page 86
default snmp trap link-status [port <portlist>]	page 76
default spanning-tree [forward-time] [hello-time] [max-age] [priority] [tagged-bpdu]	page 145
default spanning-tree [port <portlist>] [stp <1-8>] [learning] [cost] [priority]	page 147
default speed [port <portlist>]	page 95
default telnet-access	page 60
default vlan igmp {<1-4094>}	page 169
default vlan mgmt <1-4094>	page 159
disable	page 39
download [address <ip>] {image <image-name> | image-if-newer <image name> | diag <filename>}	page 66
duplex [port <portlist>] {full|half|auto}	page 96
enable	page 37
end	page 39
exit	page 39
flowcontrol [port <portlist>] {asymmetric|symmetrid|auto|disable}	page 100
help	page 35
interface FastEthernet {<portlist>}	page 38
ip address[switch] <XXX.XXX.XXX.XXX> [netmask <XXX.XXX.XXX.XXX>]	page 53
ip bootp server {last|needed|disable|always}	page 61
ip default-gateway <XXX.XXX.XXX.XXX>	page 54
logout	page 37
mac-address-table aging-time <time>	page 43
mac-security [disable|enable] [learning-ports <portlist>] [learning {enable|disable}] [snmp-lock {enable|disable}]	page 133
mac-security [port <portlist>] {disable|enable|learning}	page 136
mac-security mac-address-table address <H.H.H.> {port <portlist>}	page 134
mlt <id> [name <trunkname>] [enable|disable] [member <portlist>] [learning {disable | fast | normal}]	page 150

Table 110 CLI command list (continued)

Command	Page No.
name [port <portlist>] <LINE>	page 92
no auto-pvid	page 162
no autotopology	page 99
no flowcontrol [port <portlist>]	page 101
no ip address {switch}	page 53
no ip address unit <1-8>	page 57
no ip bootp server	page 62
no ip default-gateway	page 55
no mac-security	page 134
no mac-security mac-address-table {address <H.H.H>|port <portlist>|security-list <1-32>]	page 135
no mlt [<id>]	page 151
no name [port <portlist>]	page 93
no port-mirroring	page 153
no radius-server	page 139
no set logging	page 86
no shutdown [port <portlist>]	page 91
no snmp server [authentication-trap|community [ro|rw] contact|host [<host-ip> <community-string>] [location|name]	page 73
no snmp trap link-status [port <portlist>]	page 76
no telnet-access [source-ip [<1-10>]]	page 59
no tftp-server	page 64
ping <XXX.XXX.XXX.XXX>	page 48
port-mirroring mode disable port-mirroring mode Xrx monitor-port <portlist> mirror-port X <portlist>	page 152
radius-server host <address> [secondary-host <address>] port <num> key <string>	page 138
set logging [enable|disable] [level critical|serious|informational] [nv-level critical|serious|informational|none]	page 85
show config-network	page 51
show interfaces [names] [<portlist>]	page 69
show ip [bootp] [default-gateway] [address [switch]]	page 55

Table 110 CLI command list (continued)

Command	Page No.
show logging [critical] show logging [serious] show logging [informational]	page 83
show mac-address-table [aging-time] show mac-address-table [vid <1-4094>] [address <H.H.H.>]	page 42
show mac-security {config|mac-address-table [addr <macaddr>]|port|security-lists}	page 132
show mlt [utilization <1-6>]	page 149
show port-mirroring	page 152
show port-statistics [port <portlist>]	page 87
show radius-server	page 137
show rmon alarm	page 77
show rmon event	page 78
show rmon history	page 78
show rmon stats	page 79
show spanning-tree {config|port}	page 142
show sys-info	page 40
show telnet-access	page 58
show terminal	page 46
show tftp-server	page 63
show vlan igmp <1-4094> | unknown-mcast-no-flood	page 167
show vlan interface info [<portlist>]	page 156
show vlan interface vids [<portlist>]	page 157
show vlan mac-address <1-4094> [<H.H.H>]	page 164
show vlan multicast membership <1-4094>	page 164
shutdown [port <portlist>]	page 90
snmp trap link-status [port <portlist>]	page 75
snmp-server {{enable|disable}|authentication-trap|community <community-string> [ro|rw] contact <text>|host <host-ip> <community-string>|location >text>|name <text>}	page 72
spanning-tree [forward-time <4-30>] [hello-time <1-10>] [max-age <6-40>] [tagged-bpdu {enable|disable}] [tagged-bpdu-vid <1-4094>] [multicast-address<H.H.H>]	page 144
spanning-tree [port <portlist>] [learning {disable|normal|fast}] [cost <1-65535>]	page 146

Table 110 CLI command list (continued)

Command	Page No.
spanning-tree [forward-time <4-30>] [hello-time <1-10>] [max-age <6-40>] [priority <0-65535>] [tagged-bpdu {enable|disable}] [tagged-bpdu-vid <1-4094>]	page 144
spanning-tree [port <portlist>] [learning {disable|normal|fast}] [cost <1-65535>] [priority <0-255>]	page 147
speed [port <portlist>] {10|100|1000|auto}	page 94
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 58
terminal {2400|4800|9600|19200|38400}|length <1-132>|width <1-132>	page 47
tftp-server <XXX.XXX.XXX.XXX>	page 64
vlan create <1-4094> type port	page 159
vlan create <1-4094> type port learning	page 159
vlan delete <1-4094>	page 160
vlan igmp <1-4094> [snooping {enable|disable}] [proxy {enable|disable}] [robust-value <value>] [query-interval <time>] [v1-members <portlist>] [v2-members <portlist>]	page 168
vlan members <1-4094> <portlist> vlan members add <1-4094> <portlist> vlan members remove <1-4094> <portlist>	page 163
vlan mgmt <1-4094>	page 158
vlan name <1-4094> <line>	page 161
vlan ports [<portlist>] [tagging {enable|disable}] [pvid <1-4094>] [filter-untagged-frame {enable|disable}] [priority <0-7>] [name <line>]	page 162

Index

E

F

G

H

I

L

M

N

P

Q

R

S

T

U

V

W