Part No. 217103-A
June 2005

4655 Great America Parkway
Santa Clara, CA 95054

# Release Notes for the Ethernet Switches 460 and 470 Software Release 3.6

*217103-A*

NORTEL

## Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

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

The asterisk after a name denotes a trademarked item.

## 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.

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

## Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

**1. Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

**2. Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

**3. Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

**4. General**

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

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

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

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

# Contents

# Introduction

These Release Notes support the Release 3.6 software for the Nortel Ethernet Switches 460-24T-PWR, 470-24T, and 470-48T. They cover the supported hardware, new features, fixed issues, known issues and considerations in 3.6 software, outstanding issues from release 3.5 software, and outstanding issues from release 3.1 software.

The following topics are discussed in this document:

**Note:** The Hybrid stack mode is not supported in Release 3.6 software. All stacks must contain only Ethernet Switches 460-24T-PWR, Ethernet Switches 470-24T, and Ethernet Switches 470-48T. The Ethernet Switch 450 is no longer supported in the stack.

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

- All Ethernet Switch 470-48T units
- All Ethernet Switch 470-24T units
- All Ethernet Switch 460-24T PWR units

Any one of the switches in the stack can function as a base unit in a stack; but if an Ethernet Switch 470-48T is in the stack, it must be the base unit.

# Hardware requirements

The following are the Ethernet Switches supported by version 3.6 software:

**Table 1**

| Hardware Platform | Part Number |
|---|---|
| Ethernet Switch 460-24T PWR | AL2001?20 |
| Ethernet Switch 470-24T | AL2012?37 |
| Ethernet Switch 470-48T | AL2012?34 |

# SSH-enabled image

The Ethernet Switch Software can be installed using an SSH-enabled image that provides the following features:

- Secure Shell (SSH) connections
- Secure Socket Layer (SSL) connections for web-based management
- Password Security feature
- SHA-based user authentication and DES-based privacy encryption

**Note:** These features are not available on non-SSH images.

## Release 3.6 images

The components for the Ethernet Switch 460 and 470 release 3.6 include:

- Standard Runtime Image Software Version 3.6.0.8 (es460-470sw36008.img)
- Secure Runtime Image Software Version 3.6.0.9 (es460-470sw36009s.img)
- Boot/Diagnostic Software Version 3.6.0.3 (ES460-470diags3603.bin)
- Java Device Manager software version 5.9.2.0 (jdm _5920.exe / jdm_5920_solaris_sparc.sh / jdm5920_linux.sh / jdm_hpux_pa-risc.sh)
- Release 3.6 Management Information Base (MIB) definition files (460_470mibs_v3.6.zip)

## Upgrade instructions

When upgrading the Ethernet Switch 460-24T-PWR or Ethernet Switch 470-24T/48T to release 3.6, follow this procedure:

1. Backup the binary configuration file to a TFTP server.
2. Upgrade the boot/diagnostic code to version 3.6.0.3. The system reboots after this step.
3. Upgrade the software image to 3.6.0.8 or 3.6.0.9.

# New features

The following new features are available in this release:

- Auto-Detection and Auto-Configuration (ADAC) of Nortel IP Phones
- Auto Unit Replacement
- EAPOL Security Enhancements
- MAC Address-based Security Auto-learning
- Scaling of Spanning Tree Protocol (STP) to 16 Groups
- Multiple STG Support for MultiLink Trunking
- Virtual Link Aggregation Control Protocol (VLACP)
- Per-VLAN Spanning Tree Plus (PVST+)
- Secure Socket Layer (SSL) Web-based Management
- Password Security Enhancements
- Failed Login Attempt Trap
- Command Line Interface (CLI) Command Enhancements

## Auto-Detection and Auto-Configuration (ADAC) of Nortel IP Phones

Auto-Detection and Auto-Configuration (ADAC) of Nortel IP Phones allows a switch to perform the automatic configuration of the VLANs and Quality of Service for switch ports required for the transmission of signal and voice between the Nortel IP Phone and the connected switch.

For more information on ADAC, refer to *Configuring VLANs, Spanning Tree, and Multilink Trunking* (217460-A).

## Auto Unit Replacement

The Auto Unit Replacement (AUR) feature provides the user with the ability to retain the configuration (CFG) image of a unit in a stack when that unit is replaced. The retained CFG image from the old unit can be automatically restored to the new unit.

For more information on Auto Unit Replacement, refer to the *System Configuration Guide* (217105-A).

## EAPOL Security Enhancements

Prior to the Release 3.6 software, EAP (802.1x) Authentication supported Port Based User Access. At any time, only one user (MAC) could be authenticated on a port and the port could be assigned to only one Port-based VLAN.

EAP now supports two modes for authentication:

- Single Host with Single Authentication (SHSA) and Guest VLANs
- Multiple Host (MAC) with Multiple Authentication (MHMA) - EAP Clients only

SHSA is the default mode, in which only one device/user on that port can complete EAP Authentication. However, Guest VLANs can also be configured for access to the port. Any active VLAN can be made a Guest VLAN.

With MHMA, multiple devices, each with a different MAC address, are allowed on a port. Each device must complete EAP Authentication for the port to allow traffic with the corresponding MAC address.

**Note:** EAP and MAC security are mutually exclusive on a per-port basis.

For more information on the EAPOL Security enhancements, refer to *Configuring and Managing Security* (217104-A)

## MAC Address-based Security Auto-learning

The MAC Address-Based Security Auto-Learning feature provides the ability to add allowed MAC addresses in the MAC Security Table automatically without user intervention. The user specifies the number of addresses (1-25) per port to be added in the table. The switch then forwards traffic only for those MAC addresses that are included in the Security Table on the specified ports.

**Note:** EAP and MAC security are mutually exclusive on a per-port basis.

For more information on the MAC address-based security auto-learning, refer to *Configuring and Managing Security* (217104-A).

## Scaling of Spanning Tree Protocol (STP) to 16 Groups

The Nortel Multiple Spanning Tree Groups now suppport 16 STP instances, up from eight. For more information on Spanning Tree Protocol, refer to *Configuring VLANs, Spanning Tree, and Multilink Trunking* (217460-A).

## Multiple STG Support for MultiLink Trunking

Multiple spanning tree groups can now be assigned to Tagged MultiLink Trunking (MLT) groups. The MLT can have different learning settings for different spanning tree groups. However, all port members of a particular MLT group must be assigned to the same STGs.

For more information on Multiple STG support for MLT, refer to *Configuring VLANs, Spanning Tree, and Multilink Trunking* (217460-A).

## Virtual Link Aggregation Control Protocol (VLACP)

Virtual Link Aggregation Control Protocol is an extension of the LACP handshaking protocol to enable switches to provide end-to-end failure detection between two network interfaces. It allows the switch to detect uni-directional or bi-directional failures of links even if the switches are not directly connected to one another.

For more information on VLACP, refer to *Configuring VLANs, Spanning Tree, and Multilink Trunking* (217460-A).

## Per-VLAN Spanning Tree Plus (PVST+)

In addition to the existing Nortel Multiple Spanning Tree Groups, the 3.6 release software provides support for PVST+. PVST+ is a Cisco implementation of the Spanning Tree Protocol which provides a Spanning Tree instance per VLAN. As a result, users now have the option of running Spanning Tree Protocol in a multi-vendor network when connecting to Cisco switches running PVST+.

**Note:** PVST+ is supported only in stand-alone mode. It is not supported in a stack.

For more information on support for PVST+, refer to *Configuring VLANs, Spanning Tree, and Multilink Trunking* (217460-A).

## Secure Socket Layer (SSL) Web-based Management

SSL is available to provide security for the web-based management system. It allows access to the Web-based management using a secure https session. The user must enable SSL for the browser through the CLI.

The switch does not support concurrent secure https and non-secure http sessions. If you enable SSL on the device,  the web server provides only https sessions.

For more information on SSL Web-based management, refer to *Configuring and Managing Security* (217104-A).

## Password Security Enhancements

The Password Security feature applies stricter than normal rules to govern user passwords than normal. When the Password Security feature is running, user passwords:

- must be between 10 and 15 printable characters
- can no longer be viewed as clear text, appearing as 15 asterisks (*) in the user interfaces
- expire over a configurable period of time.

**Note:** On an SSH-enabled image, default passwords are "userpasswd" for RO and "securepasswd" for RW. These new passwords are required because Password Security is enabled by factory default. Non-SSH-enabled images retain the standard default passwords (RO: user and RW: secure).

For more information on the Password Security feature, refer to *Configuring and Managing Security* (217104-A).

## Failed Login Attempt Trap

The new SNMP trap, bsnLoginFailure, sends an SNMP trap for each failed login attempt due to a user/password mismatch, provided that at least one trap receiver is configured on the switch or stack. Also, with an SSH-enabled image, the trap is generated when DSA-Authentication fails due to key mismatch. No trap is generated when the login fails due to a wrong configuration of the RADIUS server, or when the client IP is not in the allowed IP list.

The Failed Login Attempt trap is now included in the list of supported SNMP traps in *Configuring and Managing Security* (217104-A).

## Command Line Interface (CLI) Command Enhancements

The following describes additional CLI command enhancements. For additional details on these commands, see *System Configuration Guide* (217105-A).

### *help commands mode*

The `help commands mode` command displays the list of commands available on the device, either for the current mode of operation or as a complete list of all the commands available on the device.

### *help modes*

The `help modes` command displays information regarding available CLI modes on the switch.

### *show audit log*

The show audit log command displays the command history audit log stored in NVRAM. The syntax for the show audit log command is:

```
show audit log [asccfg | serial | ssh | telnet]
```

### *show interfaces gbic-info*

The show interfaces gbic-info command displays hardware specifications for GBICs on the switch.

Detailed GBIC information is now also available to users through the Console Interface, Web-based management, and SNMP when the GBIC is plugged in.

### *show tech*

The show tech command displays detailed system and configuration information for technical support purposes.

### *show system verbose*

The show system verbose command displays additional system characteristics including the status of switch fans, the power status, and the serial number of the switch.

Detailed fan status information is now also available to users through the Console Interface, Web-based management, SNMP, and Device Manager (JDM).

### *shutdown*

The shutdown command performs a safe save of the current switch configuration and should be used before powering down the switch to reduce the possibility of corrupting the configuration image. Once the shutdown command is issued, the user is informed that they have between 1 and 10 minutes to unplug or turn-off the switch. During this time any configuration changes cannot be saved. After the shutdown time has expired, if the switch is not turned-off, the switch will reset loading the saved configuration.

The shutdown command is also available from the Console Interface.

# Fixed Issues

The following issues have been fixed in this release:

## From Release 3.5

- The Root port was not 0/0 on the root switch if a multilink trunk (MLT) or the DMLT of two or three members was configured. (Q00941950)
- The count of the Root Bridge Changes does not update correctly when the root port is changed. (Q00937743)
- A port that is set to P2P auto (Half Duplex) should be a shared port. (Q00893650)
- All Link Aggregation Group (LAG) ports were aggregated, including ports configured in different VLANs. (Q00911104)
- In Device Manager, if the Spanning Tree Protocol (STP) Participation for all ports was disabled, some the ports remained in the Normal Learn mode. (Q00881024)
- The Region Configuration Change Counter was incorrectly incremented. (Q00909771)
- The wrong Multiple Spanning Tree Protocol (MSTP) or RSTP root port was displayed for a temporary base-incomplete Distributed Multilink Trunk (DMLT). (Q00934509)
- STP remains in Blocking mode after a redundant LAG is removed. (Q00901805)
- In a Device Manager session, ports cannot be assigned to Unrestricted Role Combinations. (Q00935015)
- In MSTP and RSTP, BPDUs from a mirrored port are not displayed on the monitor port. (Q00920115)
- IGMP cannot not enable both snooping and proxy in one step. (Q00925027)
- In CLI, zero is a valid user-defined PID for a used-defined protocol-based VLAN. (Q00924944)
- In CLI, a message needs to be displayed when you are adding the same port in two protocol-based VLANs. (Q00924937)
- In Device Manager, ports cannot be assigned to unrestricted role combinations. (Q00935015)
- The No Reset option is not available on the Ethernet Switch 460 or any stack that includes an Ethernet Switch 460.

- When you create a VLAN for a stack and add all the ports in the stack as IGMP Router ports for a VLAN, not all of the ports are configured. (Q00942452)

## From Release 3.1

- Downloading the configuration file from the TFTP server failed with an "Intra-stack communication" error. Re-attempt the configuration file download should this occur. (Q00725148)
- When a tagged port was part of the multiple Spanning Tree Groups, that port had to be configured to tag all traffic using the tagAll option. (Q00728620)
- ASCII Configuration File download was not supported through a Secure Shell Session (SSH). (Q00840035)
- Downloading binary configuration files, ASCII configuration files, and software image files were not supported when a stack was in a temporary base-unit condition. (Q00840624)
- When managing the stack via a console cable connection, the download command with the no-reset option could only be executed from the base unit's console port. (Q00841927)
- After downloading an image file using the "download no-reset" option, you had to reset the switch of stack before executing subsequent downloads. (Q00841945)
- Assign an IP address to the switch or stack before enabling RADIUS authentication. If you attempted to enable RADIUS authentication using the CLI, you did not receive an error message even if the switch or stack was not configured with an IP address. (Q00752827)
- You may delete the IP address of the device using the CLI even if RADIUS authentication is enabled and you will not receive an error message. (Q00752828)
- The VLAN port configuration for MLT or DMLT ports could only be changed using the lowest numbered port in the MLT. (Q00761593)
- When using TFTP Transfers and a "file not found" error occurred, the following error message on the console screen was displayed:

  ```
  Error code 1: File not found
  ```

  Ignore this error message. (Q00726506)
- When using LAG, a maximum of one standby link is supported. (Q00783242)

- Changes to the `cmd-interface` command takes effect when the user next logs into the device. (Q00829147)
- The CLI command `default duplex` cannot be executed against a GBIC port. If you execute this command against a GBIC port, you may see the following error:

  % Cannot modify settings

  % inconsistentValue <port_number>

  (Q00779732)

# Known issues and considerations in 3.6 software

The following are known issues and considerations for this release:

## ADAC

- ADAC cannot apply Auto-Configuration settings for ports involved in Port Mirroring due to Port Mirroring restrictions (Monitor and Mirrored ports must have the same VLAN settings). In this case, when ADAC periodically tries to apply configuration on a candidate port, it logs an error message as long as the current configuration does not permit Auto-Configuration. (Q01131794)

## Auto Unit Replacement

- After a reboot, a stack requires between 5 and 10 minutes to mirror the CFG images from all units in the stack. When the process has completed successfully, the following log message is displayed: `All units mirrored for the first time.` This message indicates that you can safely begin replacing units. (Q01117484).

## Command Line Interface

- ACG execution fails at the CLI password `stack serial radius` command. (Q01043704)

  **Note:** User cannot configure passwords via ACG on the SSH image.
- ACG execution fails at the `eapol enable` command. (Q01043707)

  **Note:** User cannot configure passwords via ACG on the Non-SSH image if the password security feature is enabled.
- The SSH public key cannot be downloaded using the `\folder\key name` command. To use the windows notation for directories, the user should use the double backslash (\\) instead of a single backslash (\). (Q01031157)
- The option, “ipv6” is incorrect for the `show audit log telnet` command. Ignore this option. If the `show audit log telnet ipv6` command is used, it will return the same data as the `show audit log telnet` command. (Q01158092)

- When upgrading using "no reset" option from telnet CLI session, the user may intermitently find that the current session reverts to the menu interface and the user is not able to re-enter the CLI until the current software download has completed. Users can create a parallel Telnet connection during such an event while the software is being downloaded if access to the CLI is required. (Q01142756)

## EAPOL

- This is related to the Windows XP/2000 EAPOL client behavior already documented (Q01053497)
- EAP authentication clients connected through the HUB lose connectivity after an SSH image upgrade. (Q01109506)
- When multihost is enabled on a port, EAP authentication intermittently fails for some clients on initialization.

  **Note:** PCs running Windows XP or Windows 2000 using the built-in EAP client drop the first message so that the second message the client receives appears to be the first, which is at least 60 (quiet period configured on the switch) seconds after the link is up. Therefore, a user does not see a password window until at least 60 seconds after the link is up. (Q01106448)
- If clients are authenticated on a EAPOL multihost enabled port and user enables EAPOL multihost again on all ports (including the port already enabled ), PCs connected to that multihost port already enabled begin to lose their connectivity to the server for approximately 60 to 90 seconds. This does not happen if the user does not enable EAPOL multihost again on the enabled port. This is related to the Windows XP/2000 EAPOL client behavior described in Q01106448. (Q01053497)

## MAC Address Security Table

- One minute after the switch starts forwarding traffic, only one address is displayed in the MAC address table. (Q01051801)
- After removing the intruder address from the MAC Address Security Table, the address does not appear in the AuthViolation Table. It is displayed after removing or reinserting the link or after disabling and enabling port 1. (Q01061757)

- Sometimes when inter-connecting two Ethernet Switch 460 units, the user is unable to see the MAC address of the connected 460 in the MAC address table when using the CLI. The MAC address of the connected 460 can always be viewed correctly in the MAC address table when using the Console Interface, Web or JDM.

  **Note:**
  This has only been shown to occur on some occasions when two Ethernet Switch 460s are interconnected. If one of the switches is an Ethernet Switch 470, the issue is not present. (Q01157912)

## MSTP

- MSTP functions improperly between Ethernet Switch 3.5 and 3.6 software with MSTI and MLT enabled. Reboot the non-root switch or stack after you configure this setup. Then the MSTP is solved correctly and no broadcast storm occurs. (Q01121994)

## QoS

- When using User Based Policies with the MHMA, only the last authenticated user on a port is displayed when running a `show qos user-role` command in the CLI. If the user role changes at the RADIUS server, or if the user policies to be installed are modified at the COPS server, only elements corresponding to the last authenticated user will remain installed on a multihost-enabled interface. All previously installed user elements are deleted for that interface.

## VLACP

- VLACP MLT failure detection.

  **Note:** To detect a link failure over MLT, you need to use different types of ethertypes on each link that forms the MLT. More information about this setup can be found in *Configuring VLANs, Spanning Tree, and Multilink Trunking* (217460-A). (Q01119890)

## STP

- In the Console Interface VLAN Configuration screen, the STPG field is selectable only until the VLAN is activated. The actual setting is done when the VLAN is activated with the STP group selected until that moment. After the activation, the field displays only the current VLAN-STP group setting. This field was meant just for the time of creation to prevent possible flooding until assigning a VLAN with ports to a group. For other purposes, refer to the Spanning Tree menus.
- With release 3.6, a STP topology change can occur when LACP ports change status. This is due to the way the platform now provides support for multiple Spanning Tree Groups across MLT or LAGs (Q01157915, Q01157918).

  **Note:** Nortel Multiple Spanning Tree Groups over MLT enables the switch to assign an MLT link into multiple STGs. This means that MLT now acts as a "virtual" port having its own spanning tree settings. Individual port Spanning Tree settings do not have significance when a port is now a member of a MLT or LAG. Spanning Tree settings must be assigned as part of the MLT or LAG. There is a new command that controls Spanning Tree settings per MLT or LAG. Spanning tree will be enabled (normally) by default on new MLT or LAG connections, if the switch is connected to a Nortel switch running Split-MLT, then Spanning Tree must be disabled on the MLT.

## Web and Device Manager

- The `Download without reset` option is present in the Console Interface (CI) and CLI but not in the web/Java Device Manager (JDM) interface. (Q00999444)
- An error message - `Submit failed` - appears on the web interface when creating a Protocol Based-Vlan. The message can be ignored as the VLAN is actually successfully created. (Q01148341)
- When using JDM to enable LACP on ports with different VLANs configured, LACP will not be enabled and no error message is generated. This problem is specifically related to JDM operation. (Q01160069)

## Miscellaneous

- The Authentication Protocol SHA and Privacy Protocol DES are available only for the SSH builds. When loading a non-SSH build those settings disappear. (Q00987006)

- COPS control can be enabled even though the COPS server IP address is not configured. (Q01028193)
- The SSL server is still operation even though the SSL certificate is erased. (Q00981869)
- The cut connection is lost on fiber when downgrading from 3.5.1 to 3.5.0. (Q01095254)
- The RSTP PathCost for the MLT is incorrect after changing the PathCost type to 16 bits. When changing the PathCost type for MLT from 32 to 16 bits, the path cost is defaulted and computed based on the path cost formula. When changing the PathCost type back from 16 to 32 bits, the path cost values are kept. (Q01118153)
- The Dynamic LAG trunk is still enabled even after all links are removed. (Q01066346)
- Dynamic LAGs are not properly updated when the link is removed or reinserted. (Q01059029)
- A new Dynamic LAG is not formed after removing a previous dynamic LAG. (Q01055083)

  **Note:** For the abovementioned three CRs (Q01066346, Q01059029, and Q01055083), the links are not deaggregated at the aggregated link link-down to permit faster recovery of the trunk when the same links are reinserted.
- STP information is not discarded when the Hop Count is equal to zero. (Q01053800)
- On Nortel Ethernet Switch 460/470 products, the port may report “FCS Errors” and “Frame Errors” for the respective port when connected to an IP handset or AP that is unpowered. Also, the Link and Activity LEDs of that port may blink. These errors are reported as a result of filters inbuilt to the IP handsets/AP that reflect the link pulses when the device is unpowered. (Q01129884)
- No warning is given when upgrading a hybrid stack to Ethernet Switch Software version 3.6. After upgrading, the hybrid stack boots up as stand-alone units with no IP address. Reverting back to the previous code will resolve this issue. (Q01122876)
- The software image cannot be downloaded on the stack after the base unit is powered OFF and then ON. Download is possible only after resetting the stack. (Q01033410)
- The switch delays answering to ping.

**Note:** This is an aging issue. When a unit leaves the stack, the addresses learned on the port from that unit are not forced to age immediately. They age when the age interval expires for those addresses. Frequent FDB updates can gradually resolve this issue, but this needs to be determined on a per-network basis with the help of the Network Administrator. (Q01141876)

- When using the Console Interface in the MLT Configuration screen, the learning field is for SETs only as long as you selected ALL for the STP group. This does not reflect the learning state on any of the STP group that included that MLT because you can have different settings in each STPG. To get the exact learning, you must select an STP group. This behavior is consistent with the other screens in the Console Interface(for example, EAPOL configuration).

# Outstanding issues from Release 3.5 software

- When you create a distributed multilink trunk on a stack that is non-root and connect the ports to a standalone switch (root) with no multilink trunk configured, one port should remain in forwarding and the others should change to blocking, but they all remain in blocking and a loop is formed. (Q00942499)
- In port mirroring, BR, MC, UUN traffic are NOT mirrored for XrxYtx and XrxYtxOrXtxYrx (port Y-Harrier). (Q00891851)
- On a non-root switch, the backup multilink trunk becomes the root when you disable it from the root switch. (Q00910371)
- On an Ethernet Switch 470 switch, a port remains bound to an existing PVID even when the port is removed from the VLAN. (Q00929246)
- An IGMP stream is not flooded on all ports when you remove the last member from the group. (Q00929510)
- In the command line interface (CLI) the no MLT command does not default to the default MLT name. (Q00930403)
- The ASCII configuration generator (ACG) generates commands that set the STP learning status for tagged ports that are not in STPGx. (Q00935346)
- The timing for IGMP query packets is not correct.(Q00932337)
- Upgrading the image from 3.0 to 3.5 does not work on an allied stack. (Q00927638)
- ACG creates commands that disable a Spanning Tree Protocol Group that has already been disabled. (Q00927433)
- In RSTP, up and down counts are not incremented after several changes of Spanning Tree Protocol operation modes. (Q00925158)
- The “rcStatMltIfExtnIfHCInUcastPkts” is incremented for multicast or broadcast traffic. (Q00884953)
- In RSTP and MSTP modes, a MLT group with a smaller group ID has higher priority than the MLT group with a larger group ID. For example if MLT 1 and MLT 2 have the same path cost and they are connected to the same two switches, MLT 1 will always be Forwarding and MLT 2 will be Alternate. (Q00895970)
- The Query port, ActiveQuerier, and MRouterExpiration fields do not reset to the default value. (Q00925047)
- In CLI, a message needs to be displayed when you are creating a new protocol-based VLAN, but the protocol table is full. (Q00924933)

- In Device Manager, an error message is displayed when you try to create an Allied-VLAN SVL type. (Q00923814)
- You can add up to 200 IP filters to one group on a stand-alone unit or a 5-unit stack. (Q00888337)
- The operational display of EAPoL is inconsistant on the Release 3.5 software. (Q00912196)
- You can create up to 192 Level 2 filters on a stand-alone unit or a 5-unit stack. (Q00888333)
- You can create only 62 shapers on a switch. (Q00888339)
- You can create a maximum of 200 IP filters in one group for every Ethernet switch. (CR Q00888337)
- You can create 118 actions on an Ethernet switch. (Q00888347)
- Intruder SA can access the switch through the base unit when when MAC security is enabled globally or by port. (Q00905572).
- When there is a high rate of traffic on a base unit switch while MultiLink Trunking is configuring, traffic from the other units is lost (CR Q00922934).
- The Spanning Tree menu is missing in Web-based management when the Spanning Tree Protocol is in RSTP or MSTP mode. (Q00885550).
- ACG generates commands that set the learning status for tagged ports that are not in the Spanning Tree Protocol Group (Q00935346)

# Outstanding issues from Release 3.1 software

- You cannot execute the lacp clear-stats against all ports in a stack simultaneously. You can execute the command against all the ports in a switch simultaneously, and then against each switch in a stack. (Q00844967)
- When you create an MLT group using the Menu Interface, you must identify a unit number/port number combination in the first field in order for the port configuration to be accepted by the Menu Interface, as shown. For example:

```
Trunk Trunk Members STP Learning Trunk Mode Trunk Status
----- ------------------------------ ------------ ---------------
------------
1 [ /1 ][ / 2][ /3 ][ / ] [ Normal ] Basic [ Disabled ]
2 [ 2/6 ][ 2/7 ][ / ][ / ] [ Normal ] Basic [ Disabled ]
3 [ 3/10 ][ 4/11][ 4/12][ 5/13] [ Normal ] Basic [ Disabled ]
4 [ / ][ / ][ / ][ / ] [ Normal ] Basic [ Disabled ]
5 [ / ][ / ][ / ][ / ] [ Normal ] Basic [ Disabled ]
6 [ / ][ / ][ / ][ / ] [ Normal ] Basic [ Disabled ]
```

- You may see the MAC address table refresh by itself every few seconds after another unit in the stack has been reset. This condition may persist for one or two minutes. (Q00761481)
- If the Spanning Tree Protocol (STP) is enabled on a Link Aggregation Group (LAG), then the LAG is subject to STP convergence, just like any other port. If Spanning Tree does reconverge, you should expect there to be a loss of data on the LAG link. (Q00769684, Q00804961)
- The ports on the BPS2000 2GT MDA cannot be the target of the interface `flowcontrol` command. Changing the flow control of the ports on the BPS2000 2GT will result in autonegotiation being disabled on the port, which is an unsupported configuration. (Q00787182)
- LAG/IGMP stream does not failover immediately when standby is present. (Q00804064)
- You must enable IGMP proxy when using IGMP in conjunction with LAG or MLT. (Q00805627)
- The CLI command "`show running-config`" will display the configuration parameters that are appropriate for the user that is logged into the device. A subset of the configuration parameters is displayed to the READ-ONLY (RO), while a more verbose set of parameters is available to the READ-WRITE (RW) user. (Q00827993)
- 460-Changing from 10MB to 100 MB may result in port remaining in a down condition. (Q00630821)

- MLT/LAG console menu screen may display more port members when moving cables. Refresh the screen if this occurs. (Q00770784)

# Related publications

For more information about using these products, refer to the following publications:

- *System Configuration Guide* (217105-A)
- *Configuring and Managing Security* (217104-A)
- *Configuring VLANs, Spanning Tree, and Multilink Trunking* (217460-A)
- *Configuring IP Multicast Routing Protocols* (217459-A)
- *Configuring Quality of Service and IP Filtering* (217106-A)
- *System Monitoring Guide* (217107-A)
- *Installing the Nortel Ethernet Switch 470* (217107-A)
- *Installing the Nortel Ethernet Switch 460-24T PWR* (213318-C)

You can print selected technical manuals and release notes free of charge, directly from the Internet. Go to the www.nortel.com 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 the Adobe Systems website at www.adobe.com to download a free copy of the Adobe Acrobat Reader.

# How to get help

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

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortel.com/support URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www.nortel.com/erc URL.