

Part No. 217103-B
December 2005

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Ethernet Switches 460 and 470 Software Release 3.6.2



NORTEL

Copyright © 2005 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, the Globemark, Unified Networks, and BayStack are trademarks of Nortel Networks.

Adobe and Adobe 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 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

- 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

| | |
|---|----------|
| Contents | 5 |
| Introduction | 7 |
| Hardware requirements | 8 |
| SSH-enabled image | 9 |
| Release 3.6.2 images | 9 |
| Upgrade instructions | 10 |
| Software and hardware scaling capabilities | 10 |
| New features | 11 |
| VLACP log and trap messages | 11 |
| STP BPDU-Filtering | 12 |
| spanning-tree bpdu-filtering command | 13 |
| no spanning-tree bpdu-filtering command | 14 |
| default spanning-tree bpdu-filtering command | 15 |
| show spanning-tree bpdu-filtering command | 15 |
| STP BPDU-Filtering tab | 17 |
| Web-based management support for RSTP, MSTP, and LACP | 19 |
| Changing Spanning Tree mode | 19 |
| Rapid Spanning Tree Protocol | 21 |
| Multiple Spanning Tree Protocol | 25 |
| LACP | 38 |
| MLT shutdown ports on disable | 43 |
| mlt shutdown-ports-on-disable enable command | 44 |
| no mlt shutdown-ports-on-disable enable command | 44 |
| show mlt shutdown-ports-on-disable command | 44 |
| Stack Monitor | 45 |
| Control Parameters | 46 |
| Configuring Stack Monitor | 46 |
| Local ports shutdown while stacking | 50 |
| Fixed Issues in Release 3.6.2 | 51 |
| Fixed Release 3.6 issues | 52 |
| Fixed Release 3.5 issues | 53 |
| Fixed Release 3.1 issues | 53 |

| | |
|---|----|
| Known issues and considerations in Release 3.6.2 | 53 |
| Changes to Release 3.6 documentation | 57 |
| Outstanding issues from Release 3.6 software | 61 |
| Outstanding issues from Release 3.5 software | 66 |
| Outstanding issues from Release 3.1 software | 68 |
| Related publications | 69 |
| How to get help | 70 |
| Getting help from the Nortel web site | 70 |
| Getting help through a Nortel distributor or reseller | 70 |
| Getting help over the phone from a Nortel Solutions Center | 70 |
| Getting help from a specialist by using an Express Routing Code | 71 |

Introduction

These Release Notes support the Release 3.6.2 software for the Nortel Ethernet Switches 460-24T-PWR, 470-24T, and 470-48T. They cover the supported hardware, new features, fixed issues, and known issues in 3.6.2 software, and outstanding issues from releases 3.6, 3.5, and 3.1 software.

The following topics are discussed in this document:

| Topic | Page |
|---|------|
| Hardware requirements | 8 |
| SSH-enabled image | 9 |
| New features | 11 |
| VLACP log and trap messages | 11 |
| STP BPDU-Filtering | 12 |
| Web-based management support for RSTP, MSTP, and LACP | 19 |
| MLT shutdown ports on disable | 43 |
| Stack Monitor | 45 |
| Local ports shutdown while stacking | 50 |
| Fixed Issues in Release 3.6.2 | 51 |
| Known issues and considerations in Release 3.6.2 | 53 |
| Related publications | 69 |
| How to get help | 70 |

Note: Release 3.6.2 software does not support the Hybrid stack mode. The Ethernet Switch 450 is no longer supported in the stack. All stacks must contain only the following:

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

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

Release 3.6.2 software supports the following Ethernet Switches:

Table 1 Supported Ethernet Switch hardware

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



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
-

SSH-enabled image

The Ethernet Switch 460/470 Software is available as an SSH-enabled image or as a non-SSH image. The SSH-enabled image 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.

You can obtain software images, including the SSH-enabled image, from the Nortel Technical Support web site:

www.nortel.com/support

Release 3.6.2 images

Table 2 describes the components of the Ethernet Switch 460 and 470 Release 3.6.2 software.

Table 2 Software Release 3.6.2 components

| File Description | File Name |
|---|--|
| Standard Runtime Image Software Version 3.6.2.0 | 470_36202.img |
| Secure Runtime Image Software Version 3.6.2.0 | 470_36203s.img |
| Boot/Diagnostic Software Version 3.6.0.5 | 470_36005_diags.bin |
| Java Device Manager Software Version 5.9.4.0 | Windows — jdm_5940.exe Solaris — jdm_5940_solaris_sparc.sh Linux — jdm_5940_linux.sh HP Unix — jdm_5940_hpux_pa-risc.sh |
| Software Release 3.6.2 Management Information Base (MIB) Definition Files | ES460_470MIBS_v3.6.2.zip |

Upgrade instructions

When upgrading the Ethernet Switch 460 or Ethernet Switch 470 to release 3.6.2, follow this procedure:

- 1 Backup the binary configuration file to a TFTP server.
- 2 Upgrade the boot/diagnostic code to version 3.6.0.5. The system reboots after this step.
- 3 Upgrade the software image to 3.6.2.0 (non-SSH image) or 3.6.2.1 (SSH image).

Software and hardware scaling capabilities

Table 3 lists the current values for software and hardware scaling capabilities supported in Ethernet Switch 460 and 470 Release 3.6.2 software.

Table 3 Supported scaling capabilities in Ethernet Switches 460 and 470

| Feature | Maximum number supported |
|--|--------------------------|
| Units per stack | 8 |
| MAC Addresses | 16 000 |
| Configurable VLANs | 256 |
| Nortel Spanning Tree Groups | 16 |
| 802.1s Spanning Tree Groups | 16 |
| MultiLink Trunks (MLT)/Link Aggregation Groups (LAG) | 6 |
| Ports per MLT | 4 |
| Active links per LAG | 4 |
| 802.1x MHMA hosts per port | 32 |
| 802.1x clients per stack | 800 |
| host addresses in MAC-based VLAN | 48 |

Table 3 Supported scaling capabilities in Ethernet Switches 460 and 470 (continued)

| Feature | Maximum number supported |
|-------------------------------------|--------------------------|
| QoS Policies | |
| Total Policies | 200 |
| Total Interface groups | 100 |
| Total meters | 200 |
| Total actions | 128 |
| Shapers | 62 |
| IP filter & filter groups | 200 |
| Filters with same IP Source Address | 24 |
| Nested subnets within IP Filters | 18 |
| Layer2 filters & filter groups | 24 |

New features

The following new features are available with release 3.6.2 software:

- [“VLACP log and trap messages”](#)
- [“STP BPDU-Filtering” on page 12](#)
- [“Web-based management support for RSTP, MSTP, and LACP” on page 19](#)
- [“MLT shutdown ports on disable” on page 43](#)
- [“Stack Monitor” on page 45](#)
- [“Local ports shutdown while stacking” on page 50](#)

VLACP log and trap messages

Release 3.6.2 software supports the generation of system log and SNMP trap messages when Virtual Link Aggregation Control Protocol (VLACP) enables or disables a link. This enables administrators to determine the status of a link.

STP BPDU-Filtering

Release 3.6.2 software supports the BPDU-Filtering feature for Spanning Tree Protocol (STP).

The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. Any bridge that participates in the spanning tree exchanges information with other bridges using configuration messages known as Bridge Protocol Data Units (BPDU). Based on the BPDU information exchange, the bridge with the lowest bridge ID becomes the root. This process is called the root selection process.

Typically, when a new bridge joins the spanning tree or an existing bridge leaves the spanning tree, the root selection process is repeated and a new root is selected.

The BPDU-Filtering feature allows the network administrator to achieve the following:

- Block an unwanted root selection process when an edge device, such as a laptop running Linux and enabled with STP, is added to the network. This prevents unknown devices from influencing an existing spanning tree topology.
- Block the flooding of BPDUs from an unknown device.



Note: The STP BPDU-Filtering feature is not supported on MultiLink Trunk (MLT) ports.

When a port has BPDU-Filtering enabled and it receives an STP BPDU, the following actions take place:

- The port is immediately put in the operational disabled state.
- A trap is generated and the following log message is written to the log:
BPDU received on port with BPDU-Filtering enabled. Port <x> has been disabled.
- The port timer starts.
- The port stays in the operational disabled state until the port timer expires.

If the timer is disabled or the switch is reset before the timer expires, the port remains in the disabled state. Similarly, if a user disables BPDU-Filtering while the timer is running, the timer is stopped and that port stays in the disabled state. In this case, you must then manually enable the port to bring it back to the normal mode.

You can enable and disable the BPDU-Filtering feature on a per-port basis. The BPDU-Filtering timer is user-configurable for each port and has a valid range of between 10 and 65535 seconds. The port timer is disabled if it is configured as 0.

To configure STP BPDU-Filtering using the CLI, refer to the following:

- [“spanning-tree bpdu-filtering command”](#)
- [“no spanning-tree bpdu-filtering command” on page 14](#)
- [“default spanning-tree bpdu-filtering command” on page 15](#)
- [“show spanning-tree bpdu-filtering command” on page 15](#)

To configure STP BPDU-Filtering using JDM, refer to [“STP BPDU-Filtering tab” on page 17](#).

spanning-tree bpdu-filtering command

The `spanning-tree bpdu-filtering` command enables BPDU-Filtering on a port or list of ports.

The syntax for the `spanning-tree bpdu-filtering` command is:

```
spanning-tree bpdu-filtering [port <portlist>] [enable]
[timeout {0 | <10-65535>}]
```

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

[Table 4](#) describes the parameters and variables for the `spanning-tree bpdu-filtering` command.

Table 4 `spanning-tree bpdu-filtering` command parameters and variables

| Parameters and variables | Description |
|---|--|
| <code>port <portlist></code> | Enter a list or range of port numbers. |
| <code>enable</code> | Enables BPDU-Filtering. |
| <code>timeout {0 <10-65535>}</code> | Specifies the time in seconds during which the port remains disabled after receiving a BPDU. The port timer is disabled if it is set to 0. |

no spanning-tree bpdu-filtering command

The `no spanning-tree bpdu-filtering` command disables BPDU-Filtering on a port or list or ports.

The syntax for the `no spanning-tree bpdu-filtering` command is:

```
no spanning-tree bpdu-filtering [port <portlist>] [enable]
```

The `no spanning-tree bpdu-filtering` command is in the `config-if` command mode.

[Table 5](#) describes the parameters and variables for the `no spanning-tree bpdu-filtering` command.

Table 5 `no spanning-tree bpdu-filtering` command parameters and variables

| Parameters and variables | Description |
|------------------------------------|--|
| <code>port <portlist></code> | Enter a list or range of port numbers. |

default spanning-tree bpdu-filtering command

The `default spanning-tree bpdu-filtering` command sets the BPDU-Filtering parameters to their default values.

The syntax for the `default spanning-tree bpdu-filtering` command is:

```
default spanning-tree bpdu-filtering [port <portlist>]
[enable] [timeout]
```

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

[Table 6](#) describes the parameters and variables for the `default spanning-tree bpdu-filtering` command.

Table 6 `default spanning-tree bpdu-filtering` command parameters and variables

| Parameters and variables | Description |
|--|--|
| port <portlist> | Enter a list or range of port numbers. |
| enable | Sets the BPDU-Filtering feature to its default status (disabled). |
| timeout | Sets the BPDU-Filtering port timeout to its default value (120 seconds). |
| Note: If you do not specify a parameter for this command, all STP BPDU-Filtering parameters are set to their default values. | |

show spanning-tree bpdu-filtering command

The `show spanning-tree bpdu-filtering` command displays the current status of the BPDU-Filtering parameters.

The syntax for the `show spanning-tree bpdu-filtering` command is:

```
show spanning-tree bpdu-filtering [<interface-type>]
[port <portlist>]
```

The `show spanning-tree bpdu-filtering` command is in the `privExec` command mode.

[Table 7](#) describes the parameters and variables for the `show spanning-tree bpdu-filtering` command.

Table 7 show spanning-tree bpdu-filtering command parameters and variables

| Parameters and variables | Description |
|--------------------------|---|
| interface-type | Interface type. |
| portlist | Enter a list or range of port numbers. Note: If you omit this parameter, the system uses the port number specified by the interface command. |

[Figure 1](#) displays a sample output of the `show spanning-tree bpdu-filtering` command.

Figure 1 show spanning-tree bpdu-filtering command output

```

470-24T#show spanning-tree bpdu-filtering
Port Trunk Admin Oper Link LinkTrap Timeout TimerCount BpduFiltering
-----
1      Enable Up Up Enabled 120 0 Enabled
2      Enable Down Down Enabled 120 0 Disabled
3      Enable Down Down Enabled 120 0 Disabled
4      Enable Down Down Enabled 120 0 Disabled
5      Enable Down Down Enabled 120 0 Disabled
6      Enable Down Down Enabled 120 0 Disabled
7      Enable Down Down Enabled 120 0 Disabled
8      Enable Down Down Enabled 120 0 Disabled
9      Enable Down Down Enabled 120 0 Disabled
10     Enable Down Down Enabled 120 0 Disabled
11     Enable Down Down Enabled 120 0 Disabled
12     Enable Down Down Enabled 120 0 Disabled
13     Enable Down Down Enabled 120 0 Disabled
14     Enable Down Down Enabled 120 0 Disabled
----More (q=Quit, space/return=Continue)----

```


STP BPDU-Filtering tab

In JDM, you can set the STP BPDU-Filtering parameters for a port using the STP BPDU-Filtering tab.

To open the STP BPDU-Filtering tab:

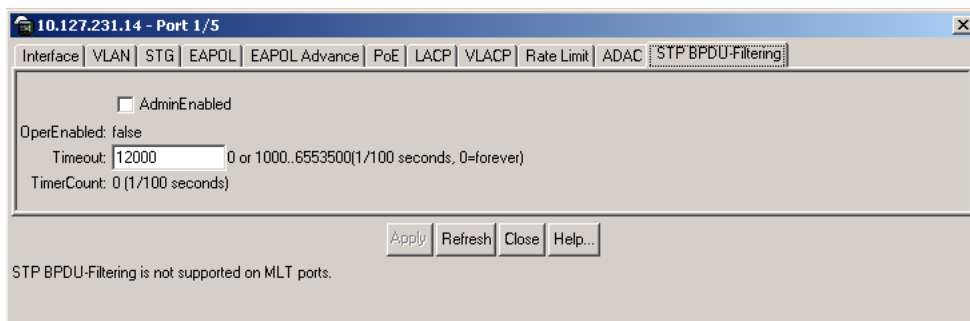
- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click the selected port.
 - From the shortcut menu, choose Edit.
 - From the Device Manager main menu, choose Edit > Port.
 - On the toolbar, click Edit.

The Port dialog box opens with the Interface tab displayed.

- 3 Click the STP BPDU-Filtering tab.

The STP BPDU-Filtering tab opens ([Figure 2](#)).

Figure 2 STP BPDU-Filtering tab



[Table 8](#) describes the STP BPDU-Filtering tab fields.

Table 8 STP BPDU-Filtering tab fields

| Item | Description |
|--------------|--|
| AdminEnabled | Enables or disables BPDU-filtering on the port. |
| OperEnabled | Displays the current status of BPDU-Filtering on the port. |

Table 8 STP BPDU-Filtering tab fields

| Item | Description |
|-------------|--|
| Timeout | Specifies the time in 1/100 seconds during which the port remains disabled after receiving a BPDU. The port timer is disabled if this value is set to 0. |
| TimerCount | Displays the current value in 1/100 seconds of the BPDU-Filtering timer. |

Web-based management support for RSTP, MSTP, and LACP

Release 3.6.2 software provides Web-based management support for Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w), Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s), and Link Aggregation Control Protocol (LACP) (IEEE 802.3ad).

For more information on Web-based management support for MSTP, RSTP, and LACP, refer to the following sections:

- [“Changing Spanning Tree mode”](#)
- [“Rapid Spanning Tree Protocol” on page 21](#)
- [“Multiple Spanning Tree Protocol” on page 25](#)
- [“LACP” on page 38](#)

Changing Spanning Tree mode

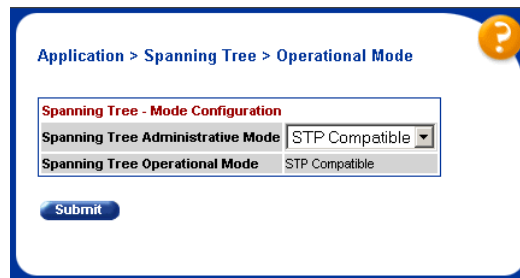
Release 3.6.2 software allows you to change the Spanning Tree mode for Ethernet Switches 460 and 470 using Web-based management.

To change the Spanning Tree mode:

- 1 From the main menu, choose Application > Spanning Tree > Operational Mode.

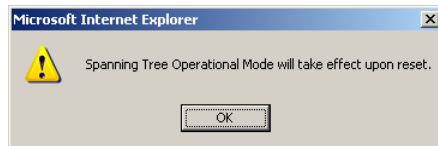
The Operational Mode page opens ([Figure 3](#)).

Figure 3 Spanning Tree Operational Mode page



- 2 Select the Spanning Tree Administrative Mode that you desire from the drop-down list. The available options are:
 - STP Compatible
 - RSTP
 - MSTP
- 3 Click Submit.
- 4 A warning appears reminding you that a switch reset is required for the change to take effect ([Figure 4](#)).

Figure 4 Operational mode change warning page



- 5 Click OK.
- 6 To reset the switch, choose Administration > Reset.

Rapid Spanning Tree Protocol

The following sections describe how to configure and manage RSTP using Web-based management:

- [“Configuring RSTP bridge settings”](#)
- [“Configuring RSTP ports” on page 23](#)

Configuring RSTP bridge settings



Note: You can access the RSTP menu command only when the switch is operating in the RSTP mode.

To configure rapid spanning tree groups:

- 1 From the main menu, choose Application > Spanning Tree > Bridge Configuration.

The Bridge Configuration page opens ([Figure 5](#)).

Figure 5 RSTP Bridge Configuration page

| Spanning Tree - Bridge Configuration | |
|--------------------------------------|-------------------------|
| STP Priority | 8000 (hex) |
| Designated Root | 80-00-00-09-97-47-34-41 |
| Stp Root Cost | 200020 |
| Stp Root Port | Port 1 |
| Bridge Max Age | 20 seconds (0 .. 40) |
| Bridge Hello Time | 2 seconds (1 .. 10) |
| Bridge Forward Delay Time | 15 seconds (4 .. 30) |
| Tx Hold Count | 3 (1 .. 10) |
| PathCost Default Type | 32-bit |

Submit

[Table 9](#) describes the items on the RSTP Bridge Configuration page.

Table 9 RSTP Bridge Configuration page items

| Item | Description |
|---------------------------|---|
| STP Priority | The value of the writable portion of the Bridge Identifier comprising the first two octets. |
| Designated Root | The unique identifier of the bridge recorded as the root in the Configuration BPDUs that the Designated Bridge transmits for the segment to which the port is attached. Reference IEEE 802.1D-1990: section 4.5.5.4. |
| Stp Root Cost | The cost of the path to the root as seen from this bridge. |
| Stp Root Port | The port number of the port that offers the lowest cost path from this bridge to the root bridge. |
| Bridge Max Age | The value in seconds that all bridges use for MaxAge when this bridge acts as the root. The range is 6 to 40. |
| Bridge Hello Time | The value in seconds that all bridges use for HelloTime when this bridge acts as the root. The range is 1 to 10. |
| Bridge Forward Delay Time | The value in seconds that all bridges use for ForwardDelay when this bridge acts as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of BridgeMaxAge. The range is 4 to 30. |
| Tx Hold Count | The value the Port Transmit state machine uses to limit the maximum transmission rate. The range is 1 to 10. |
| PathCost Default Type | Sets the version of the Spanning Tree default Path Costs that the bridge uses. A value of 16-bit uses the 16-bit default Path Costs from IEEE Std. 802.1D-1998. A value of 32-bit uses the 32-bit default Path Costs from IEEE Std. 802.1t. |

Configuring RSTP ports

To configure switch ports for participation in the Rapid Spanning Tree:

- 1 From the main menu, choose Application > Spanning Tree > Port Configuration.

The Port Configuration page opens (Figure 6).

Figure 6 RSTP Port Configuration page

Application > Spanning Tree (RSTP) > Port Configuration

Spanning Tree - Port Setting

| Port | STP Participation | Priority (hex) | Path Cost | Admin Edge Status | Oper Edge Status | Admin P2P Status | Oper P2P Status | Oper Protocol Version | Role | State |
|--------|-------------------|----------------|-----------|-------------------|------------------|------------------|-----------------|-----------------------|----------|------------|
| 1 | Enabled | 80 | 200000 | False | False | Auto | True | StpCompatible Mode | Root | Forwarding |
| 2 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 3 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 4 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 5 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 6 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 7 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 8 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 9 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 10 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 11 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| 12 | Enabled | 80 | 200000 | False | False | Auto | True | Rstp Mode | Disabled | Discarding |
| Switch | Enabled | 80 | 200000 | False | | Auto | | | | |

Submit

[Ports 13 - 24](#) [Ports 25 - 26](#)

Table 10 describes the items on the RSTP Port Configuration page.

Table 10 RSTP Port Configuration page items

| Item | Description |
|-----------------------|---|
| STP Participation | This field specifies whether a port is participating in the RSTP (802.1w) protocol. |
| Priority (hex) | The value of the priority field that is contained in the first (in network byte order) octet of the (2 octet long) Port ID. |
| Path Cost | The contribution of this port to the path cost of paths towards the spanning tree root that include this port. |
| Admin Edge Status | A value of true indicates that the spanning tree can assume this port as an edge-port and a value of false indicates that the spanning tree can assume this port as a non-edge-port. |
| Oper Edge Status | The operational value of the Edge Status parameter. The switch software sets this object to false on reception of a BPDU. |
| Admin P2P Status | The administrative point-to-point status of the LAN segment attached to this port. <ul style="list-style-type: none"> • A value of ForceTrue indicates that the spanning tree must treat this port as if it is connected to a point-to-point link. • A value of ForceFalse indicates that the spanning tree must treat this port as having a shared media connection. • A value of Auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through auto-negotiation or by management means. |
| Oper P2P Status | The operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by auto-detection. |
| Oper Protocol Version | Indicates the STP version in which the port is participating. |
| Role | Indicates the role of the port in the Spanning Tree instance. |
| State | Used to identify a port state in this RSTP instance. Port state is cataloged as Discarding, Learning, or Forwarding. |

Multiple Spanning Tree Protocol

MSTP allows you to configure multiple instances of RSTP on the same switch. Each MSTP instance can include one or more VLANs. The operation of the MSTP is similar to the Nortel proprietary STG. In MSTP mode, the Ethernet Switches support a maximum of one CIST instance and 15 MSTI instances.

The following sections describe how to configure and manage MSTP using Web-based management:

- [“Configuring MSTP bridge settings”](#)
- [“Configuring CIST bridge settings” on page 28](#)
- [“Configuring MSTI bridge settings” on page 30](#)
- [“Associating a VLAN with the CIST or with an MSTI” on page 31](#)
- [“Configuring CIST port properties” on page 33](#)
- [“Configuring MSTI port properties” on page 36](#)

Configuring MSTP bridge settings

To configure Multiple Spanning Tree bridge settings on the switch:

- 1 From the main menu, choose Application > Spanning Tree > Bridge Configuration.

The Bridge Configuration page opens (Figure 7).

Figure 7 MSTP Bridge Configuration page

Application > Spanning Tree (MSTP) > Bridge Configuration

Spanning Tree - CIST Bridge Configuration

| Action | Bridge Regional Root | Bridge Priority | Root Cost | Root Port |
|--------|-------------------------|-----------------|-----------|-----------|
| | 80-00-00-11-58-f7-0b-60 | 8000 | 200020 | Port 1 |

Spanning Tree - Msti Bridge Configuration

| Action | Msti | Bridge Regional Root | Bridge Priority | Root Cost | Root Port | State |
|--------|------|-------------------------|-----------------|-----------|-----------|---------|
| | 1 | 80-00-00-11-58-f7-0b-60 | 8000 | 0 | 0 | Enabled |

Spanning Tree - Msti Bridge Creation



Msti:

Table 11 describes the items on the MSTP Bridge Configuration page.

Table 11 MSTP Bridge Configuration page items

| Section | Item | Description |
|---|----------------------|---|
| Spanning Tree - CIST Bridge Configuration | | Displays a modification page. |
| | Bridge Regional Root | The bridge identifier of the root of the multiple spanning tree region as determined by the Spanning Tree Protocol as executed by this node. All configuration bridge PDUs originated by this node use this value as the CIST Regional Root Identifier parameter. |
| | Bridge Priority | The value of the writable portion of the bridge identifier comprising of the first two octets. |
| | Root Cost | The cost of the path to the CIST root as seen from this bridge. |
| | Root Port | The port number of the port that offers the lowest path cost from the bridge to the CIST root bridge |

Table 11 MSTP Bridge Configuration page items (continued)

| Section | Item | Description |
|---|---|--|
| Spanning Tree - Msti Bridge Configuration |  | Displays a modification page. |
| |  | Deletes the row. |
| | Bridge Regional Root | Indicates the MSTI regional root identifier value for the MSTI. All configuration bridge PDUs originated by this node use this value as the MSTI regional root identifier parameter. |
| | Bridge Priority | The value of the writable portion of the bridge identifier comprising of the first two octets. |
| | Root Cost | The cost of the path to the MSTI regional root as seen by this bridge. |
| | Root Port | The port number of the port that offers the lowest path cost from this bridge to the MSTI region root bridge. |
| | State | Indicates whether the bridge instance is enabled or disabled. |
| Spanning Tree - Msti Bridge Creation | Msti | The MSTI instance ID. |

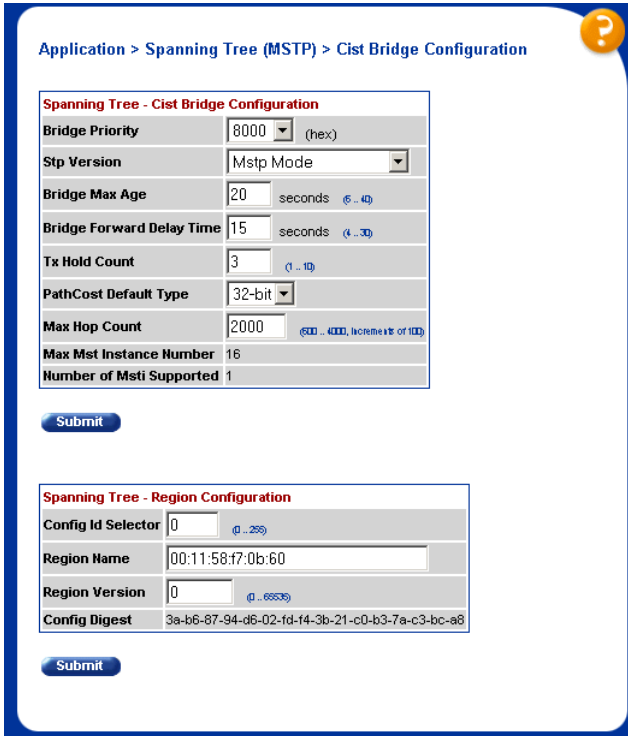
Configuring CIST bridge settings

To configure Multiple Spanning Tree CIST bridge settings on the switch:

- 1 From the main menu, choose Application > Spanning Tree > Cist Bridge Configuration.

The Cist Bridge Configuration page opens (Figure 8).

Figure 8 Cist Bridge Configuration page



Application > Spanning Tree (MSTP) > Cist Bridge Configuration

Spanning Tree - Cist Bridge Configuration

| | |
|---------------------------|-------------------------------------|
| Bridge Priority | 8000 (hex) |
| Stp Version | Mstp Mode |
| Bridge Max Age | 20 seconds (6..40) |
| Bridge Forward Delay Time | 15 seconds (4..30) |
| Tx Hold Count | 3 (1..10) |
| PathCost Default Type | 32-bit |
| Max Hop Count | 2000 (600..4000, increments of 100) |
| Max Mst Instance Number | 16 |
| Number of Msti Supported | 1 |

Submit

Spanning Tree - Region Configuration

| | |
|--------------------|---|
| Config Id Selector | 0 (0..255) |
| Region Name | 00:11:58:f7:0b:60 |
| Region Version | 0 (0..65535) |
| Config Digest | 3a-b6-87-94-d6-02-fd-f4-3b-21-c0-b3-7a-c3-bc-88 |

Submit

Table 12 describes the items on the Cist Bridge Configuration page.

Table 12 Cist Bridge Configuration page items

| Section | Item | Description |
|---|---------------------------|---|
| Spanning Tree - Cist Bridge Configuration | Bridge Priority | The value of the writable portion of the bridge identifier comprising the first two octets. |
| | Stp Version | Indicates the STP version in which the bridge is participating. |
| | Bridge Max Age | The value in seconds that all bridges use for MaxAge when this bridge acts as the root. The range is 6 to 40. |
| | Bridge Forward Delay Time | The value in seconds that all bridges use for ForwardDelay when this bridge acts as the root. IEEE 802.1D specifies that the range for this parameter is related to the value of Bridge Max Age. The range is 4 to 30. |
| | Tx Hold Count | The value used by the Port Transmit state machine to limit the maximum transmission rate. |
| | PathCost Default Type | The version of the spanning tree default path costs that this bridge uses. A 16-bit value uses the 16-bit default path costs from IEEE Standard 802.1D-1998. A 32-bit value uses the 32-bit default path costs from IEEE Standard 802.1t. |
| | Max Hop Count | The maximum hop count value in 1/100 seconds. The value must be a multiple of 100. The range is 600 to 4000. |
| | Max Mst Instance Number | The highest possible value for the MSTI ID in this mode. |
| | Number of Msti Supported | The number of MSTI supported in this mode. |
| Spanning Tree - Region Configuration | Config Id Selector | The MSTP config ID selector. The default value is 0. |
| | Region Name | The MSTP region name. The default value is the bridge MAC address. |
| | Region Version | The MSTP region version. The default value is 0. |
| | Config Digest | The configuration digest value for this region. |

Configuring MSTI bridge settings

To configure Multiple Spanning Tree MSTI bridge settings on the switch:

- 1 From the main menu, choose Application > Spanning Tree > Msti Bridge Configuration.

The Msti Bridge Configuration page opens (Figure 9).

Figure 9 Msti Bridge Configuration page

Application > Spanning Tree (MSTP) > Msti Bridge Configuration

Spanning Tree - Msti Bridge Configuration

| | |
|----------------------|-------------------------|
| Msti | 1 |
| Bridge Priority | 8000 (hex) |
| Bridge Regional Root | 80-00-00-11-58-f7-06-60 |
| Root Cost | 0 |
| Root Port | Port 0 |
| State | Enabled |

Submit Back

Table 13 describes the items on the Msti Bridge Configuration page.

Table 13 Msti Bridge Configuration page items

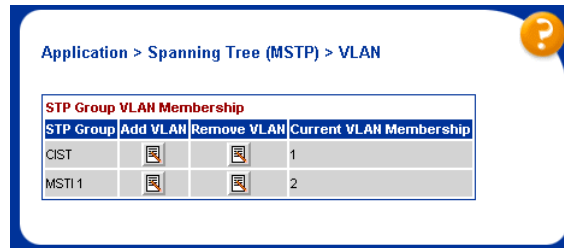
| Item | Description |
|----------------------|--|
| Msti | The Multiple Spanning Tree instance. |
| Bridge Priority | The writable portion of the MSTI bridge identifier comprising the first two octets. |
| Bridge Regional Root | Indicates the MSTI regional root identifier value for the MSTI. All configuration bridge PDUs originated by this node use this value as the MSTI Regional Root Identifier parameter. |
| Root Cost | The cost of the path to the MSTI regional root as seen by this bridge. |
| Root Port | The port number of the port that offers the lowest path cost from this bridge to the MSTI region root bridge. |
| State | Used to control whether the bridge instance is enabled or disabled. |

Associating a VLAN with the CIST or with an MSTI

To associate a VLAN with the CIST or with an MSTI instance:

- 1 From the main menu, choose Application > Spanning Tree > Bridge VLAN.
The VLAN page opens (Figure 10).

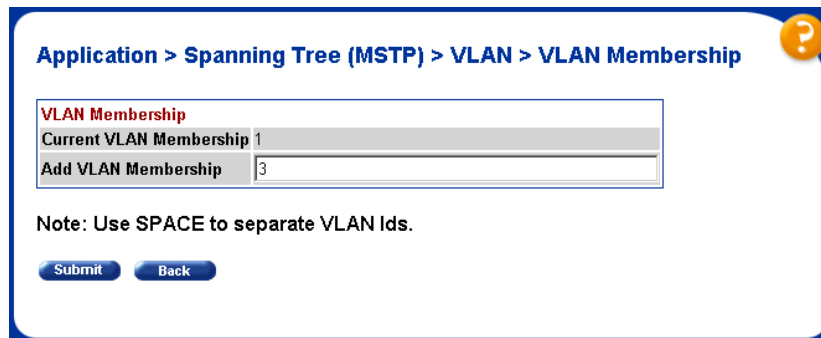
Figure 10 MSTP VLAN page



- 2 The table displays the current VLAN membership for the CIST and MSTIs.
- 3 To add a VLAN:
 - a Click the modification icon in the Add VLAN column for the CIST or MSTI.

The MSTP VLAN Membership Add VLAN page opens (Figure 11).

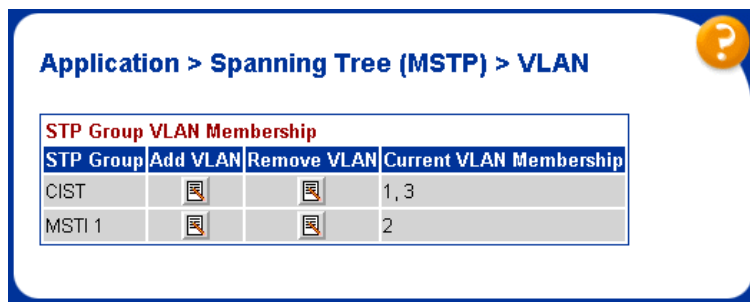
Figure 11 MSTP VLAN Membership (Add) page



- b Enter the number of the VLANs you want to add to the CIST or MSTI.
- c Click Submit.

The VLAN is added to the Current VLAN Membership column in the appropriate CIST or MSTI row (Figure 12).

Figure 12 MSTP VLAN page with VLAN added

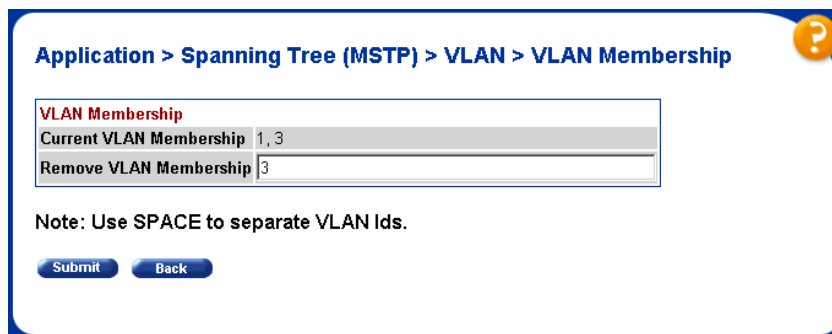


4 To remove a VLAN:

- a** Click the modification icon in the Remove VLAN column.

The MSTP VLAN Membership Remove VLAN page opens (Figure 13).

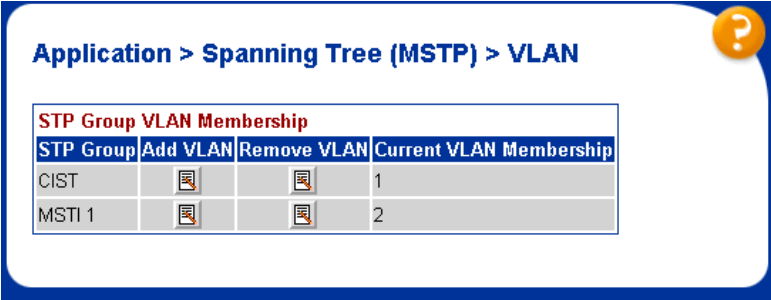
Figure 13 MSTP VLAN Membership (Remove) page







- b** Enter the number of the VLANs you want to remove from the STG.
- c** Click Submit.

The VLAN is removed from the Current VLAN Membership column in the appropriate CIST or MSTI row (Figure 14).

Figure 14 MSTP VLAN page with VLAN removed



The screenshot shows a web interface for configuring MSTP VLANs. The breadcrumb navigation is "Application > Spanning Tree (MSTP) > VLAN". A table titled "STP Group VLAN Membership" is displayed. The table has four columns: "STP Group", "Add VLAN", "Remove VLAN", and "Current VLAN Membership". There are two rows: "CIST" and "MSTI 1". Each row has a plus icon in the "Add VLAN" column and a minus icon in the "Remove VLAN" column. The "Current VLAN Membership" column shows "1" for CIST and "2" for MSTI 1. A yellow question mark icon is in the top right corner of the interface.

| STP Group VLAN Membership | | | |
|---------------------------|---|---|-------------------------|
| STP Group | Add VLAN | Remove VLAN | Current VLAN Membership |
| CIST |  |  | 1 |
| MSTI 1 |  |  | 2 |

Configuring CIST port properties

To configure CIST port properties:

- 1 From the main menu, choose Application > Spanning Tree > Cist Port Configuration.

The Cist Port Configuration page opens (Figure 15).

Figure 15 Cist Port Configuration page

Application > Spanning Tree (MSTP) > Cist Port Configuration

Spanning Tree - Cist Port Setting

| Port | STP Participation | Priority (hex) | Path Cost | Admin Edge Status | Oper Edge Status | Admin P2P Status | Oper P2P Status | Hello Time (seconds) | Role | State |
|--------|-------------------|----------------|-----------|-------------------|------------------|------------------|-----------------|----------------------|----------|------------|
| 1 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Root | Forwarding |
| 2 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 3 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 4 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 5 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 6 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 7 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 8 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 9 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 10 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 11 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| 12 | Enabled | 80 | 200000 | False | False | Auto | True | 2 | Disabled | Discarding |
| Switch | Enabled | 80 | 200000 | False | | Auto | | 2 | | |

Submit

[Ports 13 - 24](#) [Ports 25 - 26](#)

Table 14 describes the items on the Cist Port Configuration page.

Table 14 Cist Port Configuration page items

| Item | Description |
|-------------------|---|
| STP Participation | This field specifies whether a port is participating in the MSTP (802.1s) protocol. |
| Priority (hex) | The four most significant bits of the Port Identifier of the Spanning Tree instance. |
| Path Cost | The contribution of this port to the path cost of paths towards the CIST Root that include this port. |
| Admin Edge Status | The administrative value of the Edge Status parameter. A value of true indicates that the CIST can assume this port as an edge-port and a value of false indicates that the CIST can assume this port as a non-edge-port. |
| Oper Edge Status | Signifies the operational value of the Edge Status parameter. The switch software sets this object to false when the port receives a BPDU. |

Table 14 Cist Port Configuration page items (continued)

| Item | Description |
|------------------|--|
| Admin P2P Status | <p>The administrative point-to-point status of the LAN segment attached to this port.</p> <ul style="list-style-type: none"> • A value of ForceTrue indicates that the CIST must treat this port as if it is connected to a point-to-point link. • A value of ForceFalse indicates that the CIST must treat this port as having a shared media connection. • A value of Auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through auto-negotiation or by management means. |
| Oper P2P Status | <p>This field indicates the operational point-to-point status of the LAN segment attached to the port. It also indicates whether a port is considered to have a point-to-point connection. The value is determined by management or by auto-detection, as described in the Admin P2P object.</p> |
| Hello Time | <p>The amount of time between the transmission of Configuration BPDUs transmitted by this node on the port. It is measured in units of hundredths of a second.</p> |
| Role | <p>Indicates the role of the port in the spanning tree instance.</p> |
| State | <p>The current state of the port as defined by the Common Spanning Tree Protocol.</p> |

Configuring MSTI port properties

To configure MSTI port properties:

- 1 From the main menu, choose Application > Spanning Tree > Msti Port Configuration.

The Msti Port Configuration page opens (Figure 16).

Figure 16 Msti Port Configuration page

Application > Spanning Tree (MSTP) > Msti Port Configuration ?

MST Instance

Msti 1

[Submit](#)

| Spanning Tree - Msti Port Setting | | | | | |
|-----------------------------------|-------------------|----------------|-----------|----------|------------|
| Port | STP Participation | Priority (hex) | Path Cost | Role | State |
| 1 | Disabled | | | | Discarding |
| 2 | Disabled | | | | Discarding |
| 3 | Disabled | | | | Discarding |
| 4 | Disabled | | | | Discarding |
| 5 | Disabled | | | | Discarding |
| 6 | Disabled | | | | Discarding |
| 7 | Disabled | | | | Discarding |
| 8 | Disabled | | | | Discarding |
| 9 | Disabled | | | | Discarding |
| 10 | Disabled | | | | Discarding |
| 11 | Enabled | 80 | 200000 | Disabled | Discarding |
| 12 | Disabled | | | | Discarding |
| Switch | Enabled | 80 | 200000 | | |

[Submit](#)

[Ports 13 - 24](#) [Ports 25 - 26](#)

[Table 15](#) describes the items on the Msti Port Configuration page.

Table 15 Msti Port Configuration page items

| Section | Item | Description |
|-----------------------------------|-------------------|---|
| MST Instance | Msti | The MSTI instance ID. |
| Spanning Tree - Msti Port Setting | STP Participation | This field specifies whether a port is participating in the MSTP (802.1s) protocol. |
| | Priority | Indicates the four most significant bits of the Port Identifier for a given spanning tree instance. You can modify this item independently for each spanning tree instance the bridge supports. |
| | Path Cost | The contribution of this port to the cost of paths towards the MSTI root that include this port. |
| | Role | Indicates the role of the port in the spanning tree instance. |
| | State | Indicates the current state of the port as defined by the Multiple Spanning Tree Protocol. The port state can be either Forwarding or Discarding (Blocking). |

LACP

The following sections describe how to configure and manage LACP using Web-based management:

- “Viewing LACP information”
- “Configuring LACP port information” on page 40
- “Viewing LACP port statistics” on page 42

Viewing LACP information

To view LACP information:

- 1 From the main menu, choose Application > Link Aggregation > Bridge Configuration.

The Bridge Configuration page opens (Figure 17).

Figure 17 LACP Bridge Configuration page

Application > LACP > Bridge Configuration

LACP - Bridge Configuration

System Priority: 30002 (0 .. 65535)

Collector Max Delay 1

Submit

LACP - Aggregator Information

| Aggregator ID | Trunk ID | Operate | Actor Lag ID | Actor System ID | Actor Operational Key | Actor Administrative Key | Partner Lag ID | Partner System Priority | Partner System ID | Partner Operational Key |
|---------------|----------|-----------|------------------------|-------------------|-----------------------|--------------------------|------------------------|-------------------------|-------------------|-------------------------|
| 8194 | 5 | Aggregate | 7532-000438D59080-2001 | 00-04-38-D5-90-80 | 8193 | 1 | 8000-000997897080-200F | 32768 | 00-09-97-89-70-80 | 8207 |
| 8193 | 6 | Aggregate | 7532-000438D59080-2001 | 00-04-38-D5-90-80 | 8193 | 1 | 8000-0011589D5C00-200A | 32768 | 00-11-58-9D-5C-00 | 8202 |

Table 16 describes the items on the Bridge Configuration page.

Table 16 LACP Bridge Configuration page items

| Section | Item | Description |
|-----------------------------|---------------------|---|
| LACP - Bridge Configuration | System Priority | The priority value associated with the Actor System ID. |
| | Collector Max Delay | The maximum delay, in 1/100 seconds, that the Frame Collector can impose between receiving a frame from an Aggregator Parser and either delivering the frame to its MAC Client or discarding the frame. |

Table 16 LACP Bridge Configuration page items (continued)

| Section | Item | Description |
|-------------------------------------|--------------------------|--|
| LACP - Aggregator Information | Aggregator ID | The unique identifier that the local system assigns to this aggregator. This attribute identifies an aggregator instance among the subordinate managed objects of the containing object. |
| | Trunk ID | The ID of the trunk associated with this aggregator. |
| | Operate | Indicates whether the aggregation port can aggregate or can operate only as an individual link. |
| | Actor Lag ID | The combined information of Actor System Priority, Actor System ID, and Actor Operational Key in ActorSystemPriority-ActorSystemID-ActorOperationalKey hex format. |
| | Actor System ID | The MAC address value that defines the value of the System ID for the system that contains this aggregation port. |
| | Actor Operational Key | The current operational value of the key for the aggregation port. |
| | Actor Administrative Key | The current administrative value of the key for the aggregation port. |
| | Partner Lag ID | The combined information of Partner System Priority, Partner System ID, and Partner Operational Key in PartnerSystemPriority-PartnerSystemID-PartnerOperationalKey hex format. |
| | Partner System Priority | The value that indicates the priority value associated with the Partner System ID. |
| | Partner System ID | The MAC address value consisting of the unique identifier for the current protocol partner of this aggregator. |
| | Partner Operational Key | The current operational value of the key for the current protocol partner of this aggregator. |

Configuring LACP port information

To configure LACP port information:

- 1 From the main menu, choose Application > Link Aggregation > Port Configuration.

The Port Configuration page opens (Figure 18).

Figure 18 LACP Port Configuration page

Application > LACP > Port Configuration

LACP - Port Setting

| Port | Priority | LACP Mode | A/I | Timeout | Admin Key | Operational Key | Aggregator ID | Trunk ID | Partner Port | Status |
|--------|----------|------------------------------|----------------------------|-------------------------------|----------------------------|--------------------------|---------------|----------|--------------|--------|
| 1 | 32768 | Active | A | Long | 1 | 8193 | 0 | | | Active |
| 2 | 32768 | Off | I | Long | 1 | 0 | 0 | | | Down |
| 3 | 32768 | Off | I | Long | 1 | 0 | 0 | | | Down |
| 4 | 32768 | Off | I | Long | 1 | 0 | 0 | | | Down |
| 5 | 32768 | Off | I | Long | 1 | 0 | 0 | | | Down |
| 6 | 32768 | Off | I | Long | 1 | 0 | 0 | | | Down |
| 7 | 32768 | Active | A | Long | 1 | 8193 | 0 | | | Down |
| 8 | 32768 | Active | A | Long | 1 | 8193 | 0 | | | Down |
| 9 | 32768 | Off | I | Long | 1 | 0 | 0 | | | Down |
| 10 | 32768 | Off | I | Long | 1 | 0 | 0 | | | Down |
| 11 | 32768 | Off | I | Long | 1 | 0 | 0 | | | Down |
| 12 | 32768 | Off | I | Long | 1 | 0 | 0 | | | Down |
| Switch | 32768 | <input type="checkbox"/> Off | <input type="checkbox"/> I | <input type="checkbox"/> Long | <input type="checkbox"/> 1 | <input type="checkbox"/> | | | | |

[Ports 13 - 24](#) [Ports 25 - 26](#)

Table 17 describes the items on the Port Configuration page.

Table 17 LACP Port Configuration page items

| Item | Description |
|-----------------|--|
| Priority | The priority value assigned to this aggregation port. |
| LACP Mode | Sets the LACP mode: <ul style="list-style-type: none"> • Active = AdminEnabled + ActorAdminState(lacpActive) • Passive = AdminEnabled • Off = AdminDisabled |
| A/I | Indicates whether the aggregation port can aggregate (A) or can operate only as an individual link (I). |
| Timeout | Indicates whether the timeout of the aggregation port is long or short. |
| Admin Key | The current administrative value of the key for the aggregation port. |
| Operational Key | The current operational value of the key for the aggregation port. |
| Aggregator ID | The ID of the aggregator that this aggregation port has currently selected. |
| Trunk ID | The ID of the trunk associated with this aggregation port. |
| Partner Port | The operational port number the protocol partner assigned to this aggregation port. |
| Status | The status of the aggregation port: Down, Up, Active, or Standby. |

Viewing LACP port statistics

To view LACP port statistics:

- 1 From the main menu, choose Application > Link Aggregation > Port Statistics.

The Port Statistics page opens (Figure 19).

Figure 19 LACP Port Statistics page

Application > LACP > Port Statistics

LACP - Port Statistics

| Port | LACPDUs | MarkerPDUs | MarkerResponsePDUs | UnknownPDUs | IllegalPDUs | LACPDUs | MarkerPDUs | MarkerResponsePDUs |
|------|---------|------------|--------------------|-------------|-------------|---------|------------|--------------------|
| | Rx | Rx | Rx | Rx | Rx | Tx | Tx | Tx |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

[Ports 13 - 24](#) [Ports 25 - 26](#)

Table 18 describes the items on the Port Statistics page.

Table 18 LACP Port Statistics page items

| Item | Description |
|------------------------|--|
| LACPDUs Rx | The number of valid LACPDUs received on the aggregation port. |
| MarkerPDUs Rx | The number of valid MarkerPDUs received on the aggregation port. |
| Marker ResponsePDUs Rx | The number of valid MarkerResponsePDUs received on the aggregation port. |
| UnknownPDUs Rx | The number of frames received that: <ul style="list-style-type: none"> • can carry the Slow Protocols Ethernet Type value, but contain an unknown PDU. • are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type. |

Table 18 LACP Port Statistics page items (continued)

| Item | Description |
|-----------------------|--|
| IllegalPDUs Rx | The number of frames received that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype. |
| LACPDUs Tx | The number of LACPDUs transmitted on the aggregation port. |
| MarkerPDUs Tx | The number of MarkerPDUs transmitted on the aggregation port. |
| MarkerResponsePDUs Tx | The number of MarkerResponsePDUs transmitted on the aggregation port. |

MLT shutdown ports on disable

The MLT shutdown ports on disable feature is used to prevent broadcast storms when an MLT is disabled and some or all of its ports are still connected to another device.

The feature functions as follows: if an MLT is disabled, all ports that are members of the MLT are automatically shut down, and the switch generates a trap and log stating this is the reason the ports are disabled.

If the affected MLT is re-enabled, the disabled ports are enabled automatically. When the ports are re-enabled, a log and trap are generated. You can also re-enable the disabled ports manually using the `no shutdown` command, in which case no log or trap is generated.

The MLT shutdown ports on disable feature is user-configurable switch-wide. The feature is disabled by default, so that the default behaviour for MLTs remains the same as previous releases: a disabled MLT has no effect on the state of the individual trunk ports.

You can enable the new feature by using CLI commands only. No support is provided for other management interfaces.

To configure the MLT shutdown ports on disable feature, refer to the following:

- [“mlt shutdown-ports-on-disable enable command”](#)
- [“no mlt shutdown-ports-on-disable enable command” on page 44](#)
- [“show mlt shutdown-ports-on-disable command” on page 44](#)

mlt shutdown-ports-on-disable enable command

The `mlt shutdown-ports-on-disable enable` command enables the shutdown of all ports in the MLT if the MLT is disabled.

The syntax for the `mlt shutdown-ports-on-disable enable` command is:

```
mlt shutdown-ports-on-disable enable
```

The `mlt shutdown-ports-on-disable enable` command is in the config command mode.

The `mlt shutdown-ports-on-disable enable` command has no parameters or variables.

no mlt shutdown-ports-on-disable enable command

The `no mlt shutdown-ports-on-disable enable` command disables the MLT shutdown ports on disable feature, and restores MLTs to the default operational mode.

The syntax for the `no mlt shutdown-ports-on-disable enable` command is:

```
no mlt shutdown-ports-on-disable enable
```

The `no mlt shutdown-ports-on-disable enable` command is in the config command mode.

The `no mlt shutdown-ports-on-disable enable` command has no parameters or variables.

show mlt shutdown-ports-on-disable command

The `show mlt shutdown-ports-on-disable` command displays the status of the MLT shutdown ports on disable feature.

The syntax for the `show mlt shutdown-ports-on-disable` command is:

```
show mlt shutdown-ports-on-disable
```

The `show mlt shutdown-ports-on-disable` command is in the `privExec` command mode.

The `show mlt shutdown-ports-on-disable` command has no parameters or variables.

[Figure 20](#) displays a sample output of the `show mlt shutdown-ports-on-disable` command.

Figure 20 show mlt shutdown-ports-on-disable command output

```
470-24T#show mlt shutdown-ports-on-disable
Trunk loop prevention is enabled.
```

Stack Monitor

The Stack Monitor feature provides the ability to monitor the health of a stack by monitoring the number of active units in the stack.

With stacked switches, MLT links are often connected to separate units in a distributed MLT (DMLT). In the event that the connections between switches in the stack fail, a situation can arise where the DMLT links are no longer connected to a stack, but to a combination of units that are no longer connected to each other. From the other end of the DMLT, the trunk links appear to be functioning properly. However, the traffic is no longer flowing across the cascade connections to all units and so connectivity problems can occur.

To address this issue, Release 3.6.2 software supports the Stack Monitor feature. When a stack is broken, the Stack Monitor feature allows the stack and any disconnected units from the stack to send SNMP traps. If the stack or the disconnected units are still connected to the network, they generate log events and send trap messages to the management station to notify the administrator of the event. Once the problem is detected, the stack and disconnected units continue to generate log events and send traps at a user-configurable interval until the situation is remedied (or the feature is disabled).

No actions are taken to change the current operation of the standalone units or the stack.

Control Parameters

You can configure the Stack Monitor by setting the following parameters:

- Stack Monitor enable and disable (default: disabled)
- stack size (range: 2 to 8 units; default: 2)
- trap and event logging interval (range: 30 to 300 seconds; default: 60)

The Stack Monitor settings are saved to NVRAM and distributed to all units within a stack.

When the Stack Monitor is enabled, the feature determines the number of units currently in the stack and automatically sets the correct value for the stack size parameter.

Once the feature is enabled, any change to the number of units in the stack triggers the sending of traps.

To ensure that disconnected switches can send traps, Nortel recommends that you set a switch IP on any units that have MLT links. This ensures that the units have the IP capability to send traps if they become standalone units. While this requires additional IP addresses, it provides the most robust operation.

Configuring Stack Monitor

You can use the CLI to configure the Stack Monitor feature. For details, refer to the following:

- [“show stack-monitor command” on page 47](#)
- [“stack-monitor command” on page 47](#)
- [“default stack-monitor command” on page 48](#)
- [“no stack-monitor command” on page 49](#)

For details on configuring the Stack Monitor feature using JDM, refer to the following:

- [“Stack Monitor tab” on page 49](#)

show stack-monitor command

The `show stack-monitor` command displays the status of the Stack Monitor feature.

The syntax for the `show stack-monitor` command is:

```
show stack-monitor
```

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

[Figure 21](#) displays a sample output of the `show stack-monitor` command.

Figure 21 show stack-monitor command output

```
470-24T#show stack-monitor
Status: disabled
Stack size: 2
Trap interval: 60
```

stack-monitor command

The `stack-monitor` command enables the Stack Monitor feature.

The syntax for the `stack-monitor enable` command is:

```
stack-monitor [enable] [stack-size <2-8>]
[trap-interval <30-300>]
```

The `stack-monitor` command is in the `config` command mode.

[Table 19](#) describes the parameters and variables for the `stack-monitor` command.

Table 19 `stack-monitor` command parameters and variables

| Parameters and variables | Description |
|---|--|
| <code>enable</code> | Enables Stack Monitoring. |
| <code>stack-size <2-8></code> | Sets the size of the stack to be monitored. Valid range is 2 to 8. |
| <code>trap-interval <30-300></code> | Sets the interval between traps, in seconds. Valid range is 30 to 300. |

default stack-monitor command

The default `stack-monitor` command sets the Stack Monitor parameters to their default values.

The syntax for the default `stack-monitor` command is:

```
default stack-monitor [enable] [stack-size]
[trap-interval]
```

The default `stack-monitor` command is in the `config` command mode.

[Table 20](#) describes the parameters and variables for the default `stack-monitor` command.

Table 20 default `stack-monitor` command parameters and variables

| Parameters and variables | Description |
|---|---|
| <code>enable</code> | Sets the Stack Monitor feature to disabled (the default state for the feature). |
| <code>stack-size</code> | Sets the size of the stack to be monitored to the default value: 2. |
| <code>trap-interval</code> | Sets the interval between traps to the default value: 60 seconds. |
| Note: If you do not specify a parameter for this command, all Stack Monitor parameters are set to their default values. | |

no stack-monitor command

The `no stack-monitor` command disables the Stack Monitor feature.

The syntax for the `no stack-monitor` command is:

```
no stack-monitor
```

or

```
no stack-monitor enable
```

The `no stack-monitor` command is in the config command mode.

The `no stack-monitor` command has no parameters or variables.

Stack Monitor tab

To open the Stack Monitor tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens with the System tab displayed.

- 3 Click the Stack Monitor tab.

The Stack Monitor tab opens.

Figure 22 Stack Monitor tab

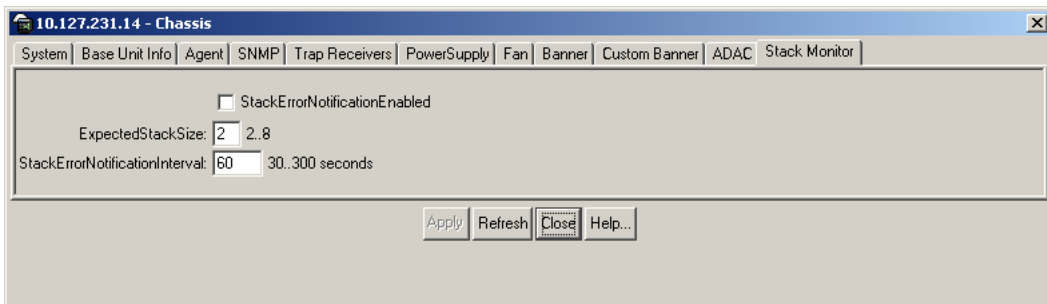


Table 21 describes the Stack Monitor tab fields.

Table 21 Stack Monitor tab fields

| Field | Description |
|--------------------------------|--|
| StackErrorNotificationEnabled | Enables or disables the Stack Monitoring feature. |
| ExpectedStackSize | Sets the size of the stack to be monitored. Valid range is 2 to 8. |
| StackErrorNotificationInterval | Sets the interval between traps, in seconds. Valid range is 30 to 300. |

Local ports shutdown while stacking

When a switch is joining a stack, DMLT and dynamic LAGs formed with LACP can still be created, because LACPDUs continue to be transmitted. This can result in a temporary traffic black hole (for a few seconds) until the switch fully joins the stack.

Release 3.6.2 software resolves this issue by momentarily shutting down the local ports on a switch before the switch joins a stack. Following a reset or power up, if the switch detects power on its stacking cables and, therefore, that it is connected to another unit, it shuts down all its local ports. When the ports are disabled, the port LEDs blink, similar to ports that are shut down. The ports are re-enabled when the unit finishes entering the stack formation or after a 60-second timeout (whichever comes first).

If the unit does not detect power on the stacking ports 20 seconds after it comes up, it allows its ports to forward traffic.

Fixed Issues in Release 3.6.2

The following issues have been fixed in this release:

- MLT ports can now be automatically disabled or enabled when the MLT Trunk Status is disabled or enabled. By disabling all ports in an MLT trunk, the possibility of creating loops is reduced. (Q00739670)
- The software performs checks on the ports of an MLT whenever the MLT is enabled, or if the stack is rebooted. If differences are detected, the MLT is disabled. An entry is now added to the non-volatile log of the Base Unit to indicate why the MLT is disabled. (Q01154324)
- MLT traffic distribution is now working correctly when three or more ports are configured and not all links are active in a DMLT bundle. (Q01116261)
- LACP traffic is no longer dropped after a stack is reset. (Q01043103)
- VLACP Ethertype can now be configured as hex value through CLI. (Q01180950)
- When MHMA is enabled, the switch no longer allows non-EAP clients connected to the port to gain access to the switch. (Q01174969)
- Ethernet Switch 460/470 no longer adds the sysName in the network-id field of the EAP Request Identity Packet. Therefore, Win XP clients no longer fail 802.1x Authentication when using PEAP-MSCHAPv2. (Q01072058-02)
- When the primary and secondary RADIUS server are configured for EAP authentication, the secondary server no longer sees any unnecessary requests from the switch. (Q01180650)
- Radius Authentication is now supported using Extensible Authentication Protocol over LAN (EAPOL) with PEAP. (Q01180650)
- After resetting a non-base unit port multiple times, EPM error messages no longer appear and the User Based Policy filter is set correctly. (Q01170710)
- Switch now correctly sends User Based Policy user name to EPM. (Q01101634)
- SNMP object ifHCOutOctets previously used only 32 bits, and now provides 64 bit counters. (Q01148220)
- Internal packets are no longer occurring under the Traffic-Separation. (Q01033226)
- Autosave can now be configured in ACG. (Q01034065)
- DMLT ports no longer stay in STP Learning mode after reboot. (Q01208297)

- Ethernet Switch 470 ports now come up if the port speed is set to 10M HDX and the following conditions are met:
 - Spanning Tree is disabled on the port
 - there is a moderate level of broadcast on the network

(Q01217147)

- COPS retry algorithm command has been implemented. (Q00878244)

The syntax of the new `cops retry algorithm` command is as follows:

```
cops retry [algorithm {round-robin | sequential}]
[count <0-32>] [interval <1-600>]
```

[Table 22](#) describes the parameters and variables for the `cops retry algorithm` command.

Table 22 cops retry algorithm command parameters and variables

| Parameters and variables | Description |
|--------------------------------------|--|
| algorithm {round-robin sequential} | Specifies a round-robin or sequential algorithm. |
| [count <0-32>] | Enter the retry count for use by the retry algorithm. |
| [interval <1-600>] | Enter the retry interval for use by the retry algorithm. |

The following two related commands have also been implemented:

- `no cops retry [count]`
- `default cops retry [algorithm] [count] [interval]`

Fixed Release 3.6 issues

- The incorrect option “ipv6” is no longer displayed for the `show audit log telnet` command. (Q01158092)
- When interconnecting two Ethernet Switch 460 units, the MAC address of the connected 460 now displays properly in the MAC address table when using the CLI. (Q01157912)
- Addresses learned on a port from another unit now age out immediately if the remote unit fails. (Q01141876)

Fixed Release 3.5 issues

- Release 3.6.2 software provides Web-based management support for RSTP and MSTP. (Q00885550)

Fixed Release 3.1 issues

- LACP traffic can now switchover immediately when using three or more standby links. (Q00783242)

Known issues and considerations in Release 3.6.2

The following are the known issues and considerations for this release:

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)

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 LACPDU 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 LACPDUs it receives. LACPDU 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 ([Figure 18 on page 40](#)), 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:

- In the ActorAdminState field, choose aggregation.
- Click Apply.
- 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.

LACP with Web-based Management

- In Web-based management, users cannot enable a second LAG if port settings such as tagging and port priority do not match the first LAG settings. (Q01255257)

To work around this issue, activate the LAG in two steps (two submits):

- First set the desired settings on the group of ports, and click Submit.
- Then set the LACP Mode to Active, and click Submit.

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)

Device Manager - PoE tab display for ports

With release 3.6.2 software on Ethernet Switch 460-PWR, the PoE tab display for single and for multiple ports has changed. The options in the Detection Status field have been updated, as described in [Table 23](#). The documentation and Device Manager online help have not been updated for this change. (Q01251705)

Table 23 Updated PoE tab item for ports

| Item | Description |
|------------------|---|
| Detection Status | <p>Displays the current status of the power-device detecting function on the port:</p> <ul style="list-style-type: none"> • disabled—detecting function disabled • searching—detecting function is enabled and the system is searching for a valid powered device on this port • deliveringPower—detection found a valid powered device and the port is delivering power • fault—power-specific fault detected on the port • test—detecting function is in test mode • otherFault—detecting function is idle due to fault <p>Note: Nortel recommends against using the test operational status.</p> |

Device Manager - delayed response with large Ethernet Switch 460-PWR stacks

With larger stacks of Ethernet Switch 460-PWR, Device Manager may delay its response to commands by a period of seconds. This delayed response also occurs when moving the mouse over toolbar items to display popup descriptions.

To work around this issue with larger Ethernet Switch 460-PWR stacks, either disable polling in Device Manager or increase the polling interval to a longer duration (for example, 300 seconds). (Q01232028)

Changes to Release 3.6 documentation

- *Configuring VLANs, Spanning Tree, and Multilink Trunking (217460-A)*

In this document, the following clarification is required for VLACP configuration:

Ethernet Switches 460 and 470 do not support multiple VLACP multicast MAC addresses.

On Ethernet Switches 460 and 470, VLACP has only one multicast MAC address (configured using the `vlacp macaddress` CLI command, or using the VLACP Global tab in JDM). This address is the Layer 2 destination address used for the VLACPDUs.

The port-specific MAC address parameter, `funcmac-addr`, is not a multicast MAC address (`funcmac-addr` is configured using the `vlacp port` CLI command or in JDM as the `EtherMacAddress` parameter, under VLACP tabs for single and multiple ports). The `funcmac-addr` parameter specifies the MAC address of the switch/stack to which this port is sending VLACPDUs.

You are not always required to configure `funcmac-addr`. If it is not configured, the first VLACP-enabled switch that receives the PDUs from a unit assumes that it is the intended recipient and processes the PDUs accordingly.

If you want an intermediate switch to drop VLACP packets, configure the `funcmac-addr` parameter to the desired destination MAC address. With `funcmac-addr` configured, the intermediate switches do not misinterpret the VLACP packets. (Q01192453)

- *Configuring VLANs, Spanning Tree, and Multilink Trunking (217460-A)*

In this document, the following additional clarification is required for VLACP configuration:

With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. However, if the `timeout-scale` is set to 1, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it (port timeout = [timeout-scale] x [periodic time]). Therefore, the delayed VLACPDU results in the link being blocked, then re-enabled when the packet arrives. (Q01201705)

To prevent this scenario from happening, set the timeout-scale to a value larger than 1.

- *Configuring VLANs, Spanning Tree, and Multilink Trunking (217460-A)*

On page 339, at the bottom of table 132 “vlacp port command parameters and variables,” the range of values indicated for VLACP ethertype should not read 1 to 65535. The valid values should be within the 4-digit hexadecimal range of 8101-81FF. (Q01180952)

- *Configuring VLANs, Spanning Tree, and Multilink Trunking (217460-A)*

In this document, the following clarification is required for Auto-Detection and Auto-Configuration (ADAC) of Nortel IP Phones (Q01225687):

[Table 24](#) describes the supported MAC address ranges for the ADAC feature. Any network device with a MAC address that falls within one of the ranges in this table is interpreted by the ADAC feature to be a Nortel IP Phone.

Table 24 Supported IP Phone MAC address ranges for ADAC

| From (low end) | --> | To (high end) |
|-------------------|-----|-------------------|
| 00-0A-E4-01-10-20 | --> | 00-0A-E4-01-23-A7 |
| 00-0A-E4-01-70-EC | --> | 00-0A-E4-01-84-73 |
| 00-0A-E4-01-A1-C8 | --> | 00-0A-E4-01-AD-7F |
| 00-0A-E4-01-DA-4E | --> | 00-0A-E4-01-ED-D5 |
| 00-0A-E4-02-1E-D4 | --> | 00-0A-E4-02-32-5B |
| 00-0A-E4-02-5D-22 | --> | 00-0A-E4-02-70-A9 |
| 00-0A-E4-02-D8-AE | --> | 00-0A-E4-02-FF-BD |
| 00-0A-E4-03-87-E4 | --> | 00-0A-E4-03-89-0F |
| 00-0A-E4-03-90-E0 | --> | 00-0A-E4-03-B7-EF |
| 00-0A-E4-04-1A-56 | --> | 00-0A-E4-04-41-65 |
| 00-0A-E4-04-80-E8 | --> | 00-0A-E4-04-A7-F7 |
| 00-0A-E4-04-D2-FC | --> | 00-0A-E4-05-48-2B |
| 00-0A-E4-05-B7-DF | --> | 00-0A-E4-06-05-FE |
| 00-0A-E4-06-55-EC | --> | 00-0A-E4-07-19-3B |
| 00-0A-E4-08-0A-02 | --> | 00-0A-E4-08-7F-31 |
| 00-0A-E4-08-B2-89 | --> | 00-0A-E4-09-75-D8 |
| 00-0A-E4-09-BB-9D | --> | 00-0A-E4-09-CF-24 |

Table 24 Supported IP Phone MAC address ranges for ADAC (continued)

| From (low end) | --> | To (high end) |
|-------------------|-----|-------------------|
| 00-0A-E4-09-FC-2B | --> | 00-0A-E4-0A-71-5A |
| 00-0A-E4-0A-9D-DA | --> | 00-0A-E4-0B-61-29 |
| 00-0A-E4-0B-BB-FC | --> | 00-0A-E4-0B-BC-0F |
| 00-0A-E4-0B-D9-BE | --> | 00-0A-E4-0C-9D-0D |

- *Configuring VLANs, Spanning Tree, and Multilink Trunking* (217460-A)

In the "Configuration Scenarios" section starting on page 78 (in Chapter 2 "Auto-Detection and Auto-Configuration of Nortel IP Phones"), the term *Untrusted Interface* should be replaced with *Unrestricted Interface* in all cases.

As a result, the affected sections should appear as follows:

At page 79 (top of page):

Auto-Configuration performs the following:

- creates an *Unrestricted Interface* with all Telephony ports (each time a new Telephony port is detected, it will be added to this interface)

At page 79 (bottom of page):

Auto-Configuration performs the following:

- For traffic coming from the Telephony ports:
 - creates an *Unrestricted Interface* with all Telephony ports (each time a new Telephony port is detected, it will be added to this interface)

At page 80 (top of page)

For traffic coming from the Uplink port:

- creates an *Unrestricted Interface* containing the Uplink port

At page 81 (top of page)

Auto-Configuration performs the following:

- For traffic coming from the Telephony ports:

— creates an *Unrestricted Interface* (Call Server interface ID will be a member of this interface group)

[...]

- For traffic coming from the IP Phones and Uplink port:

— creates an *Unrestricted Interface* containing all Telephony ports and Uplink port

- *Configuring VLANs, Spanning Tree, and Multilink Trunking (217460-A)*

The `show mlt spanning-tree` command is missing from the MLT configuration CLI commands. (Q01216647)

The `show mlt spanning-tree` command displays STP participation for MLTs. The syntax for the `show mlt spanning-tree` command is:

```
show mlt spanning-tree <1-6>
```

Where `<1-6>` specifies the MLT ID.

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

[Figure 23](#) displays a sample output of the `show mlt spanning-tree` command.

Figure 23 show mlt spanning-tree command output

```
470-24T#show mlt spanning-tree 1
STP Group      STP Learning
-----
1              Fast
```

- *Configuring and Managing Security (217104-A)*

On page 80, Figure 13 “EAPOL Security Configuration screen” should include the EAPOL User based policies field (Q01078856).

As well, Table 12 “EAPOL security configuration screen options,” should include the following related field definition:

| Option | Description |
|---------------------------|--|
| EAPOL User based policies | Enables or disables EAPOL user-based policies on the device. |

Outstanding issues from Release 3.6 software

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 for as long as the current configuration does not permit Auto-Configuration. (Q01131794)

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.

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: Users cannot configure passwords through ACG on the SSH image.
- ACG execution fails at the `eapol enable` command. (Q01043707)
Note: Users 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 must use the double backslash (`\\`) instead of a single backslash (`\`). (Q01031157)
- When upgrading from a Telnet CLI session, the user can intermittently 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 and Q01244616)

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 an EAPOL multihost-enabled port, and a user enables EAPOL multihost again on all ports (including the port already enabled), PCs connected to the multihost port 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 an 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)

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 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 must 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 for the time of creation only 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. You must assign Spanning Tree settings as part of the MLT or LAG. A new command controls Spanning Tree settings per MLT or LAG. Spanning tree is 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 is not 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 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 can report FCS errors and Frame errors for the respective port when connected to an IP handset that is unpowered. Also, the Link and Activity LEDs of that port can blink. These errors are reported as a result of filters inbuilt to the IP handsets 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 resolves 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)

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; however, all ports 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, an 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 is always Forwarding and MLT 2 is 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 inconsistent 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. (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. (Q00922934)
 - 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 and 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 can 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 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 results 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` displays 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 can result in a port remaining in a down condition. (Q00630821)

-
- MLT/LAG console menu screen can 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* (217108-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* 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 Reader.

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. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- 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 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.

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 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 by using an Express Routing Code

An Express Routing Code (ERC) is available for many Nortel 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 the ERC for your product or service, go to:

www.nortel.com/erc

