

Nortel Ethernet Switch 460/470

Release Notes — Software Release 3.7

NN47210-400 (217103-D)

Document status: Standard
Document version: 01.02
Document date: 12 March 2007

Copyright © 2005-2007, Nortel Networks
All Rights Reserved.

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.

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

Trademarks

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.
All other products or services may be trademarks, registered trademarks, service marks, or registered service marks of their respective owners.
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 reserves the right to make changes to the products described in this document without notice.

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

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

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

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

Nortel Networks 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

1. 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).
2. 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.
3. 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.
4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
6. 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 7
Hardware requirements 8
Release 3.7 software images 8
Secure software image 9
PoE firmware 9
Upgrade instructions 10
Important notes for upgrades 10
New features 11
Username and password enhancement 12
Smart Auto-negotiation for 470-PWR GBICs 12
New Unit Quick Configuration 12
Stack enhancements 13
VLAN Configuration Control 13
Spanning Tree Protocol (STP) scaled down to eight instances 14
STG port membership mode 14
802.1t STG path cost calculation 15
MSTP manual enable 15
Removal of MLT restrictions 15
ADAC extended default MAC Address Range 15
ADAC configurable MAC Address Range 16
Configurable PVID and tagging in ADAC Tagged-Frames mode 16
IEEE 802.1AB LLDP 16
Non-EAP (NEAP) hosts on EAP-enabled ports 17
Multi Host Single Authentication on EAP ports 17
802.1x Machine Authentication and PEAP support in Windows 17
Password Security enhancement 17
Configurable SNMP trap port 18
SNTP Daylight savings time enhancement 18
CPU/Memory usage 18
Save and autosave configuration enhancement 19
Save options available in JDM and Web-based management 19
Ping enhancement 19
Shutdown enhancement 19

Copyright © 2005-2007, Nortel Networks
Nortel Networks Confidential

Logout CLI enhancement 19
write memory and save config commands 20
reload command 20
restore factory-default command 20
Fixed Issues 21
Known issues and considerations in 3.7 software 21
Loss of STG configuration information during upgrade 21
Read-only access to system log 22
No error when deleting non-existent entries from NEAP MAC list 22
CLI Telnet session remains open on logout 22
No configuration allowed during software download 22
Remote syslog messages not displayed in sequence 22
JDM must be re-opened after Base Unit reset 22
ACG file must match switch STP mode 22
Disabling LACP 23
Shutdown of MLT ports cannot be saved to ACG 23
POE: Shared ports 47/48 are delivering power when fiber ports are connected. 23
spanning-tree op-mode command: command mode inconsistency 23
LLDP: re-inserted unit in a stack does not send TLVs 23
Autotopology messages from BayStack 450 23
Outstanding issues and considerations from previous software releases 24
ADAC 24
Auto Unit Replacement 24
CLI Audit feature 24
Command Line Interface 24
Disabled port status 25
EAPOL 25
LACP 26
MAC Address Security Table 27
MSTP 27
QoS 27
STP 27
STP and port mirroring on redundant link 28
Web and Device Manager 28
Miscellaneous 28
Related publications 32
How to get help 32
Getting help from the Nortel web site 32
Getting help over the phone from a Nortel Solutions Center 33
Getting help from a specialist using an Express Routing Code 33
Getting help through a Nortel distributor or reseller 33

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

Introduction

These Release Notes support the Release 3.7 software for the Nortel Ethernet Switches 460-24T-PWR, 470-24T, 470-48T, 470-24T-PWR, and 470-48T-PWR. They cover the supported hardware, new features, fixed issues, known issues and considerations in 3.7 software, and the outstanding issues from previous software releases.

The following topics are discussed in this document:

Topic
"Hardware requirements" (page 8)
"Release 3.7 software images" (page 8)
"Upgrade instructions" (page 10)
"New features" (page 11)
"Fixed Issues" (page 21)
"Known issues and considerations in 3.7 software" (page 21)
"Outstanding issues and considerations from previous software releases" (page 24)
"Related publications" (page 32)
"How to get help" (page 32)

Note: Release 3.7 software does not support the Hybrid stack mode. Neither the Ethernet Switch 450 nor the BPS2000 are supported in the stack any longer. All stacks must contain only the following:

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

Copyright © 2005-2007, Nortel Networks
Nortel Networks Confidential

The stacks can consist of a mix of Ethernet Switch 460-24T-PWR, Ethernet Switch 470-24T/24T-PWR, and Ethernet Switch 470-48T/48T-PWR units. You must stack the same types of switches sequentially, and in the following order:

- All Ethernet Switch 470-48T/48T-PWR units
- All Ethernet Switch 470-24T/24T-PWR 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/48T-PWR is in the stack, it must be the base unit.

Hardware requirements

Release 3.7 software supports the following Ethernet Switches:

Hardware Platform	Part Number
Ethernet Switch 460-24T PWR	AL2001?20
Ethernet Switch 470-24T	AL2012?37
Ethernet Switch 470-48T	AL2012?34
Ethernet Switch 470-24T-PWR	AL2012?52
Ethernet Switch 470-48T-PWR	AL2012?53

Note: In the list of part numbers, the question mark (?) represents a variable letter that indicates the type of power cord shipped with the hardware. The possible values for this variable are as follows:

- A — No power cord
- B — European Schuko power cord
- C — UK and Ireland power cord
- D — Japan power cord
- E — North American power cord
- F — Australia/New Zealand/PRC power cord

Release 3.7 software images

The components for the Ethernet Switch 460 and 470 release 3.7 include:

- Standard Runtime Image Software Version 3.7.0.04 (470_3704.img)
- Secure Runtime Image Software Version 3.7.0.05s (470_3705s.img)
- Boot/Diagnostic Software Version 3.6.0.7 (470_3607_diag.bin)

Copyright © 2005-2007, Nortel Networks
Nortel Networks Confidential

- Java Device Manager software version 6.0.5.0 (jdm_6050.exe /jdm_6050_solaris_sparc.sh / jdm_6050_linux.sh / jdm_6050_hpux_pa-risc.sh)
- Release 3.7 Management Information Base (MIB) definition files (Ethernet_Switch_4xx_MIBs_v3.7.0.zip)

Secure software image

The Ethernet Switch Software can be installed using a secure software image that provides the following features:

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

Note: These features are not available on non-secure software images.

PoE firmware

The Ethernet Switch 460-PWR and Ethernet Switch 470-PWR each support a specific PoE firmware image. The appropriate firmware is pre-loaded on the devices prior to shipping.

470-PWR PoE firmware

With this release, the existing 470-PWR PoE firmware remains unchanged. If the PoE firmware for the 470-PWR becomes corrupted, you can obtain the firmware from the Nortel web site. To download the 470-PWR PoE firmware image from a TFTP server to your switch, use the following command:

```
download [address <ip>] poe_module_image 470-pwr [<filename>]
```

The device reboots after the download.

The 470-PWR PoE firmware does *not* apply to the 460-PWR devices. Do not attempt to download the 470-PWR PoE firmware to a 460-PWR device.

460-PWR PoE firmware

With this release, the existing 460-PWR PoE firmware remains unchanged. However, if it becomes corrupted, you can obtain this firmware from the Nortel web site. To download the 460-PWR PoE firmware image from a TFTP server to your switch, use the following command:

```
download [address <ip>] poe_module_image 460-pwr [<filename>]
```

The device reboots after the download.

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

Upgrade instructions

When upgrading the Ethernet Switch 460-24T-PWR, Ethernet Switch 470-24T/24T-PWR, or Ethernet Switch 470-48T/48T-PWR to release 3.7, follow this procedure:

Note: Release 3.7 only supports eight STP groups or MSTI instances. Before upgrading the software image, ensure that all switch ports are members of STP groups or MSTI instances 1 through 8 only. You must ensure that the ports do not belong to non-supported groups or instances (9-16) to avoid configuration losses and to prevent issues such as broadcast storms. The latter can occur because any ports that are members of the non-supported STGs/MSTIs before the upgrade will have no STP membership after the upgrade.

Step	Action
1	Backup the binary configuration file to a TFTP server.
2	Upgrade the software image to 3.7.0.04 or 3.7.0.05s. (If you do not specify the Download Without Reset option, the system reboots after this step.)
3	Upgrade the boot/diagnostic code to version 3.6.0.7.

—End—

Important notes for upgrades

If you are upgrading to release 3.7 from software versions older than 3.6.4, a series of upgrades are required to prevent configuration corruption under some circumstances. You must perform the switch upgrades according to the following path:

2.5 -> 3.0 -> 3.1.9 (or 3.2.x) -> 3.5.4 -> 3.6.4 -> 3.7.

The specific number of upgrades required depends on the currently loaded code version.

For instance, if the current version is 3.1.9, you must first upgrade to 3.5.4, and then to 3.6.4, and finally to 3.7. Or, if you are upgrading from a release prior to 2.5, you must first upgrade to 2.5, and then to each subsequent release in the order listed (3.0, 3.1.9 [or 3.2.x], 3.5.4, 3.6.4, and finally 3.7).

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

Nortel recommends that you download the agent code before upgrading to the new diagnostic code. If this procedure is not followed the GBIC ports may not always function properly. Nortel also recommends that you save a copy of your configuration file to a TFTP server before you begin the upgrade process.

New features

The following new features are available in this release:

- "Username and password enhancement" (page 12)
- "Smart Auto-negotiation for 470-PWR GBICs" (page 12)
- "New Unit Quick Configuration" (page 12)
- "Stack enhancements" (page 13)
- "VLAN Configuration Control" (page 13)
- "Spanning Tree Protocol (STP) scaled down to eight instances" (page 14)
- "STPG port membership mode" (page 14)
- "802.1t STPG path cost calculation" (page 15)
- "MSTP manual enable" (page 15)
- "Removal of MLT restrictions" (page 15)
- "ADAC extended default MAC Address Range" (page 15)
- "ADAC configurable MAC Address Range" (page 16)
- "Configurable PVID and tagging in ADAC Tagged-Frames mode" (page 16)
- "IEEE 802.1ab LLDP" (page 16)
- "Non-EAP hosts on EAP-enabled ports" (page 17)
- "Muti Host Single Authentication on EAP ports" (page 17)
- "802.1x Machine Authentication and PEAP support in Windows" (page 17)
- "Password Security enhancement" (page 17)
- "Configurable SNMP trap port" (page 18)
- "SNTP Daylight savings time enhancement" (page 18)
- "CPU/Memory usage" (page 18)
- "Autosave configuration enhancement" (page 19)
- "Save options available in JDM and Web-based management" (page 19)
- "Ping enhancement" (page 19)

Copyright © 2005-2007, Nortel Networks
Nortel Networks Confidential

- "Shutdown enhancement" (page 19)
- "Logout CLI enhancement" (page 19)
- "write memory and save config commands" (page 20)
- "reload command" (page 20)
- "restore factory-default command" (page 20)

Username and password enhancement

With Release 3.7 software, you can use the CLI to set usernames as well as passwords for system access through the Console Interface, CLI, Telnet, and Web-based management. The syntax for the new **username** command is:

```
username <username> <password> {ro|rw}
```

If you set a password using the **cli password** command, the Console/Comm Port Configuration screen, or the Password Setting Web-based management page, the next time you log in to the switch, you are prompted to enter a valid username. Therefore, ensure you are aware of the valid usernames (default RW and RO) before you change passwords.

For more information, see *Nortel Ethernet Switch 460/470 Security — Configuration (NN47210-500)*.

Smart Auto-negotiation for 470-PWR GBICs

Smart mode is an intelligent mode in which GBIC ports on the 470-PWR can detect if the other end of the link can support Gigabit auto-negotiation. If the far end can support auto-negotiation, the port will enable Gigabit auto-negotiation functionality.

If the far end cannot support auto-negotiation, the port will disable Gigabit auto-negotiation functionality.

For more information, refer to the *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

New Unit Quick Configuration

This feature provides the capability to automatically apply default parameters to a switch when it is added to a stack or when a switch is added to a standalone switch to create a stack.

These default parameters include:

- VLAN ID
- Port Speed
- Duplex Settings

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

- PVID
- Spanning Tree Groups

These parameters will be automatically applied to all ports on the new switch when the switch is added to the stack or used to create a stack.

For more information on New Unit Quick Configuration, refer to the *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

Stack enhancements

With Release 3.7 software, if the Base Unit leaves the stack, the Temporary Base Unit is now chosen more rapidly (maximum of 2-3 seconds).

For more information on stacking, refer to the *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

VLAN Configuration Control

VLAN Configuration Control (VCC) is a new feature in Software Release 3.7 that allows a switch administrator to control how the PVIDs of VLAN port members are modified. VLAN Configuration Control is a superset of the existing AutoPVID functionality and incorporates this functionality for backwards compatibility. VLAN Configuration Control is globally applied to all VLANs on the switch.

VLAN Configuration Control offers four options for controlling PVID modification:

- **Strict** — With the Strict option, an untagged port can only belong to one VLAN. This option restricts you from adding an untagged port to a VLAN if the port is already a member of another VLAN. To add an untagged port to a new VLAN, you must first remove the port from all other VLANs of which it is a member. The PVID of the port is changed to the VID of the new VLAN to which it is added.

  Note: The default VLAN Configuration Control setting is Strict.

- **Automatic** — This option is similar to the Strict option in that an untagged port can only belong to one VLAN. However, when you add an untagged port to a new VLAN, it is automatically removed from any previous VLAN membership. The PVID of the port is automatically changed to the VID of the VLAN it joins. Since the port is first added to the new VLAN and then removed from any previous membership, the Spanning Tree Group participation of the port will not be disabled as long as the VLANs involved are in the same Spanning Tree Group.
- **AutoPVID** — This option functions in the same manner as previous AutoPVID functionality. When an untagged port is added to a new

Copyright © 2005-2007, Nortel Networks
Nortel Networks Confidential

VLAN, the port is added to the new VLAN and the PVID is changed to the VID of the new VLAN. The port is not removed from any previous VLAN memberships. Using this option, an untagged port can have membership in multiple VLANs.

- **Flexible** — This option functions in the same manner as disabling AutoPVID functionality. When this option is used, PVID and tagging are completely independent of each other, and there are no restrictions on the number of VLANs to which an untagged port can belong. Any new additions of an untagged port to a new VLAN does not change the PVID of that port.

  Note: When upgrading to release 3.7, the initial value for the VLAN Configuration Control depends on the AutoPVID value. If AutoPVID is disabled, then VLAN Configuration Control is set to Flexible and if AutoPVID is enabled, then the VLAN Configuration Control is set to AutoPVID.

For more information on VLAN Configuration Control, refer to *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*.

Spanning Tree Protocol (STP) scaled down to eight instances

The Nortel Spanning Tree Protocol (STPG) and Multiple Spanning Tree Protocol (MSTP) now support eight STP instances, down from 16. For more information on Spanning Tree Protocol, refer to *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*.

STG port membership mode

In release 3.7 software and later, IEEE 802.1D STGs support two different port membership modes: normal and auto.

In the normal mode, when a port is assigned to VLAN X and VLAN X is in STG Y, the port does not automatically become a member of STG Y.

In the auto mode, when a port is assigned to VLAN X and VLAN X is in STG Y, the port automatically becomes a member of STG Y.

For more information on Spanning Tree Protocol, refer to *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*.

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

802.1t STG path cost calculation

In release 3.7 software and later, you can set the switch to calculate the STG path cost using either the IEEE 802.1d standard (16-bit path cost) or the IEEE 802.1t standard (32-bit path cost). The 802.1t standard is a maintenance extension to the 802.1d standard.

For more information on Spanning Tree Protocol, refer to *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*.

MSTP manual enable

In previous releases, when a VLAN was added to a new MSTI, the MSTI was automatically enabled. With Release 3.7 software, you must enable the MSTI instance manually, as follows:

- Create the MSTI.
- Add the existing VLAN and port memberships.
- Enable the MSTI.

For more information on MSTP, see *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*.

Removal of MLT restrictions

With release 3.7 software and later, if you set any trunk member to Disabled (not active), the trunk member is no longer removed from the trunk. The trunk member remains a disabled member of the trunk, and so no longer has to be reconfigured to rejoin the trunk.

A trunk member can now be disabled even if only two members exist on the trunk.

You can also disable the lowest numbered port in a trunk. However, Nortel does not recommend disabling the lowest numbered port if Spanning Tree is enabled on the trunk.

For more information on MLT, refer to *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*.

ADAC extended default MAC Address Range

The following table lists the IP Phone MAC address ranges that have been added to the existing default ADAC MAC address list.

Note: After updating to Release 3.7 software, to add these new values to the list , you must set the ADAC MAC address ranges to their default

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

values (in CLI, **`default adac mac-range-table`**). Otherwise, the existing range from Release 3.6 software is loaded from NVRAM.

Table 1
Additional IP Phone MAC address ranges for ADAC in 3.7

From (low end)	→	To (high end)
00-13-65-FE-F3-2C	→	00-13-65-FF-ED-2B
00-15-9B-FE-A4-66	→	00-15-9B-FF-24-B5
00-16-CA-00-00-00	→	00-16-CA-01-FF-FF
00-16-CA-F2-74-20	→	00-16-CA-F4-BE-0F
00-17-65-F6-94-C0	→	00-17-65-F7-38-CF
00-17-65-FD-00-00	→	00-17-65-FF-FF-FF
00-18-B0-33-90-00	→	00-18-B0-35-DF-FF
00-19-69-83-25-40	→	00-19-69-85-5F-FF

For more information on ADAC, refer to *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*.

ADAC configurable MAC Address Range

With Release 3.7 software, you can modify and add to the default MAC address ranges using the CLI, JDM, or Web-based management.

For more information on ADAC, refer to *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*.

Configurable PVID and tagging in ADAC Tagged-Frames mode

With Release 3.7 software, the ADAC Tagged-Frames mode now offers the option of configuring the PVID and tagging for individual ports.

For more information, refer to *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*.

IEEE 802.1AB LLDP

Link Layer Discovery Protocol (LLDP) allows stations connected to a LAN to advertise their capabilities to each other, enabling the discovery of physical topology information for network management. LLDP-compatible stations can consist of any interconnection devices including PCs, IP Phones, switches, and routers. Each LLDP station stores LLDP information in a standard Management Information Base (MIB), making it possible for the information to be accessed by a network management system (NMS) or

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

application. LLDP can be used to discover duplex mismatches between an IP Phone and the switch, help identify Nortel IP Phones, and assign specific QoS parameters.

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)* .

Non-EAP (NEAP) hosts on EAP-enabled ports

For an EAPOL-enabled port configured for non-EAPOL (NEAP) host support, a finite number of non-EAPOL users or devices with unique MAC addresses are allowed access to the port.

Support for non-EAPOL hosts on EAPOL-enabled ports can be enabled in Release 3.7 software. This support is primarily intended to accommodate printers and other dumb devices that are accessing an 802.1X/EAPOL-enabled network.

NEAP can also operate with the RADIUS Assigned VLAN feature. With the RADIUS Assigned VLAN feature enabled, the first EAP-authenticated client on a port can obtain a preferred VLAN ID from the RADIUS server. The port is then added to the specified VLAN.

For more information, see *Nortel Ethernet Switch 460/470 Security — Configuration (NN47210-500)*.

Multi Host Single Authentication on EAP ports

MHSA provides network access for non-authenticated devices that are connected to an EAPOL-enabled port if another device has already been authenticated on that port.

For more information, see *Nortel Ethernet Switch 460/470 Security — Configuration (NN47210-500)*.

802.1x Machine Authentication and PEAP support in Windows

Nortel Ethernet Switch 460/470 Security — Configuration (NN47210-500) now provides an Appendix describing support for 802.1x and PEAP in Windows environments.

Password Security enhancement

When the Password Security feature is enabled, it now applies additional password restrictions. The password must contain a minimum of the following

- 2 lower-case letters
- 2 capital letters
- 2 numbers

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

- 2 special symbols, such as:!@#$%^&*()

The password is case sensitive.

Note: Password Security is enabled by default in the secure software image, and disabled by default on the non-secure software image.

For more information on the Password Security feature, refer to *Nortel Ethernet Switch 460/470 Security — Configuration (NN47210-500)*.

Configurable SNMP trap port

Release 3.7 software allows you to configure the SNMP trap port. The default SNMP trap port used for communicating with the trap receiver is port 162. You can now configure a different SNMP trap port.

For more information, see *Nortel Ethernet Switch 460/470 Security — Configuration (NN47210-500)*.

SNTP Daylight savings time enhancement

SNTP uses Universal Coordinated Time (UTC) for all time synchronizations so it is not affected by different time zones. With Release 3.7 software, you can set the switch to report the correct time for your local time zone and for daylight savings time.

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

CPU/Memory usage

You can now obtain statistics on CPU/Memory usage from the following interfaces:

- In the CLI: **`show cpu-utilization`**
- In JDM: **Edit > Chassis > CPU/Mem Utilization**
- In Web-based management: **Administration > CPU/Memory Utilization**

Note: The CPU utilization function provides a guide as to the CPU utilization in a switch or stack. Unlike software-based routers, this value is not an indication of how busy the switch is at forwarding packets. The CPU on the Ethernet Switch 460/470 is not typically involved in the packet forwarding process as all such intelligence occurs in the switching hardware. Most times, you will see the CPU reported at 50% utilization due to the sampling method utilized. This should not be viewed as a problem but considered as normal operation. However, if the CPU utilization stays consistently high at or near 100% for a prolonged period,

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

then this may indicate some issues within the customer network which need investigation.

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

Save and autosave configuration enhancement

Release 3.7 software extends the ability to set autosave enable/disable using the Console Interface (**Configuration File > Autosave Configuration**), Web-based management (**Configuration > Configuration File**), and JDM (**Edit > File System > Save Configuration**).

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

Save options available in JDM and Web-based management

The ability to save the configuration to NVRAM is now available in JDM (**Edit > File System > Save Configuration**) and in Web-Based management (**Configuration > Configuration File**).

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

Ping enhancement

Release 3.7 software extends the ping capabilities of the device. Using the **`ping`** CLI command, you can now specify additional ping parameters, including the number of ICMP packets to be sent, the packet size, the interval between packets, and the timeout. You can also set ping to continuous or set a debug flag to obtain extra debug information.

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

Shutdown enhancement

The **`shutdown`** command allows you to safely shut down and power off the switch. Once the shutdown command is initiated, the switch saves the current configuration and instructs users to power off the switch within the specified time period (1 to 60 minutes); otherwise, the switch performs a reset.

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

Logout CLI enhancement

The **`logout`** command logs you out of the CLI session and discontinues the connection with the host.

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

write memory and save config commands

Release 3.7 software provides two additional CLI commands to save the switch configuration to NVRAM. The **`write memory`** and **`save config`** commands function identically to the **`copy config nvram`** command.

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

reload command

The **`reload`** CLI command provides you with a configuration rollback mechanism to prevent loss of connectivity to a switch, typically for remote configurations. The **`reload`** command allows you to temporarily disable the autosave feature for a specified time period (1 to 60 minutes). Once the reload timer expires, the switch reloads the last saved configuration.

This allows you to make a number of configuration changes on the remote switch without affecting the current saved configuration.

As a result, if you lose connectivity while remotely configuring the switch, the last saved configuration is reloaded at the end of the configured time period, and you regain the switch connectivity.

During the interval in which the autosave feature is disabled by the **`reload`** command, you must use the **`copy config nvram`**, **`write mem`**, or **`save config`** command to force a manual save of your configurations.

To abort the switch reload before the timer expires, you must enter the **`reload cancel`** command.

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

restore factory-default command

The **`restore factory-default`** CLI command resets the switch or stack back to its default configuration.

For more information, see *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

Fixed Issues

The following issues have been fixed in this release:

- In Web-based management, users can now enable a second LAG even if port settings such as tagging and port priority do not match the first LAG settings. (Q01255257)
- If you attempt to configure a stack through the non-base unit within five minutes of a reset of the non-base unit or the base unit, the CLI session no longer freezes. This issue occurred only on serial connections to non-base units and only with CLI commands that used SNMP queries (get/set).

  If you configured the stack using the base unit at all times (as recommended by Nortel), this issue did not occur. (Q01266026)

- When upgrading using a Telnet CLI session, the current session no longer reverts to the menu interface. (Q01142756 and Q01244616)
- The Download without reset option is now present in the Web and Java Device Manager (JDM) interfaces. (Q00999444)
- An error message `- Submit failed -` no longer appears on the Web interface when creating a Protocol Based-Vlan. (Q01148341)
- LAG/IGMP stream now properly fails over immediately when the standby is present. (Q00804064)
- You are no longer required to enable IGMP proxy when using IGMP in conjunction with LAG or MLT. (Q00805627)

Known issues and considerations in 3.7 software

Loss of STG configuration information during upgrade

Release 3.7 only supports eight STP groups or MSTI instances. When upgrading to release 3.7 software, if you have STG or MSTI configurations for groups 9 to 16, these configurations are lost during the upgrade process. After the upgrade, any VLANs previously associated with these lost groups or instances are no longer mapped to any STG or MSTI.

Nortel recommends that, before you upgrade the software image, ensure that all switch ports are members of STP groups or MSTI instances 1 through 8 only. You must ensure that the ports do not belong to non-supported groups or instances (9-16) to avoid configuration losses and to prevent issues such as broadcast storms. (Q01496700)

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

Read-only access to system log

A read-only user can access the system log through the CLI but not through the Web or Console interfaces. Providing read-only access through the CLI is particularly useful for diagnostic access to the switch. (Q01367467 and Q01353119)

No error when deleting non-existent entries from NEAP MAC list

If you try to delete a non-existent MAC address from the NEAP MAC list for a port, no error is returned. Similarly, if you attempt to add a duplicate NEAP MAC address to the port NEAP MAC list, no error is returned. (Q01374994)

CLI Telnet session remains open on logout

After you log off a CLI Telnet session from Windows XP, the Telnet window remains open with the following message displayed:

`Connection to host lost` (Q01418499)

No configuration allowed during software download

While a software download is in progress, you cannot configure the switch from any interface, regardless of the download option specified (for example, Download without Reset). (Q01366688)

Remote syslog messages not displayed in sequence

When log messages are being stored on a remote syslog server, the log messages may not appear in the correct order.

If a log message transmission from the switch fails, the switch retries the transmission after one minute. As a result, the resent message may appear out of order on the remote syslog. Refer to the timestamp in the message description to confirm the correct order of the received messages. (Q01418527)

JDM must be re-opened after Base Unit reset

In JDM, after you reset the Base Unit in a stack, you will need to re-open JDM (**Device > Open** or **Device > Open Last**) to view the updated status of the Base Unit. (Q01453119)

ACG file must match switch STP mode

ASCII configuration files generated in one Spanning Tree mode are not compatible with another Spanning Tree mode. For example, you cannot use the **`copy running-config`** command to copy a saved MSTP configuration to a switch that is currently in STPG mode. Many commands return errors because of the different syntax. While the **`spanning-tree`** commands are not saved in the ACG file, other saved commands result in errors when the file is loaded on a switch running a different STP mode. For

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

example, the syntax for the **mlt learning** command in STPG mode is different from the syntax for the same command in RSTP or MSTP modes. (Q01490532)

Disabling LACP

When you want to disable LACP on a port, Nortel recommends that you both disable aggregation on the port (in CLI, **no lacp aggregation port <portlist>**) and disable LACP mode on the port (in CLI, **lacp mode port <portlist> off**). (Q01538054)

Shutdown of MLT ports cannot be saved to ACG

If you issue the **shutdown port** command on a port that is a member of an MLT, the shutdown state of the port is not saved to an ACG file. If you apply an ACG configuration file to the switch, all MLT ports are always enabled after the file is loaded. (Q01368657)

POE: Shared ports 47/48 are delivering power when fiber ports are connected.

On Ethernet Switch 470-48T-PWR, when a GBIC is inserted, the associated shared copper port (47 or 48) can continue supplying power over Ethernet even though no data is forwarded through the shared copper port. If you do not want the switch to supply PoE to these ports, you can manually disable PoE on the ports. (Q01501815)

spanning-tree op-mode command: command mode inconsistency

When in MSTP or RSTP mode, you can issue the **spanning-tree op-mode** command from the config and config-if command modes. However, in STPG mode, you can only issue the command from the config command mode. (Q01365742)

LLDP: re-inserted unit in a stack does not send TLVs

If you have a stack configured with LLDP, and you remove and re-insert one of the stack units, the ports on the re-inserted unit do not transmit LLDP TLVs. (Q01569043)

Autotopology messages from BayStack 450

A change in the operation of Nortel's SONMP based Autotopology causes directly-connected BayStack 450s to report a physical Autotopology change every 70 seconds to the local switch. This Autotopology change message should be ignored for links where there is a direct connection to a BayStack 450 switch. (Q01565432-01)

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

Outstanding issues and considerations from previous software releases

The following are outstanding issues and considerations from previous software releases:

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).

  In Release 3.7, you can determine if a particular unit is ready for replacement by issuing the following CLI command on that unit: **`show stack auto-unit-replacement`** .

CLI Audit feature

- After performing an upgrade to Release 3.6 software or higher, the following message can appear in the syslog:

  ```
  Audit data initialized (bad magic number)
  ```

  This is due to the introduction of the CLI Audit feature in Release 3.6 software. When the upgraded switch powers up for the first time, no data is collected in the CLI Audit log. The syslog identifies this situation with the message above.

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.

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

- 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)

Disabled port status

- If a port is disabled by VLACP, BPDU-Filtering, or EAPoL, the show interfaces command still indicates that the port is up. In this case, you can determine the true status of the port by using the show command for the appropriate application:
  - — show vlacp interface
  - — show spanning-tree bpdu-filtering
  - — show eapol

  (Q01246226)

EAPOL

- 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: Windows XP* or Windows 2000* PCs running the built-in EAP client drop the first received EAP message. Therefore, the second message that the client receives appears to be the first. The interval that the client must wait for the second EAP message after the link is up is defined by the EAPOL quiet period value (default value: 60 seconds). As a result, the user typically does not see a password window until 60 seconds after the link is up.
  To log out of EAP, the EAP client must explicitly send an EAP Logoff packet to the PAE. The built-in EAP client for MS Windows does not send this packet. Therefore, if you physically disconnect the client from the switch, the PAE will log out the client after a timeout period (typically about 1 minute).(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)

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

LACP

- When enabling an LAG of two links, a broadcast storm can occur during LACP timeout (Q01216169).

  The detailed explanation of this issue is as follows:

  There are two CLI commands that disable a port from an LAG:

  `no lacp aggregation enable` and **`lacp mode off`**

  The **`no lacp aggregation enable`** command determines whether a port is aggregatable; that is, whether it can become part of a trunk. When you execute this command, the affected port begins sending LACPDUs with new data showing that the port is not aggregatable. The port is then detached from its LAG. The partner port is also detached from its LAG as a result of the LACPDU it receives. LACPDUs continue to be sent until timer expiration (30s).

  The **`lacp mode off`** command also removes the affected port from its LAG. However, unlike the **`no lacp aggregation enable`** command, no additional PDUs are transmitted by this port to advertise its new state. As a result, the partner port is *not* detached at the same time as the local port. The **`lacp mode off`** command therefore results in the partner port belonging to the trunk at one end, and the local port no longer belonging to the trunk at the other end. This can produce a flood.

  If you want to disable LACP for a certain port, Nortel recommends that you first enter the **`no lacp aggregation enable`** command. This command ensures that the partner is also detached from its LAG. Then you can enter the **`lacp mode off`** command.

  If you want the port to revert to an LACP active port state, you must first enter the **`lacp aggregation enable`** command, and then enter the **`lacp mode active`** command for the port.

  With Web-based management, if you want to enable or disable LACP for a port using the Port Configuration page, first configure the settings for the A/I field, then configure the LACP Mode field. For example, to disable LACP on the port:

  — Set the **A/I** field for the port to **I**.

  — Click **Submit**.

  — Set the **LACP Mode** for the port to **Off**.

  — Click **Submit**.

  With Device Manager, to enable LACP for a port using the Port — LACP tab:

  — In the **ActorAdminState** field, choose **aggregation**.

  — Click **Apply**.

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

— Choose **AdminEnabled**.

— Click **Apply**.

To disable LACP for a port using Device Manager:

— In the **ActorAdminState** field, deselect **aggregation**.

— Click **Apply**.

— Deselect **AdminEnabled**.

— Click **Apply**.

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)

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.

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.

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

- 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.

STP and port mirroring on redundant link

- When STP and port mirroring are enabled on a redundant link port, a broadcast storm can occur even if the spanning tree state for the port is set to blocking. Because port mirroring takes priority over the STP port state, a broadcast or unicast packet coming in through a blocking port is mirrored to the unit containing the monitor port. On the monitor port unit, it is flooded on all ports based on its destination address. This issue does not occur with RSTP. (Q01198395)

Web and Device Manager

- 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 operational 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

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

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 above mentioned 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)
- By default, the Console Interface MultiLink Trunk Configuration screen displays the STP learning setting for all STPGs. To view or modify the learning setting for a particular STPG, you must change the value in the learning column from ALL to the desired STPG.

  For example, if you use the Spanning Tree Port Configuration screen to disable the STPG participation of an MLT link, the MLT Configuration screen does not display the new learning setting of disabled unless you change the STPG value from ALL to the appropriate STPG. (Q01216647)
- 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

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

should change to blocking, but they all remain in blocking and a loop is formed. (Q00942499)

- In port mirroring, broadcast, multicast, and unknown unicast traffic are NOT mirrored for XrxYtx and XrxYtxOrXtxYrx (port Y-Ethernet Switch 460). (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 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 inconsistent on the Release 3.5 software. (Q00912196)

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

- 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. (Q00888337)
- You can create 118 actions on an Ethernet switch. (Q00888347)
- Intruder SA can access the switch through the base unit 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).
- ACG generates commands that set the learning status for tagged ports that are not in the Spanning Tree Protocol Group. (Q00935346)
- 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 [ /  ] [ /  ] [ /  ][ / ] [ Normal ] Basic [ Disabled ]
 2 [ 2/6 ][ 2/7] [ / ] [ / ] [ Normal ] Basic [ Disabled ]
 3 [ 3/1 ][4/11] [4/12][5/1] [ 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)

Copyright © 2005-2007, Nortel Networks Nortel Networks Confidential

- 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:

- *Nortel Ethernet Switch 460/470 Overview — System Configuration Guide (NN47210-501)*
- *Nortel Ethernet Switch 460/470 Security — Configuration (NN47210-500)*
- *Nortel Ethernet Switch 460/470 Configuration — VLANs, Spanning Tree, and Multilink Trunking (NN47210-505)*
- *Nortel Ethernet Switch 460/470 Configuration — IP Multicast Routing Protocols (NN47210-504)*
- *Nortel Ethernet Switch 460/470 Configuration — Quality of Service and IP Filtering (NN47210-502)*
- *Nortel Ethernet Switch 460/470 Configuration — System Monitoring (NN47210-503)*
- *Nortel Ethernet Switch 470 — Installation (NN47210-301)*
- *Nortel Ethernet Switch 460-24T-PWR — Installation (NN47210-300)*

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins

Copyright © 2005-2007, Nortel Networks
Nortel Networks Confidential

- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Copyright © 2005-2007, Nortel Networks
Nortel Networks Confidential

Copyright © 2005-2007, Nortel Networks

Nortel Ethernet Switch 460/470

Release Notes — Software Release 3.7

Copyright © 2005-2007 , Nortel Networks
All Rights Reserved.

Publication: NN47210-400
Document status: Standard
Document version: 01.02
Document date: 12 March 2007

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback

Sourced in Canada and the United States of America.

The information in this document is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

