Part No. 215148-A
May 2003

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the BayStack operating System Switching Software (BoSS) 3.0 for BayStack 460, 470, and BPS 2000

215148-A

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 Inc.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, BayStack 470, and Optivity are trademarks of Nortel Networks.

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Java is a trademark of Sun Microsystems, Inc.

Macintosh is a trademark of Apple Computer, Inc.

Netscape Navigator is a trademark of Netscape Communications Corporation.

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.

Contents

Introduction

These release notes contain important information about Nortel Networks BayStack operating System Switching Software (BoSS) version 3.0 that is not available in the following:

- BayStack 450 documentation set
- BayStack 460 documentation set
- BayStack 470-24T documentation set
- BayStack 470-48T documentation set
- Business Policy Switch 2000 documentation set

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. 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.

Note: This document uses the terms “mixed stack” and “hybrid” stack interchangeably.

Note: To prevent configuration corruption of devices in a stack when upgrading to software version 3.0.0, you must disable IGMP snooping. Beginning with software version 3.0.0, this issue has been resolved.

These release notes contain sections that describe the following:

- Downloading BayStack operating System Switching Software
- Known Issues in BayStack operating System Switching (BoSS) Software Version 3.0
- Known interoperability issues with Passport 8600 v3.3 release
- Stacking

  - Pure stacking (stacking with only one type of unit - BayStack 460s, 470s, or BPS 2000s - but NO BayStack 450s)
  - Allied stacking (stacking two or more of the BPS 2000, BayStack 470-24T and 48T, and the BayStack 460-24T, but NO BayStack 450s)
  - Mixed stacking (stacking one or more of the BPS 2000, BayStack 470-24T, or the BayStack 460-24T, with the BayStack 450, but NO BayStack 470-48T).
- Secure Shell (SSH)
- Far End Fault Indication (FEFI)
- Single Fiber Fault Detection (SFFD)
- SNMPv3 enhancements
- NNCLI commands for BoSS 3.0
- Customizing the opening banner
- Displaying Unit uptime
- Default management system
- Security features of BoSS 3.0

Downloading BayStack operating System Switching Software (BoSS) 3.0

Note: If you are downloading software to a mixed stack that contains a BayStack 450 switch, refer to “Upgrading software in a mixed stack” on page 27.

There are two images of the 3.0 software:

- One image contains the Secure Shell (SSH) feature.
- One image does not contain the SSH feature

Image with SSH

Note: Encryption algorithms included in the SSH feature are subject to export controls under the U.S. Department of Commerce Bureau of Export Administration Act.

When downloading the image file that includes the SSH feature, you will first be required to fill out a questionnaire verifying that you are eligible to download the software.

Note: If you choose to download and install the image file that includes the SSH feature, you will no longer have access to the console menu on the device. However, you can use the Nortel Networks Command Line Interface (NNCLI).

To obtain the BoSS 3.0 software for the BayStack 460, 470 or BPS 2000 that contains SSH, download the following files from the Nortel Networks customer support web site at http://support.nortelnetworks.com/:

- boss300ys.img (software image file with SSH where y is an odd number)
- boss300z_diag.bin (diagnostics file - where z is a number)

You must download the diagnostics file as well as the software file.

Note: Ensure that you do not interrupt the download process; do not detach either the power cord or any of the network connections during download.

Image without SSH

To obtain the BoSS 3.0 software for the BayStack 460, 470 or BPS 2000 that *does not* contain SSH, download the following files from the Nortel Networks customer support web site at http://support.nortelnetworks.com/:

- boss300x.img (software image file where x is an even number)
- boss300z_diag.bin (diagnostics file - where z is a number)

You must download the diagnostics file as well as the software file.

Note: Ensure that you do not interrupt the download process; do not detach either the power cord or any of the network connections during download.

Device Manager image

To obtain the Device Manager (DM) software to manage the BayStack 460, 470 or BPS 2000, download the following file from the Nortel Networks customer support web site at http://support.nortelnetworks.com/:

- DM 5.6.1

For complete information on downloading and using DM, refer to the *Reference for the BayStack 470-48T 10/100/1000 Switch Management Software*.

Fixed Issues in BayStack operating System Switching (BoSS) Software Version 3.0

- Stack resets with IGMP joins/leaves no longer cause configuration corruption of other units in the stack. (CR Q00664743)

Known Issues in BayStack operating System Switching (BoSS) Software Version 3.0

Configuration issues

- Please make sure you backup your configuration file periodically. The configuration file may become corrupt if the unit experiences a loss of power. (Q00593649), (Q00604762), (Q00518226)

MAC Address Security issues

- Do not enter the following characters in the MAC Security Port list:

- [+, - or ,]

These characters might cause the switch to stop operating properly in the stack. (Q00637930)

- If you add MAC addresses to Security Lists that do not have ports associated with them, and then display the Security Lists, the lists will appear empty until a port is associated with the list. (Q00622842)
- On the BayStack 450 in a mixed stack configuration, make sure that you re-enable Global Security when you make any changes to the security parameters to ensure that the changes take effect. (Q00620973)

IGMP issues

- IGMP reports may appear to be associated with several VLANs. This display issue does not effect IGMP functionality or performance. (Q00623137)
- When using BoSS 3.0, with IGMP enabled, in conjunction with the Passport 1200, make sure that the IGMP Proxy parameter is enabled on the BoSS 3.0 unit. This is due to an issue with the Passport 1200. (Q00591972)
- When displaying the number of IGMP hosts on a stack, the number of hosts displayed may be 20 to 25 percent of the actual count. You may determine the actual count of IGMP hosts in the stack by interrogating each of the units in the stack. (Q00626413)

Stack issues

- A mixed stack may reset twice after being booted or rebooted. This may cause a slight delay in booting the stack. (Q00617280)
- Managing a stack through the console port of a BayStack 450 is not supported in this release. Please use the console port of the base unit. (Q00605113) (Q00615550)
- If you disable all Link up and down traps on the front panel interfaces, you may still see link up traps reflecting the fact that cascade ports are initializing. (Q00628942)
- The Port IfIndex allocates resources for thirty-two ports per unit on a hybrid stack and sixty-four ports per unit on a non-hybrid stack. Therefore, on a hybrid stack IfIndex ports 1-32 are assigned to unit 1, ports 33-64 are assigned to unit 2, ports 65-96 are assigned to unit 3, and so one. On a non-hybrid stack, IfIndex ports 1-64 are assigned to unit 1, ports 65-128 are assigned to unit 2, ports 129-192 are assigned to unit 3, and so one. (Q0060659)

- Occasionally, in order for a stack to reform, the entire stack must reset. This may happen when BayStack 450 is power cycled while in the stack. (Q00607599)

EAPoL issues

- On BayStack 450 software version 4.2.0.22, the EAPoL Reauthentication parameter is not supported.
- A BPS 2000 hangs when it receives an EAP access reject from an ACS radius server. The problem appears very quickly if you retrieve a show command from the cli. For example: show int or show EAPol. (Q00666030)
- The EAPoL configuration parameter "Maximum Requests" has no effect. The unit will only send out three EAP-Request/Identity frames before sending a Failure frame and restarting the authentication process. (Q00637063)

Secure Shell (SSH) issues

- When you download the DSA Authorization key for the first time, the transfer may time out. Simply re-initiate the key download sequence. (Q00626440)
- After rebooting the system, the Last key transfer result is not displayed correctly. The display shows "Other: Error 0.", but the DSA-Key works properly. (Q00597567)
- It may take up to 10 minutes for the DSA key to be generated, and you will not receive a message when the generation is completed. You cannot authenticate an SSH session to a switch using the DSA key authentication until the key has been fully generated. (Q00627029)
- For port mirroring, all packets are sent to the monitor port after SSH has been enabled and the stack has been rebooted. (Q00605912)
- If the DSA public key download fails, the following message will be displayed if the action was initiated through the console port: "Cannot modify settings, Undo Failed 1." No message is displayed if the action was initiated through telnet, but the following message will appear in the last transfer results of the "show ssh download" command: "Other: Error 5." (Q00578979)
- You cannot enable SSH while the DSA public key is being generated. If you attempt to enable SSH during the key generation period, you may see the following error: "cannot modify settings." (Q00626985)

Distributed Multilink Trunking (DMLT) issues

- If you have a DMLT configured, and one of the units that has a configured link fails, the NNCLI displays the link as belonging to port yy. For example: 2/yy. (Q00624397)
- Autotopology packets will not be transmitted on a link that is connected to a DMLT if the unit is reset. Autotopology packets will continue to be received from the units in the stack that were not reset. (Q00633687)
- Traffic flow will be interrupted on DMLT for around 30 seconds if a BayStack 450 contains one of the links that is reset when the switch loses power. (Q00606295)

Radius Security issues

- If you enter an incorrect password while using RADIUS authentication to restrict management access to the device, the following error message appears: "no response from RADIUS servers". (Q00560496)

Nortel Networks Command Line Interface (NNCLI) issues

- In a hybrid stack, when the base unit fails and the temporary base units takes over management responsibilities for the stack, the MAC address table cannot be displayed through the NNCLI. The web interface will show the proper information. (Q00637611)
- If you are running the non-SSH version of BoSS 3.0 AND you set the default user interface to be the CLI, three incorrect login attempts via telnet will allow a user to gain access to the switch without needing to properly authenticate. For the highest level of security, Nortel Networks recommends that you either do not set the default user interface to use the CLI at this time or you run the SSH enabled version of BoSS 3.0.
- In the NNCLI, changing the STP participation for all ports also changes the MLT STP settings. Use the console or web-based management interface instead of the NNCLI. (Q00598466)
- When adding a user with privacy, the NNCLI does not allow you to omit the write-view and specify the notify-view. The NNCLI requires that you enter a read-view, write-view, and notify-view. If you do not wish to enter a write-view for the user, you may use the web interface to create the user. (Q00636313)
- You cannot use the NNCLI to delete an SNMP v3 trap destination entry that was created using the web interface or Device Manager. (Q00622221)

- The "show stack-info uptime" command does not display the uptime for BayStack 450 switches. (Q00587447)
- If you clear the log using the NNCLI "clear logging" command in a stack of 8 units, the entries related to unit 8 may not be removed. (Q00625617)
- Full duplex is the only setting that is valid on GBIC ports in the BayStack 470-24T, BayStack 470-48T, and BPS2000 2GE-MDA. If you try to set this parameter to any other value, you may see the following error:

  % Cannot modify settings

  % inconsistentValue <port_number>

  (Q00539706)

Spanning Tree Protocol (STP) issues

- In a stack with a large number of units (e.g. 6 to 8), a large number of VLANs AND a large number of Spanning Tree Groups (STGs), STG configurations may fail to be propagated to the most distant units in the stack. This issue only affects non-default STGs (i.e. STG IDs not equal to 1). When this issue is being experienced, ports on a unit in the stack will fail to send out BPDUs for any affected non-default STGs. Ports on other units in the stack which belong to this same STG may still correctly carry out the tasks of the STP.

  A soft reset of an affected unit will cause the STG configuration information to be re-acquired from the base unit and will correct this problem.
- If you enable port mirroring on a port that has STP enabled, when you disable port mirroring, you must manually re-enable STP support for that port. (Q00617551)
- You cannot change STP bridge priority, port priority, or path cost using the console interface. Use the NNCLI, web-based management, or Device Manager. (Q00592138)

Device Manager (DM) issues

- When using Device Manager, and changing information on multiple ports, the Device Manager may display a message that the application is in "fetching mode." If this message appears for more than a few seconds, Device Manager application must be restarted. To avoid this error condition when using Device Manager, do not attempt to change the configuration of more than a few ports at a time. (Q00614887)

- When using Device Manager, the "UndersizePkts" count is not updated for the BPS2000 1000MB MDAs. This statistic may be obtained through the Console Interface menu system, the Nortel Networks Command Line Interface, or the Web Interface. (Q00608569)
- The MAC address security parameter "AuthCtlPartTime" is not supported through Device Manager. Use the NNCLI or the Web Interface to set this parameter. (Q00623812)
- When using Device Manager an SNMP V3 user with DES privacy cannot receive traps. (Q00622622)
- Device Manager will not identify the ports that have STP disabled on the STP->Ports screen. Use the NNCLI or Web Interface to set this parameter. (Q00607218)
- When managing a BayStack 450 switch using Device Manager, it may take up to 20 seconds for the unit to become editable after the edit menu option is invoked. (Q00607328)
- In a stacked configuration, after creating a new Spanning Tree Group (STG) using Device Manager, the stgid may return a value of "0" when you attempt to add a VLAN to the STG. Refresh the view of the stack and the stgid parameter will return the correct value. (Q00584031)
- You may encounter problems using Internet Explorer to access help items in the right-hand frame of the online help screen. To avoid this problem, access the help items you want through the Table of Contents in the left-hand frame of the online help. (Q00561521)

Web Interface issues

- Using the Web Interface, you may only change the EAPoL Re-Authentication Field for individual ports. As a workaround, you may use the Console Interface menu system, or the NNCLI. (Q00636903)
- When using the Web interface, the version number of the software shown in "Stack info > System Description" may be truncated. Use the NNCLI to query the software version number. (Q00597301)
- Using the Web interface, you cannot configure flow control for BS450 in a mixed stack. Use the NNCLI or console interface. (Q00628278)

SNMPv3 issues

- When using SNMP V3, you may only assign a notify-view address to one user. You may not use the same target IP address for multiple users. (Q00615644)

Download issues

- During the download process, the console may appear to hang. You can verify that the download is in progress by the state of the LEDs. You may see the following error message: `% error accessing image file,` but the download will continue. (Q00596530)

Port mirroring issues

- You cannot disable port mirroring through the console interface. Use another interface. (Q00620633)

Telnet issues

- If you default a unit and re-enter the same IP station addresses that were in the ARP table, you may not be able to manage the switch. Either manage the switch from another station, or reboot the stack. (Q00565566)

QoS issues

- When specifying an IP filter to a particular destination, if there are two or more filters, the source address must specify a particular host. (Q00599978)
- The ShapingQDrops parameter is not supported in Device Manager for the BayStack 470 switches. (Q00647900)

Known interoperability issues with Passport 8600 v3.3 release

- There may be STP convergence issues with Multilink trunking when there is an STP priority/port path cost change, with uplink to the 8600. To correct this problem, disable and re-enable MLT. (Q00604730).

Stacking

There are three types of stacking for BayStack 460, 470 and BPS 2000:

- Pure stacks:
  - BS470-48T only
  - BS470-24T only
  - BS460-24T only
  - BPS 2000 only
- Allied stacks (do not include BayStack 450 units):
  - BS470-48T and BS 470-24T and BS 460 and BPS 2000
  - BS470-48T and BS 470-24T and BS 460
  - BS470-48T and BS 470-24T and BPS 2000
  - BS470-48T and BS 460 and BPS 2000
  - BS470-48T and BS 460
  - BS460 and BPS 2000
  - BS470-24T and BPS 2000
- Mixed (hybrid) stacks (Include BS 450 units but not BS470-48T):
  - BPS 2000 and BS 460 and BS470-24T and BS450
  - BPS 2000 and BS450
  - BS 450 and BS460
  - BS470-24T and BS450

Table 1 Stacking options matrix

	BPS	**460-24T PWR**	**470-24T**	**470-48t**	**450**
BPS	pure	allied	allied	allied	mixed
460-24T PWR	allied	pure	allied	allied	mixed
470-24T	allied	allied	pure	allied	mixed
470-48T	allied	allied	allied	pure	no
450	mixed	mixed	mixed	no	N/A

Note: All switches except the BayStack 450 switch must be running software release 3.0. The BayStack 450 switch *cannot* load release 3.0. All BayStack 450 switches must be running software version 4.2.0.22.

Note: A mixed stack connot contain both a BayStack 450 and a BayStack 470-48T unit. You also cannot have more than 8 units in a stack.

This section covers the following topics:

Pure stacking

A pure stack is made up of 460s only, 470 -24Ts only, 470-48Ts only, or BPS 2000s only. The stacking operating mode for pure stacking is Pure Stack.

Allied stacking

An allied stack is a stack that combines BayStack 460, 470 and BPS 2000 switches. The stacking operating mode for allied stacking is Pure Stack.

Note: The BayStack 450 switch does not belong in an allied stack. For information on stacking with the BayStack 450 switch, refer to "Mixed stacking" on page 21.

All switches in the stack must be running software release 3.0. Units of the same type must be placed next to each other. Release 3.0 does not support interleaving switch types within the stack.

The base unit in an allied stack *cannot* be a BPS 2000. Any one of the following switches can function as a base unit in an allied stack; but if a BayStack 470-48T switch is in the stack, it must be the base unit:

- BayStack 460-24T switch
- BayStack 470-24T switch
- BayStack 470-48T switch

You must use either the console interface (CI) menus or the NNCLI to configure the IP addresses for each unit within a stack. You need an IP address to use the Web-based management system or Device Management (DM). Subsequently, you can change the IP address configuration from the Web management or DM, but you will lose access until you restart the Web or DM with the new IP address.

Mixed stacking

The mixed stack can be a mixture of the following switches:

- BayStack 450 switch
- BayStack 460 switch
- BayStack 470-24T switch
- BPS 2000 switch

The stacking operating mode for mixed stacking is Hybrid Stack.

Note: The BayStack 470-48T switch cannot join a mixed stack (or one containing the BayStack 450 switch). For information on stacking the BayStack 460, 470 or BPS 2000 with the BayStack 470-48T switch, refer to “Allied stacking” on page 21.

All switches except the BayStack 450 switch must be running software release 3.0; the BayStack 450 switch *cannot* load release 3.0. All BayStack 450 switches must be running software version 4.2.0.22.

Units of the same type must be placed next to each other. Release 3.0 does not support interleaving switch types within the stack.

Base unit for a mixed stack

In order of preference, one of the following switches can function as a base unit in a mixed stack:

- If a BayStack 470-48T switch is in the stack, it should be the base unit.
- Otherwise, if a BayStack 470-24T switch is in the stack, it should be the base unit.
- Otherwise, if a BayStack 460-24T PWR switch is in the stack, it should be the base unit.
- Otherwise, the BPS 2000 should be the base unit.

Note: The BayStack 450 switch can never be the base unit of a stack.

Note: The BayStack 460 and BayStack 470 switches are the preferred base units of a stack because these switches have more memory than the BPS 2000 switch.

Contiguous units

In a mixed or allied stack, the same types of switches must be stacked contiguously, and in the following order:

- All Baystack 450 units
- All BPS 2000 units
- All Baystack 460-24T PWR units
- All Baystack 470-24T units
- All Baystack 470-48T units

When stacking the switches, keep in mind the base unit restrictions, and remember that BayStack 470-48T switches cannot stack with the BayStack 450 switch. Also remember to plan for which unit will be the temporary base unit in the event of a base unit failure.

You must use either the console interface (CI) menus or the NNCLI to configure the IP addresses for each unit within a stack. You need an IP address to use the Web-based management system or Device Management (DM). Subsequently, you can change the IP address configuration from the Web management or DM, but you will lose access until you restart the Web or DM with the new IP address.

Building a mixed stack

To build a mixed stack, do the following:

1. Power up the base unit only.
2. In the console screen, go to "Switch Configuration" in the Main Menu.
3. Select "Stack Operational Mode".
4. Select " "Hybrid Stack" in the Next Stack Operational Mode.
5. Reboot the switch.
6. Turn on the power for all of the units in the stack.

Merging a switch into a stack

Nortel Networks recommends that you start up the switch you are going to add to the stack initially in a standalone mode and perform preliminary IP configuration tasks before you add it to an existing stack.

Adding a new unit does not change the designated base unit. If you want to change the designated base unit when you add a new unit to the stack, you must manually change the base unit:

7 Turn off power to all units in the stack by unplugging the power cords from each unit.

- **a** On the unit that was the Base Unit, use the Unit Select switch to deselect it as the Base Unit.
- **b** On the unit that you want to be the new Base Unit, use the Unit Select switch to select it as the Base Unit
- **c** Redo all the cabling so that all the units will work as one stack.

8 Power-up the newly joined units by plugging in the power cords.

It may take a few minutes for the entire stack to display on the console. All units will display as their new numbers within the newly formed stack.

If you are running a pure stack that consists of only BPS2000s, and you add a BayStack 460, a BayStack 470-24T switch, or a BayStack 470- 8T switch to create an allied stack, you must manually change the base unit from a BPS 2000 switch.

Joining stacks

You can join two stacks without renumbering units in either stacks.

Note: You cannot have a BayStack 450 switch in an allied stack, and you cannot have a BayStack 470-48T switch in a mixed stack.

To join two existing stacks:

1 Designate one stack as the one to join the other stack.

2 Reset the stack that will join the other stack to factory defaults.

3 Turn off power to all units in the stack that will join the other stack by unplugging the power cords from each unit.

   a On the unit that was the Base Unit for this stack, use the Unit Select switch to deselect it as the Base Unit.

   b Redo all the cabling so that all the units will work as one stack.

4 Power-up the newly joined units by plugging in the power cords.

It may take a few minutes for the entire stack to display on the console. All units will display as their new numbers within the newly formed stack.

Automatic failover

The automatic failover is a temporary safeguard only. When you lose the base unit of a stack, one of the other units in the stack takes over as the base unit. If the stack as a whole loses power or is reset, the temporary base unit does not power up as the base unit when the power is restored.

For this reason, you should always explicitly reassign the temporary base unit to act as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced. When a failure of the base unit is discovered, the Unit Select switch on the temporary base unit should be set to Base.

Note: If you do not reassign the temporary base unit as the new base unit and the temporary base unit fails, the next unit in the stack becomes the new temporary base unit. This process can continue until there are only two units left in the stack configuration.

Temporary base unit in mixed stacks

This section discusses temporary base units in two situations:

- when all units except one are BayStack 450 switches
- when other types exist in the stack along with a BayStack 450 switch

If all the units save one in your mixed stack are BayStack 450 switches, that one other unit will be the base unit. If that unit fails, the next upstream BayStack 450 switch becomes the temporary base unit and continues the stack operation.

If there are other units in your mixed stack in addition to the BayStack 450, all the other units in the stack will be exhausted, successively, as base units before assigning a BayStack 450 switch as the base unit.

Limitations of mixed stacks

Some features are not supported in the mixed stack configuration. Table 2 displays the features affected by mixed stack configurations.

Table 2 Feature limitations of mixed stack configuration

Feature	Mixed stack	Allied stack
Number of VLANs	64	256
Spanning Tree Groups	Single instance	Up to 8
VLAN learning	Shared VLAN Learning (SVL) only	Both Independent VLAN Learning (IVL) and Shared VLAN Learning (SVL) See the Using Guide for the BayStack 460, 470, or BPS 2000 switch for more information about about Independent and shared VLAN learning.
Egress VLAN tagging	Not Supported	Supported
MAC-based VLAN	Not Supported	Supported

Note: If you change from an allied stack (or pure stack) to a mixed stack, you will lose the configuration.

Upgrading software

Different procedures for upgrading must be followed depending on whether you are upgrading an allied (or pure) stack or a mixed stack.

The stacking software compatibility requirements are as follows:

- Allied (or pure) stack—All units must be running software release 3.0.
- Mixed stack:
  - — The BayStack 470-24T, BayStack 460, and BPS 2000 switches must be running software release 3.0.
  - — The BayStack 450 switches must be running software version 4.2.0.22.

This section discusses the following topics:

- "Upgrading software in an allied stack," next section
- "Upgrading software in a mixed stack" on page 27

Upgrading software in an allied stack

Using the base unit, you can download the software to all units in the stack. To download, or upgrade, software in an allied (or pure) stack:

1. Download the operational software image.
2. Download the diagnostics image.

Note: Once you begin the upgrading process, do not interrupt power to the stack.

Upgrading software in a mixed stack

The physical order of the units and the unit numbering in the mixed stack does not affect the upgrading process. However, you must ensure that either a BayStack 460, BPS 2000 or a BayStack 470-24T switch is Unit 1 and is the base unit.

Note: The software on the BayStack 450 switch in an mixed stack should be the latest version of the software.

Note: Be sure to upgrade the software on the BayStack 450 switch to version 4.2.0.22 before you incorporate the BayStack 450 switch into in a mixed stack.

Using the base unit, you can download the software to all units (except any BayStack 450 switches) in the stack. To download, or upgrade, software in a mixed stack:

1. Download the operational software image.
2. Download the diagnostics image.

Note: Once you begin the upgrading process, do not interrupt power to the stack.

Inserting or replacing units in a stack

This section provides you with the procedural steps required to successfully replace a failed unit in a stack configuration, while preserving configuration information. There are essentially four steps that you need to take:

- Prepare the new replacement unit for insertion into the stack
- Insert the replacement unit into the stack
- Download the configuration to the stack
- Re-cable the networking ports on the replacement unit

When you prepare your replacement unit for insertion into a stack, the replacement unit must have the identical configuration of the unit that it is replacing in order to work properly in the stack. The following steps will ensure that the unit will be successfully integrated into the stack:

Replacing a Failed Base Unit

1. Ensure that the software and firmware version on the replacement unit matches the software and firm ware version of the unit that was removed from the stack. This step assumes that you did not upgrade the software on the stack after the failed unit was removed.

2 Ensure that the hardware configuration of the replacement unit is the same as the failed unit. This means that the MDAs, GBIC, and other modules that were in the failed unit should be moved to the replacement unit.

3 Default the configuration of the replacement unit to ensure that there is no legacy configuration on the device to hinder the replacement unit's integration into the stack.

4 Ensure that the Stack Operational Mode is set correctly on the replacement unit. Failure to do so will cause the replacement unit not to be able to join the stack.

5 Ensure that the Base Unit Selector Switch is not activated on the replacement unit. You do not want the replacement unit to immediately take over the role of the base unit when it is inserted into the stack. If the replacement unit were to assume Base Unit responsibilities, it would over-write the existing configuration with the configuration it has in memory - which was defaulted in the last step.

6 On the stack with the failed unit, place that the Base Unit Selector Switch on the Temporary Base Unit in the Base Unit position. This will ensure that the temporary base unit will remain the base unit throughout the unit replacement process. At the end of this process you will receive instruction on how make the replacement unit the new base unit.

Replacing a Failed Non-Base Unit

1 Ensure that the software and firmware version on the replacement unit matches the software and firm ware version of the unit that was removed from the stack. This step assumes that you did not upgrade the software on the stack after the failed unit was removed.

2 Ensure that the hardware configuration of the replacement unit is the same as the failed unit. This means that the MDAs, GBIC, and other modules that were in the failed unit should be moved to the replacement unit.

3 Default the replacement unit to ensure that there is no legacy configuration on the device to hinder the replacement unit's integration into the stack.

After completing these steps, your device is now ready to be inserted into the stack at the location previously occupied by the failed unit.

There are three procedural step involved in physically inserting the replacement unit into the stack.

Inserting the replacement unit into the stack

1. Insert the replacement unit into the space that was previously occupied by the failed unit. Ensure all physical mounting devices, screws, and rack mounts are secure.
2. Attach the stacking cables to the back of the unit. Do not cable any network connections at this time.
3. Apply power to the device.
4. Ensure that the unit number of the replacement unit is the same as the failed unit.

Downloading the configuration to the stack

Once the replacement unit is physically integrated into the stack and has been provided power, the configuration must be downloaded from a TFTP (Trivial File Transfer Protocol) to the entire stack. The binary configuration file for a stack contains information about each unit in the stack. The configuration information for each unit is associated with the unit by the unit number. When the configuration file is downloaded, it will overwrite the configuration of each unit, including the replacement unit and reboot the stack.

This procedure makes two assumptions: that you have a TFTP server and know how to use it, and that you have a binary stack configuration file that was created before the unit failed.

1. Save your existing configuration, but do not overwrite any existing configuration files. This is insurance in case your configuration file is corrupt or fails to load onto the stack.
2. Download your "pre-failure" configuration file to the stack.

   The stack will reboot automatically when the configuration file downloads.

Note: This process uses the binary configuration file to apply the configuration of the settings failed unit to the replacement unit. You may also restore the unit's configuration by uploading an ASCII configuration file to the unit. ASCII configuration upload does not initiate an automatic reboot of the stack.

Recabling the network connections

1. Verify the configuration of the replacement unit. Make sure that the Spanning Tree Protocol (STP), MLT and other settings are correct. For example, you may wish to check the following MLT settings:

- Trunk members have the same PVID.
- Trunk members are on the same VLANs.
- Trunk members have same tagging.
- Trunk members filter tagged frames the same way.
- Trunk members filter untagged frames the same way.
- Trunk members do rate limiting the same way.
- Trunk members have same spanning tree mode of operation.
- Trunk members have identical IGMP participation. Static router ports and mode of operation must agree on all trunk ports.

2. Re-cable all networking connections.
3. If the failed unit had a switch IP address configured, then configure the replacement unit to match the previous configuration.

Replacing a Failed Base Unit

You may wish to make the replacement unit the base unit, since the failed unit was previously the system's base unit. To do so, follow this procedure:

1. Set the Base Unit Selector Switch on the replacement unit to the Base Unit position.
2. Set the Base Unit Selector Switch on all other units in the stack to the non-Base Unit position.
3. Reset the stack to activate the new base unit.

Troubleshooting hints

If you suspect problems with a newly installed stack configuration, start troubleshooting by verifying the following items:

- One switch is designated as the base unit.
- All other units in the stack have the Base Unit Select switch set to Off.

- In a mixed stack that includes a BayStack 450 switch, the operation mode must be set to Hybrid.
- In an allied stack or pure stack the operation mode of all units must be set to Pure.
- All units in the stack are running release 3.0, and all BayStack 450 switches are running software version 4.2.0.22.
- When the stack is powered up, ensure that the Cas Up and Cas Dwn (cascade) and Base LEDs are green (steady, not blinking).

Secure Shell (SSH)

Note: Due to export restrictions on encryption software, the default BoSS Release 3.0 software image does not include SSH functionality. The SSH server is not available without the use of this image.

This section covers the following topics:

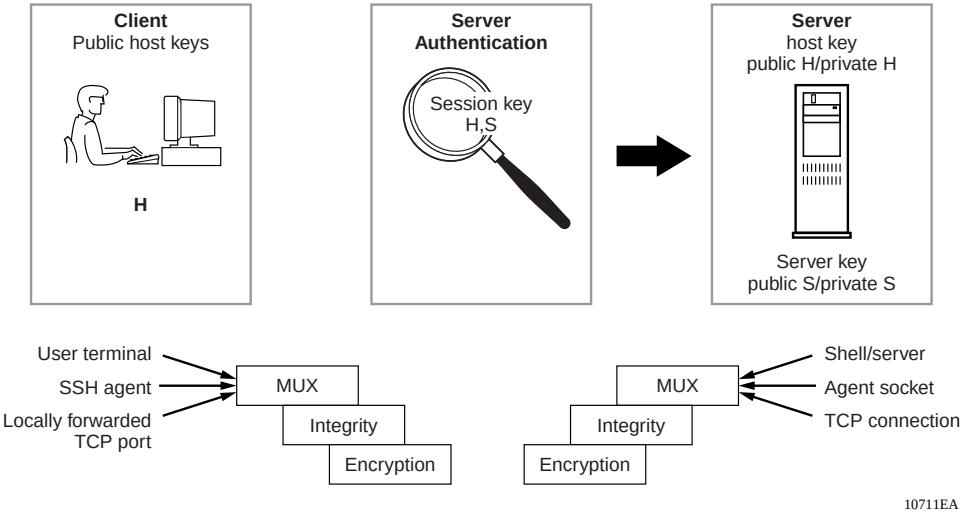
Overview

Secure Shell (SSH) is a client/server protocol that specifies the way to conduct secure communications over a network. When using other methods of remote access, such as Telnet or FTP, the traffic generated by these utilities is not encrypted. Anyone who can see the network traffic can see all data, including passwords and user names. SSH can replace telnet, ftp, and other remote logon utilities with an encrypted alternative.

In addition to standard username/password authentication, SSH supports a variety of the many different public/private key encryption schemes available. Using the public key of the host server, the client and server negotiate to generate a session key known only to the client and the server. This one-time key is then used to encrypt all traffic between the client and the server.

Figure 1 gives an overview of the SSH protocol.

Figure 1 Overview of the SSH protocol



Using a combination of host, server, and session keys, the SSH protocol can provide strong authentication and secure communication over an insecure network, offering protection from the following security risks:

- IP Spoofing
- IP source routing
- DNS spoofing
- Man-in-the-middle/TCP hijacking attacks
- Eavesdropping/Password sniffing

Even if network security is compromised, traffic cannot be played back or decrypted and the connection cannot be hijacked.

The secure channel of communication provided by SSH does not provide protection against break-in attempts or denial-of-service (DoS) attacks.

The SSH protocol supports the following security features:

- Authentication—This determines in a reliable way to identify the SSH client. During the login process the SSH client is queried for a digital proof of identity.

  Supported authentications are DSA and passwords.

- Encryption—The SSH server uses encryption algorithms to scramble data and rendered it unintelligible except to the receiver.

  Supported encryption is 3DES only.

- Integrity—This guarantees that the data is transmitted from the sender to the receiver without any alteration. If any third party captures and modifies the traffic, the SSH server will detect this alteration.

The implementation of the SSH server on the BayStack 460, 470 or BPS 2000 enables the SSH client to make a secure connection to BayStack 460, 470 or BPS 2000 and will work with commercially available SSH clients.

SSH version 2 (SSH-2)

SSH protocol, version 2 (SSH-2) is a complete rewrite of the SSH-1 protocol. While SSH-1 contains multiple functions in a single protocol, in SSH-2 the functions are divided among three layers:

- SSH Transport Layer (SSH-TRANS)

  The SSH transport layer manages the server authentication and provides the initial connection between the client and the server. Once established, the transport layer provides a secure, full-duplex connection between the client and server.

- SSH Authentication Protocol (SSH-AUTH)

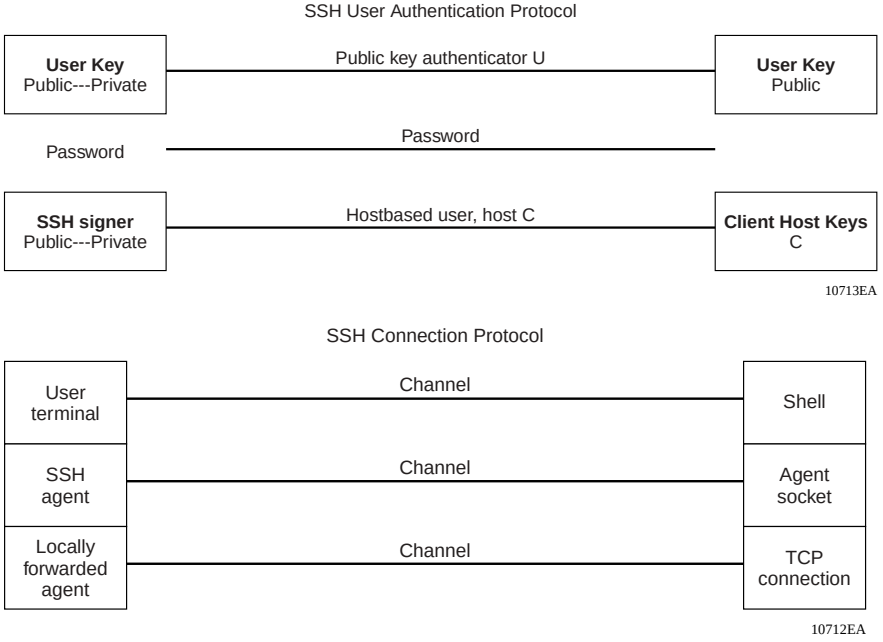
  The SSH authentication protocol runs on top of the SSH transport layer and authenticates the client-side user to the server. SSH-AUTH defines three authentication methods: public key, host-based, and password. SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- SSH Connection Protocol (SSH-CONN)

The SSH connection protocol runs on top of the SSH transport layer and user authentication protocols. SSH-CONN provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. These richer services are multiplexed into the single encrypted tunnel provided by the SSH transport layer.

Figure 2 shows the three layers of the SSH-2 protocol.

Figure 2 Separate SSH version 2 protocols



The modular approach of SSH-2 improves on the security, performance, and portability of the SSH-1 protocol.

Note: The SSH-1 and SSH-2 protocols are not compatible. The SSH implementation on the BayStack 460, 470 or BPS 2000 only supports the more secure version, the SSH-2 protocol. Ensure that your SSH client supports the SSH-2 protocol.

Establishing a secure SSH connection

To establish a secure SSH connection to the BayStack 460, 470 or BPS 2000:

1 Configure and enable the SSH service on the switch. (Refer to “Configuring SSH using the Nortel Networks Command Line Interface (NNCLI)” on page 38)

Note: You must use the NNCLI to initially configure SSH. You can use DM to change the SSH configuration parameters. However, Nortel Networks recommends using the NNCLI.

By default, the SSH service when enabled listens for connections on port 22. It allows up to 2 simultaneous SSH connections. In the default configuration, sessions can be authenticated by either password or public key authentication.

2 Connect to the switch using your SSH client.

Refer to the documentation that came with your selected SSH client for information on initiating a secure SSH connection to the switch.

a To connect to the switch using password authentication:

— Enter either the Console Read-Only switch password (default is *user*) or the Console Read-Write switch password (default is *secure*) when asked to enter the password.

When using password authentication, the user name is not required.

Note: Using the Console Read-Only or Console Read-Write password does not set read-only or read-write privileges. Either password will work to establish a secure SSH connection to the device.

b To connect to the switch using DSA public key authentication:

— Generate a DSA key pair (public and private keys) using your SSH client or key-gen tool and export your public key.

Refer to the documentation that came with your selected SSH client or key-gen tool for information on generating a DSA key pair and exporting the public key.

— Download the DSA public key file to the switch via your TFTP server. (Refer to “Configuring SSH using the Nortel Networks Command Line Interface (NNCLI)” on page 38.)

— Connect to the switch using DSA public key authentication.

Please refer to the documentation that came with your SSH client for information on establishing a secure SSH connection using DSA public key authentication.

Configuring SSH using the Nortel Networks Command Line Interface (NNCLI)

Note: Due to export restrictions on encryption software, the default BoSS Release 3.0 software image does not include SSH functionality. The SSH server is not available without the use of this image.

This section provides the NNCLI commands for configuring and managing SSH on the BayStack 460, 470 or BPS 2000. Refer to *Reference for the BayStack 460-24T-PWR Switch CLI Command Line Interface,* for complete information on using the NNCLI with the BayStack 460, 470 or BPS 2000. The SSH protocol provides secure access to the NNCLI. With the NNCLI, you use the following commands:

show ssh global command

The `show ssh global` command displays the secure shell configuration information. The syntax for the `show ssh global` command is:

```
show ssh global
```

The `show ssh global` command is in the privExec command mode.

The `show ssh global` command has no parameters or variables.

Figure 3 displays sample output from the `show ssh global` command.

Figure 3 show ssh global command output

```
BS_460_24T_PWR#show ssh global
Active SSH Sessions     :  2
Version                 :  Version 2 only
Port                    :  22
Max. Sessions           :  2
Timeout                 :  60
DSA Key Size            :  1024
DSA Authentication      :  True
Password Authentication :  True
Public Key TFTP Server  :  134.177.152.12
Public Key File Name    :  pubkey.txt
Enabled                 :  True
```

show ssh session command

The `show ssh session` command displays the SSH session information. The session information includes the session ID and the host IP address. A host address of 0.0.0.0 indicates no connection for that session ID. The syntax for the `show ssh session` command is:

```
show ssh session
```

The `show ssh session` command is in the privExec command mode.

The `show ssh session` command has no parameters or variables.

Figure 4 displays sample output from the `show ssh session` command.

Figure 4 show ssh session command output

```
BS460_24T_PWR#show ssh session
Session  Host
-------  ---------------
0        134.177.152.12
1        0.0.0.0
```

show ssh download-auth-key command

The `show ssh download-auth-key` command displays the results of the most recent attempt to download the DSA public key from the TFTP server. The syntax for the `show ssh download-auth-key` command is:

```
show ssh download-auth-key
```

The `show ssh download-auth-key` command is in the privExec command mode.

The `show ssh download-auth-key` command has no parameters or variables.

Figure 5 displays sample output from the `show ssh session` command.

Figure 5 show ssh download-auth-key command output

```
BS460_24T_PWR#show ssh download-auth-key
Public Key TFTP Server  :  134.177.152.12
Public Key File Name    :  pubkey.txt
Last Transfer Result    :  Success
```

ssh dsa-key command

The `ssh dsa-key` command initiates generation of DSA host key at next system reboot. If a key size is specified, a key of this size (in bits) will be generated. If no key size is specified, the previous provisioned key size (or default of 1024) will be used. This command can only be executed in SSH disable mode. The syntax of the `ssh dsa-key` command is:

```
ssh dsa-key [<512-1024>]
```

The `ssh dsa-key` command is in the config command mode.

Table 3 describes the parameters and variables for the `ssh dsa-key` command.

Table 3 ssh dsa-key-gen command parameters and variables

Parameters and variables	Description
<512-1024>	Sets the SSH host key size. Can be a value from 512 to 1-1024. Default is 1024.

no ssh dsa-key command

The `no ssh dsa-key-gen` command deletes the DSA host key in the switch. The syntax of the `no ssh dsa-key-gen` command is:

```
no ssh dsa-key
```

The `no ssh dsa-key` command is in the config command mode.

There are no parameters or variables for the `no ssh dsa-key` command.

ssh command

The `ssh` command enables the SSH server on the BayStack 460, 470 or BPS 2000 in non-secure mode. In addition to accepting SSH connections, the BayStack 460, 470 or BPS 2000 continues to accept Web, SNMP, and Telnet connections while in this mode.The syntax of the `ssh` command is:

```
ssh
```

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

There are no parameters or variables for the `ssh` command.

no ssh command

The `no ssh` command disables the SSH server on the BayStack 460, 470 or BPS 2000. The syntax of the `no ssh` command is:

```
no ssh
```

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

There are no parameters or variables for the `no ssh` command.

ssh secure command

The `ssh secure` command enables the SSH server on the BayStack 460, 470 or BPS 2000 in secure mode. In secure mode, the BayStack 460, 470 or BPS 2000 does not accept Web, SNMP, or Telnet connections. The syntax of the `ssh secure` command is:

```
ssh secure
```

The `ssh secure` command is in the config command mode.

There are no parameters or variables for the `ssh secure` command.

ssh max-sessions command

The `ssh max-sessions` command allows you to set the maximum number of simultaneous SSH sessions allowed. The syntax of the `ssh max-sessions` command is:

```
ssh max-sessions <0-2>
```

The `ssh max-sessions` command is in the config command mode.

Table 4 describes the parameters and variables for the `ssh max-sessions` command.

Table 4 ssh max-sessions command parameters and variables

Parameters and variables	Description
<0-2>	Specifies the maximum number of SSH sessions allowed. Default is 2.

ssh timeout command

The `ssh timeout` command sets the timeout value for session authentication. The syntax of the `ssh timeout` command is:

```
ssh timeout <1-120>
```

The `ssh timeout` command is in the config command mode.

Table 5 describes the parameters and variables for the `ssh timeout` command.

Table 5 ssh timeout command parameters and variables

Parameters and variables	Description
<1-120>	Specifies the timeout value for authentication. Default is 60.

ssh dsa-auth command

The `ssh dsa-auth` command enables DSA authentication. The syntax of the `ssh dsa-auth` command is:

```
ssh dsa-auth
```

The `ssh dsa-auth` command is in the config command mode.

There are no parameters or variables for the `ssh dsa-auth` command.

no ssh dsa-auth command

The `no ssh dsa-auth` command disables DSA authentication. The syntax of the `no ssh dsa-auth` command is:

```
no ssh dsa-auth
```

The `no ssh dsa-auth` command is in the config command mode.

There are no parameters or variables for the `no ssh dsa-auth` command.

ssh pass-auth command

The `ssh pass-auth` command enables password authentication. The syntax of the `ssh pass-auth` command is:

```
ssh pass-auth
```

The `ssh pass-auth` command is in the config command mode.

There are no parameters or variables for the `ssh pass-auth` command.

no ssh pass-auth command

The `no ssh pass-auth` command disables password authentication. The syntax of the `no ssh pass-auth` command is:

```
no ssh pass-auth
```

The `no ssh pass-auth` command is in the config command mode.

There are no parameters or variables for the `no ssh pass-auth` command.

ssh port command

The `ssh port` command sets the SSH connection port. The syntax of the `ssh port` command is:

```
ssh port <1-65535>
```

The `ssh port` command is in the config command mode.

Table 6 describes the parameters and variables for the `ssh port` command.

Table 6 ssh port command parameters and variables

Parameters and variables	Description
<1-65535>	Specifies the SSH connection port. Default is 22.

ssh download-auth-key command

The `ssh download-auth-key` command downloads the client public key from the TFTP server to the BayStack 460, 470 or BPS 2000. The syntax for the `ssh download-auth-key` is:

```
ssh download-auth-key [address <XXX.XXX.XXX.XXX>] [key-name
<file>]
```

The `ssh download-auth-key` command is in the config command mode.

Table 7 describes the parameters and variables for the `ssh download-auth-key` command.

Table 7 ssh download-auth-key command parameters and variables

Parameters and variables	Description
address <XXX.XXX.XXX.XXX>	The IP address of the TFTP server.
key-name <file>	The name of the public key file on the TFTP server.

default ssh command

The `default ssh` command resets the specific secure shell configuration parameter to the default value. The syntax of the `default ssh` command is:

```
default ssh
[dsa-auth|dsa-key|max-sessions|pass-auth|port|timeout]
```

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

Table 8 describes the parameters and variables for the `default ssh` command.

Table 8 default ssh command parameters and variables

Parameters and variables	Description
dsa-auth	Resets dsa-auth to the default value. Default is True.
dsa-key	Resets the dsa-key size to the default value of 1024 bits.
max-sessions	Resets the maximum number of simultaneous sessions to the default of 2.
pass-auth	Resets pass-auth to the default value. Default is True.
port	Resets the port number for SSH connections to the default. Default is 22.
timeout	Resets the timeout value for session authentication to the default. Default is 60.

Single Fiber Fault Detection (SFFD)

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

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

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

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

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

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.

Note: FEFI will not work with the BPS 2000-2GE MDA because it does not support autonegotiation.

Nortel Networks CLI commands for SFFD

This section lists the NNCLI 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.

The port lists may be separated by commas or dashes. For example: 2/16, 3/26 or 2/26 - 2/27.

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 change 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.

The following Single Fiber Fault Detection (SFFD) NNCLI commands are only available through the BPS 2000 switch:

```
BPS 2000>enable
BPS 2000#configure terminal
BPS 2000 (config) # interface fastethernet all
BPS 2000 (config-if) #sffd port <port #> enable
BPS 2000 (config-if) #no sffd port <port #> enable
```

SNMPv3 in BoSS Device Manager

Note: For SNMPv3, BoSS 3.0 includes SHA authentication and DES privacy encryption along with the MD5 authentication that is already available.

In previous BayStack software releases that supported SNMP, MD5 was the only authentication method supported. BoSS 3.0, in the SSH version, adds support for SHA authentication and DES privacy encryption. Only the SSH version supports SHA authentication and DES privacy encryption. The non-SSH version supports only MD5.

BoSS 3.0 allows you to configure SNMPv3 in Device Manager, Web-based Management, or by using NNCLI commands.

The SNMP agent supports exchanges using SNMPv1, SNMPv2c and SNMPv3. Support for SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities. SNMPv3 support introduces industrial grade user authentication and message security. This includes MD5 and SHA-based user authentication and message integrity verification, as well as DES-based privacy encryption. Export restrictions on SHA and DES will necessitate support for domestic and non-domestic executable images or defaulting to no encryption for all customers. BoSS 3.0 uses the SNMP Research EMANATE-Lite agent.

Configuring SNMPv3

This section describes how to use Device Manager to configure the following SNMPv3 options:

Using NNCLI commands to create an SNMPv3 view and user

Use the following procedure as a guide to using NNCLI commands to create or change a SNMPv3 access view and user:

1 In the NNCLI, create a view using the following syntax:

```
snmp-server view <view-name> <oid>
```

For example:

```
snmp-server view allView +1.3
```

Specifying +1.3 allows you to access to everything on the switch in the OID tree. You can restrict access to a particular OID or to a section of the OID tree. For example: +1.3.6.1.6.3.1.1.5 limits the user to traps only.

2 In the NNCLI, create a user and define the authentication and privacy method:

a Syntax for no authentication and no privacy:

```
snmp-server user <user-name> read-view <view-name>
write-view <view-name> notify-view <view-name>
```

For example:

```
snmp-server user fbarnes read-view allView
write-view allView notify-view allView
```

b Syntax for MD5 authentication and no privacy:

```
snmp-server user <user-name> md5
<authentication-password> read-view <view-name>
write-view <view-name> notify-view <view-name>
```

For example:

```
snmp-server user fbarnes md5 myPass read-view
allView write-view allView notify-view allView
```

c Syntax for MD5 authentication and DES encryption:

```
snmp-server user  <user-name> md5
<authentication-password> des <privacy-password>
read-view <view-name> write-view <view-name>
notify-view <view-name>
```

For example:

```
snmp-server user fbarnes md5 myPass des myPass
read-view allView write-view allView notify-view
allView
```

d Syntax for SHA authentication and no privacy:

```
snmp-server user  <user-name> sha
<authentication-password> read-view <view-name>
write-view <view-name> notify-view <view-name>
```

For example:

```
snmp-server user fbarnes sha myPass read-view
allView write-view allView notify-view allView
```

e Syntax for SHA authentication with DES encryption:

```
snmp-server user <user-name> sha
<authentication-password> des <privacy-password>
read-view <view-name> write-view <view-name>
notify-view <view-name>
```

For example: SHA authentication with DES encryption:

```
snmp-server user fbarnes sha myPass des myPass
read-view allView write-view allView notify-view
allView
```

You cannot specify both md5 and sha authentication. You may use one or the other. If you wish to access your device using both authentication methods, then define a separate user for each.

3 Set up a target address and parameter for user trap notification:

For an authenticated user:

```
snmp-server host <trap-server-ip-address> v3 auth
<user-name>
```

For a user with privacy:

```
snmp-server host <trap-server-ip-address> v3
auth-priv <user-name>
```

Using NNCLI Commands to create a default SNMPv3 user

Use the following procedure as a guide to using NNCLI commands to create a default SNMPv3 user.

1. In the NNCLI, use the `snmp bootstap` command to specify the level of security for the snmp configuration.

   For example:

   ```
   BS470(config)#snmp bootstrap
    minimum-secure  Use minimum security configuration
     semi-secure     Use partial security configuration
     very-secure     Use maximum security configuration
   BS470(config)#snmp bootstrap mini
   ```

The following warning appears, and the system prompts you to continue:

```
WARNING:  This command will destroy *all* existing SNMP
configuration
Do you want to continue (y/n) ? y
Enter authentication password/phrase for user 'initial':
```

2. Enter the authentication password or phrase. The following prompt is displayed:

   ```
   Re-Enter authentication password/phrase for user
   'initial':
   ```

3. Re-enter the authentication password or phrase. The following prompt is displayed:

   ```
   Enter authentication password/phrase for user
   'templateMD5':
   ```

4 Enter the authentication password or phrase for the user template.

```
Re-Enter authentication password/phrase for user
'templateMD5':
```

5 Re-enter the authentication password or phrase for the user template.

You can now go into Device Manager to configure the SNMPv3 options.

Creating an SNMPv3 user

Note: You must configure a valid SNMPv3 user through the NNCLI (or the Web interface) before you can access the switch in SNMPv3 mode or by using the Device Manager.

To create an SNMPv3 user:

1 From the Device Manager menu bar, click Edit > SnmpV3 > USM Table.

The USM dialog box opens (Figure 6).

Figure 6 USM dialog box

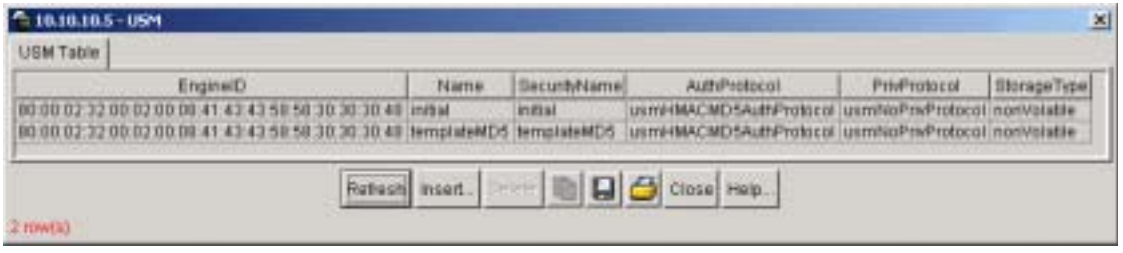


Table 9 describes the USM tab fields.

Table 9 USM dialog box fields

Field	Description
EngineID	Indicates the SNMP engine's administratively-unique Identifier
Name	Indicates the name of the user in usmUser

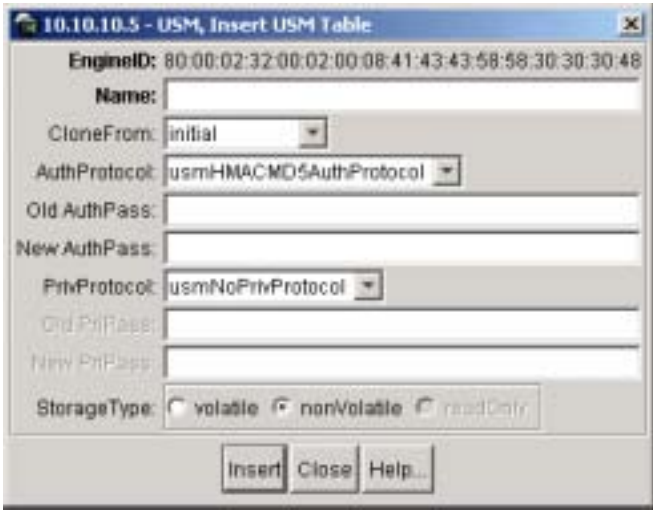
Table 9 USM dialog box fields (continued)

Field	Description
SecurityName	Creates the name used as an index to the table. The range is 1 to 32 characters.
AuthProtocol	Identifies the Authentication protocol used
PrivProtocol	Identifies the privacy protocol used

2 Click Insert.

The USM, Insert USM Table dialog box opens (Figure 7).

Figure 7 USM, Insert USM Table dialog box



3 Enter a name.

4 In the CloneFrom field, select a user name from which the new entry copies authentication data and privacy data.

5 Select an authentication protocol.

6 Enter the old authentication password.

7 Enter a new authentication password for this user

8 Select a privacy protocol.

9 Enter the old privacy password.

10 Enter a new a privacy password for this user

11 Click Insert.

The USM dialog opens. The new user is shown in the list.

Table 10 describes the USM, Insert USM Table dialog box fields.

Table 10 USM, Insert USM Table dialog box fields

Field	Description
Name	Creates the new entry with this security name. The name is used as an index to the table. The range is 1 to 32 characters.
CloneFrom	Specifies the security name from which the new entry must copy privacy and authentication parameters. The range is 1 to 32 characters.
AuthProtocol (Optional)	Assigns an authentication protocol (or no authentication) from a pulldown menu. If you select this, you must enter and old AuthPass and a new AuthPass.
Old AuthPass	Specifies the current authentication password
New AuthPass	Specifies the name of the new authentication password
PrivProtocol (Optional)	Assigns a privacy protocol (or no privacy) from a pulldown menu. If you select this, you must enter and old PrivPass and a new PrivPass.
Old PriPass	Specifies the current privacy password
New PriPass	Specifies the name of the new privacy password

Creating membership for a group

To add membership for a group in the view-based access control model (VACM):

1 From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

The VACM dialog box with the Group Membership tab options visible opens (Figure 8).

Figure 8 VACM dialog box

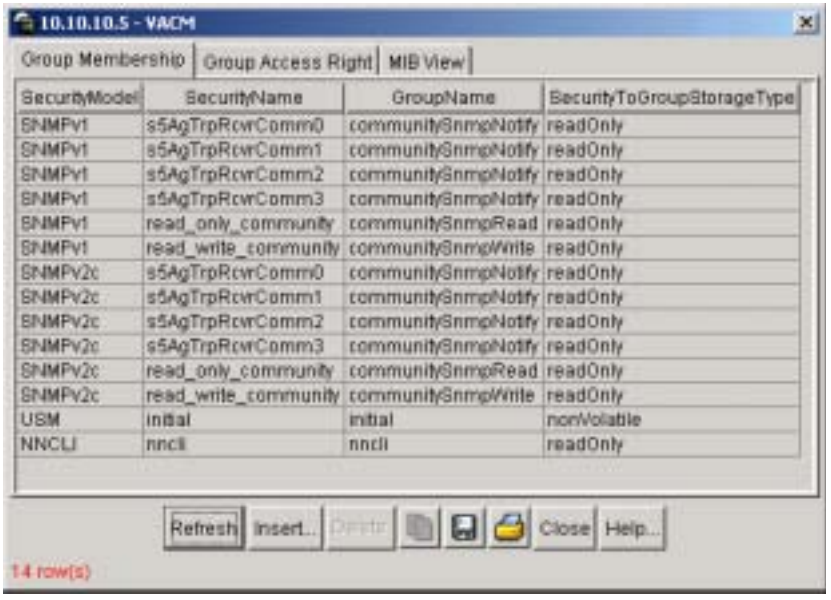


Table 11 describes the VACM tab fields.

Table 11 VACM dialog box tab fields

Field	Description
SecurityModel	The security model currently in use

Table 11 VACM dialog box tab fields (continued)

Field	Description
SecurityName	The name representing the user in usm user. The range is 1 to 32 characters.
GroupName	The name of the group to which this entry (combination of securityModel and securityName) belongs

2 Click Insert.

The VACM, Insert Group Membership dialog box opens (Figure 9).

Figure 9 VACM, Insert Group Membership dialog box

3 Select a SecurityModel.

4 Enter a SecurityName.

5 Enter a GroupName.

6 Click Insert.

The VACM dialog opens. The new group membership is shown in the list.

Table 12 describes the Insert Group Membership tab fields.

Table 12 VACM dialog box—Insert Group Membership tab fields

Field	Description
SecurityModel	The authentication checking to communicate to the switch.
SecurityName	The security name assigned to this entry in the VACM table. The range is 1 to 32 characters.
GroupName	The name assigned to this group in the VACM table. The range is 1 to 32 characters.

Creating access for a group

To create new access for a group:

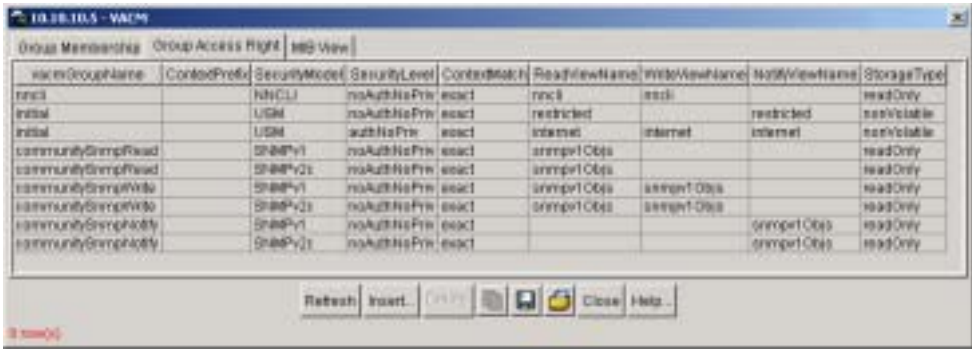
1. From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

   The VACM dialog box opens (Figure 8).

2. Click the Group Access Right tab.

   The Group Access Right tab displays (Figure 10).

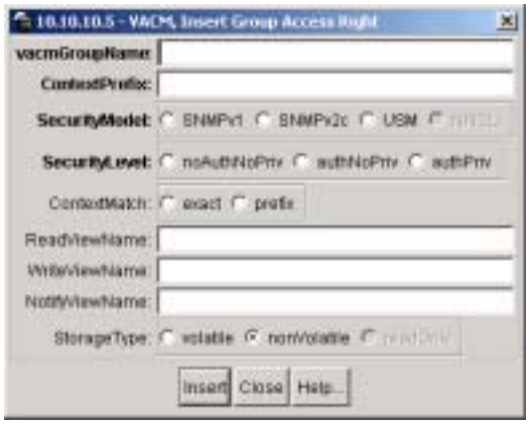
Figure 10 Group Access tab



3. Click Insert.

   The VACM, Insert Group Access Right dialog box opens (Figure 11).

Figure 11 VACM, Insert Group Access Right dialog box



4 Enter a vacmGroupName.

5 Enter a ContextPrefix.

Note: For BayStack products, the ContextPrefix value should be an empty string.

6 Select a SecurtyModel.

7 Select a SecurityLevel.

8 If desired, select a ContextMatch.

Note: For BayStack products, the ContextMatch value should be "exact", because BayStack products support only a single context.

9 In the ReadViewName field, enter the number of object instances authorized for the group when reading objects.

10 In the WriteViewName field, enter the number of object instances authorized for the group when writing objects.

11 Click Insert.

The VACM dialog opens. The new group access is shown in the list.

Table 13 describes the Group Access tab fields.

Table 13 VACM dialog box—Group Access Right tab fields

Field	Description
vacmGroupName	The name of the new group name in the VACM table. The name is a numeral. The range is 1 to 32 characters.
ContextPrefix	The contextName of an incoming SNMP packet must match exactly or partially the value of the instance of this object. The range is an SnmpAdminString, 0 to 32 characters.
SecurityModel	The security model of the entry, either SNMPv1, SNMPv2, or SNMPv3.
SecurityLevel	The minimum level of security required to gain access rights. The security levels are: • noAuthNoPriv • authNoPriv • authpriv
ContextMatch (Optional)	Specifies the contextName for an incoming SNMP packet
ReadViewName	Specifies the MIB view to which read access is authorized.
WriteViewName	Specifies the MIB view to which write access is authorized.

Assigning MIB view access for an object

To assign MIB view access for an object:

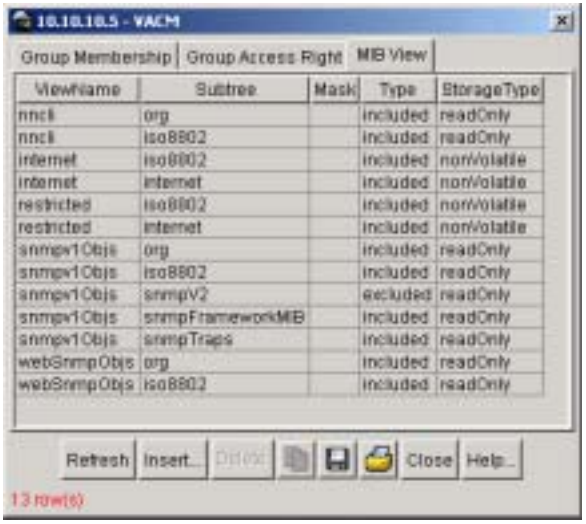
1. From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

   The VACM dialog box opens (Figure 8).

2. Select the MIB View tab.

   The MIB View tab opens (Figure 12).

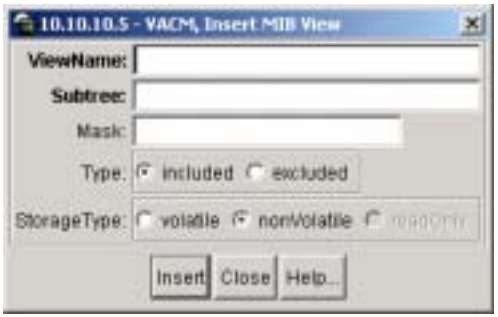
Figure 12 MIB View tab



3. Click Insert.

   The VACM, Insert MIB View dialog box opens (Figure 13).

Figure 13 VACM, Insert MIB View dialog box



4 Enter a ViewName.

5 Enter a Subtree.

6 Enter a Mask.

7 Select a Type.

8 Click Insert.

The VACM dialog opens. The assigned MIB view appears in the list.

Table 14 describes the MIB View tab fields.

Table 14 VACM dialog box—MIB View tab fields

Field	Description
ViewName	Creates a new entry with this group name. The range is 1 to 32 characters.
Subtree	Any valid object identifier that defines the set of MIB objects accessible by this SNMP entity, for example, 1.3.6.1.1.5
Mask (Optional)	Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.
Type	Determines whether access to a mib object is granted (Included) or denied (Excluded). Included is the default.

Creating a community

A community table contains objects for mapping between community strings and the security name created in VACM Group Member. To create a community:

1 From the Device Manager menu bar, click Edit > SnmpV3 > Community Table.

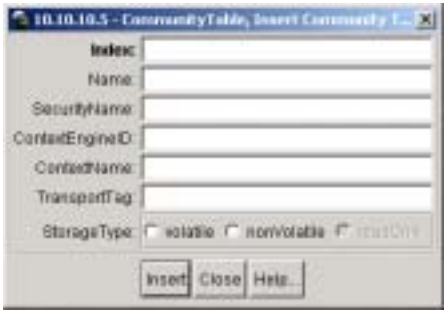
The Community Table dialog box opens (Figure 14).

Figure 14 Community Table dialog box

2 Click Insert.

The Community Table, Insert Community Table dialog box opens (Figure 15).

Figure 15 Community Table, Insert Community Table dialog box



3 Enter an Index.

4 Enter name that is a community string.

5 Enter a SecurityName.

6 Enter a ContextEngine ID.

7 Enter a ContextName. The correct value should be an empty string.

8 Enter a transport tag.

9 Specify the storage type.

10 Click Insert.

The Community Table dialog opens. The new community is shown in the list.

Table 15 describes the Community Table dialog box fields.

Table 15 Community Table dialog box fields

Field	Description
Index	The unique index value of a row in this table. SnmpAdminString 1-32 characters.
Name	The community string for which a row in this table represents a configuration
SecurityName	The security name assigned to this entry in the Community table. The range is 1 to 32 characters.

Creating a Target Table

To create a target table:

1 From the Device Manager menu bar, click Edit > SnmpV3 > Target Table.

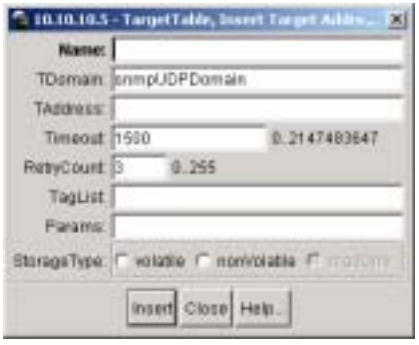
The Target Table dialog box opens (Figure 14).

Figure 16 Community Table dialog box

2 Click Insert.

The Target Table, Insert Target Table dialog box opens (Figure 15).

Figure 17 Target Table, Insert Target Table dialog box



3 Enter a Name.

4 Enter a TDomain Name.

5 Enter a TAddress Name.

6 Click Insert.

The Target Table dialog opens. The new Target address is shown in the list.

Table 15 describes the Target Table dialog box fields.

Table 16 Community Table dialog box fields

Field	Description
Name	Specifies the name of the target table.
TDomain	Specifies the TDomain for the target table.
TAddress	Specifies the TAddress for the target table.
Timeout	Specifies the length of the timeout.
RetryCount	Specifies the retrycount.
Taglist	Specifies the taglist.
Params	Specifies the parameters.
StorageType	Specifies the storage type.

Creating Target parameters

To create a target parameter:

1 From the Device Manager menu bar, click Edit > SnmpV3 > Target Table.

The Target Table dialog box opens (Figure 14).

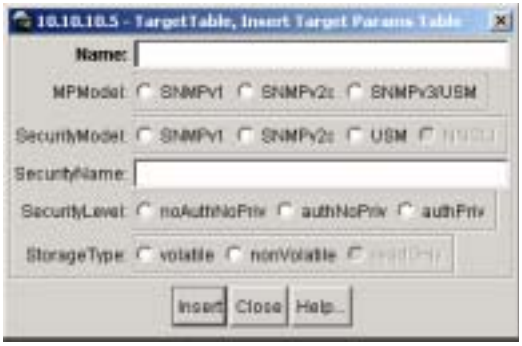
Figure 18 Target Params Table dialog box

2 Select the Target Parems table tab.

3 Click Insert.

The Target Table, Insert Target Params Table dialog box opens (Figure 15).

Figure 19 Target Table, Insert Target Params Table dialog box



4 Enter an Name.

5 Select the MPModel.

6 Select the SecurityModel.

7 Enter a SecurityName.

8 Specify a SecurityLevel value

9 Enter the storage type.

10 Click Insert.

The Target Table dialog opens. The new target parameter is shown in the list.

Table 15 describes the Target Params Table dialog box fields.

Table 17 Target Params Table dialog box fields

Field	Description
Name	Specifies the name of the target parameters table
MPModel	Specifies the Message Processing model, SNMPv1, SNMPv2c, or SNMPv3/USM.
SecurityModel	Specifies the security model, SNMPv1, SNMPv2c, or SNMPv3/USM.
SecurityName	Specifies the security name for generating SNMP messages..
SecurityLevel	Specifies the security level for SNMP messages: noAuthnoPriv, authnoPriv, or authPriv.
Storage Type	Specifies the storage type: volatile or non-volatile.

Creating a Notify Table

To create a Notify table:

1 From the Device Manager menu bar, click Edit > SnmpV3 > Notify.

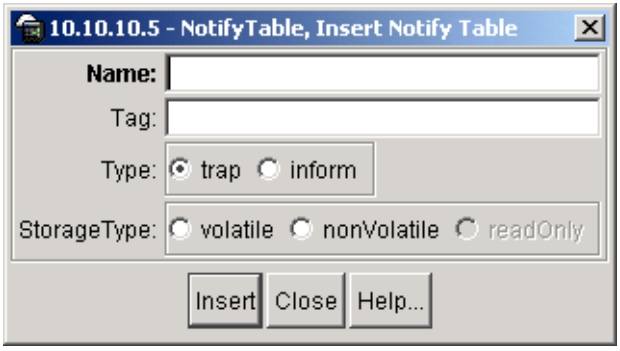
The Notify Table dialog box opens (Figure 14).

Figure 20 NotifyTable dialog box

2 Click Insert.

The Notify Table, Insert Notify Table dialog box opens (Figure 15).

Figure 21 Notify Table, Insert Notify Table dialog box



3 Enter a Name.

4 Enter a Tag name.

5 Specify the Type.

6 Specify the StorageType

7 Click Insert.

The Notify Table dialog opens. The new notify entry shown in the list.

Table 15 describes the Notify Table dialog box fields.

Table 18 Notify Table dialog box fields

Field	Description
Name	Specifes the unique identifier associated for the notify table.
Tag name	A single tag value used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object contains a value of zero length, no entries are selected.
Type	This object determines the type of notification generated for entries in the snmpTargetAddrTable selected by the corresponding instance of snmpNotifyTag. If the value of this object is trap, then any messages generated for selected rows will contain SNMPv2-Trap PDUs. If the value of this object is inform, then any messages generated for selected rows will contain Inform PDUs. Note: If an SNMP entity only supports generation of traps (and not informs), then this object may be read-only.
StorageType	Specifies the type of storage, volatile or non-volatile.

Using SNMPv3 in Device Manager

When you use Device Manager, there are parameters that you use to initially log in when the SNMPv3 check box is enabled. These parameters are also listed in the User Security Model (USM) Table. For example:

- Select the V3 enable checkbox
- Login name: initial
- Authentication Protocol: MD5
- Privacy Protocol: None
- Privacy Password: None

Using SNMPv3 in Web-based Management

Web-based management also supports the following tables in SNMPv3:

- System Information
- User Specification
- Group Membership
- Group Access Rights
- Management Information View
- Notification
- Target Address
- Target Parameters

BoSS 3.0 Nortel Networks CLI Commands for SNMPv3

Before BoSS 3.0 support for SNMPv3, there was a proprietary method used for specifying SNMPv1 configuration that included:

- A single read-only community string that could only be configured using the console menus.
- A single read-write community string that could only be configured using the console menus.
- Up to 4 trap destinations and associated community strings that could be configured either in the console menus, or using SNMP Set requests on the s5AgTrpRcvrTable

With BoSS 3.0 support for SNMPv3, the way you configure SNMP has changed. We still support previous method for backwards-compatilbility. All of the config data that is configured in the previous method is mapped into the SNMPv3 tables as read-only table entries. In the SNMPv3 configuring of SNMP, everything is configured and controlled through the SNMPv3 MIBs. The BoSS 3.0 NNCLI commands change or display the single read-only community, read-write community, or 4 trap destinations of the previous method of configuring SNMP. Otherwise, the commands change or display SNMPv3 MIB data.

BoSS 3.0 includes Nortel Networks CLI commands for SNMP that have been expanded and changed. The new SNMP commands are as follows:

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

Table 19 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 20 describes the parameters and variables for the snmp-server authentication-trap command.

Table 20 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 21 describes the parameters and variables for the `snmp-server community` for read/write command.

Table 21 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 22 describes the parameters and variables for the `snmp-server community` command.

Table 22 snmp-server community command parameters and variables

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

no snmp-server community command

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

```
no snmp-server community {ro|rw|<community-string>}
```

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

If you do not specify a read-only or read-write community parameter, all community strings are removed, including all communities controlled by the `snmp-server community` command and the `snmp-server comunity` 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 23 describes the parameters and variables for the `no snmp-server community` command.

Table 23 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 24 describes the parameters and variables for the `default snmp-server community` command.

Table 24 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 25 describes the parameters and variables for the `snmp-server contact` command.

Table 25 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 restores sysContact to the default value. The syntax for the `default snmp-server contact` command is:

```
default snmp-server contact
```

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

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

Table 26 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 27 describes the parameters and variables for the `snmp-server host` for old-style table command.

Table 27 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 28 describes the parameters and variables for the `snmp-server host` for new-style table command.

Table 28 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.

If you do not specify any parameters, this command deletes all trap destinations from the s5AgTrpRcvrTable and from SNMPv3 tables.

Table 29 describes the parameters and variables for the `no snmp-server host` for old-style table command.

Table 29 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. If both parameters are omitted, nothing is cleared. If a host IP is included, the community-string is required or an error is reported.

no snmp-server host for new-style table command

The `no snmp-server` for new-style table command deletes trap receivers from the new-style table (SNMPv3 MIB). Any trap receiver matching the IP address and SNMP version 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 30 describes the parameters and variables for the `no snmp-server host` for new-style table command.

Table 30 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 31 describes the parameters and variables for the `snmp-server location` command.

Table 31 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 <text>
```

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

Table 32 describes the parameters and variables for the `no snmp-server location` command.

Table 32 no snmp-server location command parameters and variables

Parameters and variables	Description
text	Specifies the SNMP sysLocation value. Enter a string of up to 255 characters.

default snmp-server location command

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

```
default snmp-server location
```

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

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

Table 33 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 34 describes the parameters and variables for the `snmp-server user` command.

Table 34 snmp-server user command parameters and variables

Parameters and variables	Description
username	Specifies the user names; enter an alphanumeric string of up to 255 characters.
md5 <password>	Specifies the use of an md5 password. <password> specifies the new user md5 password; enter an alphanumeric string. If this parameter is omitted, the user will be created with only unauthenticated access rights.
read-view <view-name>	Specifies the read view to which the new user has access: • view-name—specifies the viewname; enter an alphanumeric 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/DES	Specifies either SHA authentication or DES privacy encryption..

no snmp-server user command

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

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

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

Table 35 describes the parameters and variables for the `no snmp-server user` command.

Table 35 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 36 describes the parameters and variables for the `snmp-server view` command.

Table 36 snmp-server view command parameters and variables

Parameters and variables	Description
viewname	Specifies the name of the new view; enter an alphanumeric string.
OID	Specifies Object identifier. OID may be entered as a MIB object English descriptor, a dotted form OID, or a mix of the two. Each OID may also be preceded by a '+' or '-' sign (if this is omitted, a '+' sign is implied). For the dotted form, a sub-identifier can be a '*' indicating a wildcard. Here are some examples of valid OID parameters: • sysName • +sysName • -sysName • +sysName.0 • +ifIndex.1 • -ifEntry.*.1 (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 37 describes the parameters and variables for the `no snmp-server view` command.

Table 37 no snmp-server view command parameters and variables

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

snmp trap link-status command

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

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

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

Table 38 describes the parameters and variables for the `snmp trap link-status` command.

Table 38 snmp trap link-status command parameters and variables

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

no snmp trap link-status command

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

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

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

Table 39 describes the parameters and variables for the `no snmp trap link-status` command.

Table 39 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 40 describes the parameters and variables for the default `snmp trap link-status` command.

Table 40 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 33 describes the parameters and variables for the `snmp-server bootstrap` command.

Table 41 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.

Additional Features for BoSS 3.0

Customizing the opening banner

With BoSS release 3.0, you can customize the opening banner that appears when you connect to the BayStack 460, 470 or BPS 2000 console port or Telnet to the switch. The part you can customize is the portion that displays as “BAYSTACK,” written in asterisks upon first opening. You cannot customize the portion that begins with “Enter Ctrl-Y to begin” (Figure 22).

Figure 22 Portion of opening banner you *cannot* customize

```
Enter Ctrl-Y to begin.

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

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

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

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

Using NNCLI to customize banner

This sections describes the NNCLI commands you use to customize and display the banner that displays when you connect to the BayStack 460, 470 or BPS 2000 console port or Telnet to the switch. The following topics are discussed:

show banner command

The `show banner` command displays the banner.

The syntax for the `show banner` command is:

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

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

Table 42 describes the parameters and variables for the `show banner` command.

Table 42 show banner command parameters and variables

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

Figure 23 displays a sample output of the `show banner` command.

Figure 23 show banner names command output

```
BS460_24T_PWR#show banner
Current banner setting: CUSTOM
```

banner command for displaying banner

This `banner` command specifies the banner displayed at startup; either static or custom.

The syntax for this `banner` command is:

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

Table 43 describes the parameters and variables for this `banner` command.

Table 43 banner command for displaying banner parameters and variables

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

banner command for creating banner

This `banner` command allows you to create a custom banner.

The syntax for this `banner` command is:

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

Table 44 describes the parameters and variables for this `banner` command.

Table 44 banner command for creating banner parameters and variables

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

no banner command

The `no banner` command allows you to clear all lines of a previously stored custom banner.

The syntax for the `no banner` command is:

```
no banner
```

Displaying unit uptime

With release 3.0, you can display the uptime for each unit in a stack. Unit stack uptime collects the stack uptime for each unit in a stack and reports this information when requested. This allows you to determine how long each unit has been connected to the stack. You must use the Nortel Networks Command Line Interface (NNCLI) commands system to display the unit uptimes.

Using NNCLI commands to display uptimes

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

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

```
show stack-info uptime
```

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

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

Figure 24 displays sample output from the `show stack-info uptime` command.

Figure 24 show stack-info uptime command output

```
BS460_24T_PWR#show stack-info uptime
Unit# Switch Model     Unit UpTime
----- ---------------- --------------------
1     BayStack 460-24T 4 days, 21:38:46
2     BayStack 460-24T 4 days, 21:38:46
3     BayStack 460-24T 4 days, 21:38:46
4     BayStack 460-24T 4 days, 21:38:46
5     BayStack 460-24T 4 days, 21:38:44
6     BayStack 460-24T 4 days, 21:38:46
```

Default management system: NNCLI or CI menus

With release 3.0, you can set the default management interface when you connect to the BayStack 460, 470 or BPS 2000 console port or Telnet to the switch to either NNCLI or the console interface (CI) menus. This selection is stored in NVRAM and propagated to all units in a stack configuration.

On system startup, the banner displays and instructs the user to enter Ctrl+Y. After entering these characters, the system will display either the menus or the Nortel Networks Command Line Interface (NNCLI) prompt, depending on which is set using this command.

When using the console port, you must logout for the new mode to display. When using Telnet, all subsequent Telnet sessions display the selection.

Using NNCLI commands to set 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.

Table 45 describes the parameters and variables for the `cmd_interface` command.

Table 45 cmd_interface command parameters and variables

Parameters and variables	Description
cli|menu	Allows you to set the default management system when using console port or Telnet: • cli—the system automatically enters the NNCLI mode and displays the NNCLI prompt after you enter Crtl+Y • menu—the system automatically enters the CI menu mode and displays the menus after you enter Ctrl+Y **Note**: If you omit these parameters, the systems enters the NNCLI command mode.

BoSS 3.0 Security

The following tables describe the types of security available in BoSS 3.0 for the following features:

- Secure shell
- SNMPv3
- EAPoL
- MAC Security
- Password authentication
- IP Manager

Table 46 Secure Shell Security

Secure Shell	Description
Description	Secure Shell (SSH)) is a set of secure protocols that allow you to log into another computer over a network, and to execute commands in a remote machine. It provides strong authentication and secure communications over unsecured channels. It is intended as a replacement for rlogin, rsh, and rcp.
What is being secured	Telnet sessions (Secure)
Per Port or Per Switch	Per switch
Layer	Layer 4
Level of Security	Access/Encryption

Table 46 Secure Shell Security

Secure Shell	Description
Violations	Secure Shell protects against: --IP spoofing, where a remote host sends out packets which pretend to come from another, trusted host. SSH even protects against a spoofer on the local network, who can pretend he is your router to the outside. --IP source routing, where a host can pretend that an IP packet comes from another, trusted host. --DNS spoofing, where an attacker forges name server records --Interception of cleartext passwords and other data by intermediate hosts --Manipulation of data by people in control of intermediate hosts
Requirements for Setup	SSH Server needs to be configured and enabled. In the case of a DSA authentication, a DSA key needs to be generated on a client and downloaded to a server using NNCLI or SNMP commands.
Configuring using interfaces	NNCLI or SNMP.
Restrictions and Limitations	Current implementation only support SSH version 2

Table 47 SNMPv3 Security

SNMPv3	Description
Description	Latest version of SNMP, provides strong authentication and privacy for SNMP (using HMAC-MD5, HMAC-SHA, and CBC-DES), plus access control of MIB objects based on usernames.
What is being secured	Access to MIBs using SNMPv3 is secured. Access to MIBs using SNMPv1/v2c may be restricted.
Per Port or Per Switch	Per switch
Layer	SNMP Port 161, 162
Level of Security	Access/Encryption

Table 47 SNMPv3 Security

SNMPv3	Description
Violations	Received SNMPv3 packets that cannot be authenticated will be discarded. For authenticated packets which try to access MIB objects in an unauthorized manner, an error will be returned to the sender. In any case, various MIB counters will be incremented when any kind of violation occurs (these can be monitored to detect intrusions, for example, by using RMON alarms).
Requirements for Setup	Initial configuration of view, users, and keys must be done in a controlled environment, using NNCLI or Web interface. After that, configuration can be modified using SNMPv3 Set requests, NNCLI, or Web. Access using any of these may be restricted. NNCLI commands are provided to easily generate initial configuration, based on IETF RFCs.
Configuring using interfaces	NNCLI, Web, ASCII config file, SNMP Set requests.
Restrictions and Limitations	Non-SSH software versions do not support HMAC-SHA nor CBC-DES
Reference	Web Guide, Using Guide, RFCs 3410 through 3419, MIB file.
Comments	None

Table 48 EAPOL Security

EAPOL	Description
Description	Extensible Authentication Protocol Over LAN (Ethernet) - set up network access control on internal LANs.
What is being secured	User access to the network
Per Port or Per Switch	User authentication per port
Layer	Layer 2
Level of Security	Encryption

Table 48 EAPOL Security

EAPOL	Description
Violations	Switch blocks a port if intruder is seen on that port. Admin has to re-enable port
Requirements for Setup	Radius Server configuration on the switch. EAP-Radius server needs to be accessable from the switch.
Configuring using interfaces	Console/NNCLI/Web
Restrictions and Limitations	Currently supports only one user port
Reference	IEEE802.1X/ RFC 2284/ MIB files
Comments	

Table 49 MAC Security

MAC Security	Description
Description	The MAC address-based security feature allows a user to set up network access control, based on source MAC addresses of authorized stations.
What is being secured	Access to the network or specific subnets or hosts.
Per Port or Per Switch	Per port
Layer	Layer 2
Level of Security	Forwarding
Violations	SA filtering, DA filtering, Port Partitioning, SNMP Trap
Requirements for Setup	Not applicable
Configuring using interfaces	Web, Console, NNCLI, ASCII configuration file, SNMP.
Restrictions and Limitations	
Reference	s5sbs103 MIB/
Comments	

Table 50 Password Authentication Security

Password Authentication	Description
Description	Security feature
What is being secured	User access to a switch or stack
Per Port or Per Switch	For Radius authentification: - Radius server needs to be accessable from switch. - The Radius client from switch should be provisioned with Radius server IP and UDP Port and a shared secret.
Layer	Not applicable
Level of Security	Provides Read Only / Read Write access. The access rights are checked against Local Password / Radius Server.
Violations	Not applicable
Requirements for Setup	For Radius authentification: - Radius server needs to be accessable from switch. - The Radius client from switch should be provisioned with Radius server IP and UDP Port and a shared secret.
Configuring using interfaces	Console, web, NNCLI, ASCII configuration file.
Restrictions and Limitations	Not applicable

Table 51 IP Manager Security

IP Manager	Description
Description	IP Manager is an extension of Telnet. It provides an option to enable/disable access for TELNET (Telnet On/Off), SNMP (SNMP On/Off) and Web Page Access (Web On/Off) with or without a list of 10 IP Addresses and masks.
What is being secured	User access to the switch via telnet, SNMP, or Web.
Per Port or Per Switch	Per switch

Table 51 IP Manager Security

IP Manager	Description
Layer	IP
Level of Security	Access
Violations	User is not allowed to access the switch.
Requirements for Setup	Optional IP Addresses/Masks, Individual Access (enable/disable) for TELNET, SNMP or Web Page
Configuring using interfaces	Web, console, and CLI
Restrictions and Limitations	Same as BPS 200 IP Manager List