Software Release V4.3

Part No. 214110-C_Rev_01
July 2003

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the BayStack 450 10/100/1000 Series Switch

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

Trademarks

Statement of Conditions

Nortel Networks Inc. Software License Agreement

Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any

reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 2375 N. Glenville Dr., Richardson, TX 75082.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Introduction

These release notes contain important information about software version V4.3 for the Nortel Networks* BayStack* 450 Switch that may not be included in the related user guide *Using the BayStack 450 10/100/1000 Series Switch* (Part number 309978-D Rev 00). The information in these release notes supersedes the applicable information in the user guide.

These release notes contain the following sections:

Upgrading the BayStack 450 Firmware

Note: For the V4.3 software release, there are no changes to the firmware image (version 1.48). If the firmware currently installed is version 1.48, you do not need to upgrade the firmware image.

The BayStack 450 firmware provides a code load facility that allows you to upgrade the software image over any switch port, including any MDA ports.

The BayStack 400-ST1 Cascade Module *will not operate* with BayStack 450 switches that are configured with BayStack 450 software versions *earlier than* version V1.1.0. You *must upgrade all units* with BayStack 450 software version V1.1.0 (or later) *before* installing the BayStack 400-ST1 Cascade Modules.

To access the software images, see "Accessing the Software Images" on page 9.

The Upgrade Process

Upgrading the BayStack 450 switch to software version V4.3 is a two-step process:

1. **Download the *boot code image.***

Note: For the V4.3 software release, there are no changes to the firmware image (version 1.48). If the firmware currently installed is version 1.48, you do not need to upgrade the boot code image (firmware).

2. **Download the *agent image.***

To properly upgrade the BayStack 450 switch, the boot code image *must be downloaded first*, before you download the agent image. If the agent image (the operational software) is downloaded before the boot code image, the software may not be programmed into the BayStack 450 switch FLASH memory.

The switch indicates a failed image load as follows: An alternating LED pattern is displayed on the BayStack 450-24T 10/100 status LEDs (ports 13 to 24), on the BayStack 450-12T 10/100 status LEDs (ports 1 to 12), and on the BayStack 450-12F Link status LEDs (ports 1 to 12).

If this happens, cycle the switch power (power off the switch, then power it on). Use the Software Download screen to download the new boot code image. After the boot code image download completes, download the new agent image.

Upgrading to Software Version V4.3 in a Mixed Stack

Note: In this document, the term "mixed stack" refers to a stack configuration that includes BayStack 400 Series switches (BayStack 450 switches and BayStack 410-24T switches) *and* one or more Business Policy Switches.

When you upgrade a mixed stack to software version V4.3, you must first upgrade the agent code, before you upgrade the boot block. Although this is the inverse of the normal upgrade procedure, it is necessary to ensure a successful software upgrade.

For more information about mixed stack upgrades, see *Using the Business Policy Switch 2000*.

Important Considerations

When you upgrade your BayStack 450 switch:

- Download *two images* (the *boot code image* and the *agent image*). The new boot code image must be downloaded *before* the agent image is downloaded.

Note: For the V4.3 software release, there are no changes to the firmware image (version 1.48). If the firmware currently installed is version 1.48, you do not need to upgrade the boot code image (firmware).

- After upgrading your units, verify that the firmware and software versions, and the Interoperability Software Version Number (ISVN) is correct in the sysDescr field of the System Characteristics screen:
  - -- The correct firmware version is: **FW:V1.48**
  - -- The correct software version is: **SW:v4.3**
  - -- The correct ISVN number is: **2**

Recovering from a Failed Upgrade

The upgrade process is a fairly straightforward process when implemented correctly. However, if you do not follow the correct steps to upgrade your switch, the switch can become temporarily disabled.

- If you install a BayStack 400-ST1 Cascade Module before you upgrade the switch to software version V1.1.0 (or later), the code load facility may not function properly. To correct this situation, remove the BayStack 400-ST1 Cascade Module and upgrade the software properly before reinstalling it.
- If you try to download the agent image *before* you download the boot code image, the upgrade may fail: The agent software can detect an incompatible revision and will discontinue programming itself into FLASH memory. This condition is indicated by a steady pattern of alternating LEDs.

  The switch will not automatically reset. To recover from this condition, you must cycle power to the switch, upgrade the boot software, and then upgrade the agent software.

Creating a Mixed Stack

When creating a mixed stack that includes one or more Business Policy Switch 2000 switches (BPS 2000), complete the following steps:

1. **Upgrade your BayStack 450 switches and your BayStack 410-24T switches to software version V4.3:**

   Confirm that all of the switches you intend to use in your new stack have the same ISVN numbers. Upgrade all switches that have incorrect ISVN numbers (see *Using the Business Policy Switch 2000*, *Using the BayStack 410-24T 10BASE-T Switch*, and *Using the BayStack 450 10/100/1000 Series Switch* for information about ISVN version numbers and upgrade details).

2. **Power down all BayStack 450 switches and BayStack 410-24T switches.**

3. **Set the Unit Select switch for all BayStack 450 switches and BayStack 410-24T switches to the "Off" position (Off = Down).**

4. **Set the Unit Select switch on one of your BPS 2000 only, to the "Base" position (Base = Up).**

5. **Set the Stack Mode value for all BPS 2000 to "Hybrid" mode.**

   See *Using the Business Policy Switch 2000* for details.

6. **Use the Reset command to reset all Business Policy Switches in order to save current configuration.**

7. **Power down all units.**

8. **Ensure that all cascade cables are connected properly, and then power up the stack.**

   See *Using the Business Policy Switch 2000* for details on managing your stack.

See *Using the Business Policy Switch 2000*, *Using the BayStack 410-24T 10BASE-T Switch*, and *Using the BayStack 450 10/100/1000 Series Switch* for additional details about creating mixed stack configurations.

Accessing the Software Images

You can access the software image files directly from the Internet:

Note: For the V4.3 software release, there are no changes to the boot code image (firmware). If the firmware currently installed is version 1.48, you only need to download the agent image (the software).

1. **Go to** *www.nortelnetworks.com/cs.*
2. **Under the Switching Products (or Data and Internet) heading, select BayStack Switches - 450 10/100/1000 Switch, then click the Go button.**
3. **Under the Operational Software heading, click on BayStack 450 Ethernet Switch boot code V4.3.**

   Follow the prompts to download the BayStack 450 boot code image, if necessary. The boot code image file name is *b4504301.img*.
4. **After the BayStack 450 boot code image is downloaded, click on BayStack 450 Ethernet Switch agent V4.3.**

   Follow the prompts to download the BayStack 450 agent image. The agent image file name is *b4504302.img*.

For detailed information about downloading a new software image, see Chapter 3, "Using the Console Interface," in *Using the BayStack 450 10/100/1000 Series Switch*.

Upgrade Restrictions

The following restrictions apply when you upgrade the switch to software version V4.3:

- When you upgrade a stack configuration (running software versions earlier than V2.0) that uses a Gigabit distributed trunk for the uplink to the TFTP server, you must first disable the MultiLink Trunk at both ends.
- When you upgrade a stack configuration that contains a BayStack 410-24T unit (which is configured with at least one distributed trunk member), and the distributed trunk is the uplink to the TFTP server, you must first disable the MultiLink Trunk at both ends.

- The switch cannot be upgraded to software version V4.3 through a port that is configured for *tagged* traffic unless your switches are *currently* running software version V2.0 *or later.*

  If your switches are currently running software versions *earlier* than software version V2.0, you must upgrade your switch to software version V4.3 through a port that is configured as an *untagged* member of VLAN 1. (Software versions V2.0 and later now support upgrades to future versions over VLANs other than VLAN 1, with tagged or untagged ports.)

- When the BayStack 450 switch is upgraded with the new boot code image, all existing entries in the Event Log are erased. This corrects a potential problem with an earlier software version. A new entry is written to the Event Log confirming the upgrade of the boot code image.

- When you upgrade a *mixed stack* to software version V4.3, you must first upgrade the agent code, before you upgrade the boot block. Although this is the inverse of the normal upgrade procedure, it is necessary to ensure a successful software upgrade.

  For more information about mixed stack upgrades, see *Using the Business Policy Switch 2000*.

- During the load process, the ports are configured as follows:

  -- Twisted-pair ports: autonegotiation enabled

  -- Fiber optic ports: 100 Mb/s, half-duplex

  -- Gigabit MDA ports: autonegotiation disabled, Preferred Phy set to Right

Nortel Networks Online Documentation

To be sure you have the latest updates to your product documentation, including these release notes, visit the Nortel Networks* Web site at:

www.nortelnetworks.com/documentation

Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com.*

New Features

The following new features are provided with software version V4.3:

- Support for administrative capabilities for MAC addresses reporting security violations has been added. [Q00581214]
- Support for copper GBIC (GigaBit Interface Converter) has been added for this release [Q00669967]

There are no new features provided with software version V4.2.0.22.

The following new features are provided with software version V4.2.0.12:

- Power and fan status are now updated dynamically every 5 seconds. [Q00168231]
- Any interruption or failure in cascade cabling results in the following message being displayed in the Event Log: `Cascade Cable Disconnect Detected`. [Q00168227]
- TCP connections from IP addresses not in the Access list are now silently dropped. [Q00212841-2]
- RADIUS Access Challenge is now implemented. Typical use for this is with SecurID access control. [Q00206612]

  For example:

  a. Telnet in to the switch

     The switch prompts you for RADIUS authentication information (username and password).

  b. Enter username and password at the prompt.

     Access request is sent to RADIUS server.

     RADIUS server, when so configured, sends request to authentication server.

     Authentication server sends back access-challenge with state information and challenge reply information.

     Switch receives response and displays a challenge screen to the user with the challenge reply information.

c. Respond according to the challenge screen and reply information.

   Your original username and the new response are then sent to the RADIUS server in a new access request.

   The access request then goes through the same validation process as in Step b, and may get more challenges, or access accept/reject.

- When a stack of two units is unable to function as a stack because of the cascade connector or one or the units becomes unavailable, the remaining operating unit(s) generates traps indicating both units are no longer part of the stack. [Q00286025]

The following new features are provided with software version V4.1.0:

- The Event Log screen now allows you to specify which stack unit to display.
- TELNET access traps are now available for the following TELNET events:
  - -- Login/logout
  - -- Password failure
  - -- Login timeout
  - -- Inactivity timeout
  - -- Non-allowed IP address.
- IGMP-2 “Leave” messages are now processed and cause rapid ageout of all forwarding database entries for the port that received the “Leave” message.
- You can now use the rcVlAction MIB object to clear the switch’s Forwarding Database via the flushMacFdb setting. Any instance can be used to clear the Forwarding Database.
- The switch no longer caches the last successful read-write access, username, and password for validation when the RADIUS server is not reachable.

  In the event that there is no response from the RADIUS server, the (read-only or read-write) switch or stack password can be used to login, depending on the operational mode of the stack units. The Console/Comm Port Configuration Menu includes a field (RADIUS Password Fallback) to enable or disable this feature. The default configuration is Disabled.
- You can now enable or disable fast aging.

  The MAC Address Table screen has a new field that allows you to control fast aging. The default configuration is Enabled.

- The IP Configuration/Setup screen now includes a unit number field that can be used to access and update the IP configuration of any stack unit.
- The Hardware Unit Information screen (Figure 1) now displays the following status information:
  - -- The primary and redundant power status for each stack unit
  - -- The status of any cascade link
    - -- G (green) indicates cascade operational
    - -- Y (yellow) indicates cascade wrapped
  - -- The status of each of the 3 fans for each stack unit.
    - -- R indicates the fan is rotating
    - -- F indicates the fan has failed

```
                        Hardware Unit Information


Unit Switch Model         MDA Model  Cascade MDA  Up Dn  Fans 1 2 3   Power Status
 ---- ----------------    ---------  -----------  -----  -----------  ----------
   1  BayStack 450-24T    None       400-ST1      G  G        R R R   Primary
   2  BayStack 450-24T    None       400-ST1      G  G        R R R   Primary
   3  BayStack 450-24T    None       400-ST1      G  G        R R R   Primary
   4  BayStack 450-24T    None       400-ST1      G  G        R R R   Primary
   5  BayStack 450-24T    None       400-ST1      G  G        R R R   Primary
   6  BayStack 450-24T    None       400-ST1      G  G        R R R   Primary
   7  BayStack 450-24T    None       400-ST1      G  G        R R R   Primary
   8  BayStack 450-24T    None       400-ST1      G  G        R R R   Primary


Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu
```

Figure 1. Hardware Unit Information screen

- Traps:
  - -- Traps are now generated for any change in primary or redundant power.
  - -- Traps are now generated whenever the status of any fan changes.
  - -- A new Trap Control screen (Figure 2) is available from the main menu that allows you to control switch-generated traps.

```
                              Trap Control


        Remote Login     [ Enabled  ]        Unit Up          [ Enabled  ]
        Cold Start       [ Enabled  ]        Unit Down        [ Enabled  ]
        Warm Start       [ Enabled  ]        MAC Access       [ Enabled  ]
        Link Down        [ Enabled  ]        Mgmt Access      [ Enabled  ]
        Link Up          [ Enabled  ]
        Rising Alarm     [ Enabled  ]        Save Changes:    [ Enable   ]
        Falling Alarm    [ Enabled  ]
        New Root         [ Enabled  ]
        Topology Change  [ Enabled  ]
        Hot Swap         [ Enabled  ]
        Problem Trap     [ Enabled  ]


Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu
```

Figure 2. Trap Control screen

Table 1 describes the Trap Control screen fields

Table 1. Trap Control screen fields

Field	Description
Remote Login	Login TELNET access.
Cold Start	Unit has been power cycled.
Warm Start	Unit has been reset.
Link Down	Link has changed from Down to Up state.
Link Up	Link has changed from Up to Down state.
Rising Alarm	Values are outside of the limits specified in threshold entries set by user.

(continued)

Table 1. Trap Control screen fields (continued)

Field	Description
Falling Alarm	Values are outside of the limits specified in threshold entries set by user.
New Root	A new Root bridge has been detected.
Topology Change	A network Topology change has been detected.
Hot Swap	Generate trap when one stack unit is replaced.
Problem Trap	• Generate trap for any change in primary or redundant power. • Generate trap whenever the status of any fan changes.
Unit Up	A new unit has been added to the stack.
Unit Down	A stack unit has been removed or has reset.
MAC Access	An unauthorized MAC address has been detected.
Mgmt Access	Management security of allowed IP addresses for management of box.
Save Changes	Save current traps to NVRAM.

Bug Fixes

The following problems are corrected with software version V4.3:

- [Q00628017]—Users with read-only telnet access can no longer change trap control settings.
- [Q00616247]—In previous releases, under certain conditions, the error message `EAP send message failed` could appear continuously on the console. This has been fixed with software version V4.3.
- [Q00669489]—In previous releases, the switch would sometimes freeze after receiving an EAP access reject message from an ACS RADIUS server. This have been fixed with software version V4.3.
- [Q00566210]—The switch now sends a trap when there is a speed mismatch on an Ethernet connection.
- [Q00633259]—In previous releases, under certain conditions, IGMP proxy could spoof IP addresses with pseudo queriers. This has been fixed with software version V4.3. The switch will always use its own addresses for queries and proxy reports.
- [Q00630790]—In previous releases, any port that was a member of the management VLAN could ping the switch IP regardless of the PVID set on the ingress port. This has been fixed with software version V4.3.

- [Q00589101]—The IGMP version 2 reports sent by the switch now properly include the Router Alert Option field.

The following problems are corrected with software version V4.2.0.22:

- [Q00595413]—Sending 110 IGMP reports to a stack with 64 VLANs will no longer cause non-base unit devices to reset.
- [Q00589947]—RADIUS authentication for console access now works properly on non-base units.
- [Q00589962]—In previous releases, the port speed and duplex settings on non-base unit devices would sometimes incorrectly change. This has been fixed with software version V4.2.0.22.
- [Q00589926]—The port speed and duplex settings now display properly after the switch is reset.
- [Q00561936]—Retrieving the MIB object rcMltPortMembers using GetBulk (SNMPv2c) now returns the proper value.
- [Q00552885]—In previous releases, large numbers of IGMP groups could cause the switch to reset. This has been fixed with software version V4.2.0.22.
- [Q00553271]—Upon intrusion detection, MAC Security will properly partition the correct port(s).
- [Q00575899]—Flash corruption at unit startup no longer occurs because of poor startup power.

The following problems are corrected with software version V4.2.0.16:

- [Q00500160]—In some previous releases, a large stack that had DMLT configured could experience dropped packets and connectivity problems when the same MAC addresses were learned on the various DMLT interfaces. Inconsistencies in the MAC table and CAM could develop. This has been fixed with software version V4.2.0.16.
- [Q00508105]—An IGMP leave packet with a group address of 0.0.0.0 no longer causes a reset of the switch.
- [Q00433590]—The switch ignores ICMP redirect messages.
- [Q00514741]—DMLT no longer functions incorrectly when a VLAN is deleted from a stack that has multiple VLANs with trunk ports configured as static router ports.

- [Q00514963]—Downloading an ASCII configuration file will no longer result in a broadcast storm on a switch that is set to DMLT.
- [Q00471648]—When using Device Manager, the Trap Receivers tab of the Edit > Chassis dialog box displays correctly.
- [Q00469218]—There is no longer any delay when navigating menus from within a telnet session.
- [Q00522218]—Trap objects are consistent with MIB objects. Traps now report the proper value of MIB instances.

The following problems are corrected with software version V4.2.0.12:

- [Q00420120]—Using the arrow keys while in the display event log menu no longer causes the switch to reset.
- [Q00461709]—In version 4.2.0.9, under certain conditions Internet Group Multicast Protocol (IGMP) reports were not forwarded properly. IGMP reports are now properly forwarded, even if a static router port is not configured.

The following problems are corrected with software version V4.2.0.9:

- [Q00171413]—Setting traps on the switch no longer causes general errors.
- [Q00217448]—Port VLAN Identifier (PVID) no longer changes back to VLAN 1 when the port status changes to link up.
- [Q00156736]—Distributed MultiLink Trunking (DMLT) connectivity problem has been corrected.
- [Q00122482]—Slow SNMP response occurring in previous releases has been corrected.
- [Q00212720]—The switch no longer drops initial IGMP joins (reports) via the cascade interface.
- [Q00212892]—The switch no longer reports a warning for the nonexisting fourth fan.
- [Q00146221]—When proxy is disabled, the switch will no longer proxy for IGMP reports.
- [Q00146019]—Multicast traffic no longer floods under heavy load.
- [Q00094210]—Port-mirroring on stacked switches will now see egress packets.

- [Q00102366]—The switch no longer resets when the letter ‘o’ is entered in the Main Menu of the console interface screen.
- [Q00080820]—The IGMP host no longer loses communication across the stack when one station leaves.
- [Q00028092]—Setting historyControlBucketRequest to a large number no longer returns an error.
- [Q00083251]—MultiLink Trunking (MLT) properly fails over when the TX fiber is pulled from a Gigabit Ethernet link.
- [Q00084390]—BPDU packets no longer cause loops on DMLT trunks when IGMP and Spanning Tree Protocol (STP) are disabled.
- [Q00076149]—Intrusions now generate SNMP traps.
- [Q00043046]—The stack IP address is no longer unreachable after STP topology changes.
- [Q00075928]—MAC address is now properly displayed from the MAC address table when MAC security is enabled.
- [Q00075932]—The MAC address table no longer becomes filled with incorrect addresses when security is enabled.
- [Q00080612]—The switch no longer generates a Link Up trap during booting.
- [Q00080729]—STP changes now properly generate change a change trap.
- [Q00075695]—Running IGMP multicast traffic no longer displays error messages on the console.
- [Q00075875]—The power status now displays properly for standalone units.
- [Q00086787]—Device Manager (DM) 5.2 no longer sets the incorrect flag value “Discard Untagged Frames.”

The following problems are corrected with software version V4.1.0:

- [CR 143801]—You can now run IGMP multicast traffic over a DMLT while the IGMP snooping feature is disabled. The IGMP traffic that is received on one link of the DMLT will no longer loop back onto another link of the trunk.
- [CR 129397]—The switch no longer generates SNMP trap-v1 traps when the UDP source port is equal to zero.

- [CR 132649 and CR 97744]—The switch's RMON alarm threshold now supports a value of zero.
- [CR 133488]—You can now use the Optivity NMS V9.0.1 Threshold Manager application to set a threshold on the switch.
- [CR 138563]—The switch no longer resets when authenticated by the RADIUS server.
- [CR 141287]—IGMP now correctly reports the switch's MAC address.
- [CR 142112]—You can now copy config to TFTP servers without TFTP errors even when the TFTP server is located several hops from the switch.
- [CR 144932 and 145393]—You can now add a new unit to a stack that was previously configured with a total of 8 units.
- [CR 145093]—The switch no longer exhibits instability or IP Stack lockup subsequent to an SNMP Set request.
- [CR 131622]—The switch now updates the IGMP Group Membership Table even when the client application is no longer receiving IP Multicast traffic.
- [CR 143754]—The switch no longer sends multiple packets when a DMLT link is disconnected and then reconnected.

Known Restrictions

The following known restrictions apply to software version V4.3 (and earlier versions):

- Mixed stack configurations

  The following restrictions apply to mixed stack configurations:

  -- If you are managing your mixed stack using a console interface, connect the console to a Business Policy Switch.

  -- Management VLAN functionality is operational only through ports that are configured as both "ingress" and "egress" members for the management VLAN.

  -- The following BayStack 450 switch features are not available in a mixed stack configuration:

  - SNMP Security
  - Save Current Settings

- System reset due to MultiLink Trunking reconfiguration

  If you add a new unit, that is configured with at least one bounded trunk (an active trunk with all trunk members configured on the same module)—with no distributed trunks (an active trunk with trunk members configured on at least two different units within a single stack), into a stack that is configured with one or more distributed trunks, the new unit automatically resets before entering the operational mode of the stack.

- MultiLink Trunking

  MultiLink Trunking allows you to group ports of varying speeds (for example, you can group 10 Mb/s, 100 Mb/s, and 1000 Mb/s ports in any combination). Although this is a valid configuration, Nortel Networks recommends that you only group ports of equivalent speeds when configuring a trunk. The MultiLink Trunk algorithm distributes connections across all of the available links in the trunk, regardless of speed.

- Monitoring outgoing frames on trunk member ports

  When you monitor outgoing frames on a full-duplex port that is a MultiLink trunk member, Nortel Networks recommends that you use the address-based mirroring mode. If you use port-based mirroring with this type of configuration, some frames may not be displayed.

- MultiLink Trunking interoperability with Passport*

  When a Distributed MultiLink Trunk (DMLT) is connected to a Passport switch and you reset one of the stack units or change the spanning tree status of the DMLT, each unit sends out a (standalone) BPDU frame through the DMLT port. This can cause Passport switches with software versions prior to V2.0.5 to disable the DMLT.

  If this happens, reset the Passport switch. If resetting the Passport switch does not correct the problem, contact your Nortel Networks Technical Solutions Center (see “How to Get Help” in *Using the BayStack 450 10/100/1000 Series Switch*).

- BayStack switches automatically calculate the path cost for any given port, based on the port’s speed and duplex settings. If you manually change the path cost setting, the switch no longer automatically calculates the path cost for that port.

- Spanning Tree Participation value disabled for monitor port

  When you use the Port Mirroring feature in a standalone switch configuration, the Spanning Tree Participation value for the monitor port is automatically set to Disabled. If you then insert the same standalone switch into a stack, the Spanning Tree Participation value for the previously configured monitor port *remains* Disabled. You must manually reset the Spanning Tree Participation value to Normal Learning or Fast Learning using the Spanning Tree Port Configuration screen.

- IEEE 802.1D spanning tree parameters

  Spanning tree parameters cannot be configured from the console interface (CI) menus and screens.

  Configuration support is available through the Bridge MIB using Simple Network Management Protocol (SNMP). Refer to RFC 1493 for more information.

- The spanning tree configuration must be the same on both ends of a MultiLink trunk.

- Spanning tree port participation

  The Fast Learning value (used with the Participation field in the Spanning Tree Port Configuration screen) is the same as the Normal Learning value, except that the state transition timer is shortened to two seconds.

  Nortel Networks recommends using the Fast Learning value to optimize switch-to-endstation connections. When you connect one switch to another switch, the Normal Learning (default) value provides the best results.

- MAC address-based security learning process

  If you move a device from one port to another during the MAC address-based security learning process, the device's MAC address will move to the new port and will no longer be allowed on the original port. A given MAC address can be learned on only one port at a time.

- You cannot assign an *untagged* port to multiple protocol VLANs that have the same protocol ID.

- Redundant gigabit Phy

  You cannot use the redundant gigabit Phy port (the backup Phy port) to create two different paths.

- Autonegotiation restriction with gigabit ports

  The BayStack 450 switch's gigabit MDA ports comply with IEEE 802.3z Draft 3.2 and IEEE 802.3z Draft 4.1; however, the following restriction applies to the autonegotiation feature:

  -- Autonegotiation does not restart if an invalid code word is received from the link partner during the autonegotiation process. In cases where autonegotiation fails, disable and then enable autonegotiation.

- RMON Alarms and Event entries

  RMON Alarms and Event entries are *not* saved to nonvolatile random access memory (NVRAM). When a reset condition or power-down sequence occurs, the entries are not preserved. This conforms to the current RFC 1757 standard. All RMON Alarms and Events must be reentered.

- RMON Event Log table's secondary index

  The RMON Event Log table's secondary index is not incremented when all of the table's entries have been used. In this case, the existing indexes are reused. Thus, the index number cannot be used to indicate the total number of log entries received.

- RMON History Control entries

  A maximum of 85 RMON History Control entries per stack unit are supported. The entry exists on the unit containing the "ControlDataSource."

- Changing from a stack unit to a standalone switch

  When you change a switch from a stack unit into a standalone switch, or vice versa, the IP address of the switch/stack changes. As a result, all existing management applications that use the previous IP address are lost until you reconnect using the new IP address.

- Console may display a blank screen

  When you connect a console terminal to an operating switch through the Comm Port, the console may display a blank screen. This is a normal condition. Press [Ctrl]-C to refresh the screen or, to get beyond the Nortel Networks logo screen, press [Ctrl]-Y.

- Adding or removing stack units

  When you add a new unit to the stack or remove an existing stack unit, you will not be able to perform IP management functions for approximately 30 seconds.

  During this time period, the following can occur:

  -- Packets are lost when performance testing with SmartBits or any other traffic generator.

  -- IP Multicast streams stop receiving.

  -- TELNET sessions time out and users lose their TELNET connection without warning. Users must re-establish lost TELNET sessions.

  -- ICMP echo (PING) requests do not receive responses.

  -- All IP-related processes fail temporarily.

- Tagged bridge protocol data units (BPDUs)

  Tagged BPDUs are not supported in this version.

- Network interface controllers (NICs)

  The MultiLink Trunking feature supports only multiport NICs that are configured as a single MAC address, single IP address entity.

- Downgrading a switch or stack to a software version earlier than software version V1.3.

Note: Software versions earlier than software version V1.3 do not support distributed trunking (DMLT). You must remove any distributed trunks before you downgrade the switch to software versions earlier than software version V1.3 or problems will occur.

If you must downgrade a switch from software version V1.3 (or later) to an earlier version, you must first remove any existing distributed trunks using the MultiLink Trunk Configuration screen. You can remove the trunk by disabling the trunk and setting all the trunk members to none [blank field].

If you downgrade a switch with a bounded MultiLink trunk from software version V1.3 (or later) to an earlier version, some ports may become disabled. If this happens, you can enable the ports again using the Port Configuration screen.

- Monitoring outgoing frames on a gigabit Ethernet port

  When you monitor outgoing frames on a gigabit port, the multicast frames that are generated by the switch (for example, BPDUs, Autotopology, and IGMP) will not be seen on the monitor port.

- Downgrading your BayStack 450-12F switch

  You cannot downgrade your BayStack 450-12F switch or a stack configuration that contains a BayStack 450-12F switch, to a software version earlier than software version V1.3. Software versions earlier than V1.3 do not support the BayStack 450-12F switch.

- Software versions earlier than V3.1.0 do not support mixed stacks that include BPS 2000.

- Stack reset when creating the first DMLT

  When you create your first DMLT using SNMP management, your stack can reset without warning. This reset is required to enable only the first DMLT in a stack.

Known Problems

The following problems are known to exist in software version V4.3 (and earlier versions):

- The trap object 1.3.6.1.4.1.45.5.2.2 may not be correctly decoded when queried by certain network management software. When, in response to this query, bsnNotifications is sent, it could imply speed mismatch or EAP authentication failure.

- When using 1000BASE-XD and 1000BASE-ZX (long-haul) GBICs in your 450-1GBIC MDA, the System Characteristics screen *incorrectly* shows the GBIC devices as “Unsupported.” However, the GBIC devices operate properly and pass traffic correctly.

- MDAs must be *firmly secured* in the chassis for proper operation. Be sure to secure the MDA in the chassis by *firmly* tightening the two thumbscrews on the MDA front panel.

- A link state cannot be established when you connect a cable that is 100 percent utilized into a BayStack 450 switch port. As soon as a break in the traffic occurs, the link state is established.

- When mirroring a single MLT member, the monitor port will receive all of the unknown unicast traffic that is transmitted over the entire MLT.
- When you connect the BayStack 450 switch to an Alteon NIC, the switch learns invalid MAC addresses whenever autonegotiation for a gigabit MDA port is enabled (the invalid MAC addresses eventually age out). This problem occurs only when you reset the switch (via the console interface Main Menu or during a power cycle) and does not affect the correct operation of the BayStack 450 switch.

Connecting to Passport Gigabit Ports

The BayStack 450 switch supports gigabit MDA port connections to the Nortel Networks Passport switch gigabit Ethernet ports, with the following restrictions:

- Autonegotiation *is not* supported on the Passport 1000BaseSXWG (ASIC Version *GMAC 2*). When connecting to this version, disable autonegotiation on the BayStack 450 switch's gigabit MDA port.
- Autonegotiation *is* supported on the Passport 1000BaseSXWG (ASIC Version *GMAC 4*).

  When connecting to this version, set autonegotiation to enabled (or disabled) at both ends of the communications link. The autonegotiation setting must be identical at both ends of the communications link.

You can determine the ASIC version number for the 1000BaseSXWG gigabit card using the following command from the Passport console port:

```
Passport-1100# sh sys info
```

1000BASE-LX Connectors

The 1000BASE-LX (gigabit) MDAs use a longwave 1300 nm, fiber optic transceiver to connect devices over single-mode (5 km/3.1 mi) or multimode (550 m/1,805 ft) fiber optic cables.

Note: The transceiver must be mode conditioned externally via a special offset SMF/MMF patch cord for 1000BASE-LX multimode applications. The offset SMF/MMF patch cord allows the same transceiver to be used for both multimode and single-mode fiber. See your Nortel Networks sales representative for more information about the SMF/MMF patch cord.

The optical performance of this transceiver cannot be guaranteed when connected to a multimode fiber plant without the use of the special offset SMF/MMF (mode conditioning) patch cord.

The 1000BASE-LX MDA transceiver is designed to mechanically accommodate the *single-mode ferrules* used on one end of the special offset SMF/MMF patch cord. *Multimode ferrules* can bind and cause damage to the transceiver.

Caution: Do not connect multimode cables directly into the 1000BASE-LX MDA transceiver. Connect a special offset SMF/MMF patch cord into the transceiver, then connect the multimode cable into the SMF/MMF patch cord.

For more information about gigabit transmission over fiber optic cable and mode conditioning, refer to:

Reference Note: Gigabit Ethernet Physical Layer Considerations

The publication is available on the World Wide Web at *www.nortelnetworks.com/documentation*.

Network Management

Table 2 lists the supported network management applications that are available.

Table 2. Supported Network Management Applications

	BayStack 450 Software Versions				
Application	**V3.0.0 (HW Rev B, D, L)**	**V3.1.0 (HW Rev B, D, L)**	**V4.0.0 (HW Rev B, D, L)**	**V4.1.0 (HW Rev B, D, L)**	**V4.3 (HW Rev B, D, L)**
NMS 9.0	Partial support only (see Note)	Partial support only (see Note)	Partial support only (see Note)	Partial support only (see Note)	Partial support only (see Note)
NMS 9.0, with 9.0.0.2 patch[1]	Yes	Yes	Yes	Yes	Yes
NMS 9.0.1[1]	Yes	Yes	Yes	Yes	Yes
NMS 9.0.1.1[1]	Yes	Yes	Yes	Yes	Yes
Device Manager 3.0.3	No	No	No	No	No
Device Manager 3.0.4.1	Yes	No	No	No	No
Device Manager 4.0.0	Yes	Yes	No	No	No
Device Manager 4.2.0	Yes	Yes	No	No	No
Device Manager 5.1.0	Yes	Yes	Yes	Yes	Yes
Switch Manager V1.0	Partial support only (VLAN only)	Partial support only (VLAN only)	Yes	Yes	Yes
Switch Manager V1.1	Yes	Yes	Partial support only	Partial support only	Partial support only
NCS V2.2[2]	Yes	Yes	Yes	Yes	Yes

[1] Requires installation of the appropriate version Optivity* Integration Toolkit (OIT) for the BayStack 450 (see "OIT Support for Multiple Software Versions" on page 28).

[2] Requires installation of the appropriate version NCS Optivity Integration Toolkit (OIT) for the BayStack 450 switches.

Note: Optivity NMS 9.0 provides partial support only for these switch versions. For a list of Optivity modules or components that support the BayStack product, see *Release Notes for Optivity Network Management System 9.0 for Solaris and Windows NT* (Part number 205970-A). You can obtain a copy of the Optivity 9.0 release notes at: *support.baynetworks.com/library/tpubs/nav/netman/nms.htm#OPTN90.*

OIT Support for Multiple Software Versions

The Optivity Integration Toolkit (OIT) files are designed to support specific versions of the BayStack 450 switch software. If your networking environment requires you to support multiple BayStack software versions (for example, BayStack software version V2.0 on some devices and BayStack software version V4.3 on other devices), you must have both versions of the supporting OIT files loaded onto your Network Management Station (NMS).