



Nortel Ethernet Routing Switch 4500 Series

Overview — System Configuration

ATTENTION

Clicking on a PDF hyperlink takes you to the appropriate page. If necessary, scroll up or down the page to see the beginning of the referenced section.

Document status: Standard
Document version: 02.01
Document date: 23 February 2007

Copyright © 2007, Nortel Networks
All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks

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

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.

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.

Revision History

Date Revised	Version	Reason for revision
February 2007	02.01	New document for Nortel Ethernet Routing Switch 4500.

6 Revision History

Contents

Preface	13
Nortel Ethernet Routing Switch 4500 Series	14
Related publications	14
Finding the latest updates on the Nortel Web site	16
How to get help	16
Getting help from the Nortel Web site	16
Getting help over the phone from a Nortel Solutions Center	16
Getting help from a specialist using an Express Routing Code	17
Getting help through a Nortel distributor or reseller	17
<hr/>	
4500 Series user interfaces	19
Command line interface	19
Accessing the CLI	19
CLI command modes	21
Java Device Manager	22
Obtaining the Java Device Manager	23
Installing the Java Device Manager	24
Starting the Java Device Manager	36
Configuring Device Manager properties	37
Opening a Switch with the Java Device Manager	40
Device Manager interface components	42
Shortcut menus	47
Status bar	48
Using the buttons in Device Manager screens	48
Editing objects	49
Telnet session to a switch	55
Opening an SSH connection to the switch	55
Trap log	55
Accessing the Web-based Management Interface	56
Device Manager Online Help	56
Web-based Management Interface	56
Accessing the Web-based Management Interface	57
Web-based Management Interface layout	58

Basic configuration tasks	65
Factory default configuration	65
Setting user access limitations	71
Setting user access limitations using the CLI	71
Setting user access limitations using the Web-based Management Interface	75
Updating switch software	81
Changing switch software in the CLI	82
Changing switch software in the Java Device Manager	84
Changing switch software in the Web-based Management Interface	87
LED activity during software download	89
Setting TFTP parameters	89
Setting a default TFTP server	89
Displaying the default TFTP server	90
Clearing the default TFTP server	90
Working with configuration files	90
Configuration files in the CLI	90
Configuration files in the JDM	93
Configuration files in the Web-based Management Interface	97
Automatically downloading a configuration file	101
Terminal setup	103
Setting Telnet access	104
telnet-access command	104
no telnet-access command	105
default telnet-access command	106
Setting server for Web-based management	106
web-server command	106
no web-server command	107
Setting boot parameters	107
boot command	107
Defaulting to BootP-when-needed	108
Configuring with the command line interface	108
Customizing the CLI banner	110
show banner command	110
banner command	110
no banner command	111
Displaying complete GBIC information	114
Displaying hardware information	114
Shutdown command	114
Reload command	116
CLI Help	117

About the Nortel Ethernet Routing Switch 4500 Series	119
Hardware features	119

Cooling fans	119
Redundant power supply	120
DC-DC Converter Module	120
Stacking capabilities	120
Auto Unit Replacement	121
AUR function	122
Configuring AUR using the CLI	128
Configuring AUR using Device Manager	129
Agent Auto Unit Replacement	130
Features of the Nortel Ethernet Routing Switch 4500 Series	131
Flash memory storage	131
Policy-enabled networking	132
Power over Ethernet	132
Virtual Local Area Networks	132
Spanning Tree Protocol groups	133
Rapid Spanning Tree Protocol	134
Multiple Spanning Tree Protocol	134
Trunk groups	135
Security	135
Port mirroring	136
Auto-MDI/X	136
Auto-polarity	136
Autosensing and autonegotiation	137
ASCII configuration file	139
Displaying unit uptime	141
Port naming	142
Port error summary	142
IP address for each unit in a stack	142
BootP mode	142
Web Quick Start	142
Simple Network Time Protocol	143
Ping enhancement	144
Supported standards and RFCs	144
Standards	144
RFCs	144

Power over Ethernet	147
PoE overview	148
Port power priority	149
External power source	150
Stacking	150
Power pairs	150
Power availability	151
Internal power source only option	151

External power source only option	152
Power sharing option	153
Power Supply Unit (PSU) option	154
Diagnosing and correcting PoE problems	155
Messages	156
Connecting the PSU	156
Power management	157
Configuring PoE using the CLI	158
Set port power enable or disable	159
Set port power priority	159
Set power limit for channels	159
Set traps control	160
Show main power status	160
Set power usage threshold	160
Setting PoE detection method	161
Show port power status	161
Show port power measurement	161
Viewing PoE ports using the JDM	162
Configuring PoE using the JDM	163
Configuring PoE using the Web-based Management Interface	163
Configuring power management on the switch	163
Configuring power management for the ports	165

Switch administration tasks **169**

General switch administration using the Command Line Interface	169
Multiple switch configurations	170
Assigning and clearing IP addresses	171
Assigning and clearing IP addresses for specific units	174
Displaying Interfaces	175
Setting port speed	176
Enabling Autotopology	179
Enabling flow control	180
Enabling rate-limiting	183
Using Simple Network Time Protocol	185
Clock configuration	189
Custom Autonegotiation Advertisements	189
Connecting to Another Switch	190
Domain Name Server (DNS) Configuration	192
General Switch Administration using the Web-based Management Interface	194
Viewing stack information	194
Viewing summary switch information	196
Changing stack numbering	197
Identifying unit numbers	199
Configuring BootP, IP, and gateway settings	200

Modifying system settings	203
Managing remote access by IP address	205
General Switch Administration using the JDM	207
Viewing unit information	208
Viewing PoE information	209
Viewing switch IP information	209
IP Globals tab	209
IP Addresses tab	210
IP ARP tab	211
IP TCP tab	212
IP TCP Connections tab	213
IP UDP Listeners tab	214
Viewing SFP GBIC ports	215
Editing the chassis configuration	215
Editing and viewing switch ports	229
Editing and viewing switch PoE configurations	237
Editing Bridging Information	240
Configuring SNTP	245
Viewing topology information using Device Manager	247
Topology tab	247
Topology Table tab	248

Link Layer Discovery Protocol (802.1ab)

251

Link Layer Discover Protocol (IEEE 802.1ab) Overview	251
LLDP operational modes	252
Connectivity and management information	252
Configuring LLDP using the CLI	255
lldp command	255
lldp port command	256
lldp tx-tlv command	257
lldp tx-tlv dot1 command	257
lldp tx-tlv dot3 command	258
default lldp command	258
default lldp port command	259
default lldp tx-tlv command	259
default lldp tx-tlv dot1 command	260
default lldp tx-tlv dot3 command	261
no lldp port command	261
no lldp tx-tlv command	262
no lldp tx-tlv dot1 command	262
no lldp tx-tlv dot3 command	262
show lldp command	262
show lldp port command	264
Configuring LLDP using Device Manager	269

12 Contents

Viewing and configuring LLDP global and transmit properties	269
LLDP_Port_dot1 dialog box	294
LLDP_Port_dot_3 dialog box	305

Preface

This guide provides information and instructions about the basic system configuration on the Nortel* Ethernet Routing Switch 4500 series. Before you start the configuration process, consult the documentation included with the switch and the product release notes (see "[Related publications](#)" (page 14)) for errata.

The topics in "[Related topics](#)" (page 13) relate to the system configuration process but are not described in depth in this guide. For more information about a specific topic, see the book for that specific topic.

Related topics

Topic	Book
Switch security	<i>Nortel Ethernet Routing Switch 4500 Series Security — Configuration</i> (NN47205-505)
VLANs	<i>Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking</i> (NN47205-501)
Spanning Trees and Spanning Tree Groups	<i>Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking</i> (NN47205-501)
MultiLink Trunking	<i>Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking</i> (NN47205-501)
Quality of Service	<i>Nortel Ethernet Routing Switch 4500 Series Configuration — Quality of Service</i> (NN47205-504)
IP Filtering	<i>Nortel Ethernet Routing Switch 4500 Series Security — Configuration</i> (NN47205-505)

Nortel Ethernet Routing Switch 4500 Series

"4500 Series Switch platforms" (page 14) outlines the switches that are part of the Nortel Ethernet Routing Switch 4500 series of switches.

4500 Series Switch platforms

Model	Model-specific features
4526FX	24 100BaseFX ports (MTRJ connector) plus 2 10/100/1000 SFP combo ports Redundant power slot for DC/DC converter installation
4550T	48 10/100BaseTX RJ-45 ports plus 2 10/100/1000 SFP combo ports Redundant power slot for DC/DC converter installation
4550T-PWR	48 10/100BaseTX RJ-45 ports with Power over Ethernet plus 2 10/100/1000 SFP combo ports Integrated redundant power connector for RPS 15 cable connection
4548GT	48 10/100/1000BaseTX RJ-45 ports and 4 shared SFP ports Redundant power slot for DC/DC converter installation
4548GT-PWR	48 10/100/1000BaseTX RJ-45 ports with PoE and 4 shared SFP ports Integrated redundant power connector for RPS 15 cable connection

Related publications

For more information about the management, configuration, and use of the Nortel Ethernet Routing Switch 4500 Series, see the publications listed in "[Nortel Ethernet Routing Switch 4500 Series documentation](#)" (page 14).

Nortel Ethernet Routing Switch 4500 Series documentation

Title	Description	Part Number
<i>Nortel Ethernet Routing Switch 4500 Series Regulatory Information</i>	Regulatory and safety information for the Nortel Ethernet Routing Switch 4500 Series.	NN47205-100
<i>Nortel Ethernet Routing Switch 4500 Series Installation</i>	Instructions to install a switch in the Nortel Ethernet Routing Switch 4500 Series. This guide also provides an overview of hardware important to the installation, configuration, and maintenance of the switch.	NN47205-300

Title	Description	Part Number
<i>Nortel Ethernet Routing Switch 4500 Series Release Notes — Software Release 5.0</i>	An overview of new features, fixes, and limitations of the 4500 Series switches. Also included are supplementary documentation and document errata.	NN47205-400
<i>Nortel Ethernet Routing Switch 4500 Series Overview — System Configuration</i>	General instructions to configure switches in the 4500 Series that are not covered by the other documentation.	NN47205-500
<i>Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking</i>	Instructions to configure spanning and trunking protocols on 4500 Series switches.	NN47205-501
<i>Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring</i>	Instructions to configure, implement, and use system monitoring on 4500 Series switches.	NN47205-502
<i>Nortel Ethernet Routing Switch 4500 Series Configuration — Quality of Service</i>	Instructions to configure and implement QoS and filtering on 4500 Series switches.	NN47205-504
<i>Nortel Ethernet Routing Switch 4500 Series Security — Configuration</i>	Instructions to configure and manage security for switches in the 4500 Series.	NN47205-505
<i>DC-DC Converter Module for the Baystack 5000 Series Switch</i>	Instructions to install and use the DC-DC power converter.	215081-A
<i>Installing the Nortel Ethernet Redundant Power Supply Unit 15</i>	Instructions to install and use the Nortel Ethernet RPS 15.	217070-A
<i>Installing SFP and XFP Transceivers and GBICs</i>	Instructions to install and use small form-factor pluggable transceivers and gigabit interface converters.	318034-D

Finding the latest updates on the Nortel Web site

The content of this documentation was current at the time of release. To check for updates to the documentation and software for the Nortel Ethernet Routing Switch 4500 Series, go to www.nortel.com/support and use the following procedure.

Step	Action
1	Select Ethernet Routing Switches from the Product Categories list in section 1.
2	Select Ethernet Routing Switch 4500 from section 2.
3	Select one of the following from section 3. <ul style="list-style-type: none"> • Documentation • Software
4	Click Go .

—End—

How to get help

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

Getting help from the Nortel Web site

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

www.nortel.com/support

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

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

Getting help over the phone from a Nortel Solutions Center

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

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

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

www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

4500 Series user interfaces

The switch administrator can choose from three interfaces to configure switches on the Nortel Ethernet Routing Switch 4500 Series switches. This chapter provides an introduction to each user interface, instructions for use, and instructions for installation if applicable.

This chapter contains the following topics:

- ["Command line interface" \(page 19\)](#)
- ["Java Device Manager" \(page 22\)](#)
- ["Web-based Management Interface" \(page 56\)](#)

Command line interface

The command line interface (CLI) is the text-based interface used in switch configuration and management.

The following sections describe CLI access and commands:

- ["Accessing the CLI" \(page 19\)](#)
- ["CLI command modes" \(page 21\)](#)

Accessing the CLI

Access the CLI by either of the following:

- direct console connection to the switch
- remote connection to switch using a Telnet protocol

To connect to the CLI, perform the following procedure.

Step	Action
1	Connect to the switch over a Telnet session or through the console port. <ol style="list-style-type: none"> a. If you connect remotely to the switch through the Telnet protocol, ensure that access through this protocol is enabled and that the IP address of the switch is valid.

CLI command modes

The CLI has four command modes based on the level of permissions assigned to you. The password that you use to log on determines the level of permissions. Each command mode provides access to a specific group of commands.

The four command modes, from most to least restricted, are

- **User EXEC mode**

The User EXEC mode (also referred to as exec mode) is the default CLI command mode. User EXEC is the initial mode of access when you first turn on a switch. User Exec mode provides a limited subset of CLI commands, is the most restrictive CLI mode, and has few privileges.

- **Privileged EXEC mode**

Use Privileged EXEC mode (also referred to as privExe mode) to perform basic switch-level management tasks, such as downloading software images, setting passwords, and booting the switch.

- **Global Configuration mode**

Use Global Configuration mode (also referred to as config mode) to set and display general configurations for the switch, such as IP address, SNMP parameters, Telnet access, and VLANs.

- **Interface Configuration mode**

Use Interface Configuration mode (also referred to as if-config mode) to configure parameters, such as speed, duplex mode, and rate-limiting, for each port or VLAN.

The Command modes table lists the four command modes, the prompt for each, the CLI commands to use to proceed to the next mode, and the CLI commands to enter and exit the modes. Each switch displays a prompt specific to the switch type. The prompts displayed in the table are for a Nortel Ethernet Routing Switch 4500 Series 4548-GT-PWR switch.

Command modes

Current command mode	CLI prompt	To move up to the next mode	To leave current mode
User EXEC	4548GT-PWR>	Use the enable command to move to the Privileged EXEC mode.	Use one of the following commands to close the CLI session: <ul style="list-style-type: none"> • exit • logout

Current command mode	CLI prompt	To move up to the next mode	To leave current mode
Privileged EXEC	4548GT-PWR#	Use the configure command to move to the Global Configuration mode. You are prompted to specify your connection: example—terminal or console.	Use the exit command to return to the User EXEC mode. Use the logout command to close the CLI session.
Global Configuration	4548GT-PWR(config)#	Use the interface fastethernet all command to move to the Interface Configuration mode.	Use the exit command to return to the Privileged EXEC mode. Use the logout command to close the CLI session.
Interface Configuration	4548GT-PWR(config-if)#	This is the top level.	Use the exit command to return to the Global Configuration mode. Use the end command to return to the Privileged EXEC mode. Use the logout command to close the CLI session.

Java Device Manager

The Java Device Manager (JDM) is a graphical user interface (GUI) application used in switch configuration and management operations. The JDM provides a real-time graphical representation of the front panel of the switch being administered. From this view, you can perform all switch configuration tasks.

Unlike the CLI and Web-based Management Interface, the JDM is a client application that resides on a computer with network access to the devices to be monitored and configured by an administrator. This being the case, any user who wishes to access a Nortel Ethernet Routing Switch 4500 Series through the JDM must install the application on an appropriate computer.

This section contains the following topics:

- "Obtaining the Java Device Manager" (page 23)
- "Installing the Java Device Manager" (page 24)
- "Starting the Java Device Manager" (page 36)
- "Configuring Device Manager properties" (page 37)
- "Opening a Switch with the Java Device Manager" (page 40)
- "Device Manager interface components" (page 42)

Obtaining the Java Device Manager

If the JDM is not already installed on the switch management computer, you can download it from the Nortel Web site.

To obtain the JDM, perform the following procedure:

Step	Action
1	Open a new Web browser window and, in the Address area, type http://www.nortel.com/support .
2	If the Browse product support tab is not already selected, click it.
3	From the list, provided in the product family box, select Nortel Ethernet Routing Switch .
4	From the product list select Nortel Ethernet Routing Switch 4500 Series.
5	From the content list, select Software .
6	Click Go . <i>The available software list appears.</i>
7	The available software list displays all software associated with the selected switch family, in descending chronological order (newest to oldest).
8	To select the newest JDM software version, click the link next to the version that appears first in the list.

- 9 Software specific to each operating system environment is listed. To download the correct version for the operating system that runs on the switch administration computer, click the associated link.
- 10 When the prompt screen appears, select *Save the file to the local file system*.
The JDM software download starts.
- 11 When the download is complete, see "[Installing the Java Device Manager](#)" (page 24).

—End—

Installing the Java Device Manager

After you obtain the latest version of the JDM, you must install it on the computer designated for switch administration. Installation procedures vary depending on the operating system environment of the administrative computer. Refer to the appropriate section for installation procedures.

- "[Installing the JDM in a Microsoft Windows Environment](#)" (page 24)
- "[Installing the JDM in a UNIX Environment](#)" (page 30)

Before you start the installation procedure in any operating system environment, ensure that you unistall all previous versions of the software and that you install the new version of the application in a new directory.

Installing the JDM in a Microsoft Windows Environment

The minimum system requirements for installing the JDM in a Microsoft Windows environment are

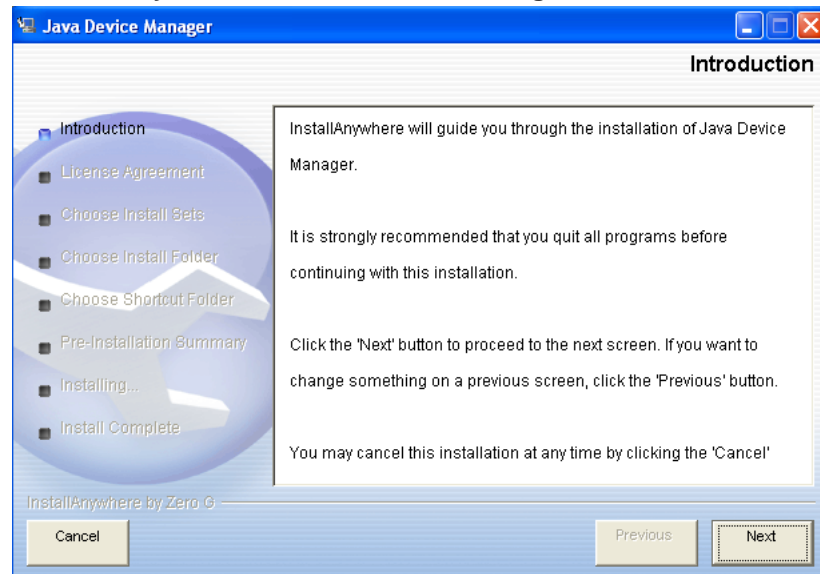
- **Operating System Version**
 - Windows NT, Windows 95, Windows 98, Windows2000, or WindowsXP
- **CPU Requirements**
 - Pentium II 350 MHz or better
- **Memory Requirements**
 - 256 MB DRAM or better
- **Hard Drive Requirements**
 - 300 MB of available space

To install the Java Device Manager in a Windows environment, perform the following procedure.

Step	Action
1	Close all programs.
2	Locate the downloaded executable file on the local computer.
3	Double-click the <code>jdm_xxx.exe</code> executable file to begin the installation process. In the downloaded file, the <code>xxx</code> is substituted with the version number of the software.
4	The installation program is loaded. When the program is ready to proceed with the installation, a message box similar to the one illustrated in "Introductory Windows installation message box" (page 25) appears. Follow all instructions on this screen before you proceed with the installation.

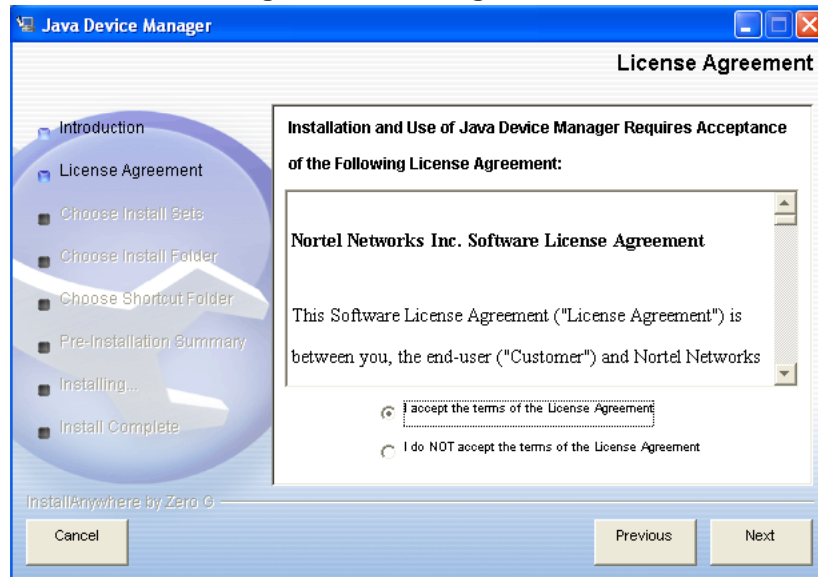
Click **Next** when you are ready.

Introductory Windows installation message box



- 5 The license agreement message box appears.
- Accept the license agreement, which is mandatory to install the JDM. Read the license agreement fully. Indicate your acceptance by selecting **I accept the terms of the License Agreement**. To proceed, click **Next**.*
- "Windows License Agreement message box" (page 26) illustrates an example of this message box.*

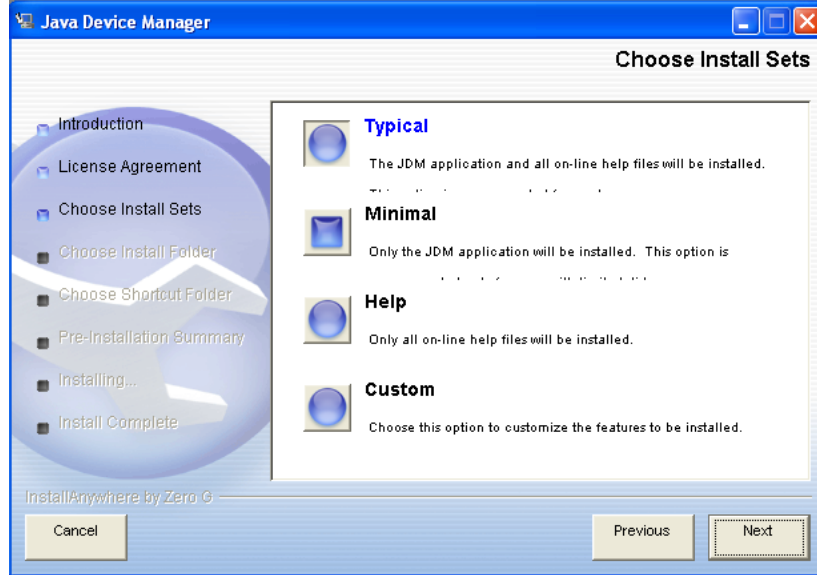
Windows License Agreement message box



- 6 After you accept the license agreement, the next dialog box (see "Windows Choose Install Sets dialog box" (page 27)) prompts you for an installation set. Although four options are available, Nortel recommends that you select **Typical** to ensure that all application components are installed. If you require a more specialized installation, select one of the other options. The four options are as follows:
- **Typical**—Install all software components and online Help is installed.
 - **Minimal**—Install only the software; do not install online Help.
 - **Help**—Install only online Help.
 - **Custom**—Select the software components and online Help that you want to install.

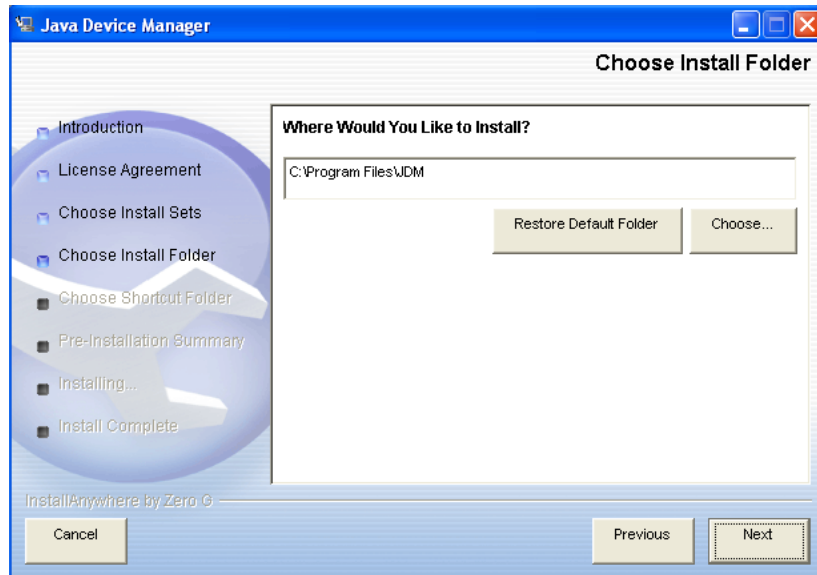
Click **Next** to proceed.

Windows Choose Install Sets dialog box



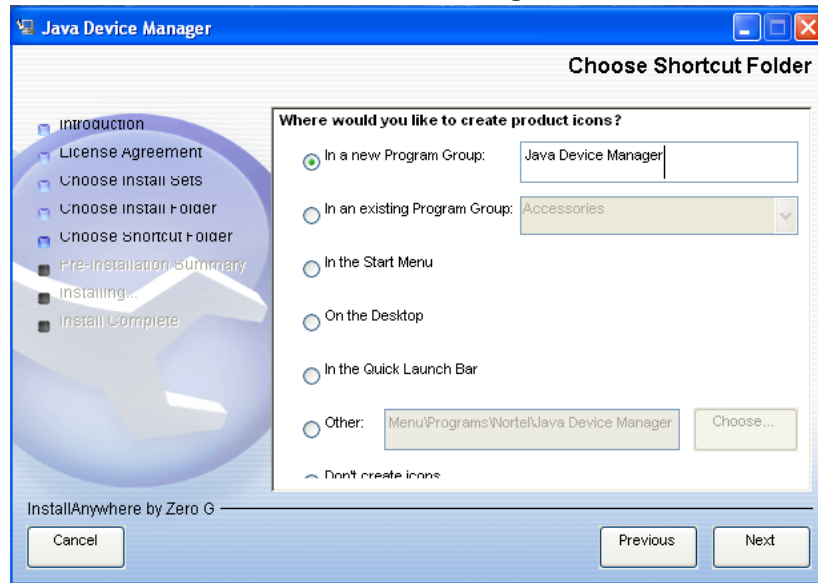
- 7 On the next dialog box (see "[Windows Choose Install Folder dialog box](#)" (page 27)), type a location on the local file system to install the JDM, or select a location by clicking **Choose**. Click **Restore Default Folder** to restore the default installation location at any time. Click **Next** to proceed.

Windows Choose Install Folder dialog box



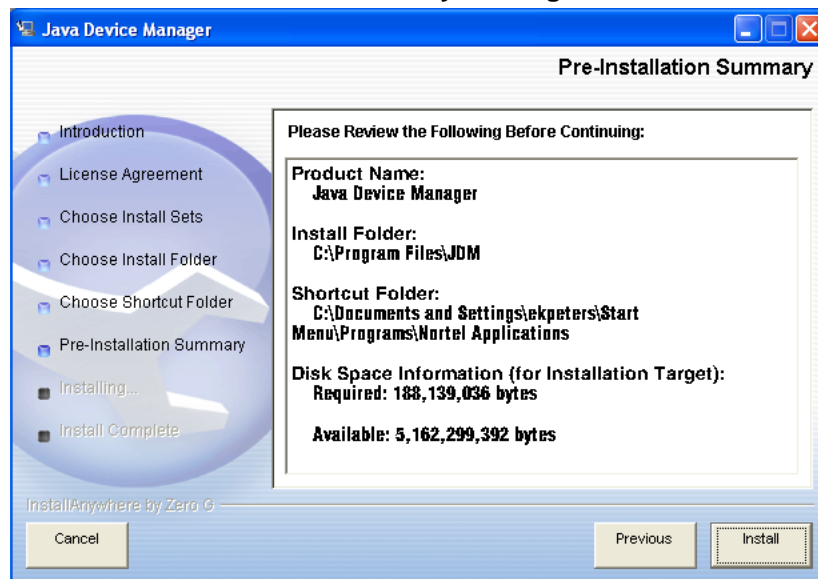
- 8 On the dialog box (see "[Windows Choose Shortcut Folder dialog box](#)" (page 28)), select a location for the placement of icons in the Start menu. After you make this selection, click **Next** to proceed.

Windows Choose Shortcut Folder dialog box



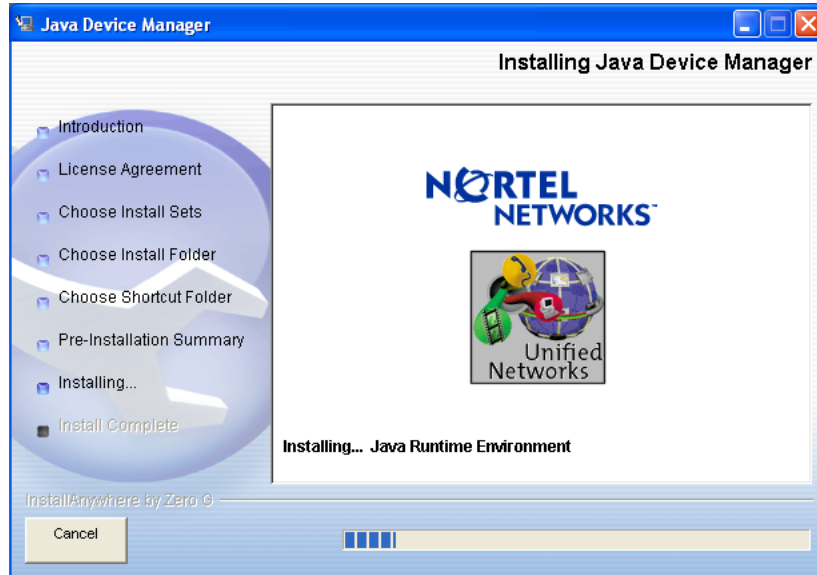
- 9 Confirm the previous selections on the Pre-Installation Summary message box (see "[Windows Pre-Installation Summary message box](#)" (page 28)). If all selections are accurate, click **Install** to begin installing the JDM on the local computer. If changes are necessary, click **Previous** to return to the screens in question.

Windows Pre-Installation Summary message box



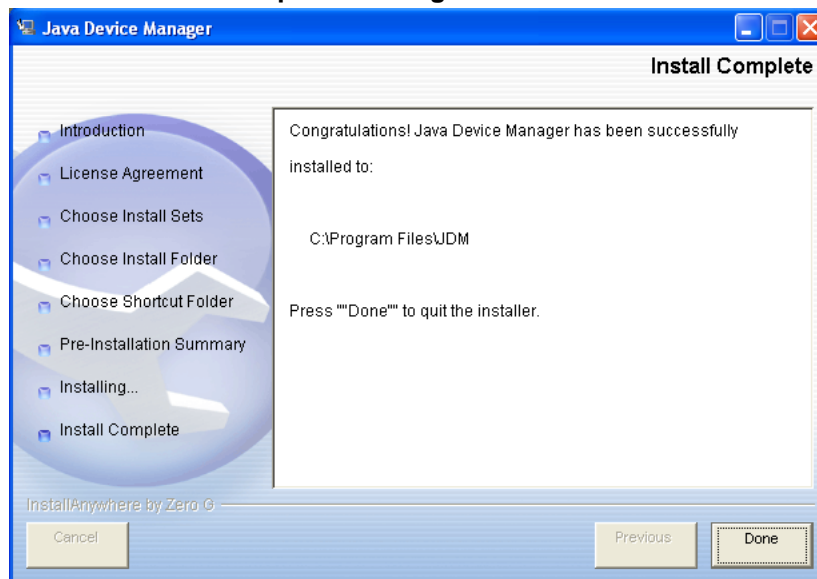
- 10 During the installation process, the message box illustrated in "[Windows Installation Progress message box](#)" (page 29) shows the progress of the installation.

Windows Installation Progress message box



- 11 When the installation process is finished, the message box displayed in "Windows Install Complete message box" (page 29) appears. Click **Done** to complete the installation.

Windows Install Complete message box



—End—

Installing the JDM in a UNIX Environment

The minimum system requirements for installing the JDM in a UNIX environment are:

- **Operating System Version**
 - Sun Solaris 2.7.x (or higher), Linux Kernel 2.2 (or higher), or HP-UX 11.x (or higher)
- **Memory Requirements**
 - 128 MB DRAM or better
- **Hard Drive Requirements**
 - 4 MB available in a temporary directory for installation
 - 300 MB available in the installation directory

If the UNIX workstation on which you install the JDM uses the Sun Solaris operating system, see the section "[Installing Solaris Patches](#)" (page 35) before you start the installation. When this procedure is complete, or if Sun Solaris does not run on the UNIX workstation, install the JDM by performing the following procedure.

Step	Action
------	--------

- | | |
|---|---|
| 1 | Close all programs. |
| 2 | Locate the downloaded executable file on the local computer. |
| 3 | Run the executable file to begin the installation. Depending on the UNIX operating system in use, the file name takes one of three forms. " UNIX JDM installation files " (page 30) outlines the form each file name takes. |

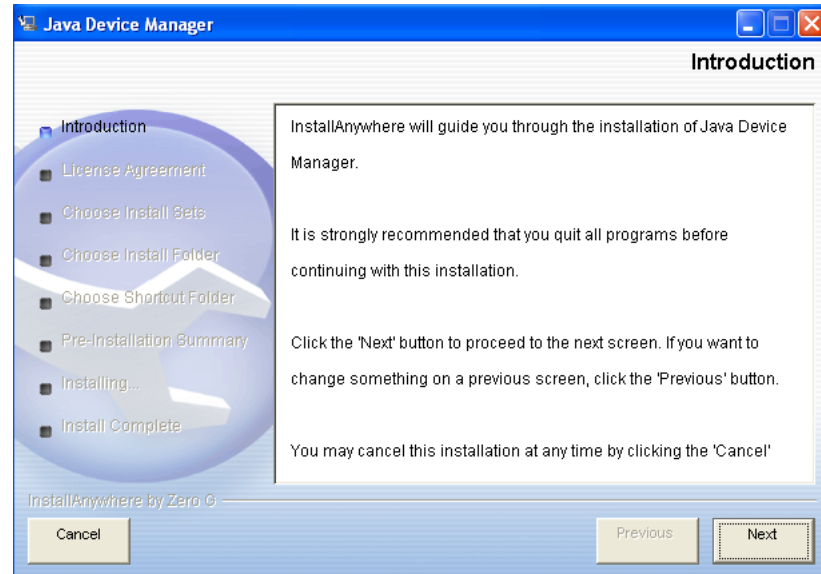
UNIX JDM installation files

Operating System	File Name
Sun Solaris	jdm_XXXX_solaris_sparc.sh
Linux	jdm_XXXX_linux.sh
HP-UX	jdm_XXXX_hpux_pa-risc.sh
In the downloaded file, substitute XXXX in the table with the version number of the JDM that you download.	

- | | |
|---|--|
| 4 | The installation program is loaded. When the program is ready to proceed with the installation, a message box similar to the one illustrated in " Introductory UNIX installation message box " (page |
|---|--|

31) appears. Follow all instructions on this screen before you proceed with the installation. Click **Next** when you are ready.

Introductory UNIX installation message box



The next message box requests acceptance of the license agreement that governs the JDM software. Acceptance of this software license is mandatory to install the JDM.

- 5 Read the license agreement fully and indicate acceptance by selecting **I accept the terms of the License Agreement**. To proceed, click **Next**.

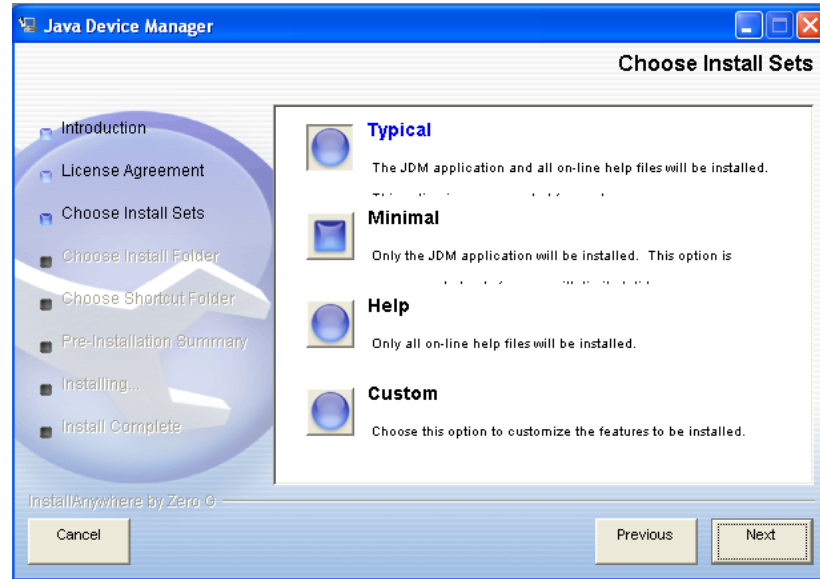
"UNIX License Agreement message box" (page 32) illustrates an example of this message box.

UNIX License Agreement message box

- 6 After you accept the license agreement, the next dialog box (see "UNIX Choose Install Sets dialog box" (page 33)) prompts you for an installation set. Although four options are available, Nortel recommends that you select **Typical**, to ensure that you install all application components. If you require a more specialized installation, select one of the other options. The four options are as follows:
- **Typical**—Install all software components and online Help.
 - **Minimal**—Install only the software; do not install online Help.
 - **Help**—Install only online Help.
 - **Custom**—Select the software components and online Help that you want to install.

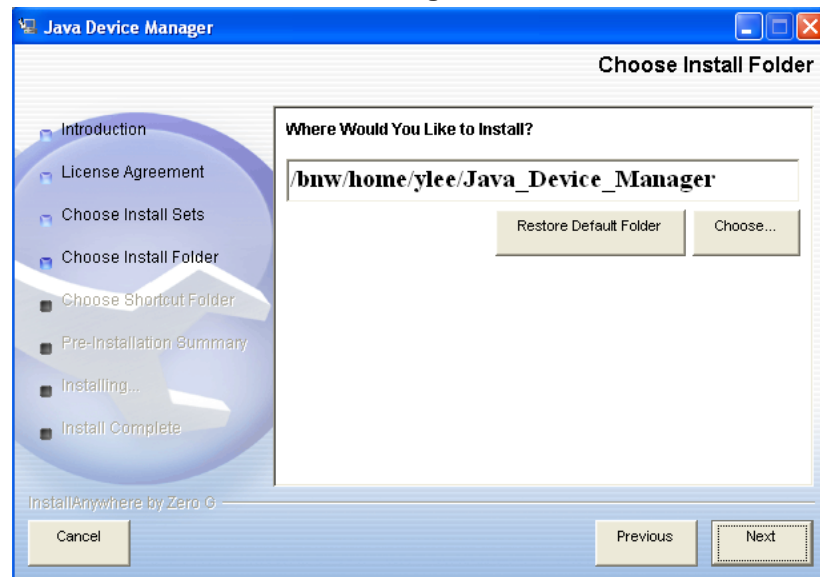
Click **Next** to proceed.

UNIX Choose Install Sets dialog box



- 7 On the next dialog box (see "UNIX Choose Install Folder dialog box" (page 33)), type a location on the local file system to install the JDM, or select a location by clicking **Choose**. Click **Restore Folder Default** to restore the default installation location at any time. Click **Next** to proceed.

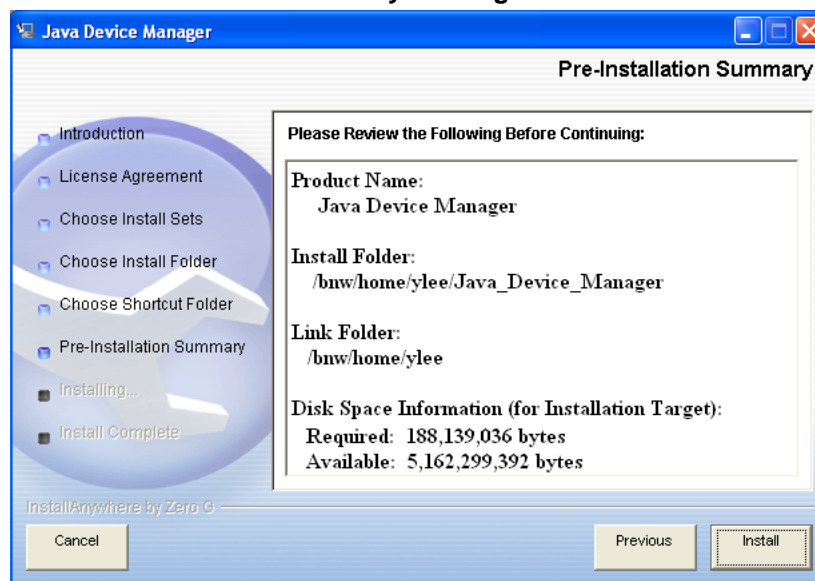
UNIX Choose Install Folder dialog box



- 8 Confirm the previous selections on the Pre-Installation Summary message box (shown in "UNIX Pre-Installation Summary message box" (page 34)). If all selections are accurate, click **Install** to begin

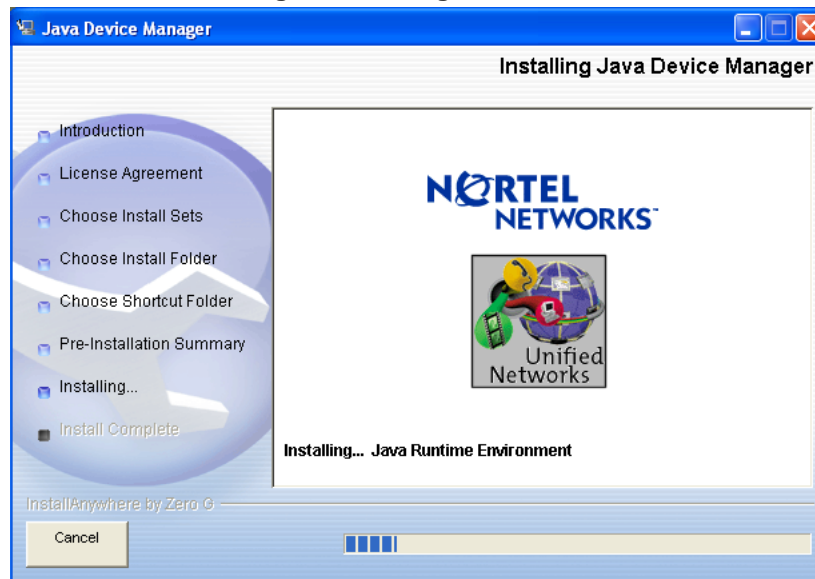
installing the JDM on the local computer. If changes are necessary, click **Previous** to return to the dialog boxes in question.

UNIX Pre-Installation Summary message box

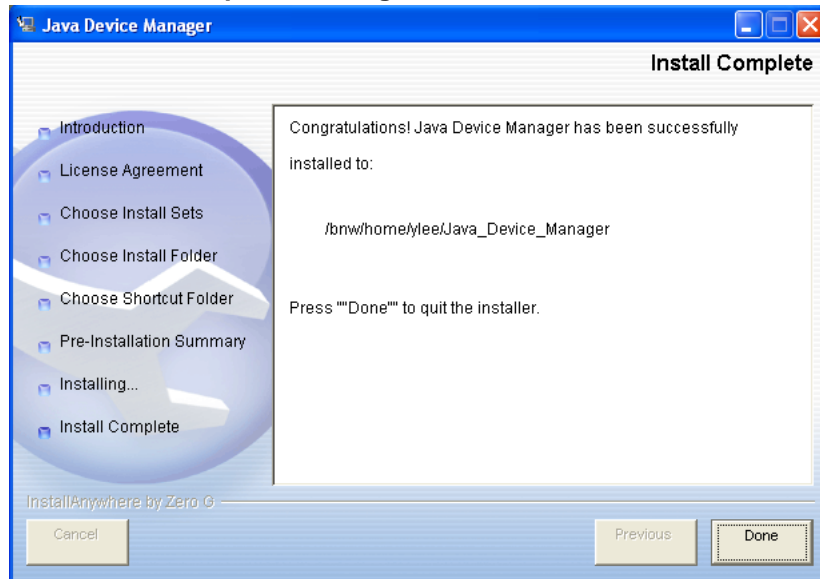


- 9 During the installation, the message box illustrated in "UNIX Installation Progress message box" (page 34) shows the progress.

UNIX Installation Progress message box



- 10 When the installation finishes, the message box shown in "UNIX Install Complete message box" (page 35) appears. Click **Done** to complete the installation.

UNIX Install Complete message box

—End—

Installing Solaris Patches For SPARC versions 5.7 and 5.8, you must install operating system patches for Sun Solaris before you install the JDM. Consult the system administrator or a network technician to determine whether these patches are installed on the workstation. You need apply these patches to the workstation only once.

To proceed with patch installation, perform the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | Use the <code>uname -a</code> command on the Solaris workstation to determine the version of Solaris that is installed. |
| 2 | Open a Web browser window and type <code>http://sun-solve.sun.com</code> in the Address area. SunSolve is the Sun Microsystems technical support Web site. Use the tools on this Web page to find the patches associated with the version of Solaris running on the workstation. Read and follow all directions carefully. |

—End—

Starting the Java Device Manager

After the JDM is successfully installed, it is ready to connect to and administer switches in the network. The procedure to run the JDM depends on the operating system environment in which it was installed. "JDM execution options" (page 36) describes how to start the JDM in the two main operating system environments supported.

JDM execution options

Operating System	JDM Execution Options
Microsoft Windows	<ul style="list-style-type: none"> If you selected the installation defaults from the Windows taskbar, select Start > Programs > Nortel > Java Device Manager > DM. Otherwise, select the commands that reflect the icon placement specified during installation.
UNIX	<ul style="list-style-type: none"> From the installation directory type the command <code>./JDM</code>. Create the environment variable JDM_HOME and include it in the search path. This variable is used to run the JDM from any directory on the computer. Consult the operating system documentation for the steps to complete this process.

After the JDM successfully starts, the JDM main window ("JDM main window" (page 36)) appears.

JDM main window



There are two ways to access the default properties settings from the JDM main window.

- Before any device has been accessed, select **Device > Properties > Current**.
- After a device has been accessed, select **Device > Properties > Devices**.

Configuring Device Manager properties

Device Manager uses the Simple Network Management Protocol (SNMP) to configure and manage Ethernet Routing Switch 4500 Series devices. You can use the Device Manager Properties dialog box to configure important communication parameters, such as the polling interval, timeout, and retry count. You can set these parameters at any time before or after you open a device.

Before you have accessed a device, to set the Device Manager properties:

Step Action

- 1 From the **Device Manager** menu bar, choose **Device > Properties > Current**.

The **Default Properties** dialog box appears.

- 2 Configure the properties as described in the Default Properties table.

3 Click **OK**.**Default Properties fields**

Area	Item	Description
Polling	Status Interval	Interval at which statistics and status information is gathered. For a full stack, set this interval from 120 to 300 seconds.
	Hotswap Detect every	The frequency at which Device Manager polls for hot swap module information. This value is relative to the Status Interval value. For example, if the Status Interval is 120, and the value for Hotswap Detect every is 2, Device Manager polls the hot swap modules every 240 seconds. If you want less frequent hot swap polling, set this value to poll every 2 or 3 intervals.
	Enable	Enables (true) or disables (false) periodic polling of the device for updated status. If polling is disabled, the chassis status is updated only when you click Refresh on the Chassis tab.
SNMP	Retry Count	Number of times Device Manager sends the same polling request if a response is not returned to Device Manager. You can set this field to three or four.
	Timeout	Length of each retry of each polling waiting period. When you access the device through a slow link, you can increase the timeout interval and then change the Retransmission Strategy to superlinear.
	Trace	The trace field is used to enable and disable SNMP tracing. When Trace is selected, SNMP protocol data units (PDUs) are displayed in the Device > Log dialog box.
	Listen for traps	When selected (enabled), Device Manager listens for traps from the device.
	Max Traps in Log	The specified number of traps that can exist in the trap log. The default is 500.
	Trap Port	The UDP port that Device Manager uses to listen for SNMP traps.
	Listen for Syslogs	Enable the Device Manager to listen to the syslog.
	Confirm row deletion	When selected (enabled), Device Manager displays a confirmation dialog box before you delete a system table row.
	Default Read Community	The default Read Community type. Edit this field by highlighting the current value and typing over it.
	Default Write Community	The default Write Community type. Edit this field by highlighting the current value and typing over it.

Area	Item	Description
Application Control	Application launch with ring tone	Enabled by default, you can modify this field only when configuring the Device Manager default properties. You cannot modify this field when configuring the per device properties.
	Save SNMPv3 Devices to Open Last	Disabled by default, if you enable this field you are prompted with a security warning message because any user can access the device without entering the SNMPv3 security criteria if this feature is enabled. If you disable this field, all previously saved SNMPv3 device data is erased and you are prompted with a warning message. You can modify this field only when configuring the Device Manager default properties. You cannot modify this field when configuring the per device properties.
	Http Port	Default port is 80. This field specifies the HTTP port for the application. To access the Device Home Page using the Web, ensure that the HTTP Port attribute matches the switch configuration. If you change the port number, the system prompts you with a warning message.

—End—

To set the Device Manager properties after a device has been accessed:

Step	Action
1	From the Device Manager menu bar, choose Device > Properties > Devices . <i>The Properties Device List appears.</i>
2	Select Default from the Properties Device List.
3	From the Properties Device List, click Edit .
4	Configure the properties as described in the Default Properties fields table.
5	Click OK .

—End—

To change the properties settings for a specific device, either before any devices have been accessed or after a device has been accessed, use the appropriate procedure and, when the Properties Device List appears, select an IP address, then click Edit.

Opening a Switch with the Java Device Manager

To open, or connect, to a switch, you need the following information.

- IP address or DNS name of the desired switch.
- SNMP community strings that determine access granted to the user.

After you obtain this information from the switch administrator, perform the following procedure to connect to a switch.

Step	Action
------	--------

- | | |
|---|--|
| 1 | Start the Java Device Manager as described in the section " Starting the Java Device Manager " (page 36). |
| 2 | Select Open > Device from the JDM menu, or press CTRL+O . The following dialog box appears. |

JDM Open Device dialog box

- | | |
|---|---|
| 3 | Enter the information necessary to connect to the switch. " Open Device fields " (page 40) describes each field on the Open Device dialog box. |
|---|---|

Open Device fields

Field	Description
Device Name	Either an IP address or a DNS name for the device, entered by the user.
Read Community	SNMP read community string for the device. The default value for this field is public (displayed as *****). The entry is case-sensitive.
Write Community	SNMP write community string for the device. Default is private (displayed as *****). The entry is case-sensitive.

Field	Description
v3 Enabled	When selected, the Open Device dialog box displays SNMPv3 options.
User Name	The name of the user.
Context Name	This field does not apply to ERS 4500 devices.
Authentication Protocol	The authentication protocol used.
Authentication Password	The current authentication password.
Privacy Protocol	The privacy protocol used.
Privacy Password	The current privacy password.

Not all information is required to connect to a switch. If you do not select the **v3 Enabled** check box, only a **Device Name**, a **Read Community**, and a **Write Community** value are needed. If you select **v3 Enabled**, then **Device Name**, **User Name**, **Authentication Protocol**, **Authentication Password**, **Privacy Protocol**, and **Privacy Password** are required.

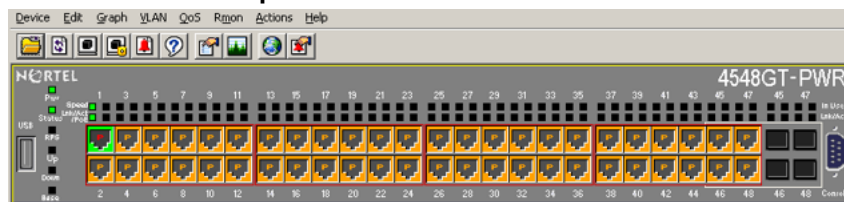
Consult the switch administrator to determine if SNMP version 3 is used for switch connectivity and administration in the network.

4 Click **Open**.

—End—

If you enter the correct information, a connection is established with the switch and a graphical representation is displayed for the switch front panel. The following figure displays the result of a successful connection to a Nortel Ethernet Routing Switch 4500 Series 4548-GT-PWR.

4548GT-PWR Front panel view



Note: After you successfully connect to a switch, the connection information is stored. You can make subsequent connections to the switch from the Device Manager menu. Select **Device > Open Last by SNMPv1/v2** (for connections made using SNMPv1/v2) or **Device > Open Last by SNMPv3** (for connections made using SNMPv3). Select

the IP address of the switch from the list. Be aware that using **Device > Open Last by SNMPv3** enables any switch user to access SNMPv3 devices.

Device Manager interface components

The Java Device Manager application comprises several user interface components. This section highlights those components and their use in the application.

This section contains the following topics:

- "Menu bar" (page 42)
- "Toolbar" (page 43)
- "Device view" (page 44)
- LEDs and ports
- "Shortcut menus" (page 47)
- "Status bar" (page 48)
- "Using the buttons in Device Manager screens" (page 48)
- "Editing objects" (page 49)
- "Telnet session to a switch" (page 55)
- "Opening an SSH connection to the switch" (page 55)
- "Trap log" (page 55)
- "Accessing the Web-based Management Interface" (page 56)
- "Device Manager Online Help" (page 56)

Menu bar

Use the menu bar to set up and operate Device Manager.

The following table "Menu bar commands" (page 42) describes the Menu bar commands.

Menu bar commands

Command	Description
Device	Open a device, refresh the device view, rediscover a device, and set the polling and SNMP properties. Use this menu to open and view the Trap Log, SysLog, and Log. Establish a Telnet or SSH connection to the device that is currently open.

Command	Description
Edit	Open edit dialog boxes for the objects selected in the device view. Open dialog boxes to manage files and run diagnostic tests. Configure SNMP, SNMP v3 and related parameters.
Graph	Open statistics dialog boxes for the selected object.
VLAN	Open dialog boxes to manage VLANs, Spanning Tree Groups, and MultiLink Trunking, and Link Aggregation Control Protocol.
QoS	Open dialog boxes to configure and monitor Quality of Service or Differentiated Services.
RMON	Open dialog boxes to configure RMON: Alarm Manager, Alarms, and Control.
Actions	Open the Home page for the Web-based management session.
Help	Open online Help topics for Device Manager and view a legend for the port colors in the device view.







See also ["Toolbar" \(page 43\)](#)





Toolbar

The toolbar contains buttons that provide quick access to commonly used commands and to some additional actions.

["Toolbar buttons" \(page 43\)](#) The following table describes the toolbar buttons.

Toolbar buttons

Button	Name	Description	Menu equivalent
	OpenDevice	Open the Open Device dialog box.	Device > Open
	Refresh Device Status	Refresh the device view information.	Device > Refresh Status
	Telnet	Open a Telnet session.	Device > Telnet
	SSH	Open a SSH session.	Device > SSH Connection
	Trap Log	Open the trap log.	Device > Trap Log
	Help	Open online Help in a Web browser.	Help > Device

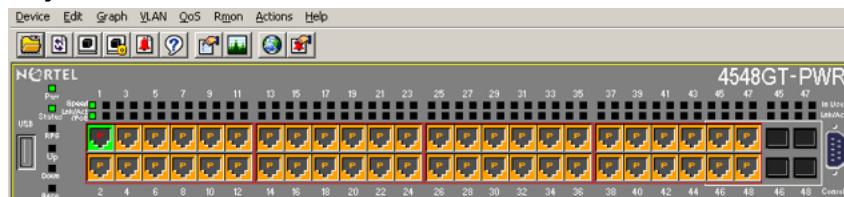
Button	Name	Description	Menu equivalent
	Edit Selected	Display configuration data for the selected chassis object.	Edit > Unit Edit > Chassis Edit > Port
	Graph Selected	Open statistics and graphing dialog boxes for the selected object.	Graph > Chassis Graph > Port
	Globe	Open a Web-based management session.	Actions > Open Home Page
	Alarm Manager	Open the Rmon Alarm Manager.	Rmon > Alarm Manager

Device view

The device view visually indicates the operating status of the various units and ports in the hardware configuration. You can also use the device view to perform management tasks on specific objects.

"Objects in the device view" (page 44) shows an example of a typical device view.

Objects in the device view



Selecting objects The types of objects contained in the device view are:

- a stand-alone switch (called a unit in the menus and dialog boxes)
- a switch stack (called a chassis in the menus and dialog boxes)
- a port (in this example, the active port, or port object, is green but the user can select any port)

See also

"Device view" (page 44)

Selecting a single object To select a single object, click the edge of the object.

The yellow outline on the object indicates that you selected it. Subsequent activities in Device Manager refer to the selected object.

See also

["Device view" \(page 44\)](#)

Selecting multiple objects To select multiple objects of the same type (such as ports or switches of the same type), perform one of the following steps:

- To select a block of contiguous ports, drag the cursor to select the group of ports.
- To select multiple ports or switches in the stack, **Ctrl+click** the objects.

To select all the ports in a stand-alone switch or in a switch stack:

- Select **Edit**.
- Click **Select**. The Select menu appears.
- Select **Ports**.

To select all the units (switches, but not ports):

- Select **Edit**.
- Click **Select**. The Select menu appears.
- Select **Units**.

To select an entire stack:

- Select **Edit**.
- Click **Select**. The Select menu appears.
- Select **Chassis**.

See also

["Device view" \(page 44\)](#)

LEDs and ports

The color of LEDs in the device view is the same as the colors of the LEDs on the physical switch. However, the device view does not show blinking LEDs.

The ports on the device view are colored to show port status.

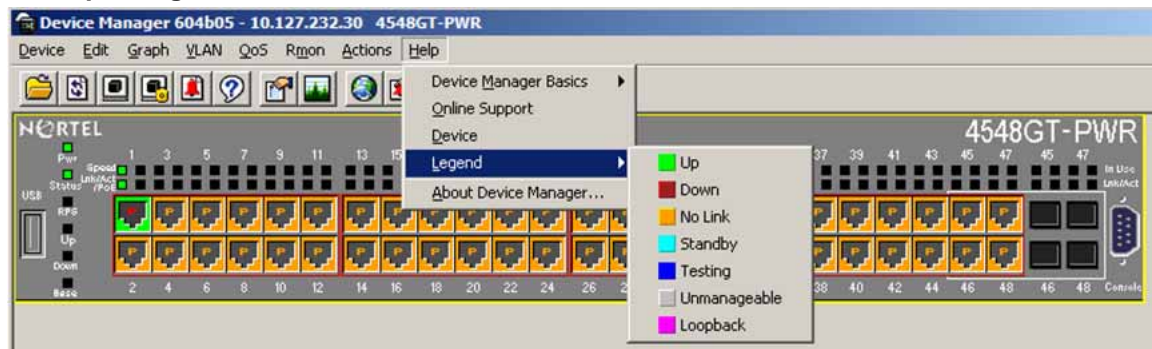
The following table "Port color codes" (page 46) shows the status assigned to each color.

Port color codes

Color	Description
Green	Port is operating.
Red	Port is manually disabled.
Orange	Port has no link.
Light Blue	Port is in standby mode. Note: This is not supported on the Nortel Ethernet Routing Switch 4500 Series.
Dark Blue	Port is being tested. Note: This is not supported on the Nortel Ethernet Routing Switch 4500 Series.
Gray	Port is unmanageable.
Purple	Port is in loopback testing mode. Note: This is not supported on the Nortel Ethernet Routing Switch 4500 Series.

In addition, the **Help** menu provides a legend as shown in "Color port legend" (page 46) that identifies the port colors and their meanings.

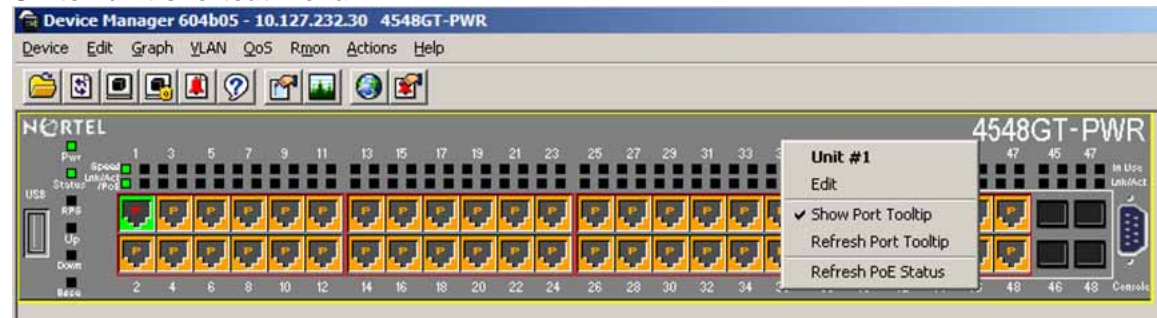
Color port legend



Shortcut menus

Each object in the device view has a shortcut menu that appears when you right-click the object. The switch shortcut menu provides access to basic hardware information about the switch and to the graphing dialog boxes for the switch. An example of this is illustrated in "[Switch unit shortcut menu](#)" (page 47).

Switch unit shortcut menu



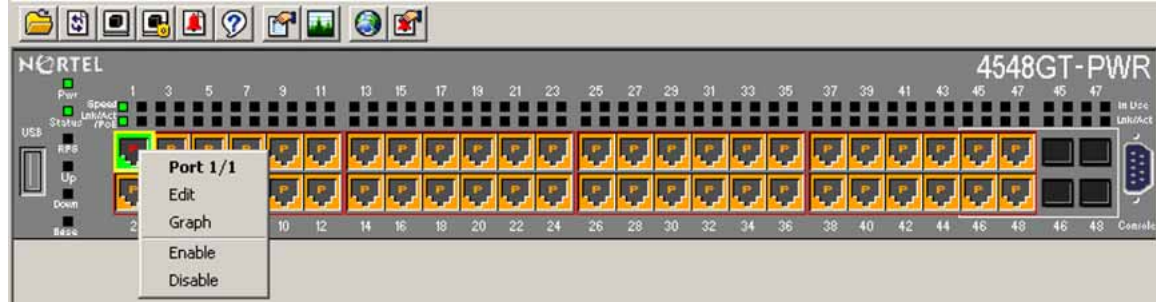
The following table "[Switch unit shortcut menu commands](#)" (page 47) describes the commands on the switch unit shortcut menu.

Switch unit shortcut menu commands

Command	Description
Unit #	Display the unit number.
Edit	Open a read-only dialog box that provides basic hardware information about the switch.
Show Port Tooltip	Display a pop-up window (tooltip) that contains the name of the port and the port speed when you move the mouse over a port in the JDM front panel view. By default, Show Port Tooltip is enabled. Clear the Show Port Tooltip to disable it.
Refresh Port Tooltip	Refresh the port tooltip information after you assign a new port name to it, or after you reconfigure the port speed. Click Refresh Port Tooltip to view updated information.
Refresh PoE Status	Refresh the status of PoE ports on the switch (available only on 4500-PWR switches).

The port shortcut menu, as shown in "[Port shortcut menu](#)" (page 48) provides a fast way to edit and graph a single port; however, you can reach the same options from the menu bar or from the toolbar..

Port shortcut menu



The following table "Port shortcut menu commands" (page 48) describes the commands on the port shortcut menu.

Port shortcut menu commands

Command	Descriptions
Edit	Open a dialog box that enables you to set operating parameters for the port.
Graph	Open a dialog box that displays statistics for the port; you can display the statistics as a graph.
Enable	Administratively starts a port.
Disable	Administratively shuts down a port. The color of the port changes to red in the device view.




Status bar





The status bar displays errors and messages from the software application. These messages are not related to the managed device.

Using the buttons in Device Manager screens

The following table "Device Manager buttons" (page 48) describes buttons in Device Manager screens. Not all buttons appear in all screens.

Device Manager buttons

Button	Name	Description
	Insert	Open a dialog box to create a new entry for a table; and then from the dialog box, insert the new entry in the table.
	Copy	Copy selected cells from a table.
	Paste	Paste copied values to a currently selected table cell.

Button	Name	Description
	Reset Changes	Changed (but not applied) fields revert to their previous values.
	Print Table or Print Graph	Print a table or graph.
	Stop	Stop the current action (for example, compiling, saving). If you update or compile a large data table, the Refresh button changes to a Stop button while this action takes place. Click the Stop button to interrupt the polling.
	Export Data	Export information to a file you specify. You can then import this file into a text editor or spreadsheet for further analysis.

Editing objects

You can edit objects and values in the Device Manager device view in the following ways:

- Select an object and, on the toolbar, click the **Edit Selected** button.
- From a switch or port shortcut menu, choose **Edit**. The edit screen appears for that object.

When you change a screen value, the new value is shown in bold. However, changes are not applied to the running configuration until you click **Apply**.

Note: Many dialog boxes contain a **Refresh** button. After you apply changes to fields, click **Refresh** to display the new information in the screen.

Working with statistics and graphs

Device Manager tracks a wide range of statistics for each switch, the stack (chassis), and each port. You can view and graph statistics for a single object or multiple objects.

This section describes the available types of statistics and graphs, the graph dialog boxes, and the procedure to create a graph.

Types of statistics The data tables in the statistics dialog boxes list the counters, or categories of statistics gathered, for the specified object. For example, the categories for ports include Interface, Ethernet Errors, Bridge, and Rmon. Each category can be associated with six types of statistics.

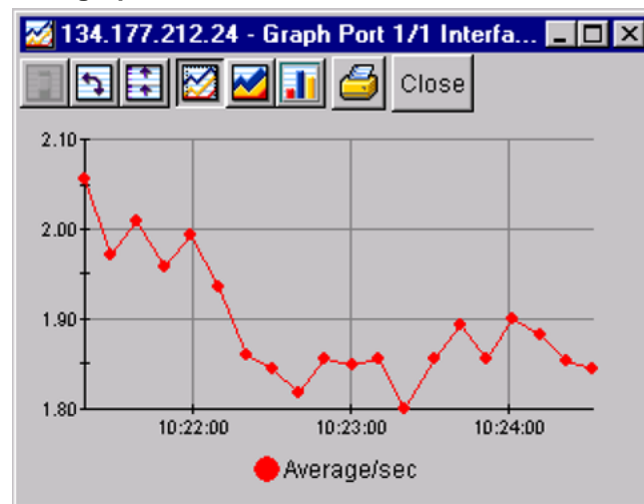
"Types of statistics" (page 50) The following table describes the types of statistics shown in the statistics dialog boxes.

Types of statistics

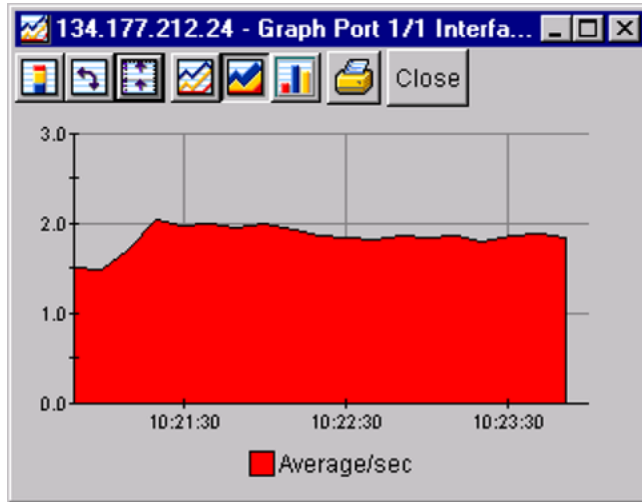
Statistic	Description
AbsoluteValue	The total count since the last time counters were reset. A system reboot resets all counters.
Cumulative	The total count since the statistics window was first opened. The elapsed time for the cumulative counter is shown at the bottom of the graph window.
Average/sec	The cumulative count for each polling interval.
Minimum/sec	The minimum average for the counter for each polling interval.
Maximum/sec	The maximum average for the counter for each polling interval.
LastVal/sec	The average value for the counter during the previous polling interval.

Types of graphs With Device Manager, you can create line, area, bar, and pie graphs. "Line graph" (page 50), "Area graph" (page 51), "Bar graph" (page 51), and "Pie graph" (page 52) illustrate the various graph styles.

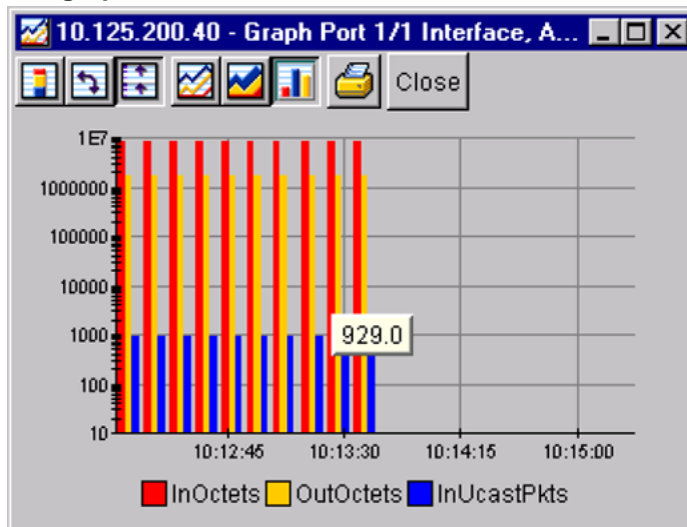
Line graph

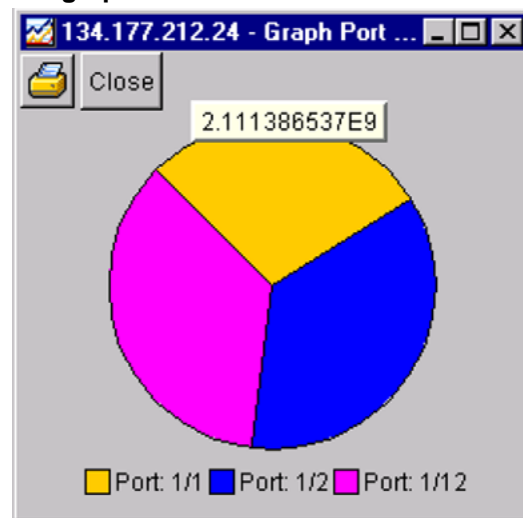


Area graph



Bar graph



Pie graph

Statistics for single and multiple objects The statistics screens display statistics for a selected object.

The dialog box for a single object shows all six types of statistics for each counter (see "Interface statistics for a single port" (page 52)).

Interface statistics for a single port

The screenshot shows a dialog box titled "10.127.232.30 - Graph Port 1/1". It has several tabs: "Interface", "Ethernet Errors", "Bridge", "Rmon", "EAPOL Stats", "EAPOL Diag", "LACP", and "Misc.". The "Interface" tab is active, displaying a table of statistics. The table has seven columns: "AbsoluteValue", "Cumulative", "Average/sec", "Minimum/sec", "Maximum/sec", and "LastVal/sec". The rows list various counters such as InOctets, OutOctets, InUcastPkts, etc. At the bottom, there are buttons for "Clear Counters", "Close", and "Help...", along with a "Poll Interval" dropdown set to "10s" and a timer showing "0 day, 00h:00m:35s".

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
InOctets	1,688,111	6,738	192.51	49.73	279.45	222.64
OutOctets	5,035,953	12,269	350.54	103.45	504.82	398.43
InUcastPkts	1,423	13	0.37	0.09	0.55	0.43
OutUcastPkts	37,459	38	1.09	0.73	1.36	1.07
InMulticastPkts	13,310	9	0.26	0.18	0.29	0.29
OutMulticastPkts	35,828	23	0.66	0.57	0.73	0.57
InBroadcastPkts	1,303	0	0	0	0	0
OutBroadcastPkts	48	1	0.03	0	0.07	0.07
InDiscards	28	0	0	0	0	0
OutDiscards	28	0	0	0	0	0
InErrors	0	0	0	0	0	0
OutErrors	0	0	0	0	0	0
InUnknownProtos	0	0	0	0	0	0

The statistics screen for multiple objects shows a single type of statistics ("Types of statistics" (page 50)) for each selected object. For example, "Interface statistics for multiple ports" (page 53) shows AbsoluteValue statistics for the selected ports.

Interface statistics for multiple ports

Interface	Ethernet Errors	Bridge	Rmon	EAPOL Stats	EAPOL Diag	LACP	Misc.	InOctets	OutOctets	InUcastPkts	OutUcastPkts	InMulticastPkts	OutMulticastPkts	InBroadcastPkts	OutBroadcastPkts	InDiscards	OutDiscards	InErrors	OutErrors	InUnknownPh
Port: 1/1								1,669,...	3,429,500	806	47,691	17,381	46,800	2,277	48	31	31	0	0	
Port: 1/3								0	0	0	0	0	0	0	0	0	0	0	0	0
Port: 1/5								0	0	0	0	0	0	0	0	0	0	0	0	0
Port: 1/7								0	0	0	0	0	0	0	0	0	0	0	0	0
Port: 1/9								0	0	0	0	0	0	0	0	0	0	0	0	0

At the bottom of the dialog box, there is a toolbar with icons for bar, pie, and line graphs, a "Gear Counters" button, "Close" and "Help..." buttons, a "Poll Interval" dropdown set to "10s", a time display "0 day, 00h:00m:45s", and a "Show:" dropdown set to "AbsoluteValue".

To change the type of statistics displayed, select a different type from the show list at the bottom right of the screen.

The statistics are updated based on the poll interval shown at the bottom of the dialog box. You can select a different polling interval.

Buttons for bar, pie, and line graphs are at the bottom of the statistics dialog box.

You can export statistics to a tab-separated-format file and import the file into other applications. To export the information, use the **Export Data** button below the table.

Viewing statistics as graphs To create a graph for an object:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select the object or objects to be graphed. |
| 2 | Perform one of the following steps: <ul style="list-style-type: none"> On the toolbar, click Graph Selected. From the shortcut menu for the object, choose Graph. Select the Graph > Chassis or Graph > Port command |

A statistics dialog box appears with tabs for categories of statistics for the selected object ("Statistics dialog box for a port" (page 54)).

Statistics dialog box for a port

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
InOctets	1,730,590					
OutOctets	5,112,697					
InUcastPkts	1,496					
OutUcastPkts	37,697					
InMulticastPkts	13,367					
OutMulticastPkts	35,981					
InBroadcastPkts	1,306					
OutBroadcastPkts	48					
InDiscards	28					
OutDiscards	28					
InErrors	0					
OutErrors	0					
InUnknownProtos	0					



Buttons: Clear Counters, Close, Help..., Poll Interval: 10s, 0 day, 00h:00m:00s






- 3 Select a tab for the group of statistics to view.
- 4 On the displayed data table, drag the cursor to select the cells to graph. (The cells must be in the same row or column.)
- 5 Click one of the graph buttons at the bottom of the dialog box.
- 6 To print the graph, click **Print**.
- 7 Use the buttons at the top of the graph screen for line, area, and bar graphs to change the orientation of the graph, to change the scale, or to change the graph type.

—End—

The following table "Graph dialog box buttons" (page 54) describes the buttons in the graph dialog boxes.

Graph dialog box buttons

Button	Name	Description
	Stacked	Stack data quantities instead of displaying them side-by-side.
	Horizontal	Rotate the graph 90 degrees.

Button	Name	Description
	Log Scale	Change the scale of the x-axis (of an unrotated graph) from numeric to logarithmic.
	Line Chart	Convert an area graph or bar graph to a line graph.
	Area Chart	Convert a line graph or bar graph to an area graph.
	Bar Chart	Convert a line graph or area graph to a bar graph.
	Pie Chart	Convert a line graph or area graph to a pie chart.

Telnet session to a switch

From Device Manager, you can initiate a Telnet session to the switch or stack.

To start a Telnet session to a switch, perform one of the following steps:

- From the Device Manager main menu, select **Device > Telnet**.
- On the toolbar, click **Telnet** .

Opening an SSH connection to the switch

From the Java Device Manager, you can initiate a Secure Shell (SSH) connection to the console interface for the switch or stack currently being accessed.

To open an SSH connection to a switch, perform one of the following steps:

- From the main menu, select **Device > SSH Connection**.
- On the toolbar, click **SSH** .

An SSH window to the switch appears.

Note: The SSH connection is established only when the device is SSH-capable and is enabled.

Trap log

You can configure the Nortel Ethernet Routing Switch 4500 Series to send SNMP generic traps. When Device Manager runs, the trap log records the received traps. You can set the maximum number of entries in the trap log using the **Properties** screen. The default number of trap log entries is 500. To view the trap log:

- On the toolbar, click **Trap Log** .
- From the Device Manager Main Menu, select **Device > Trap Log**.

Note: When you operate Device Manager from a UNIX platform, log in as root to receive traps.

Use **Export** at the bottom of the screen to export trap logs to a file.

Device Manager receives traps on port 162. If another application uses this port you cannot view the trap log until the other application terminates and Device Manager restarts.

By default, traps are sent in SNMP V2c format. However, if you use an old Network Management System (NMS) (one that supports only SNMP v1 traps), traps are sent in v1 format.

Accessing the Web-based Management Interface

You can access the Web-based Management Interface for the Nortel Ethernet Routing Switch 4500 Series from the Device Manager.

To view the Web-based Management Interface, select **Actions > Open Home Page** . The Web browser opens to the Web-based Management Interface for the switch.

Device Manager Online Help

Online Help in Device Manager is context-sensitive and is displayed in the default Web browser. The Web browser launches automatically when you click **Help** .

The default locations of the Help files are the directories listed in "[Help file locations](#)" (page 56).the following table.

Help file locations

Platform	Default path
Windows 95, Windows 98, Windows NT, Windows XP and UNIX	<p><JDM Installation directory> /help/ botanybay/v500.zip.</p> <p>After you unzip the file, help.html becomes the home page for the online Help.</p>

Web-based Management Interface

The Web-based Management Interface is a browser-based application for switch configuration and management. Unlike the JDM, you need not install the application because the management interface is an integral part of the switch.

To support the Web-based Management Interface, a computer must have one of the following Web browsers installed:

- Microsoft Internet Explorer 4.0 (or later)
- Netscape Navigator 4.51 (or later)

Accessing the Web-based Management Interface

To access the Web-based Management Interface, first ensure that the computer and the switch CPU are on the same virtual local area network (VLAN). Use the CLI and verify the VLAN assignments to confirm that the VLANs are the same. If the switch and computer are not on the same VLAN, you cannot access the Web-based Management Interface.

After VLAN verification occurs, you can access the Web-based Management Interface by performing the following procedure.

Step	Action
1	Open a Web browser window.
2	Type the IP address of the switch or stack in the Address field of the Web browser in the form <i>http://<switch IP address></i> , and press Enter . For example, if the switch or stack IP address is 10.30.31.105, then enter <i>http://10.30.31.105</i> in the Address field. You can obtain the IP address of the switch or stack from the switch administrator.
3	If applicable, enter the user name and password to gain access to the switch or stack. The user name is static and depends on the type of access required or assigned. For read-only access, the user name is RO and for read/write access it is RW. These user names are case-sensitive. You can obtain the password from the switch administrator.
4	If all information is correct, the main switch page appears. The following figure displays an example of the main switch page for a Nortel Ethernet Routing Switch 4500 Series 4548-GT-PWR.

4548-GT-PWR Main Page

The screenshot displays the Nortel Web-based Management Interface for an Ethernet Routing Switch 4548GT-PWR. The interface is divided into two main sections: a navigation menu on the left and a management page on the right.

Navigation Menu (Left):

- Access (RW)
 - Summary
 - Configuration
 - Fault
 - Statistics
 - Applications
 - Administration
 - System Information (Selected)
 - Quick Start
 - Security
 - Logout
 - Reset
 - Reset To Default
 - Support

System Information Page (Right):

Administration > System Information

Ethernet Routing Switch 4548GT-PWR

sysDescription	Ethernet Routing Switch 4548GT-PWR HW:0A FW:1.0.0.14 SW:v5.0.0.083 BN:83 (c) Nortel Networks
sysUpTime	16 Hours 34 Minutes 33 Seconds
sysContact	
sysName	4548GT-PWR
sysLocation	

Copyright © 2006 Nortel, Inc. All rights reserved.

—End—

Web-based Management Interface layout

The main page in the Web-based Management Interface and all subsequent pages have a common layout. Each page is divided into two sections: the menu and the management page.

Menu

The menu contains the main units of work that you can perform through the Web-based Management Interface and their corresponding options. Some options are available only when the switch is part of a stack configuration; the options are not displayed when the switch is in a stand-alone configuration. To navigate the menu, click a main header. The corresponding options appear beneath. Click an option to display the associated management page.

"Web-based Management Interface menu options" (page 58) lists the Web-based Management Interface menu options.

Web-based Management Interface menu options

Main Heading	Options	Description
Summary	Stack Information* Switch Information	View information about the current state of the individual switch or stack.
* These options are available only when the switch is part of a stacked configuration.		
** These options have additional associated options.		

Main Heading	Options	Description
	Identify Unit Numbers* Stack Numbering*	
Configuration	IP System Remote Access SNMPv1 SNMPv3** SNMP Trap MAC Address Find MAC Address Port Management High Speed Flow Control Software Download Ascii Config Download Configuration File	Configure aspects of the switch or stack operation.
Fault	RMON Threshold RMON Event Log System Log	Configure fault thresholds and view event logs.
Statistics	Port Port Error Summary Interface Ethernet Errors Transparent Bridging RMON Ethernet RMON History	View statistics for a variety of switch functions.
<p>* These options are available only when the switch is part of a stacked configuration.</p> <p>** These options have additional associated options.</p>		







Main Heading	Options	Description
Applications	Port Mirroring Rate Limiting EAPOL Security MAC Address Security** IGMP** VLAN** Spanning Tree** Multilink Trunk** Link Aggregation** QoS**	Configure and manage a variety of switch applications.
Administration	System Information Quick Start Security** Logout Reset Reset to Default	Configure and manage administrative items.
Support	Help Release Notes Manuals Upgrade	Access the various support facilities, such as Help, manuals, and switch upgrade procedures.
<p>* These options are available only when the switch is part of a stacked configuration.</p> <p>** These options have additional associated options.</p>		

**CAUTION**

Nortel recommends that you use the navigation tools in the interface instead of those in the Web browser, such as page forward, page back, and page refresh. Web browser functions do not enhance the use of the interface and can interfere with the logical navigation of the Web-based Management Interface.

The menu of the Web-based Management Interface contains several iconic cues to the type and operation of the menu options. "Menu icons" (page 61) describes the icons that appear in the menu.

Menu icons

Icon	Description
	This icon identifies a collapsed menu title. Click the icon to expand the menu and view all associated options.
	This icon identifies an expanded menu title. All options associated with the menu title are displayed underneath. Click the icon to collapse the menu and hide all associated options.
	This icon identifies a menu option. Click the icon to see the management page associated with this menu option.
	This icon identifies a menu option with a hyperlink to related pages. Click the icon to see the management page associated with this menu option and any related hyperlinks.
	This icon identifies a menu option associated with an action. Actions have no associated management page and take place immediately.
	This icon is a link to the Nortel corporate home page. Click this icon to open a new Web browser window and load the Nortel corporate home page.

Management Page

The Management Page, as illustrated in [Web-based Management Interface layout](#), is the main work area in the Web-based Management Interface. As you select various items and options, the associated Management Page loads. "Quick Start Management page" (page 62) illustrates the Quick Start Management Page that you access by selecting **Administration > Quick Start**.

Quick Start Management page**Administration > Quick Start**

IP		
	Configurable	In Use
In-Band Stack IP Address	192.168.248.206	192.168.248.206
In-Band Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.248.1	192.168.248.1

Community String	
Read-Only Community String	●●●●●●●●●●
Read-Write Community String	●●●●●●●●●●

Trap Receiver		
Index	IP Address	Community
1	0.0.0.0	
2	0.0.0.0	
3	0.0.0.0	
4	0.0.0.0	

VLAN	
Quick Start VLAN	<input type="text"/>

Submit

Every Management Page comprises one or more of the following elements:

- **Display Field**

Display fields show preexisting values or statistical information. Display fields have a gray background and are read-only. If the data in the field is highlighted blue and is underlined, it is a hyperlink to a related Management Page.

- **Input Field**

Use input fields to enter or change information. Input fields have a white background and are editable.

- **Check Box**







Use check boxes to change data on the switch that exists in either an on or off state. When a check box displays a check mark, that data item is enabled (on); otherwise, it is disabled (off). Click in the check box to enter a check mark or to remove a check mark.

- **Icons and Buttons**

Icons and buttons on a Management Page represent the actions that you can perform. Click the icon or button to initiate the associated

action. "Management Page icons and buttons" (page 63) describes the main icons and buttons that can appear on a Management Page.

Management Page icons and buttons

Icon / Button	Name	Description
	Submit	Submit entered information to the switch. If this button is present, ensure that you click it every time you enter new information on the Management Page.
	Modify	Open a modification page for the data row in which the button appears.
	View	Open a read-only statistics page for the data row in which the button appears.
	Delete	Delete the data row in which the button appears.
	Help	Open Help for the current Management Page in a new Web browser window.
	Context-sensitive Help	Open Help for the current data item in a new Web browser window.

Basic configuration tasks

This chapter outlines basic configuration tasks that you can perform on a Nortel Ethernet Routing Switch 4500 Series. After you successfully install a switch, you can perform the following tasks to enable basic switch functionality.

This chapter contains the following topics:

- "Factory default configuration" (page 65)
- "Setting user access limitations" (page 71)
- "Updating switch software" (page 81)
- "Setting TFTP parameters" (page 89)
- "Working with configuration files" (page 90)
- "Terminal setup" (page 103)
- Setting the default management interface
- "Setting Telnet access" (page 104)
- "Setting server for Web-based management" (page 106)
- "Setting boot parameters" (page 107)
- "Defaulting to BootP-when-needed" (page 108)
- "Customizing the CLI banner" (page 110)
- "Displaying complete GBIC information" (page 114)
- "Displaying hardware information" (page 114)
- "Shutdown command" (page 114)
- "CLI Help" (page 117)

Factory default configuration

When you initially access a newly installed switch or you reset a switch to factory defaults, the switch is in a factory default configuration. This factory default configuration is the base configuration from which you build the switch configuration.

"Factory default configuration settings" (page 66) outlines the factory default configuration settings present in a switch in a factory default state.

Factory default configuration settings

Setting	Factory default configuration value
Unit Select switch	non-Base
Unit	1
BootP Request Mode	BootP When Needed
In-Band Stack IP Address	0.0.0.0 (no IP address assigned)
In-Band Switch IP Address	0.0.0.0 (no IP address assigned)
In-Band Subnet Mask	0.0.0.0 (no subnet mask assigned)
Default Gateway	0.0.0.0 (no IP address assigned)
Read-Only Community String	public
read/write Community String	private
Trap IP Address	0.0.0.0 (no IP address assigned)
Community String	Zero-length string
Authentication Trap	Enabled
Autotopology	Enabled
sysContact	Zero-length string
sysName	Zero-length string
sysLocation	Zero-length string
Aging Time	300 seconds
Find an Address	00-00-00-00-00-00 (no MAC address assigned)
Select VLAN ID [1]	
MAC Address Security	Disabled
MAC Address Security SNMP-Locked	Disabled
Partition Port on Intrusion Detected:	Disabled
Partition Time	0 seconds (the value 0 indicates forever)
DA Filtering on Intrusion Detected:	Disabled
Generate SNMP Trap on Intrusion	Disabled

Setting	Factory default configuration value
Clear by Ports	NONE
Learn by Ports	NONE
Current Learning Mode	Not Learning
Trunk	blank field
Security	Disabled
Port List	blank field
Find an Address	blank field
MAC Address	00-00 00-00 -00-00
Allowed Source	- (blank field)
Display/Create MAC Address	00-00-00-00-00-00
Create VLAN	1
Delete VLAN	blank field
VLAN Name	VLAN #
Management VLAN	Yes (VLAN #1)
VLAN Type	Port-based
Protocol ID (PID)	None
User-Defined PID	0x0000
VLAN State	Active (VLAN #1)
Port Membership	All ports assigned as members of VLAN 1
Unit	1
Port	1
Filter Untagged Frames	No
Filter Unregistered Frames	Yes
Port Name	Unit 1, Port 1
PVID	1
Port Priority	0
Tagging	Untag All
AutoPVID	Enabled
Unit	1
Port	1
PVID	1 (read only)
Port Name	Unit 1, Port 1 (read only)

Setting	Factory default configuration value
Unit	1
Status	Enabled (for all ports)
Linktrap	On
Autonegotiation	Enabled (for all ports)
Speed/Duplex	(Refer to Autonegotiation)
Trunk	1 to 6 (depending on configuration status)
Trunk Members (Unit/Port)	Blank field
STP Learning	Normal
Trunk Mode	Basic
Trunk Status	Disabled
Trunk Name	Trunk #1 to Trunk #6
Traffic Type	Rx and Tx
Port	1
Monitoring Mode	Disabled
Monitor/Unit Port	Zero-length string
Unit/Port X	Zero-length string
Unit/Port Y	Zero-length string
Address A	00-00-00-00-00-00 (no MAC address assigned)
Address B	00-00-00-00-00-00 (no MAC address assigned)
Rate Limit Packet Type	Both
Limit	None
VLAN	1
Snooping	Disabled
Proxy	Disabled
Robust Value	2
Query Time	125 seconds
Set Router Ports	Version 1
Static Router Ports	- (for all ports)
Multicast Group Membership screen	
Unit	1
Port	1
Console Port Speed	9600 baud

Setting	Factory default configuration value
Console Switch Password	None
Console Stack Password	None
Telnet/Web Stack Password	None
Telnet/Web Switch Password	None
Console Read-Only Switch Password	user
Console Read/Write Switch Password	Passwords are user/secure for non-SSH SW images and userpasswd/securepasswd for SSH SW images.
Console Read-Only Stack Password	user
Console Read/Write Stack Password	secure
Radius password/server	secret
New Unit Number	Current stack order
Renumber units with new setting?	No
Group	1
Bridge Priority	8000
Bridge Hello Time	2 seconds
Bridge Maximum Age Time	20 seconds
Bridge Forward Delay	15 seconds
Add VLAN Membership	1
Tagged BPDU on tagged port	STP Group 1--No Other STP Groups--Yes
STP Group State	STP Group 1--Active Other STP Groups--Inactive
VID used for tagged BPDU	4001-4008 for STGs 1-8, respectively
STP Group	1
Participation	Normal Learning
Priority	128
Path Cost	1
STP Group	1

Setting	Factory default configuration value
STP Group	1
TELNET Access/SNMP/ Web	By default, SNMP access is disabled in the SSH image and enabled in the non-SSH image. Telnet and Web are enabled by default in both SSH and non-SSH images. Use list: Yes
Login Timeout	1 minute
Login Retries	3
Inactivity Timeout	15 minutes
Event Logging	All
Allowed Source IP Address (50 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned) Remaining 49 fields: 255.255.255.255 (any address is allowed)
Allowed Source Mask(50 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned) Remaining 49 fields: 255.255.255.255 (any address is allowed)
Image Filename	Zero-length string
Diagnostics image filename	Zero-length string
TFTP Server IP Address	0.0.0.0 (no IP address assigned)
Start TFTP Load of New Image	No
Configuration Image Filename	Zero-length string
Copy Configuration Image to Server	No
Retrieve Configuration Image from Server	No
ASCII Configuration Filename	Zero-length string
Retrieve Configuration file from Server	No

Setting	Factory default configuration value
Auto Configuration on Reset	Disabled
EAPOL Security Configuration	Disabled
High Speed Flow Control Configuration	
VLAN Configuration Control	Strict
Agent Auto Unit Replacement	Enabled

Setting user access limitations

By default, a 4500 Series switch has no access limitations configured. This section illustrates how to set user access limitations on the switch. User access limitations are an important facet of switch security that you must be aware of during the initial configuration .

For more information about switch user interfaces, consult "[4500 Series user interfaces](#)" (page 19).

This section describes the following procedures to set user access limitations:

- "[Setting user access limitations using the CLI](#)" (page 71)
- "[Setting user access limitations using the Web-based Management Interface](#)" (page 75)

Setting user access limitations using the CLI

The administrator can use the CLI to limit user access by creating and maintaining passwords for Web, Telnet, and Console access. This is a two-step process that requires that you first create the password and then enable it.

Ensure that **Global Configuration** mode is entered in the CLI before you start these tasks.

Setting the read-only and read/write passwords

The first step to requiring password authentication when the user logs in to the switch is to edit the password settings. To complete this task, perform the following steps:

- | Step | Action | | | | | | |
|--------------------------|--|-----------|-------------|--------------------------|---|------------|---|
| 1 | Access the CLI through the Telnet protocol or a Console connection. For detailed information about this subject, see "Accessing the CLI" (page 19) . | | | | | | |
| 2 | <p>From the command prompt, use the <code>cli password</code> command to change the desired password.</p> <pre>cli password {read-only read-write} <password></pre> <p>"cli password parameters" (page 72) explains the parameters for the <code>cli password</code> command.</p> <p>cli password parameters</p> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>{read-only read-write}</td> <td>This parameter specifies if the password change is for read-only access or read/write access.</td> </tr> <tr> <td><password></td> <td>If password security is disabled, the length can be 1-15 chars. If password security is enabled, the range for length is 10-15 chars.</td> </tr> </tbody> </table> | Parameter | Description | {read-only read-write} | This parameter specifies if the password change is for read-only access or read/write access. | <password> | If password security is disabled, the length can be 1-15 chars. If password security is enabled, the range for length is 10-15 chars. |
| Parameter | Description | | | | | | |
| {read-only read-write} | This parameter specifies if the password change is for read-only access or read/write access. | | | | | | |
| <password> | If password security is disabled, the length can be 1-15 chars. If password security is enabled, the range for length is 10-15 chars. | | | | | | |
| 3 | Press Enter . | | | | | | |

—End—

Enabling and disabling passwords

After you set the read-only and read/write passwords, you can individually enable or disable them for the various switch-access methods. To enable passwords, perform the following task.

- | Step | Action |
|------|--|
| 1 | Access the CLI through the Telnet protocol or a Console connection. For detailed information about this subject, see "Accessing the CLI" (page 19) . |
| 2 | <p>From the command prompt, use the <code>cli password</code> command to enable the desired password.</p> <pre>cli password {telnet serial} {none local radius tacacs}</pre> |

"cli password parameters" (page 73) explains the parameters for the `cli password` command.

cli password parameters

Parameter	Description
{telnet serial}	Specify whether the password is enabled or disabled for Telnet or the console. Telnet and Web access are connected so that enabling or disabling passwords for one enables or disables passwords for the other.
{none local radius}	Specify whether the password is to be disabled (none), whether the password to be used is the locally stored password created in "Setting the read-only and read-write passwords" (page 71), or whether RADIUS authentication is used.

3 Press **Enter**.

—End—

Configuring RADIUS authentication

The Remote Authentication Dial-In User Service (RADIUS) protocol is a means to authenticate users through a dedicated network resource. This network resource contains a list of eligible user names and passwords and their associated access rights. When RADIUS is used to authenticate access to a switch, the user supplies a user name and password and this information is checked against the existing list. If the user credentials are valid they can access the switch.

If you select RADIUS Authentication when you set up passwords through the CLI, you must specify the RADIUS server settings to complete the process. Ensure that you enter **Global Configuration** mode in the CLI before you start this task.

To enable RADIUS authentication through the CLI, follow these steps.

Step	Action
1	Access the CLI through the Telnet protocol or a Console connection. For detailed information about this subject, see " Accessing the CLI " (page 19) .
2	From the command prompt, use the <code>radius-server</code> command to configure the server settings.

```
radius-server host <address> [secondary-host <address>]
port <num> key <string> [password fallback] timeout
```

"radius-server parameters" (page 74) explains the parameters for the `radius-server` command.

radius-server parameters

Parameter	Description
host <address>	The IP address of the RADIUS server that is used for authentication.
[secondary-host <address>]	The secondary-host <address> parameter is optional. If you specify a backup RADIUS server, include this parameter with the IP address of the backup server.
port <num>	The UDP port number the RADIUS server uses to listen for requests.
key <string>	A secret text string that is shared between the switch and the RADIUS server. Enter the secret string, which is a string up to 16 characters in length.
[password fallback]	An optional parameter that enables the password fallback feature on the RADIUS server. This option is disabled by default.
timeout	The RADIUS timeout period.

3 Press **Enter**.

—End—

Related RADIUS Commands When you configure RADIUS authentication, three other CLI commands are useful to the process:

Step Action

- 1 `show radius-server`
The command has no parameters and displays the current RADIUS server configuration.
- 2 `no radius-server`
This command has no parameters and clears any previously configured RADIUS server settings.

3 radius-server password fallback

This command has no parameters and enables the password fallback RADIUS option if you did not set the option when you initially configured the RADIUS server.

—End—

Setting user access limitations using the Web-based Management Interface

The administrator can use the Web-based Management Interface to limit user access by creating and maintaining passwords for Web, Telnet, and Console access. The following sections describe how to perform the procedures:

- ["Setting the Web password" \(page 75\)](#)
- ["Setting the Telnet password" \(page 77\)](#)
- ["Setting the Console password" \(page 78\)](#)
- ["Configuring RADIUS authentication" \(page 80\)](#)

Setting the Web password

To require password authentication when the user logs on to the switch through the Web-based Management Interface, you must edit the Web password. To do this, select **Administration > Security > Web** from the main menu and perform the following procedure.

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the Web Switch Password Type list, select the password type. Three options are available in the Web Switch Password Type list: |
|---|---|

- **None**

Users who access the switch through the Web-based Management Interface require no password.



CAUTION

Using None means that any user who knows the IP address of the switch and the appropriate network access can change the switch configuration.

- **Local Password**

The user must enter a password that determines their individual access rights. These passwords are configured in steps 2 and 3

of this procedure. These passwords must be 1 to 15 characters in length.

- **RADIUS Authentication**

A RADIUS server on the local area network authenticates the user. For information about configuring the parameters for RADIUS server authentication, see "[Configuring RADIUS authentication](#)" (page 80).

- 2 If you selected the Local Password option in step 1, specify a password to grant read-only access to the switch in the **Read-Only Switch Password** field.
- 3 If you selected the Local Password option in step 1, specify a password to grant read/write access to the switch in the **read/write Switch Password** field.

Note: A value of **None** or **RADIUS Authentication** in the **Web Switch Password Type** list always overrides the values in the **Read-Only Switch Password** and **read/write Switch Password** fields.

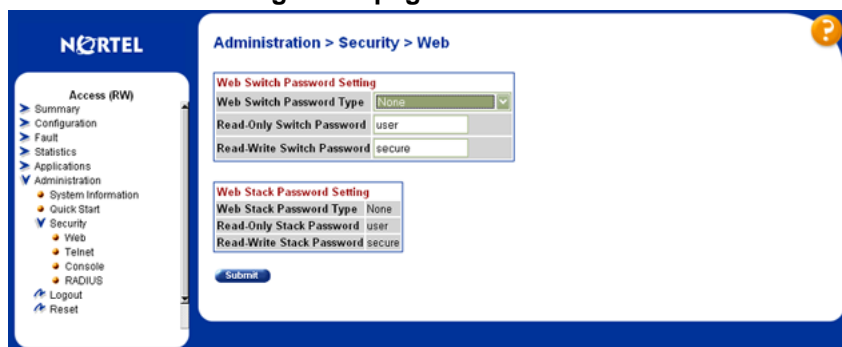
- 4 Click **Submit**.

Note: You cannot change **Web Stack Password** settings on this screen; the settings are for information only. For procedures to change this password, see "[Setting user access limitations using the CLI](#)" (page 71).

—End—

"[Web Password Management page](#)" (page 76) shows an example of the Web Password Management Page in the Web-based Management Interface.


Web Password Management page



Setting the Telnet password

To require password authentication when the user logs into the switch through the Telnet protocol, you must edit the Telnet password. Select **Administration > Security > Telnet** from the main menu and perform the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | <p>Select the password type from the Telnet Switch Password Type list. Three options are available in the Telnet Switch Password Type list:</p> <ul style="list-style-type: none"> • None <p>Users who access the switch through the Telnet protocol require no password.</p> <div data-bbox="564 779 1402 959" data-label="Complex-Block" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <div style="display: flex; align-items: center;">  <div> <p>CAUTION</p> <p>Using None means that any user who knows the IP address of the switch and the appropriate network access can change the switch configuration.</p> </div> </div> </div> • Local Password <p>The user must enter a password that determines their individual access rights. These passwords are configured in Steps 2 and 3 of this procedure. These passwords must be 1 to 15 characters in length.</p> • RADIUS Authentication <p>A RADIUS server on the local area network authenticates the user. For information about configuring the parameters for RADIUS server authentication, see "Configuring RADIUS authentication" (page 80).</p> |
| 2 | <p>If you selected the Local Password option in Step 1, specify a password to grant read-only access to the switch in the Read-Only Telnet Password field.</p> |
| 3 | <p>If you selected the Local Password option in Step 1, specify a password to grant read/write access to the switch in the Read/Write Telnet Password field.</p> |

Note: A value of **None** or **RADIUS Authentication** in the **Telnet Switch Password Type** list always overrides the values in the **Read-Only Telnet Password** and **Read/Write Telnet Password** fields.

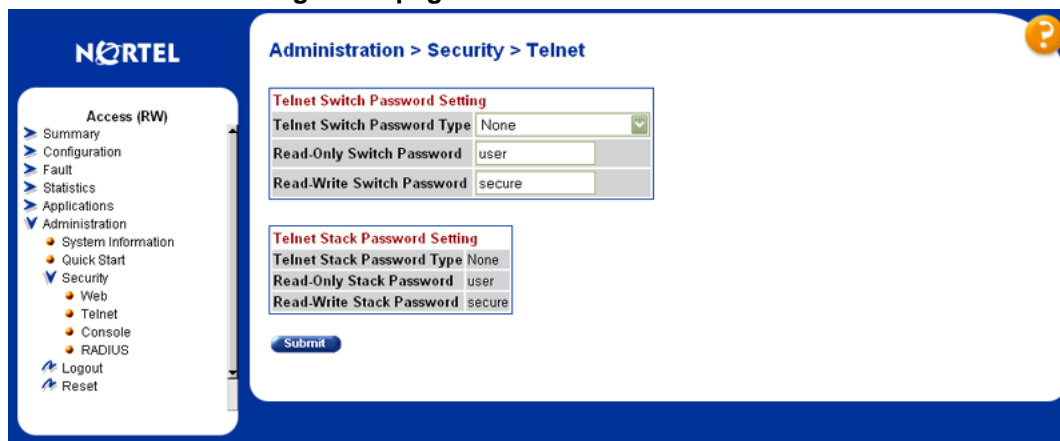
4 Click **Submit**.

Note: You cannot change the **Telnet Stack Password** settings on this screen; the settings are for information only. For procedures to change this password, see "[Setting user access limitations using the CLI](#)" (page 71).

—End—

"[Telnet Password Management page](#)" (page 78) shows an example of the Telnet Password Management Page in the Web-based Management Interface.

Telnet Password Management page



Setting the Console password

To require password authentication when the user logs in to the switch through the Console, you must edit the Console password. Select **Administration > Security > Console** from the main menu and perform the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select the password type from the Console Switch Password Type list. Three options are available in the Console Switch Password Type list: |
|---|--|

- **None**

Users who access the switch through the Console require no password.

**CAUTION**

Using None means that any user with access to a switch Console connection can change the switch configuration.

- **Local Password**

The user must enter a password that determines their individual access rights. These passwords are configured in steps 2 and 3 of this procedure. These passwords must be from 1 to 15 characters in length.

- **RADIUS Authentication**

A RADIUS server on the local area network authenticates the user. For information about configuring the parameters for RADIUS server authentication, see "[Configuring RADIUS authentication](#)" (page 80).

- 2 If you selected the Local Password option in step 1, specify a password to grant read-only access to the switch in the **Read-Only Console Password** field.
- 3 If you selected the Local Password option in step 1, specify a password to grant read/write access to the switch in the **Read/Write Console Password** field.

Note: A value of **None** or **RADIUS Authentication** in the **Console Switch Password Type** list always overrides the values in the **Read-Only Console Password** and **Read/Write Console Password** fields.

- 4 Click **Submit**.

Note: You cannot change the **Console Stack Password** settings on this screen; the settings are for information only. For procedures to change this password, see "[Setting user access limitations using the CLI](#)" (page 71).

—End—

"[Console Password Management page](#)" (page 80) shows an example of the Console Password Management Page in the Web-based Management Interface.

Console Password Management page

The screenshot shows the Nortel Administration > Security > Console page. On the left is a navigation menu with options like Summary, Configuration, Fault, Statistics, Applications, Administration (System Information, Quick Start, Security, Web, Telnet, Console, RADIUS), Logout, and Reset. The main content area has a breadcrumb trail 'Administration > Security > Console'. There are two sections: 'Console Switch Password Setting' and 'Console Stack Password Setting'. Each section has a dropdown for 'Password Type' (set to 'None'), and input fields for 'Read-Only' and 'Read-Write' passwords. The 'Read-Only' password is 'user' and the 'Read-Write' password is 'secure'. A 'Submit' button is at the bottom of the second section.

Configuring RADIUS authentication

The RADIUS protocol provides a way to authenticate users by using a dedicated network resource. This network resource contains a list of eligible user names and passwords and their associated access rights. When you use RADIUS to authenticate access to a switch, the user supplies a user name and password and this information is checked against the existing list. If the user credentials are valid, the user can access the switch.

If you selected RADIUS Authentication for any of the switch authentication options in the previous three sections, you must specify the RADIUS server settings to complete the process. To set the RADIUS Authentication parameters, select Administration > Security > RADIUS and perform the following procedure.

Step	Action
1	In the Primary RADIUS Server field, type the IP address of the primary RADIUS server that is used for user authentication.
2	In the Secondary RADIUS Server field, type the IP address of a secondary RADIUS server that is used as a backup for the primary server.
3	In the UDP RADIUS Port field, type the UDP port number the RADIUS servers that is used to listen for RADIUS authentication requests.
4	In the RADIUS Timeout Period field, type the number of seconds (1 to 60) to specify the timeout period.
5	In the RADIUS Shared Secret field, type the password that the RADIUS server requires to authenticate a valid RADIUS request. This password is 1 to 16 characters in length.

6 Click **Submit**.

—End—

"RADIUS Authentication Management page" (page 81) displays the RADIUS Authentication Management Page in the Web-based Management Interface.

RADIUS Authentication Management page

Administration > Security > RADIUS

RADIUS Authentication Setting

Primary RADIUS Server	<input type="text" value="0.0.0.0"/>
Secondary RADIUS Server	<input type="text" value="0.0.0.0"/>
UDP RADIUS Port	<input type="text" value="1812"/>
RADIUS Timeout Period	<input type="text" value="2"/> seconds
RADIUS Shared Secret	<input type="password" value="....."/> <small>Re-enter to verify</small>

Updating switch software

Updating switch software is a necessary part of switch configuration and maintenance. You can update the version of software running on the switch through either the Web-based Management Interface, Device Manager (JDM) or the CLI.

Before you attempt to change the switch software, ensure that the following prerequisites are in place:

- The switch has a valid IP address.
- A Trivial File Transfer Protocol (TFTP) server is on the network that is accessible by the switch and that has the desired software version loaded.
- If you change the switch software on a Nortel Ethernet Routing Switch 4500 Series 4548-GT-PWR using a USB Mass Storage Device, ensure that the Mass Storage Device has the desired software version and is inserted into the front panel USB port.
- If you use the CLI, ensure that the CLI is in Privileged EXEC mode.
- If you use the Device Manager, ensure that SNMP is enabled.
- If you use the Web-based Management Interface, ensure that you use **read/write** access.

For details about updating switch software, see the following sections:

- "Changing switch software in the CLI" (page 82)
- "Changing switch software in the Java Device Manager" (page 84)
- "Changing switch software in the Web-based Management Interface" (page 87)
- "LED activity during software download" (page 89)

Changing switch software in the CLI

To change the software version that runs on the switch using the CLI, perform the following procedure.

Step	Action
1	Access the CLI through the Telnet protocol or through a Console connection. For detailed information about this subject, see "Accessing the CLI" (page 19) .
2	From the command prompt, use the download command with the following parameters to change the software version: <pre>download [address <ip>] {image <image name> image-if-newer <image name> diag <image name> poe_module_image <image name>} [no-reset] [usb]</pre> <p>"download parameters" (page 82) explains the parameters for the <code>download</code> command.</p>

download parameters

Parameter	Description
address <ip>	The IP address of the TFTP server you use. The address <ip> parameter is optional and if you omit it, the switch defaults to the TFTP server specified by the <code>tftp-server</code> command unless software download is to occur using a USB Mass Storage Device.
image <image name>	The name of the software image to be downloaded from the TFTP server.
image-if-newer <image name>	This parameter is the name of the software image to be downloaded from the TFTP server if it is newer than the currently running image.
The <code>image</code> , <code>image-if-newer</code> , <code>diag</code> , and <code>poe_module_image</code> parameters are mutually exclusive; you can execute only one at a time. The address <ip> and <code>usb</code> parameters are mutually exclusive; you can execute only one at a time.	

Parameter	Description
diag <image name>	The name of the diagnostic image to be downloaded from the TFTP server.
poe_module_image <image name>	The name of the Power over Ethernet module image to be downloaded from the TFTP server. This option is available only for 4500 Series switches that support Power Over Ethernet.
no-reset	This parameter forces the switch to not reset after the software download is complete.
usb	In the Nortel Ethernet Routing Switch 4500 Series switch, this parameter specifies that the software download is performed using a USB Mass Storage Device and the front panel USB port.
<p>The <code>image</code>, <code>image-if-newer</code>, <code>diag</code>, and <code>poe_module_image</code> parameters are mutually exclusive; you can execute only one at a time.</p> <p>The <code>address <ip></code> and <code>usb</code> parameters are mutually exclusive; you can execute only one at a time.</p>	

3 Press **Enter**.

—End—

The software download occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download. Depending on network conditions, this process may take up to 10 minutes.

When the download is complete, the switch automatically resets unless you used the `no-reset` parameter. The software image initiates a self-test and returns a message when the process is complete. An example of this message is illustrated in "[Software download message output](#)" (page 83).

Software download message output

```
Download Image [/]

Saving Image [-]

Finishing Upgrading Image
```

During the download, the switch is not operational.

You can track the progress of the download by observing the front panel LEDs. For more information about this topic, see "[LED activity during software download](#)" (page 89).

Changing switch software in the Java Device Manager

To change the software version running on the switch that uses the Java Device Manager, perform the following procedure.

Step	Action
------	--------

1	Connect to the switch using the Java Device Manager (JDM) . For specific information about this topic, see " Opening a Switch with the Java Device Manager " (page 40).
---	--

2	From the JDM menu, select Edit > File System .
---	--

The File System screen appears, as shown in "[Java Device Manager File System screen](#)" (page 84).

Java Device Manager File System screen

3	Select the Config/Image/Diag file tab if it is not already selected.
---	---

4	Specify the information necessary to perform the download. " File System screen fields " (page 84) outlines each field on this screen.
---	--

File System screen fields

Field	Description
LoadServerAddr	The IP address of the TFTP server on which the new software images are stored for download.

Field	Description
BinaryConfigFileName	The binary configuration file currently associated with the switch. Use this field when you work with configuration files; do not use this field when you download a software image. For further information, see " Working with configuration files " (page 90).
ImageFileName	The name of the image file currently associated with the switch. If needed, change this field to the name of the software image to be downloaded.
FwFileName (Diagnostics)	The name of the diagnostic file currently associated with the switch. If needed, change this field to the name of the diagnostic software image to be downloaded.
UsbTargetUnit	Indicates the unit number of the USB port to be used to upload or download a file.
Action	<p>This group of options represent the actions taken during this file system operation. The options applicable to a software download are</p> <ul style="list-style-type: none"> • <code>dnldImgFromUsb</code>: Download a new software image to the switch using the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. • <code>dnldImgIfNewer</code>: Download a new software image to the switch only if it is newer than the one currently in use. • <code>dnldFw</code>: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. • <code>dnldConfig</code>: Download a configuration to the switch. • <code>dnldConfigFromUsb</code>: Download a configuration to switch using the front panel USB port. • <code>dnldImgNoReset</code>: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer

Field	Description
	<p>or older than the current image. After the download is complete, the switch is not reset.</p> <ul style="list-style-type: none"> • dnldFwNoReset: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • upldConfig: Upload a configuration to the switch from a designated location. • dnldImg: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. • dnldImgFromUsb: Download a new software image to the switch using the front panel USB port. • dnldFwFromUsb: Download a new diagnostic software image to the switch from the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. <p>Note: For information about additional options, see "Working with configuration files" (page 90).</p>
Status	<p>Display the status of the last action that occurred since the switch last booted. The values that are displayed are</p> <ul style="list-style-type: none"> • other: No action occurred since the last boot. • inProgress: The selected operation is in progress. • success: The selected operation succeeded. • fail: The selected operation failed.

- 5 Click **Apply**.

—End—

The software download occurs automatically after you click Apply. This process erases the contents of flash memory and replaces it with the new software image. Do not interrupt the download. Depending on network conditions, this process can take up to 10 minutes. When the download is complete, the switch automatically resets and the new software image initiates a self-test. During the download, the switch is not operational.

Changing switch software in the Web-based Management Interface

To change the software version running on the switch that uses the Web-based Management Interface, perform the following procedure.

Step Action

- 1 Log in to the Web-based Management Interface. For specific information about this topic, see ["Accessing the Web-based Management Interface"](#) (page 57).
- 2 Navigate to the Software Download Management page by selecting **Configuration > Software Download**.

The Software Download Management page appears, as shown in ["Software Download Management page"](#) (page 87).

Software Download Management page

- 3 Specify the information needed to complete the software download procedure. "Software download page fields" (page 88) outlines each field on this page.

Software download page fields

Field	Description
Current Running Version	The version of software currently running on the switch.
Local Store Version	The version of software currently stored in flash memory.
Software Image File Name	The name of the software image to be downloaded to the switch. This field is optional if you perform a diagnostics image download only. The field is 1 to 30 characters in length.
Diagnostics Image File Name	The name of the diagnostics image to be downloaded on to the switch. This field is optional if you perform a software image download only. The field is 1 to 30 characters in length.
Select Target	The target from which the software images are downloaded. Select either TFTP Server or USB as the download target.
TFTP Server IP Address	The IP address of the TFTP Server to be used in the software download.
Start TFTP Load of New Image	The type of software download to perform. Select the appropriate option from the list: <ul style="list-style-type: none"> • No: Perform no software download. • Software Image: Perform a download of the software image specified in the Software Image File Name field regardless of whether it is newer than the current software image. • Diagnostics: Perform a download of the diagnostics image specified in the Diagnostics Image File Name field. • Software Image If Newer: Perform a download of the software image specified in the Software Image File Name field only if it is newer than the current image.

- | | |
|--|---|
| | <ul style="list-style-type: none">• Download without Reset: Perform a download of the specified software images and do not reset the switch at the end of the process. |
|--|---|

4 Click **Submit**.

—End—

The software download occurs automatically after you click Submit. This process erases the contents of flash memory and replaces it with the new software image. Do not interrupt the download. Depending on network conditions, this process can take up to 10 minutes. When the download is complete, the switch automatically resets and the new software image initiates a self-test. During the download, the switch is not operational.

LED activity during software download

During the software download, the port LEDs light one after another in a chasing pattern, except for ports 35, 36, 47, and 48 on a Nortel Ethernet Routing Switch 4500 Series 4548GT.

This chasing pattern is initially fast as the software image is downloaded but gradually slows as the switch erases the flash memory. This pattern speeds up again as the switch programs the new image into the flash memory.

When the process is complete, the port LEDs are no longer lit and the switch resets.

Setting TFTP parameters

Many processes in the switch can use a Trivial File Transfer Protocol (TFTP) server. The following sections describe how to set a default TFTP server for the switch and how to clear these defaults through the CLI:

- ["Setting a default TFTP server" \(page 89\)](#)
- ["Displaying the default TFTP server" \(page 90\)](#)
- ["Clearing the default TFTP server" \(page 90\)](#)

Setting a default TFTP server

The switch processes that use a TFTP server often give the switch administrator the option to specify the IP address of a TFTP server to use. Instead of entering this address every time, the switch can store a default IP address.

Specify a default TFTP server for the switch with the `tftp-server` command. The syntax of this command is

```
tftp-server <XXX.XXX.XXX.XXX>
```

To complete the command, replace the `<XXX.XXX.XXX.XXX>` with the IP address of the default TFTP server. You must run this command in Global Configuration command mode.

Displaying the default TFTP server

You can display the default TFTP server configured for the switch in the CLI at any time by using the `show tftp-server` command. This command has no parameters and you run it in Privileged EXEC mode.

Clearing the default TFTP server

You can clear the default TFTP server from the switch and reset it to 0.0.0.0 with the following two commands:

- `no tftp-server`

This command has no parameters and you run it in Global Configuration command mode.

- `default tftp-server`

This command has no parameters and you run it in Global Configuration command mode.

Working with configuration files

This section details working with configuration files through the various switch interfaces. The administrator uses ASCII-text configuration files to quickly change the configuration of a switch.

This section contains the following topics:

- ["Configuration files in the CLI" \(page 90\)](#)
- ["Configuration files in the JDM" \(page 93\)](#)
- ["Configuration files in the Web-based Management Interface" \(page 97\)](#)
- ["Automatically downloading a configuration file" \(page 101\)](#)

Configuration files in the CLI

The CLI provides many options for working with configuration files. Through the CLI, you can display, store, and retrieve configuration files.

For details, see the following sections:

- ["Displaying the current configuration" \(page 91\)](#)
- ["Storing the current configuration" \(page 91\)](#)
- ["Restoring a system configuration" \(page 91\)](#)

- ["Saving the current configuration" \(page 92\)](#)

Displaying the current configuration

To display the current configuration of switch or a stack, use the `show running-config` command, with the following syntax, in Privileged EXEC command mode with no parameters:

- `show running-config`

Storing the current configuration

To copy the contents of the current configuration file to another location for storage, use the `copy running-config` command, with the following syntax, in Privileged EXEC command mode:

- `copy running-config {tftp | (usb)} address <XXX.XXX.XXX.XXX> filename <name>`

For all switches in the 4500 Series, you can save the configuration file to a TFTP server. On the Nortel Ethernet Routing Switch 4500 Series, you can save the configuration file to a USB Mass Storage Device through the front panel USB drive.

["copy running-config parameters" \(page 91\)](#) outlines the parameters for using this command.

copy running-config parameters

Parameter	Description
{tftp usb}	Specify a location to save the configuration file.
address <XXX.XXX.XXX.XXX>	If you use a TFTP server, specify the IP address.
filename <name>	The name of the file that is created when you save the configuration to the TFTP server or to a USB Mass Storage Device.

Restoring a system configuration

The CLI provides three commands for restoring a system configuration to a switch:

- `copy tftp config`

Use this command to restore a configuration file from a TFTP server. The syntax is

```
— copy tftp config address <XXX.XXX.XXX.XXX>
  filename <name>
```

"[copy tftp config parameters](#)" (page 92) outlines the parameters for this command.

copy tftp config parameters

Parameter	Description
address <XXX.XXX.XXX.XXX>	The IP address of the TFTP server.
filename <name>	The name of the file to be retrieved.

- **copy usb config**

Use this command to restore a configuration file from a USB Mass Storage Device. The syntax is

— **copy usb config filename <name>**

The only parameter for this command is the name of the file to be retrieved from the USB device.

- **copy tftp config**

Use this command to copy the configuration of a switch in a stack to a stand-alone switch and to replace units in the stack. The syntax is

— **copy tftp config address <XXX.XXX.XXX.XXX>
filename <name> unit <unit number>**

"[copy tftp config parameters](#)" (page 92) outlines the parameters for this command.

copy tftp config parameters

Parameter	Description
address <XXX.XXX.XXX.XXX>	The IP address of the TFTP server.
filename <name>	The name of the file.
unit <unit number>	The number of the stack unit.

Saving the current configuration

The configuration currently in use on a switch is regularly saved to the flash memory automatically. However, you can manually initiate this process using the **copy config nvram** command. This command takes no parameters and you must run it in Privileged EXEC mode. If you have disabled the AutosaveToNvramEnabled function by removing the default check in the AutosaveToNvRamEnabled field, the configuration is not automatically saved to the flash memory.

Configuration files in the JDM

The Java Device Manager (JDM) provides tools to store and retrieve configuration files.

For details, see the following topics:

- "Storing the current ASCII configuration" (page 93)
- "Retrieving an ASCII configuration file" (page 94)
- "Storing a binary configuration file" (page 95)
- "Retrieving a binary configuration file" (page 96)

Storing the current ASCII configuration

To store the current ASCII switch configuration file to a TFTP server or USB storage device, perform the following procedure.

Step	Action
1	Open the JDM FileSystem screen by selecting Edit > File System from the JDM menu.
2	Select the Ascii Config File tab. This tab is displayed in "AsciiConfigFile tab" (page 93).

AsciiConfigFile tab

10.127.232.30 - FileSystem

Config/Image/Diag file | **Ascii Config File** | Save Configuration

LoadServerAddr: 10.127.125.101

AsciiConfigFilename:

UsbTargetUnit: 0 0..9 (1-8=usb in stack, 9=usb in standalone unit, 0=tftp server)

AsciiConfigAutoDownload: disabled useBootp useConfig

AsciiConfigAutoDldStatus: passed

AsciiConfigManualDownload: downloadNow downloadFromUsb

AsciiConfigManualDldStatus: passed

AsciiConfigManualUpload: uploadNow uploadToUsb

AsciiConfigManualUpldStatus: passed

Apply Refresh Close Help...

- 3 In the **LoadServer Addr** field, type the IP address of the desired TFTP server. If the configuration file is saved to a USB storage device, skip this step.
- 4 In the **AsciiConfigFilename** field, type the name under which to store the configuration file.
- 5 If you save the configuration file to a USB storage device, enter the stack unit number in which the USB device is inserted in the **UsbTargetUnit** field.
- 6 Select **uploadNow** in the **AsciiConfigManualUpload** field to transfer the file to a TFTP server; or, select **uploadToUsb** in the **AsciiConfigManualUpload** field to transfer the file to a USB mass storage device.
- 7 Click **Apply**.
- 8 Check the **AsciiConfigManualUpldStatus** field for the file transfer status. If the status of the file upload is **InProgress**, wait for up to 2 minutes, and then click **Refresh** to see any new status applied to the upload. The file upload is complete when the status displays either **Passed** or **Failed**.

—End—

Retrieving an ASCII configuration file

To retrieve an ASCII configuration file from a TFTP server or from a USB storage device and apply it to the switch, perform the following procedures.

Step	Action
1	Open the JDM FileSystem screen by selecting Edit > File System from the JDM menu.
2	Select the Ascii Config File tab. This tab is displayed in "AsciiConfigFile tab" (page 93).
3	If you retrieve the configuration file from a USB storage device, skip this step. Otherwise, in the LoadServer Addr field, type the IP address of the desired TFTP server.
4	In the AsciiConfigFilename field, type the name under which to store the configuration file.
5	If you retrieve the configuration file from a USB storage device, enter the stack unit number in which the USB device is inserted in the UsbTargetUnit field.

- 6 Select **downloadNow** in the **AsciiConfigManualDownload** field to transfer the file from a TFTP server; or, select **downloadFromUsb** in the **AsciiConfigManualDownload** field to transfer the file from a USB mass storage device.
- 7 Click **Apply**.
- 8 Check **AsciiConfigManualDldStatus** field for the file transfer status. If the status of the file download is **inProgress**, wait for up to 2 minutes, and then click **Refresh** to see any new status applied to the download. The file download is complete when the status displays either **Passed** or **Failed**.

—End—

Storing a binary configuration file

To store the current binary configuration file to a TFTP server or a USB storage device, perform the following procedure.

Step	Action
1	Open the FileSystem screen by selecting Edit > File System from the JDM menu.
2	Select the Config/Image/Diag file tab. This tab is illustrated in " Java Device Manager File System screen " (page 84).
3	If the file is stored on a USB storage device, skip this step; otherwise, if a default TFTP server is not already specified (or another TFTP server is to be used), enter the IP address of the TFTP server to use in the LoadServerAddr field.
4	In the BinaryConfigFilename field, enter the name to assign to the configuration file.
5	If the configuration file to be stored is part of a stack, enter the stack unit number in the BinaryConfigUnitNumber field. If it is a stand-alone unit, specify 0.
6	If you save the configuration file to a USB storage device, enter the stack unit number in which the USB device is inserted in the UsbTargetUnit field.
7	In the Action field, select upldConfig to upload the file to a TFTP server or upldConfigtoUsb to upload the configuration file to a USB storage device.
8	Click Apply .

—End—

Retrieving a binary configuration file

To retrieve a binary configuration file from a TFTP server, perform the following procedure.

Step	Action
1	Open the FileSystem screen by selecting Edit > File System from the JDM menu.
2	Select the Config/Image/Diag file tab. This tab is illustrated in " Java Device Manager File System screen " (page 84).
3	If you retrieve the file from a USB storage device, skip this step; otherwise, if a default TFTP server is not already specified (or another TFTP server is to be used), enter the IP address of the TFTP server to use in the LoadServerAddr field.
4	In the BinaryConfigFilename field, enter the name of the configuration file to retrieve.
5	If the configuration file to be retrieved to a member of a stack, enter the stack unit number in the BinaryConfigUnitNumber field. If it is a stand-alone unit, specify 0.
6	If you retrieve the configuration file from a USB storage device, enter the stack unit number in which the USB device is inserted in the UsbTargetUnit field.
7	In the Action field, select dnldConfig to download the file from a TFTP server or dnldConfigFromUsb to download the file from a USB storage device.
8	Click Apply .

—End—

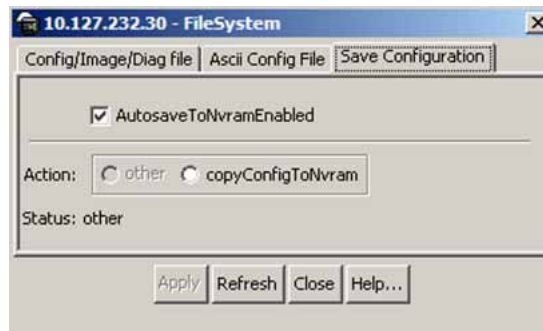
Saving the current configuration

The configuration currently in use on a switch is regularly saved to the flash memory automatically. However, you can manually initiate this process using the **Save Configuration** tab.

If you have disabled the AutosaveToNvramEnabled function by removing the default check in the AutosaveToNvRamEnabled field on the Save Configuration tab, the configuration is not automatically saved to the flash memory.

To save the current configuration manually:

- | Step | Action |
|------|---|
| 1 | From the JDM menu, select Edit > File System Open by . the FileSystem dialog box appears with the Config/Image/Diag file tab displayed. |
| 2 | Choose the Save Configuration tab.
The Save Configuration tab appears. |



- | | |
|---|---|
| 3 | In the Action field, select copyConfigToNvram . |
| 4 | Click Apply . |
| 5 | Click Refresh
The Status field displays the file copy progress. |

—End—

Configuration files in the Web-based Management Interface

The Web-based Management Interface provides tools to store and retrieve configuration files.

For details, see the following topics:

- "Storing and retrieving a configuration file through TFTP or USB" (page 98)
- "Retrieving a configuration file through HTTP or USB" (page 100)

Storing and retrieving a configuration file through TFTP or USB

Use the Configuration File Download/Upload page in the Web-based Management Interface to store or retrieve a configuration file. This page is illustrated in "Configuration File page" (page 98).

Configuration File page

The screenshot shows the 'Configuration File Setting' form with the following fields:

Field	Value
Configuration Image Filename	4548config.txt
Select Target	TFTP Server
TFTP Server IP Address	192.167.120.13
Copy Configuration Image to Target	No
Retrieve Configuration Image from Target	No

To upload (store) a configuration file from this page, complete the following procedure:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the page by selecting Configuration > Configuration File from the Web-based Management Interface. |
| 2 | Complete the fields on this page to upload the file. "File upload fields" (page 98) outlines the relevant fields. |

File upload fields

Field	Description
Configuration Image Filename	The name of the file create during the upload.
Select Target	The location of the uploaded file. This can be either TFTP (TFTP Server) or USB (USB Mass Storage Device).
TFTP Server IP Address	The IP address of the TFTP server if applicable.

Field	Description
Copy Configuration Image To Target	To perform a file upload, select YES from this list.
Retrieve Configuration Image From Target	To perform a file upload, select NO from this list.

- 3 Click **Submit**.

—End—

To download (retrieve) a configuration file from this page, complete the following procedure:

Step	Action
1	Open the page by selecting Configuration > Configuration File from the Web-based Management Interface.
2	Complete the fields on this page to download the file. " File download fields " (page 99) outlines the relevant fields.

File download fields

Field	Description
Configuration Image Filename	The name of the file to retrieve during the download process.
Select Target	The location of the file to download. This can be either TFTP (TFTP Server) or USB (USB Mass Storage Device).
TFTP Server IP Address	The IP address of the TFTP server to use if applicable.
Copy Configuration Image To Target	To perform a file download, select NO from this list.
Retrieve Configuration Image From Target	To perform a file upload, select YES from this list.
Target Unit For Retrieve	This field is available only in stand-alone switches. Instead of downloading a fixed configuration file, you can download the configuration from another switch in stack when you replace a particular stack unit. Select a number from this list if this is the desired type of file download. The configuration of the selected unit is downloaded to the current switch.

- 3 Click **Submit**.

—End—

Retrieving a configuration file through HTTP or USB

"Ascii Configuration File Download page" (page 100) illustrates the Ascii Configuration File download page.

Ascii Configuration File Download page

You can download an ASCII configuration file either from a computer or through the switch USB port.

To download an ASCII configuration file from a computer, use the following procedure.

Step	Action
------	--------

- 1 Select **Configuration > Ascii Config Download** to open the page from the Web-based Management Interface.
- 2 In the **Ascii Configuration File Download Setting** table, type the name of the file, including the full local path, in the **Ascii Configuration File** field. Alternatively, click **Browse** and select the file from the dialog window.
- 3 Click **Submit**.

—End—

The **Last Manual Configuration Status** field displays the outcome of the operation.

To download the configuration file through the USB port, perform the following procedure.

Step	Action
1	Select Configuration > Ascii Config Download to open the page from the Web-based Management Interface.
2	In the Ascii Configuration USB File Download Setting table, type the name of the file, and supply the necessary information to complete the file download. " Ascii USB file download fields " (page 101) outlines the available fields.

Ascii USB file download fields

Field	Description
Select Target	The target from which the file is downloaded. The only option in this case is USB .
Ascii Configuration File	The name of the configuration file to download to the switch.
Retrieve Configuration File from Target	To proceed with the file transfer, change the value in the list from NO to YES .

3 Click **Submit**.

—End—

The **Last Manual Configuration Status** field displays the outcome of the operation.

Automatically downloading a configuration file

You can configure the switch to automatically download a configuration when it boots. This section describes how to configure a switch to perform this task:

- "[Using the CLI](#)" (page 101)
- "[Using the JDM](#)" (page 102)

Using the CLI

Enable this feature through the CLI by using the `configure network` command. Use this command to immediately load and run a script and to configure parameters to automatically download a configuration file when the switch or stack is booted.

The syntax for the `configure network` command is

```
configure network load-on-boot {disable | use-bootp |
use-config} address <XXX.XXX.XXX.XXX> filename <name>
```

"configure network parameters" (page 102) outlines the parameters for this command.

configure network parameters

Parameter	Description
load-on-boot {disable use-bootp use-config}	<p>The settings to automatically load a configuration file when the system boots:</p> <ul style="list-style-type: none"> • disable: disable the automatic loading of config file • use-bootp: load the ASCII configuration file at boot and use BootP to obtain values for the TFTP address and file name • use-config: load the ASCII configuration file at boot and use the locally configured values for the TFTP address and file name <p>Note: If you omit this parameter, the system immediately downloads and runs the ASCII configuration file.</p>
address <XXX.XXX.XXX.XXX>	The IP address of the TFTP server.
filename <name>	The name of the configuration file to use in this process

You must run this command in the Privileged EXEC mode.

You can view the current switch settings for this process using the `show config-network` command. This command takes no parameters.

Using the JDM

Enable this feature through the Java Device Manager (JDM) by using the **File System** screen. To automatically download a configuration file, perform the following procedure.

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the File System screen by selecting Edit > File System from the JDM menu. |
|---|---|

- 2 Select the **AsciiConfigFile** tab. This tab is illustrated in "AsciiConfigFile tab" (page 93).
- 3 In the **LoadServerAddr** field, type the IP address of the desired TFTP server.
- 4 In the **AsciiConfigFilename** field, type the name of the configuration file to use.
- 5 From the **AsciiConfigAutoDownload** field, select the option to specify how to download the configuration file:
 - **disabled**: Disable automatic downloading.
 - **useBootp**: Obtain the settings needed to connect to the TFTP server that contains the configuration file. Using this option overrides the value in the **LoadServerAddr** field.
 - **useConfig**: Use the TFTP settings on the screen to connect to the TFTP server.
- 6 Click **Apply**.
- 7 Click **Refresh** to check AsciiConfigAutoDldStatus field for automatic download configuration file status.

The automatic download configuration file status can be one of the following:

- passed
- in progress
- failed

—End—

Terminal setup

You can customize switch terminal settings to suit the preferences of a switch administrator. You must perform this operation in the Command Line Interface.

The **terminal** command configures terminal settings. These settings include terminal length and terminal width.

The syntax of the **terminal** command is

```
terminal length <0-132> width <1-132>
```

Run the terminal command in User EXEC command mode. "[terminal parameters](#)" ([page 104](#)) describes the parameters and variables for the terminal command.

terminal parameters

Parameter	Description
length	Set the length of the terminal display in lines; the default is 23. Note: If you set the terminal length to 0, the pagination is disabled and the display scrolls continuously.
width	Set the width of the terminal display in characters; the default is 79.

You can use the `show terminal` command at any time to display the current terminal settings. This command takes no parameters and you must run it in the EXEC command mode.

Setting Telnet access

You can access the CLI through a Telnet session. To access the CLI remotely, the management port must have an assigned IP address and remote access must be enabled.

Note: Multiple users can simultaneously access the CLI system through the serial port, a Telnet session, and modems. The maximum number of simultaneous users is 4, plus 1 each at the serial port for a total of 12 users on the stack. All users can configure the switch simultaneously.

For details about viewing and changing the Telnet-allowed IP addresses and settings, see the following sections:

- "[telnet-access command](#)" ([page 104](#))
- "[no telnet-access command](#)" ([page 105](#))
- "[default telnet-access command](#)" ([page 106](#))

telnet-access command

The `telnet-access` command configures the Telnet connection that you use to manage the switch. Run the `telnet-access` command through the console serial connection.

The syntax for the `telnet-access` command is

```
telnet-access [enable | disable] [login-timeout <1-10>]
[retry <1-100>] [inactive-timeout <0-60>] [logging {none
```



```
| access | failures | all}] [source-ip <1-50>
<XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]
```

Run the `telnet-access` command in Global Configuration command mode.

"[telnet-access parameters](#)" (page 105) describes the parameters for the `telnet-access` command.

telnet-access parameters

Parameters	Description
enable disable	Enable or disable Telnet connection.
login-timeout <1-10>	Specify in minutes the time for the Telnet connection to be established after the user connects to the switch. Enter an integer from 1 to 10.
retry <1-100>	Specify the number of times the user can enter an incorrect password before the connection closes. Enter an integer from 1 to 100.
inactive-timeout <0-60>	Specify in minutes the duration before an inactive session terminates.
logging {none access failures all}	Specify the events for which you want to store details in the event log: none: Do not save access events in the log. access: Save only successful access events in the log. failure: Save failed access events in the log. all: Save all access events in the log.
[source-ip <1-50> <XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]	Specify the source IP address from which connections can occur. Enter the IP address in dotted-decimal notation. Mask specifies the subnet mask from which connections can occur; enter IP mask in dotted-decimal notation.

no telnet-access command

The `no telnet-access` command disables the Telnet connection. The `no telnet-access` command is accessed through the console serial connection.

The syntax for the `no telnet-access` command is

```
no telnet-access [source-ip [<1-50>]]
```

Run the `no telnet-access` command in Global Configuration command mode.

"no telnet-access parameters" (page 106) describes the parameters and variables for the `no telnet-access` command.

no telnet-access parameters

Parameters and variables	Description
source-ip [<1-50>]	<p>Disable the Telnet access.</p> <p>When you do not use the optional parameter, the source-ip list is cleared, which means the first index is 0.0.0.0/0.0.0.0. and the second to fiftieth indexes are 255.255.255.255/255.255.255.255.</p> <p>When you specify a source-ip address, the specified pair is 255.255.255.255/255.255.255.255.</p> <p>Note: These same source IP addresses are in the IP Manager list. For more information about the IP Manager list, see Chapter 3.</p>

default telnet-access command

The `default telnet-access` command sets the Telnet settings to the default values.

The syntax for the `default telnet-access` command is

```
default telnet-access
```

Run the `default telnet-access` command in Global Configuration command mode.

Setting server for Web-based management

You can use the CLI to enable or disable a Web server for use with the Web-based Management Interface. For details, see the following sections.

- "Web-server command" (page 106)
- "no Web-server command" (page 107)

web-server command

The `web-server` command enables or disables the Web server used for Web-based management.

The syntax for the `web-server` command is

```
web-server {enable | disable}
```

Run the `web-server` command in Global Configuration command mode.

"[Web-server parameters](#)" (page 107) describes the parameters and variables for the `web-server` command.

web-server parameters

Parameters and variables	Description
enable disable	Enable or disable the Web server.

no web-server command

The `no web-server` command disables the Web server used for Web-based management.

The syntax for the `no web-server` command is

```
no web-server
```

Run the `no web-server` command in Global Configuration command mode.

Setting boot parameters

The command described in this section is used to boot the switch or stack and to set boot parameters.

boot command

The `boot` command performs a soft-boot of the switch or stack.

The syntax for the `boot` command is

```
boot [default] [unit <unitno>]
```

Run the `boot` command in Privileged EXEC command mode.

The table "boot parameters" (page 108) describes the parameters for the `boot` command.

boot parameters

Parameters and variables	Description
default	Restore switch or stack to factory-default settings after rebooting.
unit <unitno>	Specify which unit of the stack is rebooted. This command is available only in stack mode. Enter the unit number of the switch you want to reboot.

Note: When you reset to factory defaults, the switch or stack retains the stack operational mode, the last reset count, and the reason for the last reset; these three parameters are not reset to factory defaults.

Defaulting to BootP-when-needed

The BootP default value is BootP-when-needed. The switch can boot and the system can automatically seek a BootP server for the IP address.

If the device has an assigned IP address and the BootP process times out, the BootP mode remains in the default mode BootP-when-needed.

However, if the device has no assigned IP address and the BootP process times out, the BootP mode automatically changes to BootP disabled. This change to BootP disabled is not stored, and the BootP reverts to the default value of BootP-when-needed after the device reboots.

When you upgrade the system, the switch retains the previous BootP value. When the switch resets to default after an upgrade, the system moves to the default value of BootP-when-needed.

Configuring with the command line interface

This section covers the CLI commands needed to configure BootP parameters:

- "ip bootp server command" (page 108)
- "no ip bootp server command" (page 109)
- "default ip bootp server command" (page 109)

ip bootp server command

The `ip bootp server` command configures BootP on the current instance of the switch or server. Use this command to change the value of BootP from the default value, which is BootP-when-needed.

The syntax for the `ip bootp server` command is

```
ip bootp server {always | disable | last | needed}
```

Run the `ip bootp server` command in Global Configuration command mode.

"[ip bootp server parameters](#)" (page 109) describes the parameters for the `ip bootp server` command.

ip bootp server parameters

Parameters and variables	Description
always disable last needed	<p>Specify when to use BootP:</p> <ul style="list-style-type: none"> • always: Always use BootP. • disable: Never use BootP. • last: Use BootP or the last known address. • needed: Use BootP only when needed. <p>Note: The default value is to use BootP when needed.</p>

no ip bootp server command

The `no ip bootp server` command disables the BootP server.

The syntax for the `no ip bootp server` command is

```
no ip bootp server
```

Run the `no ip bootp server` command in Global Configuration command mode.

default ip bootp server command

The default `ip bootp server` command uses BootP when needed.

The syntax for the `default ip bootp server` command is

```
default ip bootp server
```

Run the `default ip bootp server` command in Global Configuration command mode.

Customizing the CLI banner

You can configure the banner that is presented when a user logs in to the switch through the CLI to a user-defined value. The banner cannot exceed 1539 bytes, or 19 rows by 80 columns plus line termination characters.

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

To customize the CLI banner using the CLI, see the following commands:

- ["show banner command" \(page 110\)](#)
- ["banner command" \(page 110\)](#)
- ["no banner command" \(page 111\)](#)

To customize the CLI banner using Java Device Manager, see the following:

- ["Banner tab" \(page 111\)](#)
- ["Custom Banner tab" \(page 113\)](#)

show banner command

The `show banner` command displays the banner.

The syntax for the `show banner` command is

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

Run the `show banner` command in Privileged EXEC command mode.

["show banner parameters" \(page 110\)](#) describes the parameters for the `show banner` command.

show banner parameters

Parameters and variables	Description
static custom	Specify which banner is currently set to be displayed: <ul style="list-style-type: none"> • static • custom

banner command

The `banner` command specifies the banner that is displayed at startup; either static or custom.

The syntax for the banner command is

```
banner {static | custom} <line number> "<LINE>"<disabled>
```

"[banner parameters](#)" (page 111) describes the parameters for this command.

banner parameters

Parameters and variables	Description
static custom	Set the display banner as <ul style="list-style-type: none"> • static • custom
line number	Enter the banner line number you are setting. The range is 1 to 19.
LINE	Specify the characters in the line number.
disabled	Disable the banner display.

Run the **banner** command in Global Configuration command mode.

no banner command

The **no banner** command clears all lines of a previously stored custom banner. This command sets the banner type to the default setting (STATIC).

The syntax for the **no banner** command is

```
no banner
```

Run the **no banner** command in Global Configuration command mode.

Banner tab

The Banner tab controls the CLI banner display.

To configure the Banner Control, perform the following procedure.

Step	Action
1	Open the Edit Chassis screen in the manner detailed at the beginning of this section.
2	Select the Banner tab, as illustrated in " Edit Chassis screen -- Banner tab " (page 112).

Edit Chassis screen--Banner tab

—End—

The following table "Banner tab items" (page 112) describes the **Banner** tab items.

Banner tab items

Field	Description
BannerControl	<p>Specify the banner to be displayed as soon as you connect to a Nortel Ethernet Routing Switch 4500 Series device. BannerControl has the following three options:</p> <ul style="list-style-type: none"> • The static option uses the predefined static banner. • The custom option uses the previously set custom banner. • The disabled option prevents the display of any banner.

See also:

- "System tab" (page 216)
- "Base Unit Info tab" (page 219)
- "Stack Info tab" (page 221)
- "Agent tab" (page 224)
- SNMP tab
- Trap Receivers tab
- " Power Supply tab" (page 226)
- " Fan tab" (page 227)
- "Custom Banner tab" (page 113)

Custom Banner tab

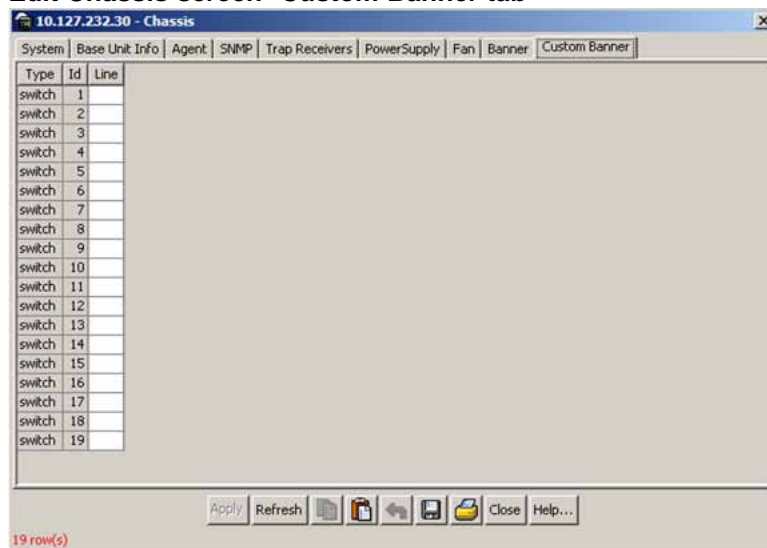
Use the Custom Banner tab to customize the CLI banner display.

To customize the banner display, perform the following procedure.

Step	Action
1	Open the Edit Chassis screen in the manner detailed at the beginning of this section.
2	Select the Custom Banner tab, as shown in " Edit Chassis screen -- Custom Banner tab " (page 113).

—End—

Edit Chassis screen--Custom Banner tab



The following table "[Custom Banner tab](#)" (page 113) describes the Custom Banner tab fields.

Custom Banner tab

Field	Description
Type	Identify the banner type. Two banner types are available: one type is used in switch or stand-alone mode while the other is used in the stack mode.
Id	Identify the line of text within a custom banner
Line	Display one line of a 19-line banner. If the line contains non printable ASCII characters, then the line is rejected and an error message is returned.

Displaying complete GBIC information

You can obtain complete information for a GBIC port using the following command:

```
show interfaces gbic-info <port-list>
```

Substitute `<port-list>` with the GBIC ports for which to display information. If no GBIC is detected, this command shows no information.

This command is available in all command modes.

Displaying hardware information

To display a complete listing of information about the status of switch hardware in the CLI, use the following command:

```
show system [verbose]
```

The `[verbose]` option displays additional information about fan status, power status, and switch serial number.

Switch hardware information is displayed in a variety of locations in the Web-based Management Interface and Java Device Manager. You need no special options in these interfaces to display the additional information.

Shutdown command

The switch administrator can use this feature to safely shut down the switch without interrupting a process or corrupting the software image.

After you issue the command, the configuration is saved and blocking is performed, and the user is notified that it is safe to power off the switch. This notification is supplied every second until the switch is shut down manually or the command automatically resets the switch.

The syntax for the `shutdown` command is

```
shutdown [<minutes_to_wait>]
```

Substitute `<minutes_to_wait>` with the number of minutes to wait for user intervention before the switch resets. If this parameter is not specified, the switch waits for 10 minutes before resetting.

Use the shutdown command to safely shut down and power off the switch. After you initiate the shutdown command, the switch saves the current configuration which allows users to power off the switch within the specified time period (1 to 60 minutes); otherwise, the switch performs a reset.

When you initiate the shutdown command in the CLI, the following message appears: **Shutdown (y/n) ?**

Enter **yes** at this prompt to shut down the switch.

The following warning message appears:

```
Warning the switch/stack has been set to reboot in <xx>
minutes. Current configuration has been saved, no
further configuration changes can be saved until reboot
occurs or 'shutdown cancel' command is issued.
```

The syntax for the shutdown command is

```
shutdown [force] [minutes-to-wait <1-60> [cancel]]
```

After you initiate the shutdown command, all existing and subsequent sessions display the following message:

```
Stack will reset in <xxxx> seconds.
```

While existing CLI sessions do not receive a warning message, all subsequent CLI sessions display the following message:

```
The shutdown process is in progress. It is safe to
poweroff the stack. Configuration changes will not be
saved. Shutdown has blocked the flash. Autoreset in
<xxxx> seconds.
```

Neither Web-based management nor Device Manager receives any shutdown warning messages.

The following table describes the parameters and variables for the **shutdown** command.

Shutdown command parameters and variables

Parameters and variables	Description
force	Instruct the switch to skip the shutdown confirmation prompt.
minutes-to-wait <1-60>	Specify the number of minutes that pass before the switch resets itself. The default wait time is 10 minutes.
cancel	Cancel all scheduled switch shutdowns.

Note: Any configurations or logins performed on the switch after you initiate the shutdown command are not saved to NVRAM and are lost after the reset.

Run the **shutdown** command in **privExec** command mode.

Reload command

The `reload` CLI command provides you with a configuration rollback mechanism to prevent loss of connectivity to a switch, typically for remote configurations.

Use the `reload` command to temporarily disable the autosave feature for a specified time period (1 to 60 minutes), so you can make configuration changes on remote switches without affecting the currently saved configuration.

During the interval in which the autosave feature is disabled by the `reload` command, you must use the `copy config nvram` command to manually save your configurations.

Initiate the `reload` command before you start the switch configuration commands. After you initiate the command in the CLI, the following message appears:

```
Reload (y/n) ?
```

Enter **yes** at this prompt to set the switch reload.

The following warning message appears:

```
Warning the switch/stack has been set to reload in <xx>
minutes. Current configuration has NOT been saved.
Configuration must be explicitly saved.
```

After the reload timer expires, the switch resets, reloads the last saved configuration, and re-enables the autosave feature.

The syntax for the `reload` command is

```
reload [force] [minutes-to-wait <1-60>] [cancel]
```

The following table describes the parameters and variables for the `reload` command.

Reload command parameters and variables

Parameters and variables	Description
<code>force</code>	Instruct the switch to skip the reload confirmation prompt.
<code>minutes-to-wait <1-60></code>	Specify the number of minutes that pass before the switch resets itself. The default wait time is 10 minutes.
<code>cancel</code>	Cancel all scheduled switch reloads.

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

The `reload` command provides you with a safeguard against any misconfigurations when you perform dynamic configuration changes on a remote switch.

The following example describes how you can use the `reload` command to prevent connectivity loss to a remote switch:

- Enter the CLI command `reload force 30`. This instructs the switch to reboot in 30 minutes and load the configuration from NVRAM. During the 30-minute period, autosave of the configuration to NVRAM is disabled.
- Execute dynamic switch configuration commands, which take effect immediately. These configurations are not saved to NVRAM.
- If the configurations cause no problems and switch connectivity is maintained, you can perform one of the following tasks:
- Save the current running configuration using the `copy config nvram` command.
- Cancel the reload using the `reload cancel` command.

If you make an error while executing the dynamic switch configuration commands that results in loss of switch connectivity (for example, if you make an error in the IP address mask, in the MLT configuration, or in VLAN trunking), the `reload` command provides you with a safeguard. When the reload timer expires, the switch reboots to the last saved configuration, and connectivity is re-established. Consequently, you need not travel to the remote site to reconfigure the switch.

CLI Help

To obtain help on the navigation and use of the Command Line Interface (CLI), use the following command:

```
help {commands | modes}
```

Use `help commands` to obtain information about the commands available in the CLI organized by command mode. A short explanation of each command is also included.

Use `help modes` to obtain information about the command modes available and the CLI commands used to access them.

These commands are available in any command mode.

About the Nortel Ethernet Routing Switch 4500 Series

This chapter provides a general overview of the functionality and capabilities of the Nortel Ethernet Routing Switch 4500 Series. This chapter contains information the following topics:

- "Hardware features" (page 119)
- "Auto Unit Replacement" (page 121)
- "Features of the Nortel Ethernet Routing Switch 4500 Series" (page 131)
- "Supported standards and RFCs" (page 144)

Hardware features

This section provides information about the hardware features of the Nortel Ethernet Routing Switch 4500 Series switch platforms.

Hardware description by model

Model	Key Features
4526FX	24 100BaseFX ports (MTRJ connector) plus 2 10/100/1000 SFP combo ports Redundant power slot for DC/DC converter installation
4550T	48 10/100BaseTX RJ-45 ports plus 2 10/100/1000 combo ports Redundant power slot for DC/DC converter installation
4550T-PWR	48 10/100BaseTX RJ-45 ports with PoE plus 2 10/100/1000 SFP combo ports
4548GT	48 10/100/1000BaseTX RJ-45 ports and 4 shared SFP ports Redundant power slot for DC/DC converter installation
4548GT-PWR	48 10/100/1000BaseTX RJ-45 ports with Power over Ethernet and 4 shared SFP ports

Cooling fans

When you install the switch, always allow enough space on both sides for adequate air flow.

See *Nortel Ethernet Routing Switch 4500 Series Installation* (NN47205-300) for detailed information about installation.

Redundant power supply

The Nortel Ethernet Routing Switch 4500 Series Power over Ethernet (PoE) switches, ERS 4548GT-PWR, and ERS 4550T-PWR, can use an optional 470-Watt (W) Nortel Ethernet Routing Switch RPS 15 redundant power supply. The RPS 15 power supply chassis is two units high and can accommodate up to three RPS modules, each supporting up to four devices, to provide redundant power and uninterrupted operation in the event of power failure. One RPS module connected to a PoE switch can provide up to 15.4 W for each port on all 48 ports. The RPS modules fit into the rear of the RPS 15 chassis. The UPS and associated battery pack module fit into the front of the chassis.

The non-PoE switches, ERS 4548GT, 4550T, and 4526FX, can use an optional 150W Nortel Ethernet Switch Power Supply Unit 10 and require the DC-DC Converter Module. The Nortel Ethernet Switch Power Supply Unit 10 provides scalable power redundancy and protection to low-wattage networking equipment. The PSU modules slide into the front of the Nortel Ethernet Routing Switch RPS 15 chassis.

DC-DC Converter Module

The DC-DC Converter Module for the non-PoE switches operates with the optional Nortel Ethernet Switch Power Supply Unit 10. The PoE switches do not require a DC-DC Converter Module.

The 100 W DC-DC Converter Module provides a Plug and Play redundant power supply unit for the Ethernet Routing Switch Series 4500 non-PoE switches. Contact your Nortel sales representative to order the converter module.

For further information about the DC-DC converter module, see *DC-DC Converter Module for the BayStack 5000 Series Switch (215081-A)*.

Stacking capabilities

You can use the Nortel Ethernet Routing Switch 4500 Series switches in either of the following configurations:

- stand-alone
- stack

The Nortel Ethernet Routing Switch 4500 Series switches have a built-in cascade port to stack up to eight units. The cascade port provides an 40-Gigabit (Gb) cascading mechanism for the stacks.

A stack can consist of any combination of Nortel Ethernet Routing Switch 4500 Series switches.

Note: All units in the stack must use the same software version.

To set up a stack, perform the following procedure.

Step	Action
1	Power down all switches.
2	Set the Unit Select switch in the back of the non base units to the off position.
3	Set the Unit Select switch in the back of the base unit to base position.
4	Ensure all cascade modules are properly seated.
5	Ensure all the cascade cables are properly connected and screwed into the unit.
6	Power up the stack.

Note: In a mixed stack, any switch can act as the base unit.

—End—

Auto Unit Replacement

You can use the Auto Unit Replacement (AUR) feature to replace a unit from a stack while retaining the configuration of the unit. This feature requires the stack power to be on during the unit replacement.

The main feature of the AUR is the ability to retain the configuration (CFG) image of a unit in a stack during a unit replacement. The retained CFG image from the old unit is restored to the new unit. Because retained CFG images are kept in the DRAM of the stack, the stack power must be on during the procedure.

Note 1: For Auto Unit Replacement to function properly, the new unit and the existing units in the stack must all run the same version of software.

Note 2: Auto Unit Replacement does not work on a stack of two units only. In this configuration, if a unit fails, the remaining unit becomes a stand-alone switch and Auto Unit Replacement does not load the configuration of the failed unit if it is replaced.

The following information also relates to this feature:

- The new unit must be the same hardware configuration as the old, including the same number of ports.

- If the administrator adds a new unit with a different hardware configuration, the configuration of this unit is used.
- If the administrator adds a new unit with the same hardware configuration, the previous configuration of the new unit is lost. The configuration is overwritten with the restored configuration from the stack.
- You can enable or disable this feature at any time using the CLI. The default mode is ENABLE.
- Customer log messages are provided.

Note: After booting a stack, use the CLI command `show stack auto-unit-replacement` from a unit console to find out if that unit is ready for replacement.

AUR function

The CFG mirror image is a duplicate CFG image (stored in the flash drive) of a unit in a stack. The mirror image does not reside in the same unit with the CFG image. The unit that contains the CFG image is called the Associated Unit (AU) of the CFG mirror image. The MAC Address of the AU is called the Associated Mac Address (AMA) of the CFG mirror image.

An active CFG Mirror Image is a CFG mirror image that has its AU in the stack. An INACTIVE CFG Mirror Image is a CFG mirror image for which the associated AU is removed from the stack. When a CFG mirror image becomes INACTIVE, the INACTIVE CFG mirror image is copied to another unit.

The stack always keeps two copies of an INACTIVE CFG mirror image in the stack in case one unit is removed—the other unit can still provide the backup INACTIVE CFG mirror image.

CFG mirror image process

The CFG mirror image process is triggered by specific events.

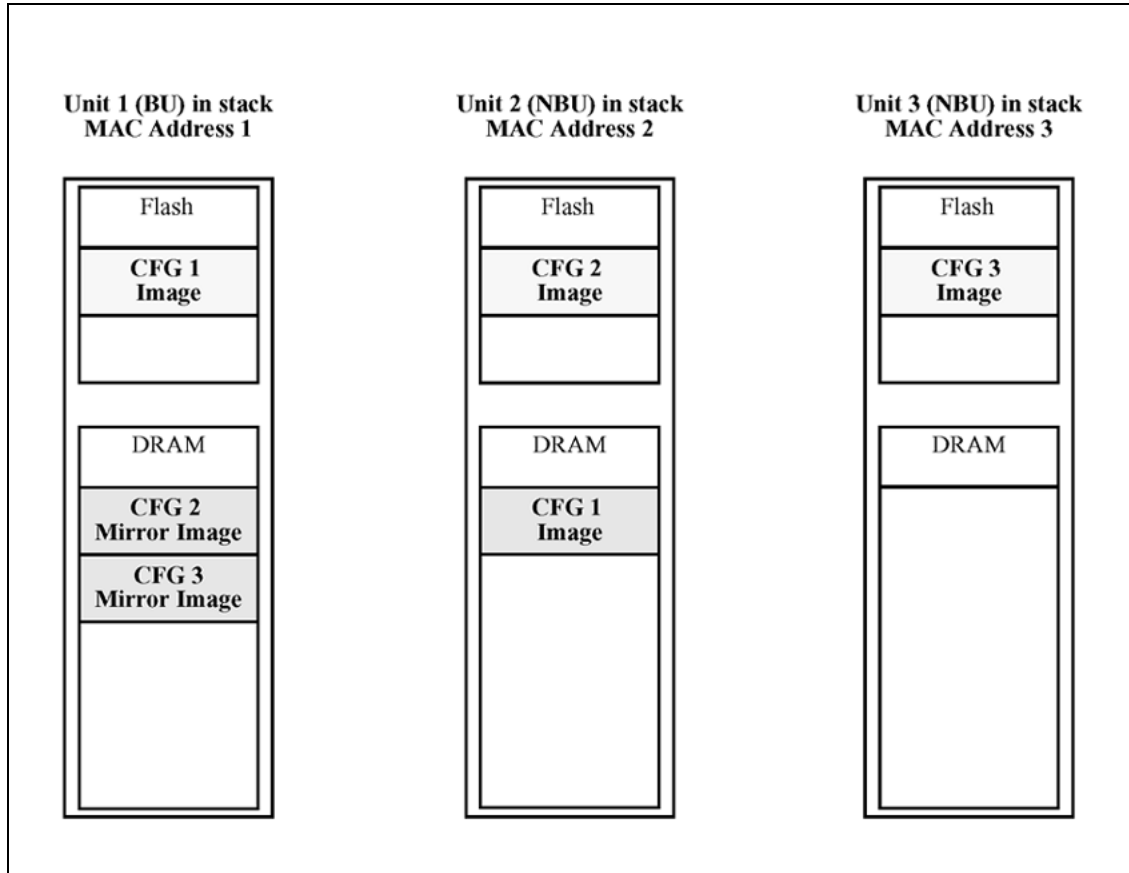
Power Cycle After a power cycle, all the CFG images in a stack are mirrored.

"CFG mirror process in stack" (page 123) illustrates the CFG mirror images in a three-unit stack after the stack is powered on. Unit 1 is the Based Unit (BU) and all other units are Non-Based Units (NBU).

- Unit 1 (BU) contains mirror images for unit 2 (CFG 2) and unit 3 (CFG3).
- Unit 2 (NBU), is the TEMP-BU. It contains a mirror image of unit 1 (CFG1), in case the BU (unit 1) is removed from the stack.
- All three mirror images (CFG 1, CFG 2, and CFG 3) are active.

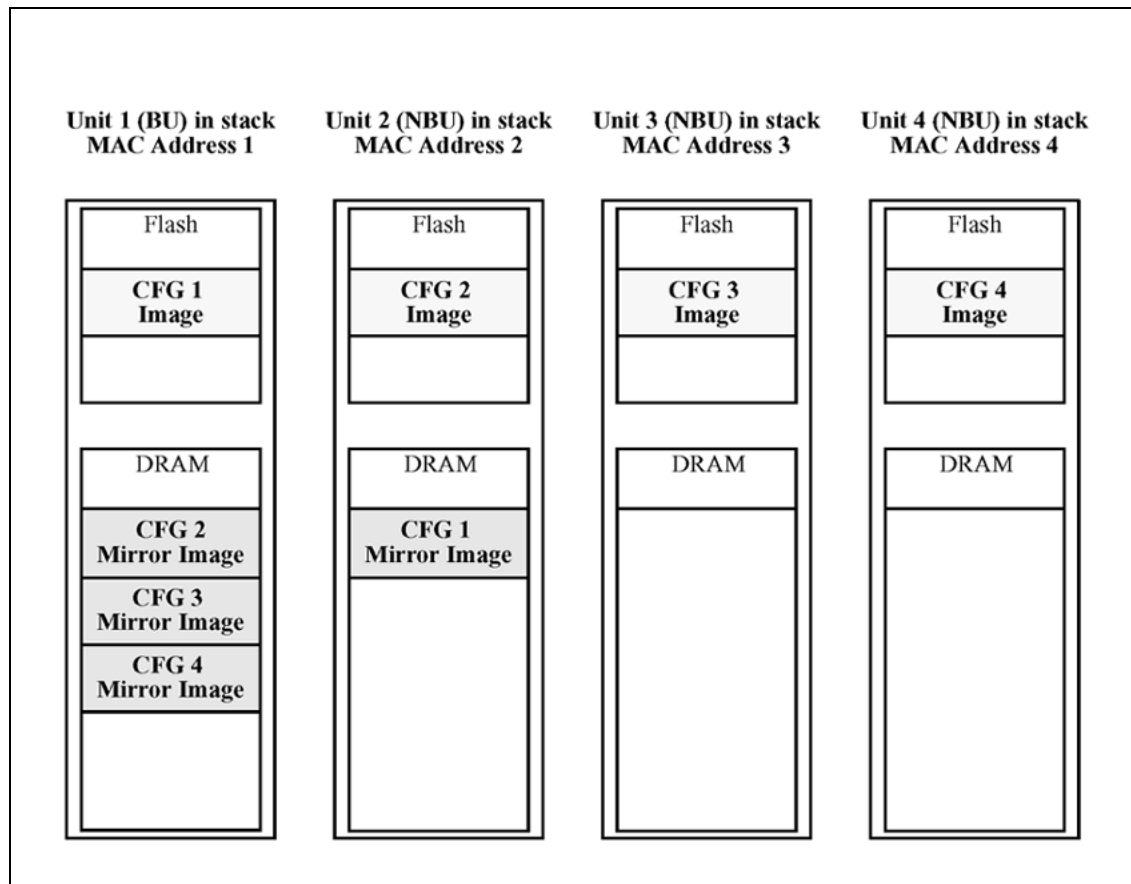
- Unit 2 is the AU of the CFG 2 mirror image.
- The Mac Address 2 is the AMA of the CFG2 mirror image.

CFG mirror process in stack



Adding a unit In a stack that has no any INACTIVE CFG mirror images, a new unit causes the CFG image of the new unit to be mirrored in the stack. For example, in "[CFG mirror images in the stack after adding unit 4](#)" (page 124), after you add unit 4 to the stack, the CFG 4 mirror image is created in the BU (unit 1).

CFG mirror images in the stack after adding unit 4

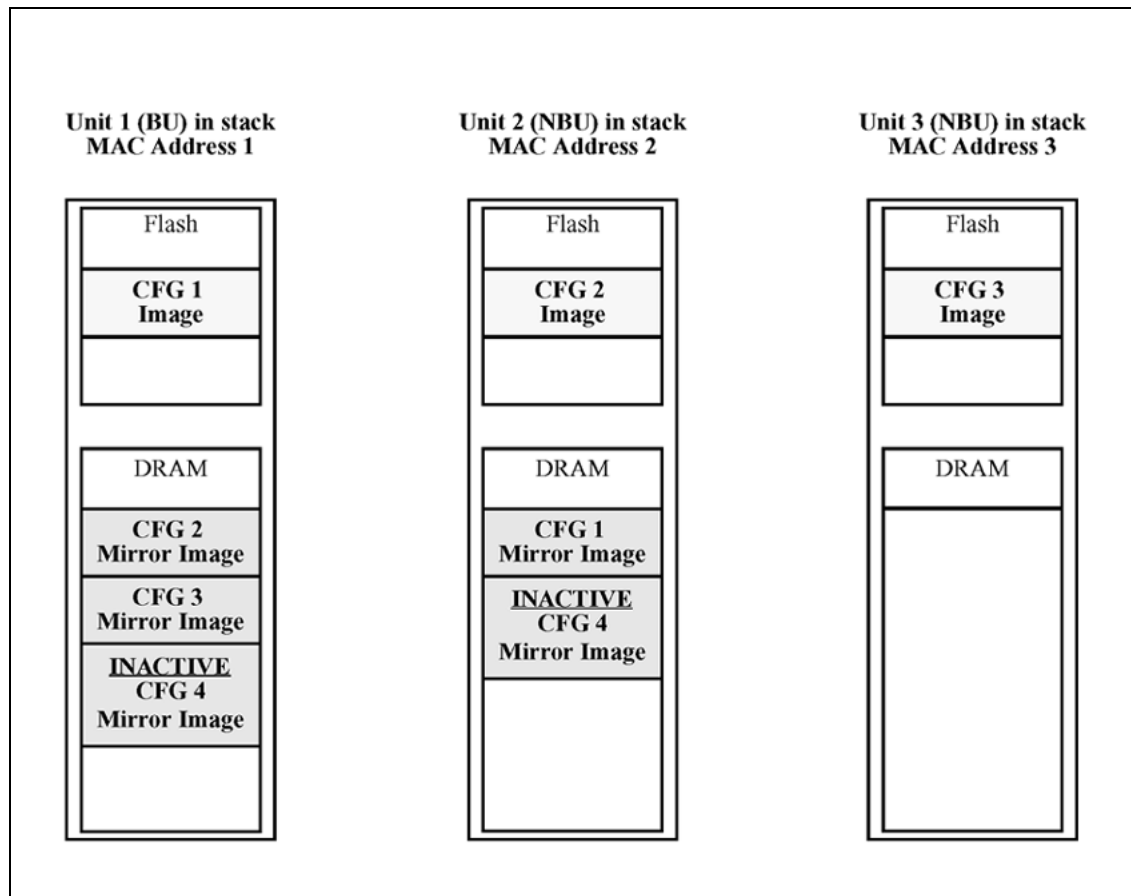


Removing an NBU When you remove an NBU from a stack, the related CFG mirror image in the stack becomes INACTIVE.

The AUR feature ensures that the stack always has two copies of an INACTIVE CFG mirror image. These two copies must not reside in the same unit in the stack.

For example, after you remove unit 4 from the stack shown in "CFG mirror images in the stack after adding unit 4" (page 124), the CFG 4 mirror image becomes INACTIVE (see "CFG mirror images after removing unit 4" (page 125)). Another copy of the INACTIVE CFG 4 mirror image is also created in unit 2.

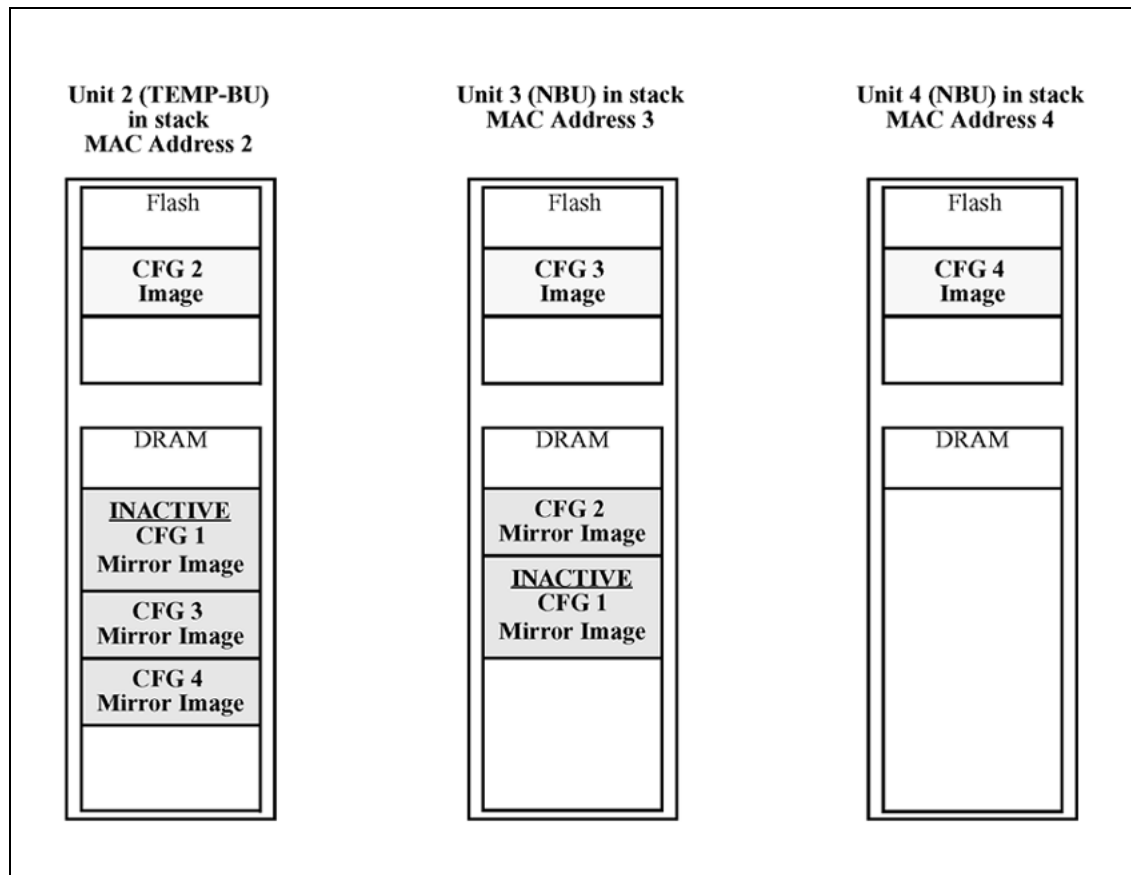
CFG mirror images after removing unit 4



Removing a BU When you remove a BU, the TEMP-BU assumes the role of the BU. Because all the CFG mirror images of the NBUs reside in the removed BU, the TEMP-BU mirrors all the CFG image of the NBUs in the stack.

After you remove the BU from the stack shown in "CFG mirror images in the stack after adding unit 4" (page 124), the TEMP-BU (unit 2) must mirror all the CFG images in the stack (see "CFG mirror images in the stack after removing the BU (unit 1)" (page 126)). The feature also ensures that the stack always has two copies of an INACTIVE CFG mirror image.

CFG mirror images in the stack after removing the BU (unit 1)



As shown in "CFG mirror images in the stack after removing the BU (unit 1)" (page 126)

- Unit 2 becomes the TEMP-BU.
- The CFG 1 mirror image (residing in unit 2) becomes INACTIVE.
- A second copy of the INACTIVE CFG 1 mirror image is created in unit 3.
- The TEMP-BU (unit 2) contains all CFG mirror images of the NBUs in the stack.
- The CFG 2 mirror image is created in unit 3. Unit 3 becomes the next TEMP-BU in case you remove the current TEMP-BU.

Restoring a CFG image

Restoring a CFG image overwrites the CFG image of a new unit in a stack with an INACTIVE mirror image stored in the stack.

Note: Restore a CFG image to a new unit happens only if you meet the following conditions.

- The AUR feature is enabled.

- At least one INACTIVE CFG mirror image exists in the stack.
- The MAC Address of the new unit is different from all the AMA of the INACTIVE CFG mirror images in the stack.

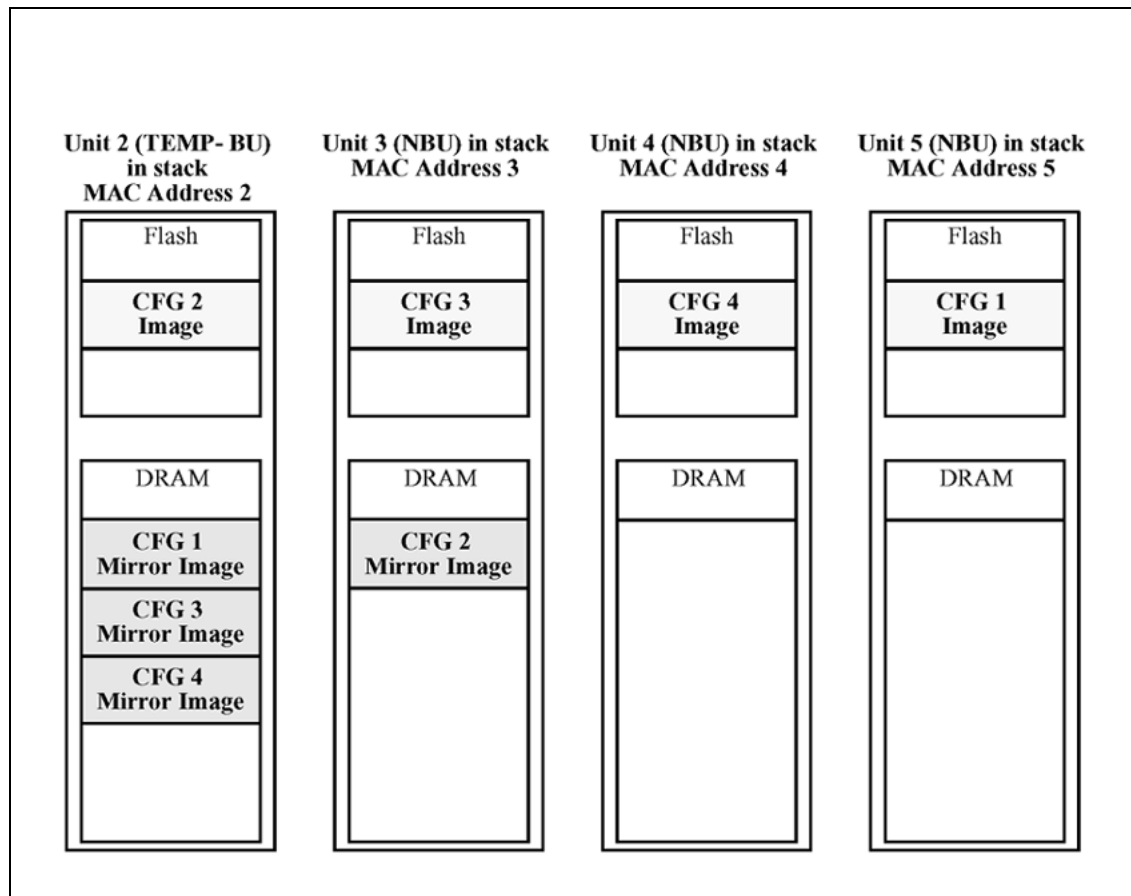
The image restore process consists of the following steps.

Step	Action
1	<p>Add a new unit to a stack:</p> <ol style="list-style-type: none"> If more than one INACTIVE CFG mirror image is in the stack, select the one with the smallest unit ID for restoration. Send the INACTIVE CFG mirror image in the stack to the new unit. The INACTIVE CFG mirror image becomes ACTIVE. The new unit saves the received CFG image to the flash drive. The new unit resets itself.
—End—	

For example, if you add a unit 5 (MAC Address 5) to the stack shown in ["CFG mirror images in the stack after removing the BU \(unit 1\)"](#) (page 126), the following occurs (see ["CFG mirror images in the stack after adding unit 5"](#) (page 128)):

- The INACTIVE CFG 1 mirror image is copied to the CFG 5 image. Unit5 now has the configuration of unit 1, which is no longer in the stack.
- The INACTIVE CFG 1 mirror image in unit 2 becomes ACTIVE.
- The INACTIVE CFG 1 mirror image in unit 3 is removed.
- The MAC Address 5 of the unit 5 becomes the new AMA of the CFG1 mirror image.

CFG mirror images in the stack after adding unit 5



Synchronizing the CFG mirror images with CFG images

A CFG mirror image is updated whenever a CFG flash drive synchronization occurs in the AU.

Configuring AUR using the CLI

This section describes the CLI commands used in AUR configuration.

show stack auto-unit-replacement command

The `show stack auto-unit-replacement` command displays the current AUR settings.

The syntax for this command is

```
show stack auto-unit-replacement
```

The `stack auto-unit-replacement enable` command is in all command modes.

No parameters or variables are available for the `show stack auto-unit-replacement` command.

stack auto-unit-replacement enable command

The `stack auto-unit-replacement enable` command enables AUR on the switch.

The syntax for this command is

```
stack auto-unit-replacement enable
```

Run the `stack auto-unit-replacement enable` command in Global Configuration mode.

No parameters or variables are available for the `stack auto-unit-replacement enable` command.

no stack auto-unit-replacement enable command

The `no stack auto-unit-replacement enable` command disables AUR on the switch.

The syntax for this command is

```
no stack auto-unit-replacement enable
```

Run the `no stack auto-unit-replacement enable` command in Global Configuration mode.

No parameters or variables are available for the `no stack auto-unit-replacement enable` command.

default stack auto-unit-replacement enable command

The `default stack auto-unit-replacement enable` command restores the default AUR settings.

The syntax for this command is

```
default stack auto-unit-replacement enable
```

Run the `default stack auto-unit-replacement enable` command in Global Configuration mode.

No parameters or variables are available for the `default stack auto-unit-replacement enable` command.

Configuring AUR using Device Manager

Click in the `AutoUnitReplacementEnabled` field to enable or disable AUR using Device Manager in the **System** tab (see "[System tab](#)" (page 216)).

Agent Auto Unit Replacement

Use the enhancement to the Auto Unit Replacement functionality, known as Agent Auto Unit Replacement (AAUR), to ensure that all units in a stack have the same software image by inspecting units joining a stack and downloading the stack software image to any unit that has a dissimilar image. AAUR is enabled by default.

Agent Auto Unit Replacement functions in the following manner:

1. When a stand-alone switch joins an AAUR-enabled stack, the switch software image is inspected.
2. If the switch software image differs from the stack software image, the AAUR functionality downloads the stack software image to the joining unit.
3. The joining unit is then reset and becomes a member of the stack upon a reboot.

Use the CLI commands in the following sections to manage and configure AAUR. You can currently manage this functionality only through the CLI.

stack auto-unit-replacement-image enable command

Use the `stack auto-unit-replacement-image enable` command to enable AAUR. Because AAUR is enabled by default, use this command only if this functionality was previously disabled.

The syntax for this command is

```
stack auto-unit-replacement-image enable
```

Run the `stack auto-unit-replacement-image enable` command in Global Configuration command mode.

no stack auto-unit-replacement-image-enable command

Use the `no stack auto-unit-replacement-image enable` command to disable AAUR. Because AAUR is enabled by default, you must run this command if you do not want AAUR functionality on a switch.

The syntax for this command is

```
no stack auto-unit-replacement-image enable
```

The `no stack auto-unit-replacement-image enable` command is executed in the Global Configuration command mode.

default stack auto-unit-replacement-image enable command

Use the `default stack auto-unit-replacement-image enable` command to set the AAUR functionality to the factory default of enabled.

The syntax of this command is

```
default stack auto-unit-replacement-image enable
```

Run the `default stack auto-unit-replacement-image enable` command in Global Configuration command mode.

show stack auto-unit-replacement-image command

Use the `show stack auto-unit-replacement-image` command to view the current status of the AAUR functionality.

The syntax of this command is

```
show stack auto-unit-replacement-image
```

Run the `show stack auto-unit-replacement-image` command in User EXEC command mode.

Features of the Nortel Ethernet Routing Switch 4500 Series

The Nortel Ethernet Routing Switch 4500 Series provides wire-speed switching that enables high-performance and low-cost connections to full-duplex 10/100/100 and half-duplex 10/100 Mb/s Ethernet Local Area Networks (LAN).

This section describes the general features of the Nortel Ethernet Routing Switch 4500 Series.

Flash memory storage

Switch software image storage

The Nortel Ethernet Routing Switch 4500 Series uses flash memory to store the switch software image.

You can update the software image with a new version from flash memory.

You must have an in-band connection between the switch and the TFTP load host to the software image.

Configuration parameter storage

All configuration parameters in the Nortel Ethernet Routing Switch 4500 Series are stored in flash memory.

These parameters are updated every 60 seconds if a change occurs, or upon execution of a reset command.

Note: Do not power off the switch within 60 seconds of changing any configuration parameters.

If you power down the switch within 60 seconds you can lose the changed configuration parameters.

Policy-enabled networking

With the Nortel Ethernet Routing Switch 4500 Series, you can implement classes of services and assign priority levels to different types of traffic. You can also configure policies to monitor the characteristics of traffic.

For example, in the Nortel Ethernet Routing Switch 4500 Series, you can determine the sources, destinations, and protocols used by the traffic. You can also perform a controlling action on the traffic when certain user-defined characteristics match.

The Nortel Ethernet Routing Switch 4500 Series supports Differentiated Services (DiffServ). DiffServ is a network architecture through which service providers and enterprise network environments can offer various levels of services for different types of data traffic.

You can use DiffServ Quality of Service (QoS) to designate a specific level of performance on a packet-by-packet basis. If you have applications that require high performance and reliable service, such as voice and video over IP, you can use DiffServ to give preferential treatment to this data over other traffic.

Power over Ethernet

The Nortel Ethernet Routing Switch 4500 Series 4548-GT-PWR and the 4550T-PWR (PoE switches) provide IEEE 802.3af-compliant power or PoE on all 10/100/1000 RJ-45 ports.

PoE refers to the ability of the switch to power network devices over an Ethernet cable. Some of these devices include IP Phones, Wireless LAN Access Points, security cameras, and access control points.

The PoE switches automatically detect the network device requirements and dynamically supply the required DC voltage at a set current to each appliance.

To configure and manage the PoE features, you must use either the CLI, the Web-based management system, or the Java Device Manager.

Note: You must use a four-pair Category 5 UTP cable for PoE. A standard two-pair UTP Cable does not support PoE.

Virtual Local Area Networks

Virtual Local Area Network (VLAN) provides a mechanism to fine-tune broadcast domains.

The Nortel Ethernet Routing Switch 4500 Series can create two types of VLANs:

- IEEE 802.1Q port-based VLANs

Port-based VLANs filter on the 802.1Q value of the packet. Tagged packets enter the device that contains an 802.1Q value. Untagged packets assume the PVID value assigned to the inbound port as the 802.1Q value. The packets are forwarded only to those ports with VLAN membership lists that contain the same 802.1Q value as the packet.

Automatic PVID (AutoPVID) automatically sets the PVID when you configure a port-based VLAN. When you add the port to the VLAN, the PVID value is the same value as the last port-based VLAN ID that you associated with this port. You can also manually change the PVID value.

The default global setting for AutoPVID is On.

- Protocol-based VLANs

A protocol-based VLAN is a VLAN in which you assign the switch ports as members of a broadcast domain based on the protocol information within the packet.

Protocol-based VLANs can localize broadcast traffic and ensure that only the protocol-based VLAN ports are flooded with the specified protocol type packets. The maximum number of available protocols is 14, including the User Defined Protocols option.

VLANs are classified based on the following information:

1. Is the packet tagged?
2. Does the packet belong to a protocol-based VLAN?

If none of the criteria apply, the packet belongs to the VLAN identified by the PVID of the ingress port.

The Nortel Ethernet Routing Switch 4500 Series supports up to 256 VLANs, including VLAN #1, which is always port-based. The 256 VLANs can be on a stand-alone Nortel Ethernet Routing Switch 4500 Series or across a stack of switches.

Spanning Tree Protocol groups

The Nortel Ethernet Routing Switch 4500 Series supports the Spanning Tree Protocol (STP) as defined in IEEE 802.1D.

STP detects and eliminates logical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm configures the network to use only the most efficient path. If that path fails, the protocol automatically reconfigures the topology to select a new active path.

The Spanning Tree Groups (STG) forms a loop-free topology that includes one or more VLANs. The Nortel Ethernet Routing Switch 4500 Series supports a maximum of eight STGs running simultaneously.

The Nortel Ethernet Routing Switch 4500 Series supports a maximum of 256 VLANs. Therefore each STG may have 32 VLANs.

Rapid Spanning Tree Protocol

The standard spanning tree implementation in 4500 Series switches is based on IEEE 802.1d, which is slow to respond to a topology change in the network (for example, a dysfunctional link in a network).

The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. RSTP also maintains a backward compatibility with the IEEE 802.1d. In certain configurations, the recovery time of RSTP is less than 1 second. You can maintain backward compatibility by configuring a port to be in STP-compatible mode. A port that operates in the STP-compatible mode transmits and receives only STP BPDUs and drops any RSTP BPDUs.

RSTP also reduces the amount of flooding in the network by enhancing the way Topology Change Notification (TCN) packet is generated.

Multiple Spanning Tree Protocol

With Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s), you can configure multiple instances of RSTP on the same switch. Each RSTP instance can include one or more VLANs. The operation of the MSTP is similar to the current Nortel proprietary STP.

The 4500 Series switch can use RSTP and MSTP to achieve the following:

- Reduce converging time from 30 seconds to less than 1 second when topology changes in the network (that is, the port goes up or down).
- Eliminate unnecessary flushing of the MAC database and flooding of traffic to the network with a new Topology Change mechanism.
- Provide backward compatibility with other switches that run legacy 802.1d STP or Nortel MSTG (STP group 1 only).
- Provide simultaneous support for eight instances of RSTP under MSTP mode. Instance 0 or CIST is the default group, which includes default VLAN 1. Instances 1 to 7 are called MSTIs 1-7.
- You can configure the switch to run Nortel STPG (IEEE 802.1d), RSTP (IEEE 802.1w), or MSTP (IEEE 802.1s).

Trunk groups

The Nortel Ethernet Routing Switch 4500 Series supports two types of trunk groups:

- Link Aggregation Group (LAG): Trunk groups that are formed by Link Aggregation are referred to as Link Aggregation Groups (LAG).
- Multilink Trunk (MLT): Trunk groups that are formed by Nortel Ethernet Routing Switch 4500 Series Multilink Trunking are referred to as Multilink Trunks (MLT).

Link Aggregation

Link Aggregation (LA) provides a mechanism to create and manage trunk groups. You can control and automatically configure a trunk group with the Link Aggregation Control Protocol (LACP).

As defined by IEEE 802.3ad standard, the switch uses LACP the switch to "learn" the presence and capabilities of a remote switch by exchanging relevant information with the remote switch. Either switch can accept or reject the aggregation request. A link that does not join a trunk group operates as an individual link.

By default, Link Aggregation is set to off on all ports.

MultiLink Trunking

With MultiLink Trunking (MLT) you can group multiple ports, two to eight together, when you link ports to another switch or server. This grouping increases the aggregate throughput of the interconnection between two devices by 8 Gb in full-duplex mode.

You can configure the Nortel Ethernet Routing Switch 4500 Series with up to 6 multilink trunks.

You can configure the trunk members within a single unit in the stack. You can distribute trunk members between any of the units within the stack configuration. This is referred to as distributed trunking.

Security

The following table describes the types of security supported by the Ethernet Routing Switch 4500 Series.

Security Type	Description
RADIUS-based security	Limit administrative access to the switch through user authentication.
MAC address-based security	Limit access to the switch based on allowed source and destination MAC addresses.

Security Type	Description
EAPOL-based security (IEEE 802.1X)	Enable the exchange of authentication information between any end station or server connected to the switch and authentication server, such as a RADIUS server.
IP manager list	Limit access to management features of the switch based on the management station IP address.
SNMPv3	Enable access to the various services by using password authentication (MD5), secure-hash algorithm, and encryption using the Data Encryption Standard.
SSL	Provide a secure Web management interface.
SSH	Replace telnet and provide a secure access to the CLI.

For more information about specific security features, see *Configuring and Managing Security for Nortel Ethernet Routing Switch 4500 Series, Software Release 5.0* (NN47205-505).

Port mirroring

with port mirroring, also referred to as *conversation steering*, you can designate a single switch port as a traffic monitor for a specified port.

You can specify *port-based* monitoring for ingress and egress at a specific port. You also can attach a probe device, such as a Nortel StackProbe*, or equivalent, to the designated monitor port.

Note: Use the CLI or the Web-based Management Interface to configure port mirroring.

Auto-MDI/X

The term *auto-MDI/X* refers to automatic detection of transmit and receive twisted pairs.

When auto-MDI/X is active, any straight or crossover category 5 cable can provide connection to a port. If autonegotiation is disabled, then auto-MDI/X is not active.

Auto-polarity

Auto-polarity refers to the ability of the port to compensate for positive and negative signals being reversed on the receive cables.

The Nortel Ethernet Routing Switch 4500 Series support auto-polarity. With autonegotiation enabled, auto-polarity automatically reverses the polarity of a pair of pins from positive to negative or negative to positive. This

corrects the polarity of the received data, if the port detects that the polarity of the data is reversed due to a wiring error. If autonegotiation is disabled, auto-polarity is not active.

Autosensing and autonegotiation

The Nortel Ethernet Routing Switch 4500 Series are autosensing and autonegotiating devices:

- The term *autosense* refers to the ability of a port to *sense* the speed of an attached device.
- The term *autonegotiation* refers to a standard protocol (IEEE 802.3u or 802.3z or 802.3ab) that exists between two IEEE-capable devices. Autonegotiation enables the switch to select the best speed and duplex modes.

Autosensing occurs when the attached device cannot autonegotiate or uses a form of autonegotiation that is not compatible with the IEEE 802.3z autonegotiation standard. If it is not possible to sense the duplex mode of the attached device, the Nortel Ethernet Routing Switch 4500 Series reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the Nortel Ethernet Routing Switch 4500 Series, the ports negotiate down from 1000 Mb/s and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

Custom Autonegotiation Advertisements

In the Nortel Ethernet Routing Switch 4500 Series, you can use the Custom Autonegotiation Advertisements (CANA) feature to control the speed and duplex settings that each Ethernet port of the device advertises as part of the autonegotiation process.

Without CANA, a port with autonegotiation enabled advertises all speed and duplex modes supported by the switch and attempts to establish a link at the highest common speed and duplex setting. By using CANA, you can configure the port to advertise only certain speed and duplex settings, thereby establishing links only at these settings, regardless of the highest commonly supported operating mode.

CANA provides control over the IEEE802.3x flow control settings advertised by the port, as part of the autonegotiation process. You can set flow control advertisements to Symmetric, Asymmetric, or Disabled.

You may not want a port to advertise all supported speed and duplex modes in the following situations:

- If a network can support only a 10 Mb/s connection, you can configure a port to advertise only 10 Mb/s capabilities. Devices that uses

autonegotiation to connect to this port connect at 10 Mb/s, even if both devices are capable of higher speeds.

- If you configure a port to advertise only 100 Mb/s full-duplex capability, the link becomes active only if the link partner can autonegotiate a 100 Mb/s full-duplex connection. This prevents mismatched speed or duplex settings if autonegotiation is disabled on the link partner.
- For testing or network troubleshooting, you can configure a link to autonegotiate at a particular speed or duplex mode.

Configuring CANA using the CLI Use the `auto-negotiation-advertisements` command to configure CANA.

To configure port 5 to advertise the operational mode of 10 Mb/s and full duplex, enter the following command:

```
auto-negotiation-advertisements port 5 10-full
```

The following example displays sample output for the `auto-negotiation-advertisements` command to set port 5 to 10 Mb/s and full duplex.

auto-negotiation-advertisements command sample output

```
4548GT-PWR<config>#interface fastethernet 5
4548GT-PWR<config-if>#auto-negotiation-advertisements port
5 10-full
4548GT-PWR<config-if>#
```

Viewing current autonegotiation advertisements To view the autonegotiation advertisements for the device, enter the following command:

```
show auto-negotiation-advertisements [port <portlist>]
```

The following example displays sample output for the `show auto-negotiation-advertisements` command after port 5 is set to 10 Mb/s and full duplex.

show auto-negotiation-advertisements command sample output

```
4548GT-PWR#show auto-negotiation-advertisements port 5
Unit/Port Autonegotiation Advertised Capabilities
-----
-----
1/5      10Full
```

Viewing hardware capabilities To view the operational capabilities of the device, enter the following command:

```
show auto-negotiation-capabilities [port <portlist>]
```

The following example displays sample output for the `show auto-negotiation-capabilities` command for port 5.

show auto-negotiation-capabilities command sample output

```
4548GT-PWR#show auto-negotiation-capabilities port 1/5
```

```

Unit/Port Autonegotiation Capabilities
-----
1/5      10Full 10Half 100Full 100Half 1000Full
4548GT-PWR#

```

Setting default advertisements To set default autonegotiation advertisements for the device, enter the following command in the Interface Configuration command mode:

```
default auto-negotiation-advertisements [port <portlist>]
```

To set default advertisements for port 5 of the device, enter the following command:

```
default auto-negotiation-advertisements port 5
```

The following example displays sample output for the default auto-negotiation-advertisements command to return port 5 to default auto-negotiation-advertisements status.

```

default auto-negotiation-advertisements command sample output
4548GT-PWR<config>interface fastethernet all
4548GT-PWR<config-if>#default-auto-negotiation-advertiseme
nts port 1/5
4548GT-PWR(config-if)#

```

Silencing advertisements To set a port transmit no autonegotiation advertisements, enter the following command in the Interface Configuration command mode:

```
no auto-negotiation-advertisements [port <portlist>]
```

To silence the autonegotiation advertisements for port 5 of the device, enter the following command:

```
no auto-negotiation-advertisements port 5
```

The following example displays sample output for the no auto-negotiation-advertisements command to silence the auto-negotiation-advertisements for port 5.

```

no auto-negotiation-advertisements command sample output
4548GT-PWR<config-if>#no auto-negotiation-advertisements
port 1/5
4548GT-PWR<config-if>#

```

ASCII configuration file

With the Nortel Ethernet Routing Switch 4500 Series you can download a user-editable ASCII configuration file from a TFTP server.

Load the ASCII configuration file automatically at boot time or on demand by using the CLI.

After you download the file, the configuration file automatically configures the switch or stack according to the CLI commands in the file.

With this feature, you can generate command configuration files that can be used by several switches or stacks with minor modifications.

The maximum size for an ASCII configuration file is 500 KB; split large configuration files into multiple files.

Use a text editor to edit the ASCII configuration. The command format is the same as that of the CLI.

Download the ASCII configuration file to the base unit by using CLI commands. The ASCII configuration script completes the process.

Sample ASCII configuration file

This section shows a sample ASCII configuration file. This file is an example only and shows a basic configuration for a stand-alone switch that includes multilink trunking, VLANs, port speed and duplex, and SNMP configurations.

The following text represents a sample ASCII configuration file:

```
! -----
! example script to configure different features from CLI
! -----
!
enable
configure terminal
!
!
! -----
! add several MLTs and enable
! -----
mlt 3 name seg3 enable member 13-14
mlt 4 name seg4 enable member 15-16
mlt 5 name seg5 enable member 17-18
!
!
! -----
! add vlans and ports
! -----
!
! create vlan portbased
vlan create 100 name vlan100 type port
!
! add Mlts created above to this VLAN
vlan members add 100 17
!
! create vlan ip protocol based
vlan create 150 name vlan150 type protocol-ipEther2
```

```

!
! add ports to this VLAN
! in this case all ports
vlan members add 150 ALL
vlan ports ALL priority 3
!
! igmp
! you could disable proxy on vlan 100
vlan igmp 100 proxy disable
!
! -----
! Examples of changing interface parameters
! -----
! change speed of port 3
interface Fastethernet 3
speed 10
duplex half
exit
!
! change speed of port 4
interface Fastethernet 4
speed auto
duplex auto
exit
!
!
! -----
! SNMP configuration
! -----
snmp-server host 192.168.100.125 private
snmp-server community private
!
!
exit
end
! -----
! Finished
! -----

```

Note: To add comments to the ASCII configuration file, add an exclamation point (!) to the beginning of the line.

Displaying unit uptime

You can display the uptime for each unit in a stack. Unit stack uptime collects the stack uptime for each unit in a stack and reports this information when requested. You can determine how long each unit is connected to the stack. You can use the CLI commands to display the unit uptimes.

Port naming

You can name or specify a text string for each port. This feature provides easy identification of the connected users.

Use the CLI, DM, or the Web-based management system to name ports.

Port error summary

You can view all ports that have errors in an entire stack.

If a particular port has no errors, it is not displayed in the port error summary.

This feature is available only through the Web-based management system.

IP address for each unit in a stack

You can assign an IP address to each unit in a stack. Use the CLI to configure the IP addresses for each unit within a stack.

BootP mode

The Nortel Ethernet Routing Switch 4500 Series supports the Bootstrap protocol (BootP).

You can use BootP to retrieve an ASCII configuration file name and configuration server address.

With a properly configured BootP server, the switch automatically learn its assigned IP address, subnet mask, and the IP address of the default router (default gateway).

The Nortel Ethernet Routing Switch 4500 Series has a unique 48-bit hardware address, or MAC address, that is printed on a label on the back panel. Use this MAC address when you configure the network BootP server to recognize the Nortel Ethernet Routing Switch 4500 Series BootP requests.

The BootP modes supported by the Nortel Ethernet Routing Switch 4500 Series are

- BootP or Last Address mode
- BootP-When-Needed
- BootP Always
- BootP Disabled

Note: The default BootP mode is BootP-When-Needed.

Web Quick Start

You can use the Web Quick Start feature to enter the setup mode through a single screen.

This feature is supported only by the Web interface.

During the initial setup mode, all ports in the switch or stack are assigned to the default VLAN.

You can use the Web Quick Start screen to configure the following information:

- switch or stack IP address
- subnet mask
- default gateway
- SNMP Read community
- SNMP Write community
- SNMP Trap IP addresses and communities (up to four4)
- Quick Start VLAN

Simple Network Time Protocol

The Simple Network Time Protocol (SNTP) is a subset of the Network Time Protocol. It provides a simple mechanism for time synchronization.

Clocks use NTP to synchronize to a few milliseconds, depending on the clock source and local clock hardware.

SNTP synchronizes the Universal Coordinated Time (UTC) to accuracy within 1 second.

This feature adheres to the RFC 2030 (MIB is the s5agent). With this feature, the system can obtain the time from any RFC 2030-compliant NTP or SNTP server.

The SNTP client implementation for this feature is unicast. The SNTP client operates typically in a unicast mode but can use the broadcast and multicast modes.

SNTP accuracy is typically in the order of significant fractions of a second. This accuracy correlates to the latencies between the SNTP client device and the NTP server. In a low-latency network, the SNTP accuracy can be reduced to less than a 100 millisecond range and, to further increase the accuracy, you can use a simple latency measurement algorithm.

The intended accuracy for this implementation is 1 second, which is sufficient for logs and time displays on UIs.

The system retries connecting with the NTP server a maximum of three times, with 5 minutes between each retry.

When SNTP is enabled (the default value is Disabled), the system synchronizes with the configured NTP server at boot-up (after network connectivity is established) and at user-configurable periods thereafter (the default synchronization interval is 24 hours). The synchronization also can happen upon manual request.

The SNTP feature supports both primary and secondary NTP servers. It attempts to contact the secondary NTP server only if the primary NTP server is unresponsive. When a server connection fails, SNTP retries for a maximum of three times, with 5 minutes between each retry.

Ping enhancement

Using the CLI you can specify additional ping parameters, including the number of ICMP packets to be sent, the packet size, the interval between packets, and the timeout. You can also set ping to continuous, or you can set a debug flag to obtain extra debug information.

See "[ping command](#)" (page 190).

Supported standards and RFCs

This section lists the standards and RFCs supported by the Nortel Ethernet Routing Switch 4500 Series.

Standards

The following IEEE Standards contain information pertinent to the Nortel Ethernet Routing Switch 4500 Series:

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1X (EAPOL)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3x (Flow Control)
- IEEE 802.3ad (Link Aggregation)

RFCs

For more information about networking concepts, protocols, and topologies, consult the following RFCs:

- RFC 791 (IP)

- RFC 894 (IP over Ethernet)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 1350 (TFTP)
- RFC 826 (ARP)
- RFC 768 (UDP)
- RFC 854 (Telnet)
- RFC 951 (BootP)
- RFC 1213 (MIB-II)
- RFC 1493 (Bridge MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2665 (Ethernet MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 1757 (RMON)
- RFC 1271 (RMON)
- RFC 1157 (SNMP)
- RFC 1112 (IGMPv1)
- RFC 2236 (IGMPv2)
- RFC 1945 (HTTP v1.0)
- RFC 2865 (RADIUS)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 3410 (SNMPv3)
- RFC 3411 (SNMP Frameworks)
- RFC 3413 (SNMPv3 Applications)
- RFC 3414 (SNMPv3 USM)
- RFC 3415 (SNMPv3 VACM)
- RFC 3412 (SNMP Message Processing)

Power over Ethernet

The Nortel Ethernet Routing Switch 4500 Series 4550T-PWR and 4548-GT-PWR are Power Sourcing Equipment (PSE). They support Power over Ethernet (PoE) on all 10/100/1000 ports.

PoE is based on the IEEE 802.3af standard.

PoE is the ability of the 4550T-PWR and the 4548-GT-PWR to power network devices over the Ethernet cable. These devices include IP Phones, wireless LAN access points, security cameras, and access control points.

The PoE features supported by the 4550T-PWR and the 4548-GT-PWR switches are as follows:

- DTE power
- powered device (PD) discovery and classification
- capacitive detection to support legacy PD devices, including the Nortel and Cisco Legacy IP Phones
- per-port power management and monitoring
- AC and DC disconnection
- load under voltage/current and over voltage/current detection
- at least 320 watts (W) power available for PSE ports from the internal power supply
- up to 6.6 W for each port on all 48 ports
- a total of 740 W power available for PSE ports using both the internal and external power supply
- 15.4 W (Max) for each port on a 48 port unit
- per-port PoE status LED
- port prioritizing to guarantee DTE power available on high-priority ports
- port pruning to prevent system failure

You can configure PoE from the CLI, SNMP, and Web interfaces. For details, see the following sections.

- "PoE overview" (page 148)
- "Port power priority" (page 149)
- "External power source" (page 150)
- "Stacking" (page 150)
- "Power pairs" (page 150)
- "Power availability" (page 151)
- "Diagnosing and correcting PoE problems" (page 155)
- "Power management" (page 157)
- "Configuring PoE using the CLI" (page 158)
- "Viewing PoE ports using the JDM" (page 162)
- "Configuring PoE using the JDM" (page 163)
- "Configuring PoE using the Web-based Management Interface" (page 163)

PoE overview

The Nortel Ethernet Routing Switch 4500 Series 4550T-PWR and the 4548-GT-PWR are ideal to use with Nortel Business Communication Manager system, IP phones, hubs, and wireless access points. You can use these switches with all network devices.

By using the Nortel Ethernet Routing Switch 4500 Series 4550T-PWR or the 4548-GT-PWR, you can plug any IEEE802.3af-compliant powered device into a front-panel port and receive power in that port. Data also can pass simultaneously on that port. This capability is called PoE.

The IEEE 802.3af draft standard regulates a maximum of 15.4 W of power for each port; that is, a power device cannot request more than 15.4 W of power. As different network devices require different levels of power, the overall available power budget of the Ethernet Routing Switch 4500 depends on your power configuration and the particular connected network devices. If you connect an IP device that requires more than 16 W of power, you see an error on that port notifying you of an overload.

The Nortel Ethernet Routing Switch 4500 Series 4550T-PWR and the 4548-GT-PWR automatically detect each IEEE 802.3af-draft-compliant powered device attached to each front-panel port and immediately sends power to that appliance. The switches also automatically detect how much

power each device requires and supply the required DC voltage at a set current based on the load conditions and current availability. The switches support both PoE and standard LAN devices.

The power detection function of the Nortel Ethernet Routing Switch 4500 Series 4550T-PWR and the 4548-GT-PWR operate independently of the data link status. A device that is already operating the link for data or a device that is not yet operational can request power. That is, the switches provide power to a requesting device even if the data link for that port is disabled. The switches monitor the connection and automatically disconnect power from a port when you remove or change the device, as well as when a short occurs.

The switches automatically detect devices that require no power connections from them, such as laptop computers or other switching devices, and send no power to those devices. You control the supply of power to specific ports by setting the maximum allowed power to each port in 1 W increments, from 3 W to 16 W.

Note: Allow 30 seconds between unplugging and replugging an IP device to the switch to enable the IP device to discharge. If you attempt to connect earlier, the switch may not detect the IP device.

Port power priority

You can configure the power priority of each port by choosing low, high, or critical power priority settings.

The switch automatically drops low-priority ports when the power requirements exceed the available power budget. When the power requirements becomes lower than the switch power budget, the power returns to the dropped port. When several ports have the same priority, one of them must be dropped. In this case, the port with the highest port number is dropped.

For example, assume the following scenario:

- Ports 1 to 40 are configured as low priority.
- Port 41 is configured as high priority.
- Ports 1 to 40 are connected to powered devices.

The devices connected to the ports consume the available Nortel Ethernet Routing Switch 4500 Series 4550T-PWR and 4548-GT-PWR switch power.

The device connected to port 41 requests power from the 4550T-PWR or the 4548-GT-PWR. The switch provides the required power as port 41 is configured as high priority. However, to maintain the power budget, the

switch drops one of the ports configured as low priority. In this case, the switch drops power to port 40 and provides power to port 41. If another port drops power, the system automatically reinstates power to port 40.

External power source

The Nortel Ethernet Redundant Power Supply 15 is available as an optional external power source. Contact your Nortel representative for more information about the Nortel Ethernet Redundant Power Supply Unit 15.

The following are the available options to power the Nortel Ethernet Routing Switch 4500 Series 4550T-PWR or the 4548-GT-PWR switch:

- internal power source only
- external power source only
 - Nortel Ethernet Redundant Power Supply 15
- internal power source plus external power source
 - Nortel Ethernet Redundant Power Supply 15

In a stack configuration, each unit can have its own external power source.

Stacking

You can stack the PoE switches up to eight units high. You can configure these stacks for redundancy.

Power pairs

The PoE switches support wiring as mentioned in the IEEE 802.3af draft standard.

The PoE switches support power to Signal pair only.

Note: The RJ-45 ports 45, 46, 47, and 48 in the 4548-GT-PWR can still supply PoE power to the attached devices, even if the corresponding SFP ports are used for data connectivity.

"[Signal power pair RJ-45 port connector pin assignments](#)" (page 150) shows the RJ-45 connector pin assignments for configuring a power pair for the signal pair. When you choose the signal power pair, the data and the power are transmitted from the same pins.

Signal power pair RJ-45 port connector pin assignments

Pin	Signal	Description
1	RX+/power+	Receive Data +/power+
2	RX-/power+	Receive Data -/power+

Pin	Signal	Description
3	TX+/power-	Transmit Data +/power-
4	Not applicable	Not applicable
5	Not applicable	Not applicable
6	TX-/power-	Transmit Data -/power-
7	Not applicable	Not applicable
8	Not applicable	Not applicable

Power availability

You can use the Nortel Ethernet Redundant Power Supply Unit 15 as an external power source for the 4550T-PWR and the 4548-GT-PWR switches.

The following are the three options to power the switch:

- internal power source only
- external power source only
 - Nortel Ethernet Redundant Power Supply Unit 15
- internal power source plus external power source
 - Nortel Ethernet Redundant Power Supply Unit 15

You can add an external power source to the 4550T-PWR and the 4548-GT-PWR. You can use an optional power and control cable for this purpose and plug it in the back of the switch.

You can allocate a maximum of 16 W of power for each port to the PoE devices connected to the 4550T-PWR or the 4548-GT-PWR. You can allocate power by using the physical power sources.

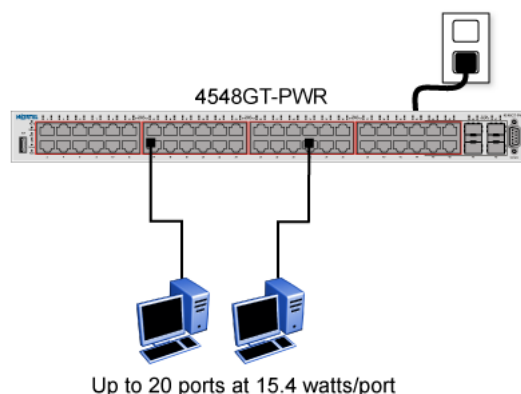
The power sources are physically attached to the switch. You can have only the internal power or you can attach an optional Nortel Ethernet Redundant Power Supply Unit 15. Ensure that you know the actual physical power sources for your 4550T-PWR or your 4548-GT-PWR.

Internal power source only option

Using the 4550T-PWR or the 4548-GT-PWR switch and its internal power source only option, you have a total of 320 W of available power. You can power up to 48 ports at 6.6 W for each port with this configuration or 20 ports at a maximum power of 15.4 W for each port.

The following figure illustrates the switch operating on internal power source only.

Nortel Ethernet Routing Switch 4548GT-PWR operating on internal power source only



"Power source and available power for powered devices" (page 152) describes the power source and available power by using only the internal power source option.

Power source and available power for powered devices

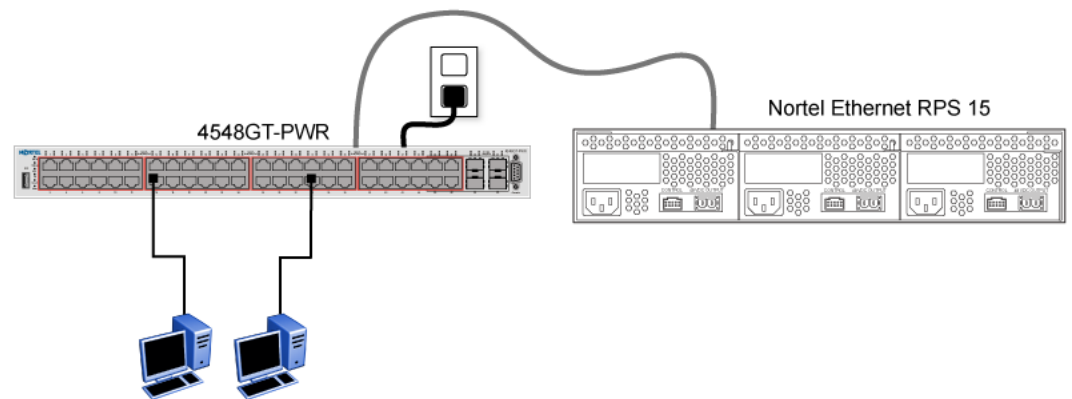
Power Source	Available Power for Powered Devices
AC Connection	320 W

External power source only option

Using the Nortel Ethernet Routing Switch 4500 Series 4550T-PWR and the 4548-GT-PWR switches and their external power source, your only option (Nortel Ethernet Redundant Power Supply Unit 15) is a total of 320W of available power. You can power up to 48 ports at 6.6W for each port with this configuration or 20 ports at the maximum power of 15.4W for each port.

The following figure illustrates the Nortel Ethernet Routing Switch 4548GT-PWR operating only on the external power source.

Nortel Ethernet Routing Switch 4548GT-PWR operating on Nortel Ethernet RPS 15 as an external power source only



"Power source and available power for powered devices" (page 153) describes the power source and available power by only using the external power source option.

Power source and available power for powered devices

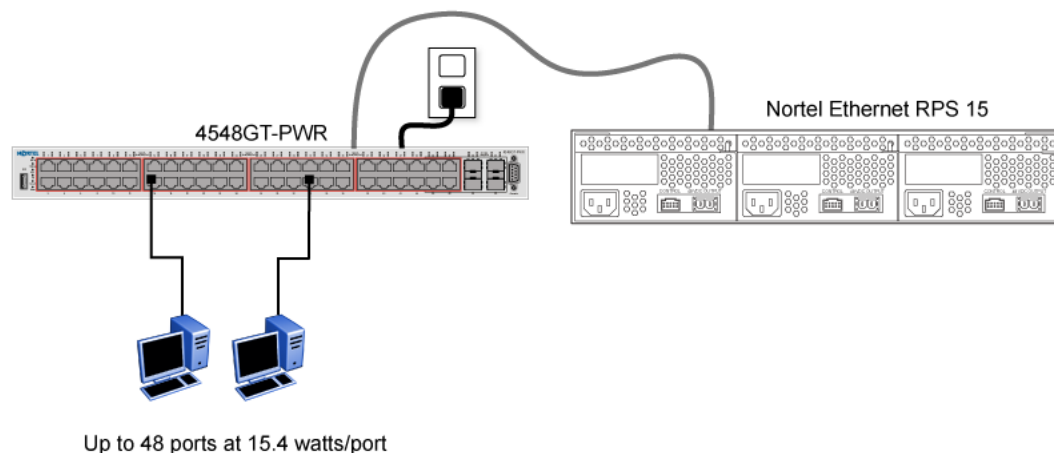
Power Source	Available Power for Powered Devices
Nortel Ethernet RPS 15	320 W

Power sharing option

"Power-sharing with the Nortel Ethernet Routing Switch 4548GT-PWR and the Nortel Ethernet RPS 15" (page 154) shows the use of the 4548-GT-PWR with the Nortel Ethernet 15 RPS as an external power source with the power-sharing configuration.

In this case, the internal power (AC) source is connected along with the Nortel Ethernet 10 PSU (DC) source. This power-sharing configuration supplies 740 W to the 4548-GT-PWR. This enables all 48 ports to supply the maximum power of 15.4 W for each port.

Power-sharing with the Nortel Ethernet Routing Switch 4548GT-PWR and the Nortel Ethernet RPS 15



"Power availability for power sharing with external power source" (page 154) shows the available PoE power when you configure an Nortel Ethernet Routing Switch 4548GT-PWR or 4550T-PWR for power sharing along with an external power source.

Power availability for power sharing with external power source

Power Source	Available Power for Powered Devices
AC	320 W
Nortel Ethernet RPS 15	320 W
Total Power (Power Sharing)	740 W

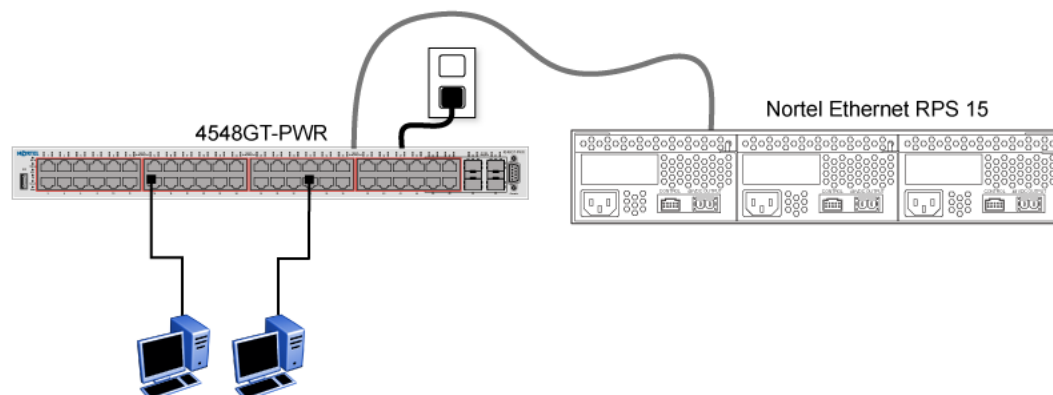
With the addition of the Nortel Ethernet RPS 15, you have a total of 740 W of PoE non redundant power, which provides up to 48 ports to be powered at 15.4 W.

Power Supply Unit (PSU) option

An external power source (Nortel Ethernet RPS 15) can provide redundant power to the Nortel Ethernet Routing Switch 4548GT-PWR or to the 4550T-PWR. That is, the power fails over to the Nortel Ethernet RPS 15 in case a problem occurs with the switch internal power.

The following figure illustrates the use of the 4548-GT-PWR switch with the Nortel Ethernet RPS 15 as an external power source with RPS configuration.

Nortel Ethernet Routing Switch 4548GT-PWR and the Nortel Ethernet RPS 15



If the Nortel Ethernet Routing Switch 4548GT-PWR supplies 320 W of power to a powered device and the supply to the internal power source is interrupted, the power to all powered devices is uninterrupted due to failover to the Nortel Ethernet RPS 15.

"Power availability with the PSU option" (page 155) shows the available PoE power when you configure a Nortel Ethernet Routing Switch 4548GT-PWR for RPS with an external power source.

Power availability with the PSU option

Power Source	Available Power for Powered Devices
AC	320 W
Nortel Ethernet RPS 15	320 W
Total Power (RPS)	320 W

By using the Nortel Ethernet RPS 15, you have a total of 320 W of PoE redundant power, which provides 6.6 W of power to up to 48 ports..

Diagnosing and correcting PoE problems

This section discusses some common problems that you can encounter while using the PoE features of the Nortel Ethernet Routing Switch 4548GT-PWR and the 4550T-PWR.

Messages

"Error messages displayed by PoE ports" (page 156) describes the error messages displayed by a port that supports PoE.

Error messages displayed by PoE ports

Error Message	Descriptions
Detecting	The port detects an IP device that is requesting power.
Delivering power	The port delivers the requested power to the IP device.
Disabled	The port power state is disabled.
Invalid PD	The port detects a device that is not authorized to request for power.
Deny low priority	Power is disabled from the port because of port setting and demands on power budget.
Overload	Power is disabled from the port because the port is overloaded.
Test	The port is in testing mode. This was set by using SNMP.
Error	An unspecified error condition occurred.

Connecting the PSU

Perform the following steps in the order specified to connect the PSU to the Nortel Ethernet Routing Switch 4548GT-PWR or the 4550T-PWR.

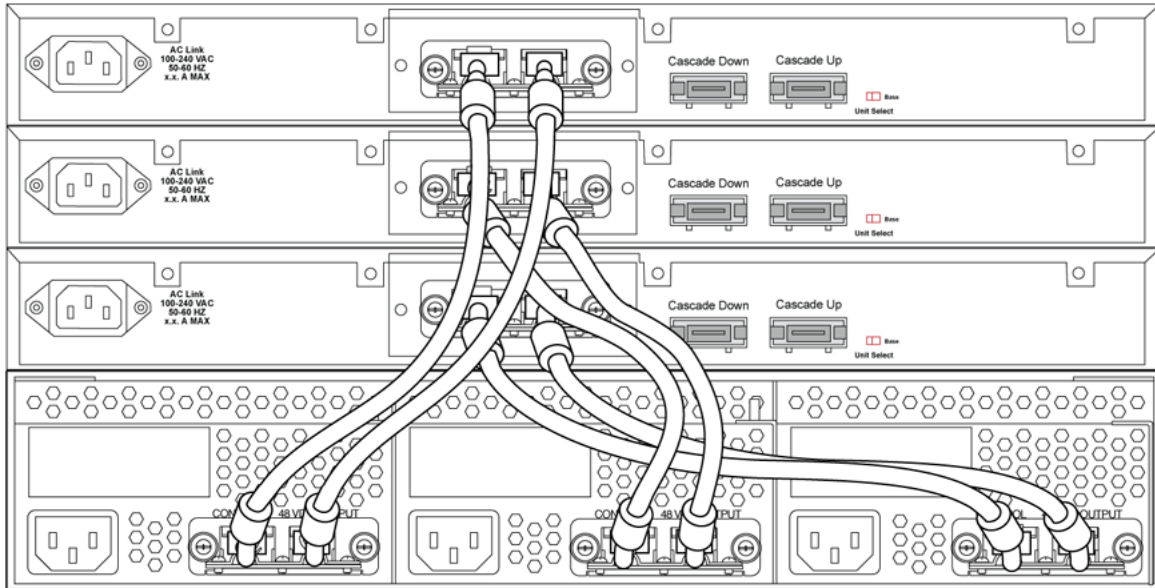
Step	Action
1	Plug the external power source into the DC connector receptacle on the back of the switch by using the 2-pin power connector and the 10-pin control connector.
2	Attach the ground lug on a cable to a grounding point.
3	Plug the power cord from the Nortel Ethernet RPS 15 into the wall outlet.
4	Plug the power cord from switch into the wall outlet.

—End—

The following figure illustrates three Nortel Ethernet RPS 15s connected to the back of a stack of three Nortel Ethernet Routing Switch 4548GT-PWR switches.

Note: A screw connects the ground wire, and a star washer is on the base of the Nortel Ethernet Routing Switch 4548GT-PWR.

External power source connected to back of the Nortel Ethernet Routing Switch 4548GT-PWR



Power management

The Nortel Ethernet Routing Switch 4548GT-PWR and the 4550T-PWR use several device-management systems, such as the Web-based Management Interface, the CLI, and Device Manager (DM), as well as Enterprise for network-level management services.

By using the CLI, Web, or DM, you can configure the level of power to specific ports, and enable or disable power to each port. You can set the maximum power level for each port by increments of 1 W—in the range of 3 W to 16 W. The default power level for each port is 16 W.

You can configure the power priority of each port by choosing low, high, or critical power priority settings. The switch automatically drops low-priority ports when the power requirements exceed the available power budget. If the power requirements are lower than the switch power budget, the power returns to the dropped port.

For example, assume the following scenario:

- ports 1 to 40 are configured as low priority
- port 41 is configured as high priority
- ports 1 to 40 are connected to powered devices
- devices on ports are consuming all the available switch power

- a device is connected to port 41 and requests power

In this scenario, the Nortel Ethernet Routing Switch 4548GT-PWR provides power to the device on port 41 because that port is configured as high priority. However, to maintain the power budget, the switch drops one of the ports configured as low priority. As all the other ports (1 to 40) are configured with a low priority, the switch drops power to the highest port number. In this case, the switch drops power to port 40 and provides power to port 41. If another port drops power, the switch automatically reinstates power to port 40.

You configure the autodiscovery power process as either IEEE 802.3af-compliant or IEEE 802.3af-draft-compliant and legacy:

- 802.3af: detection method described in the IEEE 802.3af draft standard
- legacy: detection standard in use prior to the IEEE 802.3af draft standard

The default value is IEEE 802.3af-draft-compliant. You can set this parameter for the entire switch; you cannot set the discovery mode for each port.

You can obtain power usage information from the management systems. Statistics do not accumulate. The system automatically disconnects the port from power when it detects an overload on any port, and the remainder of the ports remain functional.

Note: Ensure that you set the switch for the power- detection mode used by the connected powered device. Consult the device documentation for this information.

Configuring PoE using the CLI

The following section describes the commands necessary to configure PoE using the CLI:

- "Set port power enable or disable" (page 159)
- "Set port power priority" (page 159)
- "Set power limit for channels" (page 159)
- "Set traps control" (page 160)
- "Show main power status" (page 160)
- "Set power usage threshold" (page 160)
- "Setting PoE detection method" (page 161)
- "Show port power status" (page 161)
- "Show port power measurement" (page 161)

Set port power enable or disable

Use the `poe-shutdown` command to disable PoE to a port.

The syntax for the `poe-shutdown` command is

```
poe poe-shutdown [port <portlist>]
```

Use the `no poe-shutdown` command to enable PoE to a port.

The syntax for the `no poe-shutdown` command is

```
no poe-shutdown [port <portlist>]
```

In either command, substitute `<portlist>` with the ports on which PoE is enabled or disabled.

Run the `poe-shutdown` and `no poe-shutdown` commands in Interface Configuration command mode.

Set port power priority

The `poe-priority` command sets the port power priority.

The syntax for the `poe-priority` command is

```
poe poe-priority [port <portlist>] {critical | high | low}
```

"[poe-priority parameters](#)" (page 159) outlines the parameters for this command.

poe-priority parameters

Parameter	Description
port <portlist>	The ports to set priority for
{low high critical}	The PoE priority for the port

Run the `poe-priority` command in Interface Configuration command mode.

Set power limit for channels

The `poe-limit` command sets the power limit for channels.

The syntax for the `poe-limit` command is

```
poe poe-limit [port <portlist>] <3-16>
```

"[poe-limit parameters](#)" (page 160) outlines the parameters for this command.

poe-limit parameters

Parameter	Description
port <portlist>	The ports to set the limit on
<3 - 16>	The power range to limit at from 3 to 16 W

Run the `poe-limit` command in Interface Configuration command mode.

Set traps control

The `poe-trap` command enables PoE-related traps for PoE-enabled ports.

The syntax for the `poe-trap` command is

```
poe poe-trap [unit <1-8>]
```

Substitute <1-8> with the number of the unit on which to enable traps.

Show main power status

The `show poe-main-configuration` command displays the power configuration.

The syntax for the `show poe-main-configuration` command is

```
show poe-main-status [unit <1-8>]
```

Substitute <1-8> with the number of the unit for which to display the configuration.

Run the `show poe-main-status` command in Privileged EXEC command mode.

Set power usage threshold

The `poe-power-usage-threshold` command sets the power usage threshold in percentage on individual units.

The syntax for the `poe-power-usage-threshold` command is

```
poe poe-power-usage-threshold [unit <1-8>] <1-99>
```


"[poe-power-usage-threshold parameters](#)" (page 161) outlines the parameters for this command.

poe-power-usage-threshold parameters

Parameter	Description
unit <1 - 8>	The unit for which to set the power threshold.
<1 - 99>	1—99 percent

Run the `show poe-main-configure` command in Global Configuration command mode.

Setting PoE detection method

The `poe-pd-detect-type` command enables either 802.3af or Legacy compliant PD detection methods.

The syntax for the `poe-pd-detect-type 802dot3af_and_legacy` command is

```
poe poe-pd-detect-type [unit <1-8>] {802dot3af |
802dot3af_and_legacy}
```

Run the `poe-pd-detect-type 802dot3af_and_legacy` command in Global Configuration command mode.

Show port power status

The `show port power status` command displays the power configuration.

The syntax for the `show port power status` command is

```
show poe-port-status [<portlist>]
```

Substitute `<portlist>` with the ports for which to display configuration.

Run the `show poe-port-status` command in Global Configuration command mode.

Show port power measurement

The `show port power measurement` command displays the power configuration.

The syntax for the `show port power measurement` command is

```
show poe-power-measurement [<portlist>]
```

Substitute `<portlist>` with the ports for which to display configuration.

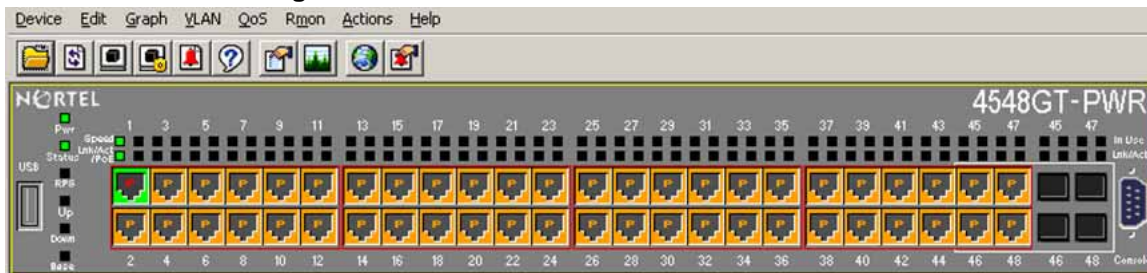
Run the `show poe-power-measurement` command in Global Configuration command mode.

Viewing PoE ports using the JDM

The front panel view of the Java Device Manager provides additional information for PoE ports on the Nortel Ethernet Routing Switch 4548GT-PWR. This additional information is in the form of a colored P that appears inside the graphic representation of the port. This colored P represents the current power aspect of the PoE port.

"Nortel Ethernet Routing Switch 4548GT-PWR" (page 162) displays an example of the front panel view of a Nortel Ethernet Routing Switch 4548GT-PWR.

Nortel Ethernet Routing Switch 4548GT-PWR



"Power Aspect color codes" (page 162) explains the different colors displayed by the power aspect.

Power Aspect color codes

Color	Description
Green	The port is currently delivering power.
Red	The power and detection mechanism for the port is disabled.
Orange	The power and detection mechanism for the port is enabled. The port is not currently delivering power.
White/Gray	The power and detection mechanism for the port is unknown.

Note: The data and power aspect coloring schemes are independent of each other. You can view the initial status for both data and power aspect for the port. To refresh the power status, right-click the unit, and select **Refresh PoE Status** from the shortcut menu.

Configuring PoE using the JDM

For information about configuring Power over Ethernet (PoE) using the Java Device Manager, see "Editing and viewing switch PoE configurations" (page 237).

Configuring PoE using the Web-based Management Interface

The following sections describe PoE configuration and management using the Web-based Management Interface:

- "Configuring power management on the switch" (page 163)
- "Configuring power management for the ports" (page 165)

Configuring power management on the switch

Use the Global Power Management screen to configure and view power settings for the switch.

To configure power management, complete the following procedure.

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Global Power Management screen by selecting Configuration > PoE Management > Global Power Management . The following figure illustrates the Global Power Management dialog box. |
|---|---|

Configuration > Power Management > Global Power Management

Unit 3	
Global Power Management	
Available DTE Power	320 Watt
DTE Power Status	Normal
DTE Power Consumption	0 Watt
DTE Power Usage Threshold	80 % (1..99)
Power Pair	Signal
Traps Control	Enable
PD Detect Type	802.3af and Legacy
Power Source Present	AC Only
AC Power Status	Present
DC Power Status	Not present

Submit

- | | |
|---|------------------------------|
| 2 | Enter the required settings. |
| 3 | Click Submit . |

—End—

"Global Power Management fields" (page 164) describes the items on the **Global Power Management** dialog box.

Global Power Management fields

Item	Description
Available DTE Power	The power provided by the Ethernet Routing Switch 4500 to the devices. The range of power that is available from internal power supply is 320 W to 740 W.
DTE Power Status	The status of the PoE feature. The values that maybe displayed are Normal or Error.
DTE Power Consumption	The total power usage.
Power Pair	The Power Pair (part of the RJ-45 pin connectors) that you chose to supply power.
DTE Power Usage Threshold	The power usage threshold, inserted by user.
Traps Control	The status of the traps control. You can enable or disable this feature.
PD Detect Type	The standard that you use for power detection. The standard that you select can be one of the following: <ul style="list-style-type: none"> • IEEE 802.3af • IEEE 802.3af and legacy.
Power Source Present	The mode of power supply that the Ethernet Routing Switch 4500 currently uses. The mode of power supply can be one of the following values: <ul style="list-style-type: none"> • AC only: signifies that the switch uses internal power supply. • DC only: signifies that the switch uses external power supply. • AC and DC: signifies that the switch uses both external and internal <p>This is a read-only field.</p>

Item	Description
AC Power Status	The status of the AC power supply.
DC Power Status	The status of the DC power supply.

Configuring power management for the ports

Configuring power management for the ports involves setting a priority for the ports on the switch.

To configure power management for the ports, complete the following procedure.

Step Action

- 1 Open the Port Property page by selecting **Configuration > PoE Management > Port Property**. The following figure illustrates the Port Property dialog box..

Options, skins, help and informat

Configuration > Power Management > Port Property

Port Power Setting

Unit 1

Port	Admin. Status	Current Status	Classification	Limit (Watt)	Priority	Volt (V)	Current (mA)	Power (Watt)
1	Enabled	Detecting	0	16	Low	0.0	0	0.000
2	Enabled	Detecting	0	16	Low	0.0	0	0.000
3	Enabled	Detecting	0	16	Low	0.0	0	0.000
4	Enabled	Detecting	0	16	Low	0.0	0	0.000
5	Enabled	Detecting	0	16	Low	0.0	0	0.000
6	Enabled	Detecting	0	16	Low	0.0	0	0.000
7	Enabled	Detecting	0	16	Low	0.0	0	0.000
8	Enabled	Detecting	0	16	Low	0.0	0	0.000
9	Enabled	Detecting	0	16	Low	0.0	0	0.000
10	Enabled	Detecting	0	16	Low	0.0	0	0.000
11	Enabled	Detecting	0	16	Low	0.0	0	0.000
12	Enabled	Detecting	0	16	Low	0.0	0	0.000
Switch	Enabled	<input type="checkbox"/>		16 <input type="checkbox"/>	Low <input type="checkbox"/>			
Stack	Enabled	<input type="checkbox"/>		16 <input type="checkbox"/>	Low <input type="checkbox"/>			

Unit 3

Submit

- 2 Enter the required settings.
- 3 Click **Submit**.

—End—

"Port Property fields" (page 166) describes the items on the **Port Property** fields.

Port Property fields

Item	Description
Port	The port number.
Admin. Status	<p>Set the power status to one of the following:</p> <ul style="list-style-type: none"> • Enabled • Disabled <p>The default value is Enabled.</p>
Current Status	<p>The current status of the port, which is one of the following values:</p> <ul style="list-style-type: none"> • Disable • Detecting • Detected • Delivering Power • Error • Invalid PD • Test • Deny Low Priority • Overload
Classification	The operational status of the port PD classification.
Limit (W)	Set the maximum power that the switch can supply to a port. The default value is 16W.
Priority	<p>Set the priority of a port. The Priority of a port is used to detect the ports that can be dropped when the power requirements exceed the available power budget.</p> <p>The priority that can be assigned to a port can be one of the following:</p> <ul style="list-style-type: none"> • Low • High • Critical

Item	Description
	Power to the dropped ports is restored when the power requirement becomes lower than the power budget. When several ports have the same priority, the port with the higher port number is dropped.
Volt (v)	The voltage supplied by the port.
Current (mA)	The current supplied by the port.
Power (W)	The power supplied by the port.

Switch administration tasks

This chapter describes basic switch administration tasks that apply to no specific switch application. For complete information about administration tasks specific to a switch application, consult the appropriate book.

This chapter contains the following topics:

- "General switch administration using the CLI" (page 169)
- "General Switch Administration using the Web-based Management Interface" (page 194)
- "General Switch Administration using the JDM" (page 207)

General switch administration using the Command Line Interface

This section describes the Command Line Interface (CLI) commands used in general switch administration. This section contains the following topics:

- "Multiple switch configurations" (page 170)
- New Unit Quick Configuration
- IP blocking
- "Assigning and clearing IP addresses" (page 171)
- "Assigning and clearing IP addresses for specific units" (page 174)
- "Displaying Interfaces" (page 175)
- "Setting port speed" (page 176)
- "Enabling Autotopology" (page 179)
- "Enabling rate-limiting" (page 183)
- "Using Simple Network Time Protocol" (page 185)
- "Clock configuration" (page 189)
- "Custom Autonegotiation Advertisements" (page 189)
- "Connecting to Another Switch" (page 190)
- "Domain Name Server (DNS) Configuration" (page 192)

Multiple switch configurations

The Nortel Ethernet Routing Switch 4500 Series supports the storage of two switch configurations in flash memory. The switch can use either configuration and must be reset for the configuration change to take effect.

A regular reset of the switch synchronizes configuration changes to the active configuration, whereas a reset to defaults sets configuration to factory defaults. The inactive block is not affected.

In stack configurations, all units in the stack must use the same active configuration. If a unit joins a stack, a check is performed between the unit active configuration and the stack active configuration. If the two differ, the new stack unit resets and loads the stack active configuration.

Use the following CLI commands to configure and use multiple switch configuration:

- ["show nvram block command" \(page 170\)](#)
- ["copy config nvram block command" \(page 170\)](#)
- ["copy nvram config block command" \(page 171\)](#)

show nvram block command

This command shows the configurations currently stored on the switch. The syntax for this command is

```
show nvram block
```

Run this command in Global Configuration command mode.

copy config nvram block command

This command copies the current configuration to one of the flash memory locations. The syntax for this command is

```
copy config nvram block <1-2> name <block_name>
```

["copy config nvram block parameters" \(page 170\)](#) outlines the parameters for this command.

copy config nvram block parameters

Parameter	Description
block <1—2>	The flash memory location to store the configuration.
name <block_name>	Name to attach to this block. Names can be up to 40 characters in length with no spaces.

Run this command in Global Configuration command mode.

copy nvram config block command

This command copies the configuration stored in flash memory at the specified location and makes it the active configuration. The syntax for this command is

```
copy nvram config block <1-2>
```

Substitute <1-2> with the configuration file to load.

This command resets the switch to reset so that the new configuration load.

Run this command in Global Configuration command mode.

Assigning and clearing IP addresses

Use the CLI, to assign, clear, and view IP addresses and gateway addresses. For details, see the following sections:

- ["ip address command" \(page 171\)](#)
- ["no ip address command" \(page 172\)](#)
- ["ip default-gateway command" \(page 172\)](#)
- ["no ip default-gateway command" \(page 173\)](#)
- ["show ip command" \(page 173\)](#)

ip address command

The `ip address` command sets the IP address and subnet mask for the switch or a stack.

The syntax for the `ip address` command is

```
ip address [stack | switch | unit] <XXX.XXX.XXX.XXX> [netmask  
<XXX.XXX.XXX.XXX>
```

Run the `ip address` command in Global Configuration command mode.

If the stack or switch parameter is not specified, the system automatically modifies the stack IP address when in stack mode and modifies the switch IP address when in stand-alone mode.

"[ip address parameters](#)" (page 172) describes the parameters for the `ip address` command.

ip address parameters

Parameters	Description
stack switch unit	Set the IP address and netmask of the stack or the switch, or another unit in at a stack..
XXX.XXX.XXX.XXX	Enter the IP address in dotted-decimal notation; netmask is optional.
netmask	The IP subnet mask for the stack or switch.

Note: When you change the IP address or subnet mask, connectivity to Telnet and the Web can be lost.

no ip address command

The `no ip address` command clears the IP address and subnet mask for a switch or a stack. This command sets the IP address and subnet mask for a switch or a stack to all zeros (0).

The syntax for the `no ip address` command is

```
no ip address {stack | switch | unit}
```

Run the `no ip address` command in Global Configuration command mode.

"[no ip address parameters](#)" (page 172) describes the parameters for this command.

no ip address parameters

Parameters	Description
stack switch	Zeroes out the stack IP address and subnet mask or the switch IP address and subnet mask.
unit	Zeroes out the IP address for the specified unit.

Note: When you change the IP address or subnet mask, connectivity to Telnet and the Web Interface can be lost. Any new Telnet connection can be disabled and must connect to the serial console port to configure a new IP address.

ip default-gateway command

The `ip default-gateway` command sets the default IP gateway address for a switch or a stack to use.

The syntax for the `ip default-gateway` command is

```
ip default-gateway <XXX.XXX.XXX.XXX>
```

Run the `ip default-gateway` command in Global Configuration command mode.

"[ip default-gateway parameters](#)" (page 173) describes the parameters for the `ip default-gateway` command.

ip default-gateway parameters

Parameters	Description
XXX.XXX.XXX.XXX	Enter the dotted-decimal IP address of the default IP gateway.

Note: When you change the IP gateway, connectivity to Telnet and the Web Interface can be lost.

no ip default-gateway command

The `no ip default-gateway` command sets the IP default gateway address to zero (0).

The syntax for the `no ip default-gateway` command is

```
no ip default-gateway
```

Run the `no ip default-gateway` command in Global Configuration command mode.

Note: When you change the IP gateway, connectivity to Telnet and the Web Interface can be lost.

show ip command

The `show ip` command displays the IP configurations, BootP mode, stack address, switch address, subnet mask, and gateway address. This command displays these parameters for what is configured, what is in use, and the last BootP. The sub command, `Display DNS configuration`, provides information about the DNS configuration.

The syntax for the `show ip` command is

```
show ip [bootp] [default-gateway] [address]
```

Run the `show ip` command in User EXEC or Privileged EXEC command mode.

If you do not enter any parameters, this command displays all IP-related configuration information.

"show ip parameters" (page 174) describes the parameters and variables for the `show ip` command.

show ip parameters

Parameters and variables	Description
bootp	BootP-related IP information.
default-gateway	The IP address of the default gateway.
address	The current IP address.

Assigning and clearing IP addresses for specific units

You can use the CLI to assign and clear IP addresses for a specific unit in a stack. For details, see the following sections:

- "ip address unit command" (page 174)
- "no ip address unit command" (page 174)
- "default ip address command" (page 175)

ip address unit command

The `ip address unit` command sets the IP address and subnet mask of a specific unit in the stack.

The syntax for the `ip address unit` command is

```
ip address unit <1-8> [A.B.C.D]
```

Run the `ip address unit` command in Global Configuration command mode.

"ip address unit parameters" (page 174) describes the parameters this command.

ip address unit parameters

Parameters and variables	Description
unit <1—8>	Sets the unit you are assigning an IP address.
A.B.C.D	Enter IP address in dotted-decimal notation.

Note: When the IP address or subnet mask changes, connectivity to Telnet and the Internet can be lost.

no ip address unit command

The `no ip address unit` command sets the IP address for the specified unit in a stack to zeros (0).

The syntax for the `no ip address unit` command is

```
no ip address unit <1-8>
```

Run the `no ip address unit` command in Global Configuration command mode.

"[no ip address parameters](#)" (page 175) describes the parameters this command.

no ip address parameters

Parameters and variables	Description
unit <1—8>	Zeroes out the IP address for the specified unit.

Note: When you change the IP address or subnet mask, connectivity to Telnet and the Internet can be lost.

default ip address command

The `default ip address` command sets the IP address for the specified unit in a stack to all zeros (0).

The syntax for the `default ip address` command is

```
default ip address
```

Run the `default ip address` command in Global Configuration command mode.

Note: When the IP gateway changes, connectivity to Telnet and the Internet can be lost.

Displaying Interfaces

You can view the status of all interfaces on the switch or stackd, including MultiLink Trunk membership, link status, autonegotiation, and speed.

show interfaces command

The `show interfaces` command displays the current configuration and status of all interfaces.

The syntax for the `show interfaces` command is

```
show interfaces [names] [<portlist>] [gbic-info]
```

Run the `show interfaces` command in User EXEC command mode.

"[show interfaces parameters](#)" (page 176) describes the parameters and variables for the `show interfaces` command.

show interfaces parameters

Parameters and variables	Description
names <portlist>	Display interface names; enter specific ports to see only those ports .
gbic-info	Display GBIC details.
LINE	Display a list of existing ports with names (displays interface names).

Setting port speed

To set port speed and duplexing using the CLI, see the following sections:

- "[speed command](#)" (page 176)
- "[default speed command](#)" (page 177)
- "[duplex command](#)" (page 177)
- "[default duplex command](#)" (page 178)

speed command

The `speed` command sets the port speed.

The syntax for the `speed` command is

```
speed [port <portlist>] {10 | 100 | 1000 | auto}
```

Run the `speed` command in Interface Configuration command mode.

"[speed parameters](#)" (page 176) describes the parameters and variables for the `speed` command.

speed parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers to configure the speed. Enter the port numbers you want to configure.

Parameters and variables	Description
	Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.
10 100 1000 auto	Set the speed to <ul style="list-style-type: none"> • 10: 10 Mb/s • 100: 100 Mb/s • 1000: 1000 Mb/s or 1 GB/s • auto: autonegotiation

Note: Enabling or disabling autonegotiation for speed also enables or disables it for duplex operation.

When you set the port speed for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

default speed command

The `default speed` command sets the port speed to the factory default speed.

The syntax for the `default speed` command is

```
default speed [port <portlist>]
```

Run the `default speed` command in Interface Configuration command mode.

"[Default speed parameters](#)" (page 177) describes the parameters for this command.

Default speed parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers for which to set the speed to factory default. Enter the port numbers to set. <p>Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.</p>

duplex command

The `duplex` command specifies the duplex operation for a port.

The syntax for the `duplex` command is

```
duplex [port <portlist>] {full | half | auto}
```

Run the `duplex` command in Interface Configuration command mode.

"Duplex parameters" (page 178) describes the parameters for this command.

Duplex parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers to reset the duplex mode to factory default values. Enter the port number to configure. The default value is autonegotiation. Note: If you omit this parameter, the system uses the ports you specified in the <code>interface</code> command.
full half auto	Set duplex to <ul style="list-style-type: none"> • full: full-duplex mode • half: half-duplex mode • auto: autonegotiation

Note: Enabling or disabling autonegotiation for speed also enables or disables it for duplex operation.

When you set the duplex mode for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

default duplex command

The `default duplex` command sets the duplex operation for a port to the factory default duplex value.

The syntax for the `default duplex` command is

```
default duplex [port <portlist>]
```

Run the `default duplex` command in Interface Configuration command mode.

"Default duplex parameters" (page 179) describes the parameters for this command.

Default duplex parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers for which to reset the duplex mode to factory default values. Enter the port numbers to configure. The default value is autonegotiation. Note: If you omit this parameter, the system uses the ports you specified in the <code>interface</code> command.

Enabling Autotopology

Use CLI to configure the Enterprise Autotopology protocol.

For more information about Autotopology, see <http://www.nortel.com/support>. (The product family for Enterprise and Autotopology is Data and Internet.)

To enable autotopology using the CLI, see the following sections:

- "autotopology command" (page 179)
- "no autotopology command" (page 179)
- "default autotopology command" (page 180)
- "show autotopology settings command" (page 180)
- "show autotopology nmm-table command" (page 180)

autotopology command

The `autotopology` command enables the Autotopology protocol.

The syntax for the `autotopology` command is

```
autotopology
```

Run the `autotopology` command in Global Configuration command mode.

no autotopology command

The `no autotopology` command disables the Autotopology protocol.

The syntax for the `no autotopology` command is

```
no autotopology
```

Run the `no autotopology` command in Global Configuration command mode.

default autotopology command

The `default autotopology` command enables the Autotopology protocol.

The syntax for the `default autotopology` command is

```
default autotopology
```

Run the `default autotopology` command in Global Configuration command mode.

The `default autotopology` command has no parameters or values.

show autotopology settings command

The `show autotopology settings` command displays the global autotopology settings.

The syntax for the `show autotopology settings` command is

```
show autotopology settings
```

Run the `show autotopology settings` command in Privileged EXEC command mode.

The `show autotopology settings` command has no parameters or values.

show autotopology nmm-table command

The `show autotopology nmm-table` displays the Autotopology network management module (NMM) table.

The syntax for the `show autotopology nmm-table` command is

```
show autotopology nmm-table
```

Run the `show autotopology nmm-table` command in Privileged EXEC command mode.

The `show autotopology nmm-table` command has no parameters or values.

Enabling flow control

Gigabit Ethernet, when used with the Nortel Ethernet Routing Switch 4500 Series, can control traffic on this port using the `flowcontrol` command.

Note: Due to Quality of Service (QoS) interaction, the Ethernet Routing Switch 4500 cannot send pause-frames.

To enable flow control using the CLI, see the following sections:

- "flowcontrol command" (page 181)
- "no flowcontrol command" (page 181)
- "default flowcontrol command" (page 182)

flowcontrol command

Use the `flowcontrol` command only on Gigabit Ethernet ports to control the traffic rates during congestion.

The syntax for the `flowcontrol` command is

```
flowcontrol [port <portlist>] {asymmetric | symmetric | auto
| disable}
```

Run the `flowcontrol` command in Interface Configuration mode.

"Flowcontrol parameters" (page 181) describes the parameters for this command.

Flowcontrol parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers to configure for flow control. Note: If you omit this parameter, the system uses the ports you specified in the <code>interface</code> command but only those ports that have speed set to 1000/full.
asymmetric symmetric auto disable	Set the mode for flow control: <ul style="list-style-type: none"> • asymmetric: PAUSE frames can flow only in one direction. • symmetric: PAUSE frames can flow in either direction. • auto: Set the port to automatically determine the flow control mode (default). • disable: Disable flow control on the port.

no flowcontrol command

Use the `no flowcontrol` command only on Gigabit Ethernet ports to disable flow control.

The syntax for the `no flowcontrol` command is

```
no flowcontrol [port <portlist>]
```

Run the `no flowcontrol` command in Interface Configuration mode.

"No flowcontrol parameters" (page 182) describes the parameters for this command.

No flowcontrol parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers for which to disable flow control. Note: If you omit this parameter, the system uses the ports you specified in the <code>interface</code> command, but only those ports that have speed set to 1000/full.

default flowcontrol command

Use the `default flowcontrol` command only on Gigabit Ethernet ports to set the flow control to automatic, which automatically detects the flow control.

The syntax for the `default flowcontrol` command is

```
default flowcontrol [port <portlist>]
```

Run the `default flowcontrol` command in Interface Configuration mode.

"Default flowcontrol parameters" (page 182) describes the parameters for the command.

Default flowcontrol parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers to default to automatic flow control. Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.

Enabling rate-limiting

The percentage of multicast traffic, or broadcast traffic, or both, can be limited using the CLI. For details, see the following sections:

- "show rate-limit command" (page 183)
- "rate-limit command" (page 183)
- "no rate-limit command" (page 184)
- "default rate-limit command" (page 184)

show rate-limit command

The `show rate-limit` command displays the rate-limiting settings and statistics.

The syntax for the `show rate-limit` command is

```
show rate-limit
```

Run the `show rate-limit` command in Privileged EXEC command mode.

rate-limit command

The `rate-limit` command configures rate-limiting on the port.

The syntax for the `rate-limit` command is

```
rate-limit [port <portlist>] {multicast <pct> | broadcast <pct> | both <pct>}
```

Run the `rate-limit` command in Interface Configuration command mode.

"Rate-limit parameters" (page 183) describes the parameters for this command.

Rate-limit parameters

Parameters and values	Description
port <portlist>	Specify the port numbers to configure for rate-limiting. Enter the port numbers to configure. Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.
multicast <pct> broadcast <pct> both <pct>	Apply rate-limiting to the type of traffic. Enter an integer from 1 to 10 to set the rate-limiting percentage: <ul style="list-style-type: none"> • multicast: Apply rate-limiting to multicast packets.

Parameters and values	Description
	<ul style="list-style-type: none"> • broadcast: Apply rate-limiting to broadcast packets. • both: Apply rate-limiting to both multicast and broadcast packets.

no rate-limit command

The `no rate-limit` command disables rate-limiting on the port.

The syntax for the `no rate-limit` command is:

```
no rate-limit [port <portlist>]
```

Run the `no rate-limit` command in Interface Configuration command mode.

"No rate-limit parameters" (page 184) describes the parameters for this command.

No rate-limit parameters

Parameters	Description
port <portlist>	<p>Specify the port numbers to disable for rate-limiting. Enter the port numbers to disable.</p> <p>Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.</p>

default rate-limit command

The `default rate-limit` command restores the rate-limiting value for the specified port to the default setting.

The syntax for the `default rate-limit` command is

```
default rate-limit [port <portlist>]
```

Run the `default rate-limit` command in Interface Configuration command mode.

"Default rate-limit parameters" (page 185) describes the parameters for this command.

Default rate-limit parameters

Parameters	Description
port <portlist>	Specify the port numbers to reset rate-limiting to factory default. Enter the port numbers to set rate-limiting to default. Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.

Using Simple Network Time Protocol

The Simple Network Time Protocol (SNTP) feature synchronizes the Universal Coordinated Time (UTC) to an accuracy within 1 second. This feature adheres to the IEEE RFC 2030 (MIB is the s5agent). With this feature, the system can obtain the time from any RFC 2030-compliant NTP/SNTP server.

Note: If problems occur when you use this feature, try various NTP servers. Some NTP servers can be overloaded or currently inoperable.

The system retries connecting with the NTP server a maximum of three times, with 5 minutes between each retry.

Use SNTP to provide a real-time timestamp for the software, shown as Greenwich Mean Time (GMT).

If you run SNTP, the system synchronizes with the configured NTP server at boot-up and at user-configurable periods thereafter (the default synchronization interval is 24 hours). The first synchronization does not occur until network connectivity is established.

SNTP supports primary and secondary NTP servers. The system tries the secondary NTP server only if the primary NTP server is unresponsive.

To configure SNTP, see the following commands:

- "Show SNTP command" (page 186)
- "show sys-info command" (page 186)
- "SNTP enable command" (page 186)
- "No SNTP enable command" (page 186)
- "SNTP server primary address command" (page 186)
- "SNTP server secondary address command" (page 187)
- "No SNTP server command" (page 187)

- "SNTP sync-now command" (page 188)
- "SNTP sync-interval command" (page 188)

Show SNTP command

The `show sntp` command displays the SNTP information, as well as the configured NTP servers.

The syntax for the `show sntp` command is

```
show sntp
```

Run the `show sntp` command in Privileged EXEC command mode.

show sys-info command

The `show sys-info` command displays the current system characteristics.

The syntax for the `show sys-info` command is

```
show sys-info
```

Run the `show sys-info` command in Privileged EXEC command mode.

Note: You must have SNTP enabled and configured to display GMT time.

SNTP enable command

The `SNTP enable` command enables SNTP.

The syntax for the `SNTP enable` command is

```
sntp enable
```

Run the `SNTP enable` command in Global Configuration command mode.

Note: The default setting for SNTP is Disabled.

No SNTP enable command

The `no sntp enable` command disables SNTP.

The syntax for the `no sntp enable` command is

```
no sntp enable
```

Run the `no sntp enable` command in Global Configuration command mode.

SNTP server primary address command

The `SNTP server primary address` command specifies the IP addresses of the primary NTP server.

The syntax for the `SNTP server primary address` command is

```
sntp server primary address <A.B.C.D>
```

Run the `SNTP server primary address` command in Global Configuration command mode.

"[SNTP server primary address parameters](#)" (page 187) describes the parameters for this command.

SNTP server primary address parameters

Parameters and Variables	Description
<A.B.C.D>	Enter the IP address of the primary NTP server in dotted-decimal notation.

SNTP server secondary address command

The `SNTP server secondary address` command specifies the IP addresses of the secondary NTP server.

The syntax for the `SNTP server secondary address` command is

```
sntp server secondary address <A.B.C.D>
```

Run the `SNTP server secondary address` command in Global Configuration command mode.

"[SNTP server secondary address parameters](#)" (page 187) describes the parameters for this command.

SNTP server secondary address parameters

Parameters	Description
<A.B.C.D>	Enter the IP address of the secondary NTP server in dotted-decimal notation.

No SNTP server command

The `no SNTP server` command clears the NTP server IP addresses. The command clears the primary and secondary server addresses.

The syntax for the `no SNTP server` command is

```
no sntp server {primary | secondary}
```

Run the `no SNTP server` command in Global Configuration command mode.

"no SNTP server parameters" (page 188) describes the parameters for this command.

no SNTP server parameters

Parameters	Description
primary	Clear the primary SNTP server address.
secondary	Clear the secondary SNTP server address.

SNTP sync-now command

The `SNTP sync-now` command forces a manual synchronization with the NTP server.

The syntax for the `SNTP sync-now` command is

```
sntp sync-now
```

Run the `SNTP sync-now` command in Global Configuration command mode.

Note: SNTP must be enabled before this command can take effect.

SNTP sync-interval command

The `SNTP sync-interval` command specifies recurring synchronization with the secondary NTP server in hours relative to initial synchronization.

The syntax for the `SNTP sync-interval` command is

```
sntp sync-interval <0-168>
```

Run the `SNTP sync-interval` command in Global Configuration command mode.

"SNTP sync-interval parameters" (page 188) describes the for this command.

SNTP sync-interval parameters

Parameters and Variables	Description
<0-168>	Enter the number of hours for periodic synchronization with the NTP server. Note: 0 is boot-time only, and 168 is once a week.

Clock configuration

In addition to SNTP time configuration, a clock provides the switch with time information. This clock provides the switch information in the instance that SNTP time is not available.

Use the following commands to view and configure the clock:

- "Clock source command" (page 189)
- `default clock source`

Clock source command

This command sets the default clock source for the switch.

The syntax for this command is

```
clock source {sntp | sysUpTime}
```

Substitute `{sntp | sysUpTime}` with the clock source selection.

Run this command in Global Configuration command mode.

Custom Autonegotiation Advertisements

Custom Autonegotiation Advertisement (CANA) customizes the capabilities that are advertised. It also controls the capabilities that the Nortel Ethernet Routing Switch 4500 Series advertises as part of the auto negotiation process.

The following sections describe configuring CANA using the CLI:

- "Configuring CANA" (page 189)
- "Viewing current autonegotiation advertisements" (page 189)
- "Viewing hardware capabilities" (page 190)
- "Setting default auto-negotiation-advertisements" (page 190)
- "no auto-negotiation-advertisements command" (page 190)

Configuring CANA

Use the `auto-negotiation-advertisements` command to configure CANA.

To configure port 5 to advertise the operational mode of 10 Mb/s and full duplex enter the following command:

```
auto-negotiation-advertisements port 5 10-full
```

Viewing current autonegotiation advertisements

To view the autonegotiation advertisements for the device, enter the following command:

```
show auto-negotiation-advertisements [port <portlist>]
```

Viewing hardware capabilities

To view the available operational modes for the device, enter the following command:

```
show auto-negotiation-capabilities [port <portlist>]
```

Setting default auto-negotiation-advertisements

The `default auto-negotiation-advertisements` command makes a port advertise all auto negotiation capabilities.

The syntax for the `default auto-negotiation-advertisements` command is

```
default auto-negotiation-advertisements [port <portlist>]
```

To set default advertisements for port 5 of the device, enter the following command:

```
default auto-negotiation-advertisements port 5
```

Run the `default auto-negotiation-advertisements` command in Interface Configuration mode.

no auto-negotiation-advertisements command

The `no auto-negotiation-advertisements` command makes a port silent.

The syntax for the `no auto-negotiation-advertisements` command is

```
no auto-negotiation-advertisements [port <portlist>]
```

Run the `no auto-negotiation-advertisements` command in Interface Configuration mode.

Connecting to Another Switch

Use the CLI to communicate with another switch while maintaining the current switch connection, by running the `ping` and `telnet` commands.

ping command

Use the `ping` command to determine whether communication with another switch can be established.

The `ping` command tests the network connection to another network device by sending an Internet Control Message Protocol (ICMP) packet from the switch to the target device.

Note: You must set the local IP address before you issue the ping command.

The syntax for this command is

```
ping <ip_address | dns_host_name> [datasize <64-4096>]
[{count <1-9999> | continuous}] [{timeout | -t} <1-120>]
[interval <1-60>] [debug]
```

Substitute `<ip_address | dns_host_name>` with either the IP address or the DNS host name of the unit to test.

Run this command in User EXEC command mode or any of the other command modes.

ping parameters

Parameter	Description
ip_address dns_host_name	IP address or DNS host name of the unit to test.
datasize <64-4096>	Specify the size of the ICMP packet to be sent. The data size range is from 64 to 4096 bytes.
count <1-9999> continuous	Set the number of ICMP packets to be sent. The continuous mode sets the ping running until the user interrupts it by entering Ctrl+C.
timeout -t <1-120>	Set the timeout using either the <code>timeout</code> with the <code>-t</code> parameter followed by the number of seconds the switch must wait before timing out.
interval <1-60>	Specify the number of seconds between transmitted packets.
debug	Provide additional output information such as the ICMP sequence number and the trip time.

telnet command

Use the `telnet` command to establish communications with another switch during the current CLI session. Communication can be established to only one external switch at a time using the `telnet` command.

The syntax for this command is

```
telnet <ip_address | dns_host_name>
```

Substitute `<ip_address | dns_host_name>` with either the IP address or the DNS host name of the unit with which to communicate.

Run this command in User EXEC command mode.

Domain Name Server (DNS) Configuration

Use domain name servers when the switch needs to resolve a domain name (such as nortel.com) to an IP address. Use the following commands to configure the switch domain name servers:

- "show ip dns command" (page 192)
- "ip domain-name command" (page 192)
- "no ip domain-name command" (page 192)
- "default ip domain-name command" (page 193)
- "ip name-server command" (page 193)
- "no ip name-server command" (page 193)

show ip dns command

Use the `show ip dns` command to display DNS-related information. This information includes the default switch domain name and any configured DNS servers.

The syntax for this command is

```
show ip dns
```

Run this command in User EXEC command mode.

ip domain-name command

Use the `ip domain-name` command to set the default DNS domain name for the switch. This default domain name is appended to all DNS queries or commands that do not already contain a DNS domain name.

The syntax for this command is

```
ip domain-name <domain_name>
```

Substitute `<domain_name>` with the default domain name. A domain name is deemed valid if it contains alphanumeric characters and at least one period (.).

Run this command in Global Configuration command mode.

no ip domain-name command

Use the `no ip domain-name` command to clear a previously configured default DNS domain name for the switch.

The syntax for this command is

```
no ip domain-name
```

Run this command in Global Configuration command mode.

default ip domain-name command

Use the `default ip domain-name` command to set the system default switch domain name. Because this default is an empty string, this command has the same effect as the `no ip domain-name` command.

The syntax for this command is:

```
default ip domain-name
```

Run this command in Global Configuration command mode.

ip name-server command

Use the `ip name-server` command to set the domain name servers the switch uses to resolve a domain name to an IP address. A switch can have up to three domain name servers specified for this purpose.

The syntax of this command is

```
ip name-server <ip_address_1>
ip name-server [<ip_address_2>]
ip name-server [<ip_address_3>]
```

Note: To enter all three server addresses, you must enter the command three times, each with a different server address.

"[ip name-server parameters](#)" (page 193) outlines the parameters for this command.

ip name-server parameters

Parameter	Description
<ip_address_1>	The IP address of the domain name server used by the switch.
<ip_address_2>	Optional. The IP address of a domain name server to add to the list of servers used by the switch.
<ip_address_3>	Optional. The IP address of a domain name server to add to the list of servers used by the switch.

Run this command in Global Configuration command mode.

no ip name-server command

Use the `no ip name-server` command to remove domain name servers from the list of servers used by the switch to resolve domain names to an IP address.

The syntax for this command is

```
no ip name-server <ip_address_1>
no ip name-server [<ip_address_2>]
no ip name-server [<ip_address_3>]
```

Note: To remove all three server addresses, you must enter the command three times, each with a different server address.

"[no ip name-server parameters](#)" (page 194) outlines the parameters for this command.

no ip name-server parameters

Parameter	Description
<ip_address_1>	The IP address of the domain name server to remove.
<ip_address_2>	Optional. The IP address of a domain name server to remove from the list of servers used by the switch.
<ip_address_3>	Optional. The IP address of a domain name server to remove from the list of servers used by the switch.

Run this command in Global Configuration command mode.

General Switch Administration using the Web-based Management Interface

This section contains the following topics:

- "[Viewing stack information](#)" (page 194)
- "[Viewing summary switch information](#)" (page 196)
- "[Changing stack numbering](#)" (page 197)
- "[Identifying unit numbers](#)" (page 199)
- "[Configuring BootP, IP, and gateway settings](#)" (page 200)
- "[Modifying system settings](#)" (page 203)
- "[Managing remote access by IP address](#)" (page 205)
- [Configuring the Real-Time Clock](#)

Viewing stack information

Note: The Embedded Web Server automatically detects the operational mode of your system. If the system is in stand-alone mode, the Stack Information page option is not listed in the menu.

Step	Action
------	--------

- 1 Open the **Stack Information** screen by selecting **Summary > Stack Information** from the menu. The following message box is displayed.

Summary > Stack Information

Stack Information	
System Description	Ethernet Routing Switch 4548GT-PWR
Software Version	v5.0.0.103
MAC Address	00-16-CA-DA-C4-01
IP Address	192.167.120.43
Manufacturing Date Code	03312006
Serial #	SDL17001G
Operational State	Normal

Stack Inventory							
Unit	Description	Pluggable Port	Pluggable Port	Pluggable Port	Pluggable Port	Software Version	Operational State
1	Ethernet Routing Switch 4548GT-PWR 48 ports 10/100/1000 BaseT with PoE and 4 shared SFP ports	(45) None	(46) None	(47) None	(48) None	v5.0.0.103	Normal
2	Ethernet Routing Switch 4550T 48 ports 10/100BaseT plus 2 10/100/1000/SFP combo ports	(49) None	(50) None			v5.0.0.103	Normal

—End—

The following table "Stack Information screen fields" (page 195) describes the fields on the Stack Information and Stack Inventory sections of the Stack Information screen.

Stack Information screen fields

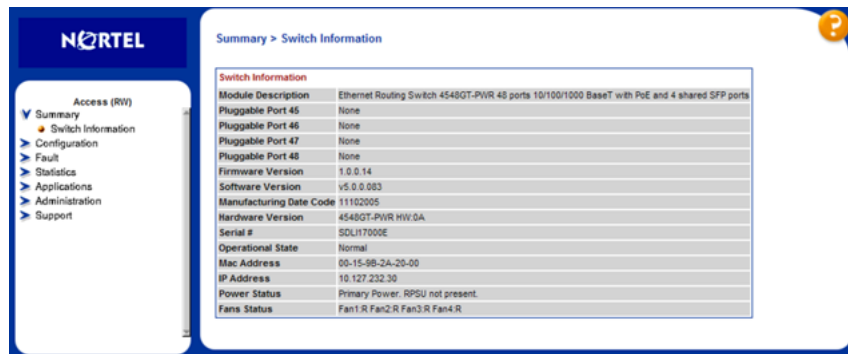
Section	Fields	Description
Stack Information	System Description	The name created in the configuration process to identify the stack.
	Software Version	The version of the running software.
	MAC Address	The MAC address of the stack.
	IP Address	The IP address of the stack.

Section	Fields	Description
	Manufacturing Date Code	The date of manufacture of the board in ASCII format: YYYYMMDD.
	Serial Number	The serial number of the base unit.
	Operational State	The current operational state of the device. The operational states are Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.
Stack Inventory	Unit	The unit number assigned to the device by the network manager. For more information about stack numbering, see " Changing stack numbering " (page 197).
	Description	The description of the device or its subcomponent.
	Pluggable port	The SFP GBICs connected to the switch.
	Software Version	The current running software version.
	Operational State	The current operational state of the stack. The operational states are Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.

Viewing summary switch information

Step	Action
------	--------

- | | |
|---|--|
| 1 | Open the Switch Information screen by selecting Summary > Switch Information from the menu. The following message box is displayed. |
|---|--|



The following table "Switch Information page fields" (page 197) describes the fields on the Switch Information screen.

Switch Information page fields

Item	Description
Unit, if in a stack configuration	Select the number of the device on which to view summary information. The page is updated with information about the selected switch. For more information about stack numbering, see " Changing stack numbering " (page 197).
Pluggable Port	Indicates the presence of an SFP. Fields are present and numbered as appropriate to the switch model.
Module Description	The factory set description of the policy switch.
Firmware Version	The version of the running firmware.
Software Version	The version of the running software.
Manufacturing Date Code	The date of manufacture of the board in ASCII format.
Hardware Version	The hardware version of the switch.
Serial Number	The serial number of the policy switch.
Operational State	The current operational state of the device. The operational states are Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.
Power Status	The current power status of the device <ul style="list-style-type: none"> • Primary Power. RPS not present • Primary Power. RPS present • Redundant Power. Primary power failed • Unavailable
Fans Status	The current status of switch cooling fans.

- 2 In stacked configurations, click the number of the device to view in the upper-left corner of the screen.

—End—

Changing stack numbering

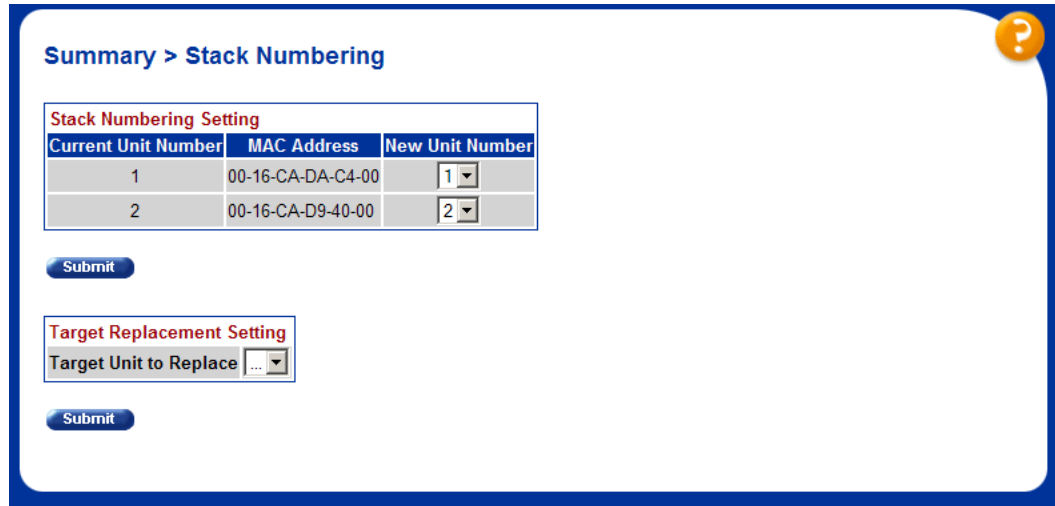
If the system is in a stack, you can view and renumber existing stack numbering information.

Note: The unit number does not affect the base unit designation.

To view or renumber devices within the stack framework, perform the following procedure.

Step Action

- 1 To open the **Stack Numbering** screen, select **Summary > Stack Numbering**, as illustrated in the Stack Numbering dialog box.



The following table "Stack Numbering screen fields" (page 198) describes the fields on the Stack Numbering screen.

Stack Numbering screen fields

Field	Item	Range	Description
Stack Numbering Setting	Current Unit Number	1—8	Unit number previously assigned to the policy switch. The entries in this column are displayed in order of their current physical cabling with respect to the base unit and can show non consecutive unit numbering if one or more units were previously moved or modified. The entries can include unit numbers of units that are no longer active.
	MAC Address	XX.XX.XX.XX.XX.XX	MAC address of the corresponding unit listed in the Current Unit Number field.
	New Unit Number	1—8, None	Choose a new number to assign to your selected policy switch.

Field	Item	Range	Description
			Note: If you leave the field blank, the system automatically selects the next available number.
Target Replacement Setting	Target Unit to Replace	1—8	Choose the unit number to replace. You use this field when you replace a failed unit with a new switch.

- 2 Choose the new number to assign to the switch.
- 3 Click **Submit**. A message prompts you to confirm the request.
- 4 Click **Yes**.

—End—

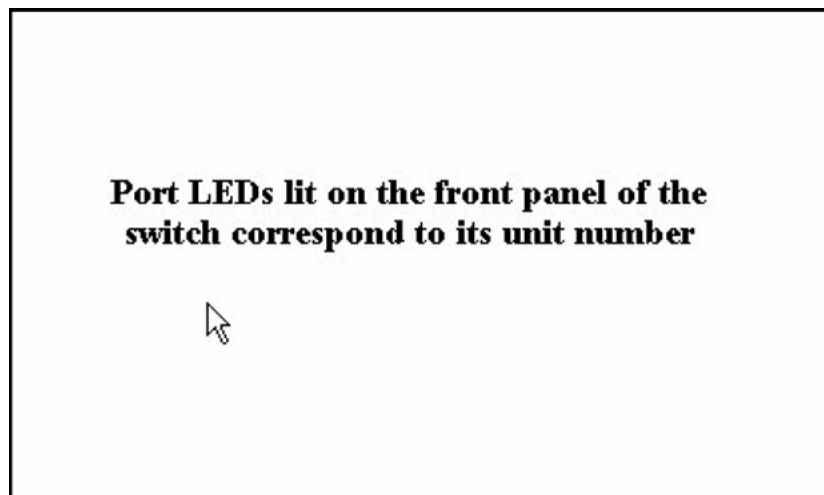
Identifying unit numbers

Identify the unit numbers of the switches participating in a stack configuration by viewing the LEDs on the front panel of each switch.

To identify unit numbers in your configuration, perform the following procedure.

Step Action

- 1 To open the **Identify Unit Numbers** screen select **Summary > Identify Unit Numbers**, as illustrated below.



- 2 To continue viewing summary information or to start the configuration process, choose another command.

—End—

Configuring BootP, IP, and gateway settings

You can configure and modify BootP mode settings for in-band stack and in-band switch IP addresses, in-band subnet mask parameters, and the IP address of your default gateway.

Note: Settings take effect immediately after you click Submit.

To configure BootP, IP, and gateway settings, perform the following procedure.

Step Action

- 1 To open the **IP** screen, select **Configuration > IP**, as illustrated in "IP page for a stand-alone Nortel Ethernet Routing Switch 4500 Series" (page 200) and "IP page for a stack" (page 201).

IP page for a stand-alone Nortel Ethernet Routing Switch 4500 Series

IP Setting	Configurable	In Use	Last BootP
BootP Request Mode	BootP When Needed		
In-Band Stack IP Address	0.0.0.0	0.0.0.0	0.0.0.0
In-Band Switch IP Address	10.127.232.30	10.127.232.30	0.0.0.0
In-Band Subnet Mask	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	10.127.232.1	10.127.232.1	0.0.0.0

IP page for a stack

Configuration > IP

IP Setting

Unit **1** 2

	Configurable	In Use	Last BootP
BootP Request Mode	BootP Disabled		
In-Band Stack IP Address	192.167.120.43	192.167.120.43	0.0.0.0
In-Band Switch IP Address	192.167.120.41	0.0.0.0	0.0.0.0
In-Band Subnet Mask	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	192.167.120.1	192.167.120.1	0.0.0.0

Submit

Note: To change the IP information for a specific unit in the stack, choose that unit and enter the desired IP information into the In-Band Switch IP address field.

The following table "IP page items" (page 201) describes the items on the IP screen.

IP page items

Section	Item	Range	Description
Boot Mode Setting	BootP Request Mode	BootP When Needed	Choose this mode to inform the switch to send a BootP request when the switch IP address stored in non volatile memory is the factory default value. If the stored IP address differs from the factory default value, the switch uses the stored network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings. Note: This is the default.
		BootP Always	Choose this mode to inform the switch, each time the switch boots, to ignore stored network parameters and send a BootP request. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables

Section	Item	Range	Description
			remote management if no BootP server is set up for the switch, but it enables the switch to boot normally.
		BootP Disabled	Choose this mode to inform the switch, each time the switch boots, to use the IP configuration parameters stored in non volatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.
Boot Mode Setting (continued)		BootP or Last Address	Choose this mode to inform the switch, at each startup, to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its non volatile memory. Note: Valid parameters obtained in using BootP always replace current information stored in the non volatile memory.
		Note: Whenever the switch broadcasts BootP requests, the BootP process times out if a reply is not received within (approximately) 7 minutes. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to one of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.	
IP Setting	In-Band Stack IP Address	XXX.XXX.XXX.XXX	Type a new stack IP address in the appropriate format.
	In-Band Switch IP Address	XXX.XXX.XXX.XXX	Type a new switch IP address in the appropriate format. Note: When you enter the IP address in the In-Band IP Address field, and the In-Band Subnet Mask field value is not present, the software provides an in-use default value for the In-Band Subnet Mask field that is based on the class of the IP address entered in the In-Band IP Address field.

Section	Item	Range	Description
	In-Band Subnet Mast	XXX.XXX.XXX.XXX	Type a new subnet mask in the appropriate format.
Gateway Setting	Default Gateway	XXX.XXX.XXX.XXX	Type an IP address for the default gateway in the appropriate format.

Note: If you assign an IP address to the device and the BootP process times out, the BootP mode remains the default mode of BootP when needed.

However, if you do not assign an IP address to the device and the BootP process times out, the BootP mode automatically changes to BootP disabled. But this change to BootP disabled is not stored, and the BootP reverts to the default value of BootP when needed after you reboot the device.

- 2 In the fields provided, enter the IP configuration information.
- 3 Click **Submit**.

—End—

Modifying system settings

The you can configure or change the system name, system location, and network manager contact information.

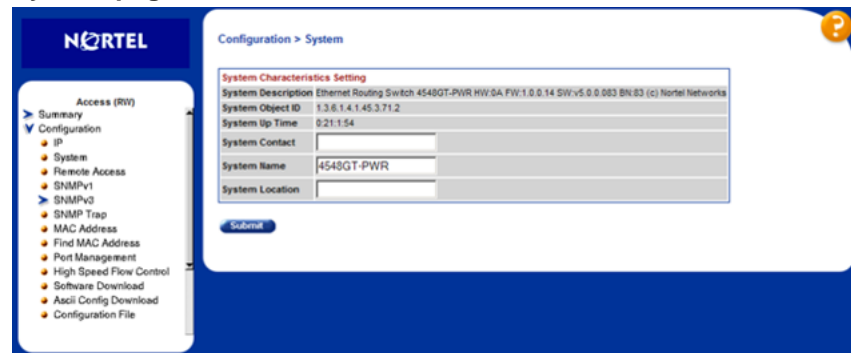
Note: The configurable parameters on the System screen are displayed in a read only-format on the Web-based Management Interface System Information home page.

To configure system settings, perform the following procedure:

Step Action

- 1 To open the **System** screen, select **Configuration > System**, as illustrated in "[System page](#)" (page 204).

System page



The following table "System page items" (page 204) describes the items on the **System** screen.

System page items

Item	Description
System Description	The factory set description of the hardware and software versions.
System Object ID	The character string that the vendor created to uniquely identify this device.
System Up Time	The elapsed time since the last network management portion of the system was last reinitialized. Note: This field is updated only when the screen is redisplayed.
System Contact	Type a character string to create the contact information for the network manager or the selected person to contact regarding switch operation; for example, networkmanager@company.com Note: To operate correctly with the Web Interface, the system contact must be an e-mail address.
System Name	Type a character string to create a name to identify the switch; for example, Finance Group.
System Location	Type a character string to create a name for the switch location; for example, First Floor.

- 2 In the fields provided, enter the desired information.
- 3 Click **Submit**.

—End—

Managing remote access by IP address

Configuration of the remote access is allowed through the Web interface. Up to 50 IP addresses can be specified to allow Web access, SNMP access, or Telnet access to the switch.

To configure remote access, perform the following procedure.

Step	Action
1	To open the Remote Access screen, select Configuration > Remote Access , as illustrated in " Remote Access page " (page 206).

Remote Access page

Configuration > Remote Access

Remote Access Settings

	Access	Use List
Telnet	Allowed	Yes
SNMP	Allowed	Yes
Web Page	Allowed	Yes

Submit

Allowed Source IP and Subnet Mask

	Allowed Source IP	Allowed Source Mask
1	0.0.0.0	0.0.0.0
2	255.255.255.255	255.255.255.255
3	255.255.255.255	255.255.255.255
4	255.255.255.255	255.255.255.255
5	255.255.255.255	255.255.255.255
6	255.255.255.255	255.255.255.255
7	255.255.255.255	255.255.255.255
8	255.255.255.255	255.255.255.255
9	255.255.255.255	255.255.255.255
10	255.255.255.255	255.255.255.255
11	255.255.255.255	255.255.255.255
12	255.255.255.255	255.255.255.255
13	255.255.255.255	255.255.255.255
14	255.255.255.255	255.255.255.255
15	255.255.255.255	255.255.255.255
16	255.255.255.255	255.255.255.255
17	255.255.255.255	255.255.255.255
18	255.255.255.255	255.255.255.255
19	255.255.255.255	255.255.255.255
20	255.255.255.255	255.255.255.255
21	255.255.255.255	255.255.255.255
22	255.255.255.255	255.255.255.255
23	255.255.255.255	255.255.255.255
24	255.255.255.255	255.255.255.255
25	255.255.255.255	255.255.255.255
26	255.255.255.255	255.255.255.255
27	255.255.255.255	255.255.255.255
28	255.255.255.255	255.255.255.255
29	255.255.255.255	255.255.255.255
30	255.255.255.255	255.255.255.255
31	255.255.255.255	255.255.255.255
32	255.255.255.255	255.255.255.255
33	255.255.255.255	255.255.255.255
34	255.255.255.255	255.255.255.255
35	255.255.255.255	255.255.255.255
36	255.255.255.255	255.255.255.255
37	255.255.255.255	255.255.255.255
38	255.255.255.255	255.255.255.255
39	255.255.255.255	255.255.255.255
40	255.255.255.255	255.255.255.255
41	255.255.255.255	255.255.255.255
42	255.255.255.255	255.255.255.255
43	255.255.255.255	255.255.255.255
44	255.255.255.255	255.255.255.255
45	255.255.255.255	255.255.255.255
46	255.255.255.255	255.255.255.255
47	255.255.255.255	255.255.255.255
48	255.255.255.255	255.255.255.255
49	255.255.255.255	255.255.255.255
50	255.255.255.255	255.255.255.255

Submit

The following table "Remote Access page fields" (page 207) describes the fields on the **Remote Access** page.

Remote Access page fields

Section	Item	Range	Description
Remote Access Settings	Telnet/Access	Allowed Disallowed	Enable Telnet access.
	Telnet/Use List	Yes No	Restrict Telnet access to the specified 50 source IP addresses.
	SNMP/Access	Allowed Disallowed	Enable SNMP access.
	SNMP/Use List	Yes No	Restrict SNMP access to the specified 50 source IP addresses.
	Web Page/Access		Display allowed Web Interface access.
	Web/Use List	Yes No	Restrict Web Interface access to the specified 50 source IP addresses.
Allowed Source IP and Subnet Mask	Allowed Source IP	XXX.XXX.XXX.XXX	Enter the source IP address to allow switch access.
	Allowed Source Mask	XXX.XXX.XXX.XXX	Enter the source IP mask to allow switch access.

- 2 Complete fields as described in the table.
- 3 Click **Submit**.

—End—

General Switch Administration using the JDM

This section contains the following topics:

- "Viewing unit information" (page 208)
- "Viewing switch IP information" (page 209)
- "Viewing SFP GBIC ports" (page 215)
- "Editing the chassis configuration" (page 215)

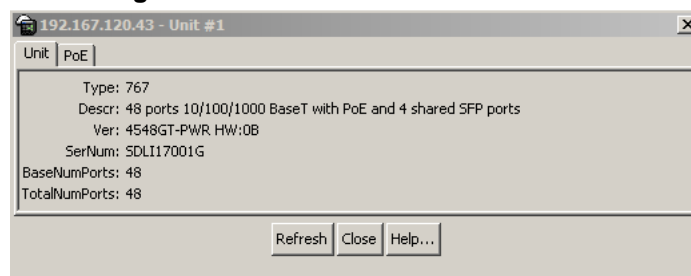
- "Editing and viewing switch ports" (page 229)
- "Editing and viewing switch PoE configurations" (page 237)
- "Editing Bridging Information" (page 240)
- "Configuring SNTP" (page 245)
- "Viewing topology information using Device Manager" (page 247)

Viewing unit information

To view Unit information, perform the following procedure.

Step	Action
1	Select the unit by clicking in the Device View area of the switch.
2	To open the Unit screen, select Edit > Unit , as illustrated in "Unit dialog box" (page 208).

Unit dialog box



The following table "Unit tab items" (page 208) describes the Unit screen fields.

Unit tab items

Field	Description
Type	The type number
Descr	The type of switch
Ver	The version number of the switch
SerNum	The number of the switch
BaseNumPorts	The base number of ports
TotalNumPorts	The total number of ports

—End—

Viewing PoE information

To view PoE information, select the PoE tab in the [Unit dialog box](#) and read the information associated with the fields. See ["PoE tab for a single unit" \(page 239\)](#)

Viewing switch IP information

You can view the switch IP information using the IP dialog box.

To open the Edit IP dialog box from the Device Manager main menu, perform the following procedure.

Step	Action
1	Select Edit . The Edit selection list appears.
2	Select IP from the Edit selection list. The IP dialog box opens with the Globals tab displayed.

—End—

The following sections provide a description of the tabs in the IP dialog box and details about each item on the tab. The IP tabs are read-only.

- ["IP Globals tab" \(page 210\)](#)
- [IP Addresses tab](#)
- [IP ARP tab](#)
- [IP TCP tab](#)
- [IP TCP Connections tab](#)
- [IP UDP Listeners tab](#)

IP Globals tab

To open the Globals tab from the Device Manager main menu, perform the following procedure.

Step	Action
1	Select Edit . The Edit selection list appears.
2	Select IP . The IP Globals tab appears.
3	Click Refresh to refresh the tab information display.

—End—

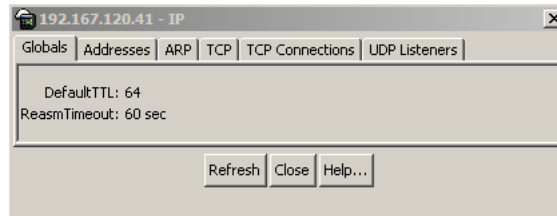
IP Globals tab

Table 1
IP Globals tab fields

Field and MIB association	Description
DefaultTTL	Default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch whenever a TTL value is not supplied by the transport layer protocol. Default value is 64.
ReasmTimeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly by the switch. Default value is 60.

IP Addresses tab

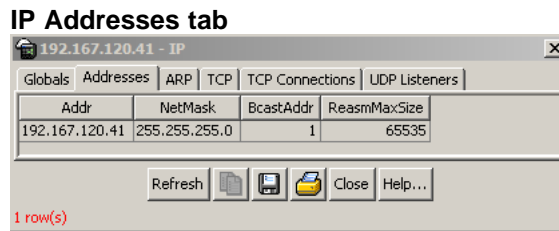
The Addresses tab contains the IP address information for the device.

To open the Addresses tab from the Device Manager main menu, perform the following procedure.

Step	Action
------	--------

- 1 Select **Edit**. The Edit selection list appears.
- 2 Select **IP**. The IP Globals tab appears.
- 3 Select the **Addresses** tab. The Addresses tab opens.
- 4 Click **Refresh** to refresh the tab information display.

—End—



IP Addresses tab fields

Field	Description
Addr	The device IP address.
NetMask	The subnet mask address.
BcastAddr	The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address for this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.
ReasmMaxSize	The size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface.

IP ARP tab

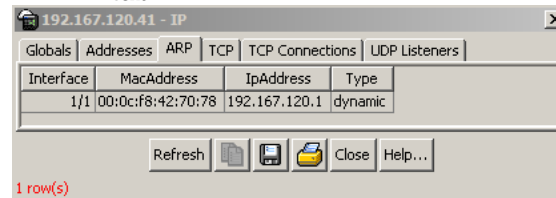
The Address Resolution Protocol (ARP) tab contains the MAC addresses and the associated IP addresses for the switch.

To open the ARP tab from the Device Manager main menu, perform the following procedure.

Step Action

- 1 Select **Edit**. The Edit selection list appears.
- 2 Select **IP**. The IP Globals tab appears.
- 3 Select the **ARP** tab. The ARP tab opens.
- 4 Click **Refresh** to refresh the tab information display.

—End—

IP ARP tab**IP ARP tab fields**

Field	Description
Interface	The unit and port number.
MacAddress	The unique hardware address of the device.
IPAddress	The Internet Protocol (IP) address of the device used to represent a point of attachment in a TCP/IP internetwork.
Type	The type of mapping.

IP TCP tab

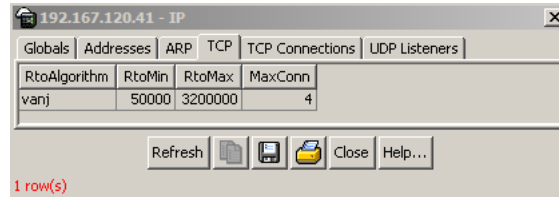
The Transport Control Protocol (TCP) tab contains the TCP information for the switch.

To open the TCP tab from the Device Manager main menu, perform the following procedure.

Step Action

- 1 Select **Edit**. The Edit selection list appears.
- 2 Select **IP**. The IP Globals tab appears.
- 3 Select the **TCP** tab. The TCP tab opens.
- 4 Click **Refresh** to refresh the tab information display.

—End—

IP TCP tab

Field	Description
RtoAlgorithm	The algorithm that determines the timeout value used for retransmitting unacknowledged octets.
RtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
RtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
MaxConn	The limit on the total number of TCP connections that the entity can support. In entities where the maximum number of connections is dynamic, this object contains the value -1.

IP TCP Connections tab

The TCP Connections tab contains the xxxxxx for the switch.

To open the TCP Connections tab from the Device Manager main menu, perform the following procedure.

Step Action

- 1 Select **Edit**. The Edit selection list appears.
- 2 Select **IP**. The IP Globals tab appears.
- 3 Select the **TCP Connections** tab. The TCP Connections tab opens.
- 4 Click **Refresh** to refresh the tab information display.

—End—

IP TCP Connections tab

LocalAddress	LocalPort	RemAddress	RemPort	State
0.0.0.0	23	0.0.0.0	0	listen
0.0.0.0	80	0.0.0.0	0	listen

IP TCP Connections tab fields

Field	Description
LocalAddress	The local IP address for this TCP connection: the value is 0.0.0.0 for a connection in the listen state. A connection in the listen state is a connection willing to accept connections for any IP interface associated with the node .
LocalPort	The local port number for this TCP connection.
RemAddress	The remote IP address for this TCP connection.
RemPort	The remote port number for this TCP connection.
State	The state of this TCP connection.

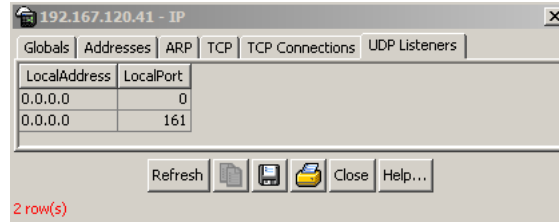
IP UDP Listeners tab

The User Datagram Protocol (UDP) Listeners tab contains information on the UDP listeners currently maintained by the switch.

To open the UDP Listeners tab from the Device Manager main menu, perform the following procedure.

Step	Action
1	Select Edit . The Edit selection list appears.
2	Select IP . The IP Globals tab appears.
3	Select the UDP Listeners tab. The UDP Listeners tab opens.
4	Click Refresh to refresh the tab information display.

—End—

IP UDP Listeners tab**IP UDP Listeners tab fields**

Field	Description
LocalAddress	The local IP address for this UDP listener. The value for a UDP listener that accepts datagrams for any IP interface associated with the node is 0.0.0.0.
LocalPort	The local port number for this UDP listener.

Viewing SFP GBIC ports

You can view the details of an SFP GBIC port only if the port is active.

To view the SFP GBIC ports, perform the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select the SFP GBIC ports from the Device View . |
| 2 | To open the Port screen, select Edit > Port . |

—End—

Editing the chassis configuration

You can edit the chassis configuration from the Edit Chassis screen "[Edit Chassis screen -- System tab](#)" (page 217).

To open the Edit Chassis screen, perform the following procedure.

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select the chassis in the Device View . |
| 2 | To open the Edit Chassis screen, select Edit > Chassis . |

—End—

The following sections describe the tabs in the **Edit Chassis** screen:

- "[System tab](#)" (page 216)

- "Base Unit Info tab" (page 219)
- "Stack Info tab" (page 221)
- "Agent tab" (page 224)
- "SNMP tab" (page 226)
- " Power Supply tab" (page 226)
- " Fan tab" (page 227)

For information about the **Banner** tab or the **Custom Banner** tabs, see "Banner tab" (page 111) or "Custom Banner tab" (page 113).

For information about the **SNMP** and **Trap Receivers** tabs, see *Nortel Ethernet Routing Switch 4500 Series Security — Configuration* (NN47205-505).

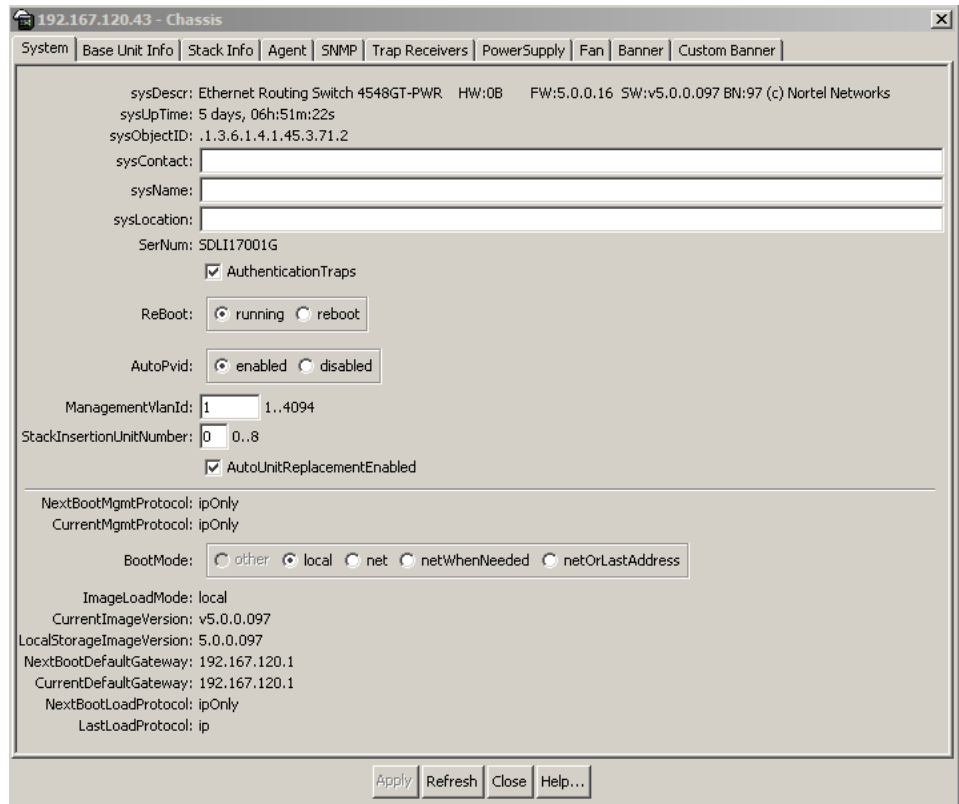
System tab

Use the **System** tab to specify, among other things, tracking information for a device and device descriptions.

Step	Action
-------------	---------------

- | | |
|----------|--|
| 1 | Open the System tab using the procedure at the beginning of this section. The following dialog box appears. |
|----------|--|

Edit Chassis dialog box -- System tab




Note: The chassis tracks the elapsed time and calculates the time and date using the system clock of the Device Manager machine as a reference.

The following table "System tab items" (page 217) describes the System tab items.

System tab items

Field	Description
sysDescr	A description of the device.
sysUpTime	The time since the system was last booted.
sysObjectID	Displays the system object identification number.
sysContact	Type the contact information (in this case, an e-mail address) for the system administrator.
sysName	Type the name of this device.
sysLocation	Type the physical location of this device.

Field	Description
SerNum	Displays the individual switch serial number.
AuthenticationTraps	<p>Click enable or disable. When you select enabled, SNMP traps are sent to trap receivers for all SNMP access authentication. When you select disabled, no traps are received.</p> <p>To view traps, click the Trap toolbar button.</p> 
Reboot	<p>Action object to reboot the agent.</p> <p>Reset - initiates a hardware reset.</p> <p>The agent attempts to return a response before the action occurs. If any of the combined download actions are requested, neither action occurs until the expiration of s5AgInfoScheduleBootTime, if set.</p>
AutoPvid	Click enabled or disabled. When you select enabled, Port VLAN ID (PVID) is automatically assigned.
ManagementVlanId	The current management VLAN ID.
StackInsertionUnitNumber	The unit number to be assigned to the next unit that joins the stack. You cannot set the value to the unit number of an existing stack member. When a new unit joins the stack, and the value of this object is used as its unit number, the value reverts to 0. If the value of this object is 0, it is not used to determine the unit number of new units.
AutoUnitReplacement Enabled	Determine whether auto-unit-replacement is enabled or disabled.
NextBootMgmtProtocol	The transport protocols to use after the next boot of the agent.
CurrentMgmtProtocol	The current transport protocols that the agent supports.

Field	Description
BootMode	The source from which to load the initial protocol configuration information to boot the switch the next time. The options available are local, net, netWhenNeeded, netOrLastAddress, or none.
ImageLoadMode	The source from which to load the agent image at the next boot.
CurrentImageVersion	The version number of the agent image that is currently used on the switch.
LocalStorageImage Version	The version number of the agent image that is stored in flash memory on the switch.
NextBootDefaultGateway	The IP address of the default gateway for the agent to use after the next time you boot the switch.
CurrentDefaultGateway	The IP address of the default gateway that is currently in use.
NextBootLoadProtocol	The transport protocol that the agent uses to load the configuration information and the image at the next boot.
LastLoadProtocol	The transport protocol last used to load the image and configuration information about the switch.

See also:

- ["Base Unit Info tab" \(page 219\)](#)
- ["Stack Info tab" \(page 221\)](#)
- ["Agent tab" \(page 224\)](#)
- [" Power Supply tab" \(page 226\)](#)
- [" Fan tab" \(page 227\)](#)
- ["Banner tab" \(page 111\)](#)
- ["Custom Banner tab" \(page 113\)](#)

—End—

Base Unit Info tab

The **Base Unit Info** tab provides read-only information about the operating status of the hardware and whether the default factory settings are used.

- | Step | Action |
|------|---|
| 1 | Open the Edit Chassis screen in the manner detailed at the beginning of this section. |
| 2 | Select the Base Unit Info tab, as illustrated in "Edit Chassis screen -- Base Unit Info tab" (page 220). |

Edit Chassis screen -- Base Unit Info tab

The following table "Base Unit Info tab items" (page 220) describes the **Base Unit Info** tab items.

Base Unit Info tab items

Field	Description
Type	The switch type.
Descr	A description of the switch hardware, including number of ports and transmission speed.
Ver	The switch hardware version number.
SerNum	The switch serial number.
LstChng	The value of sysUpTime at the time the interface entered its current operational state. If you entered the current state prior to the last reinitialization of the local network management subsystem, the value is zero.
AdminState	Administrative state of the switch. Select either enable or reset . Note: In a stack configuration, Reset resets only the base unit.

Field	Description
OperState	The operational state of the switch.
Location	Type the physical location of the switch.
RelPos	The relative position of the switch.
BaseNumPorts	The number of base ports of the switch.
TotalNumPorts	The number of ports of the switch.
IpAddress	The base unit IP address.

See also

- ["System tab" \(page 216\)](#)
- ["Stack Info tab" \(page 221\)](#)
- ["Agent tab" \(page 224\)](#)
- [" Power Supply tab" \(page 226\)](#)
- [" Fan tab" \(page 227\)](#)
- ["Banner tab" \(page 111\)](#)
- ["Custom Banner tab" \(page 113\)](#)

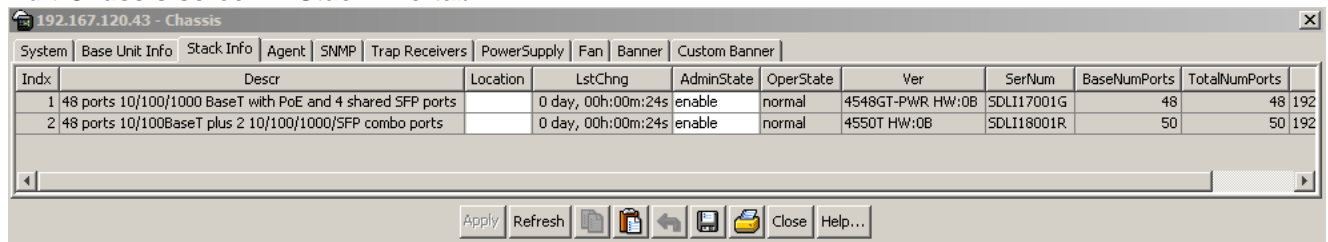
—End—

Stack Info tab

The **Stack Info** tab provides read-only information about the operating status of the *stacked* switches and whether the default factory settings are used.

Step Action

- 1 Open the Edit **Chassis screen** in the manner detailed at the beginning of this section.
- 2 Click the **Stack Info** tab, as illustrated in ["Edit Chassis screen -- Stack Info tab" \(page 221\)](#).

Edit Chassis screen -- Stack Info tab


Indx	Descr	Location	LstChng	AdminState	OperState	Ver	SerNum	BaseNumPorts	TotalNumPorts
1	48 ports 10/100/1000 BaseT with PoE and 4 shared SFP ports		0 day, 00h:00m:24s	enable	normal	4548GT-PWR HW:0B	SDL117001G	48	48 192
2	48 ports 10/100BaseT plus 2 10/100/1000/SFP combo ports		0 day, 00h:00m:24s	enable	normal	4550T HW:0B	SDL118001R	50	50 192

The following table "Stack Info tab fields" (page 222) describes the **Stack Info** tab fields.

Stack Info tab fields

Field	Description
Indx	A line number for stack info
Descr	A description of the component or subcomponent. If not available, the value is a zero length string.
Location	<p>The geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: 4th flr wiring closet in blg A.</p> <p>Notes: 1. This field applies only to components that are in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in a Board or Unit group, the value is a zero-length string.</p> <p>2. If this field is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value defaults to the value of the object s5ChasComSerNum.</p>
LstChng	The value of sysUpTime when it was detected that the component or sub-component was added to the chassis. If this action has not occurred since the cold or warm start of the agent, then the value is zero.

Field	Description
AdminState	<p>The state of the component or subcomponent.</p> <p>The values that are read-only are</p> <ul style="list-style-type: none"> • other: currently in another state • notAvail: actual value is not available <p>The possible values that can be read and written are</p> <ul style="list-style-type: none"> • disable: disables operation • enable: enables operation • reset: resets component • test: starts self test of the component, with a result of normal, warning, nonFatalErr, or fatalErr in object s5ChasComOperState The component type determines the allowable (and meaningful) values.
OperState	<p>The current operational state of the component. The possible values are</p> <ul style="list-style-type: none"> • other: another state • notAvail: state not available • removed: component removed • disabled: operation disabled • normal: normal operation • resetInProgress: reset in progress • testing: performing a self test • warning: operating at warning level • nonFatalErr: operating at error level • fatalErr: error stopped operation <p>The component type determines the allowable (and meaningful) values.</p>

Field	Description
Ver	The version number of the component or subcomponent. If not available, the value is a zero-length string.
SerNum	The serial number of the component or subcomponent. If not available, the value is a zero-length string.
BaseNumPorts	The number of base ports of the component or subcomponent.
TotalNumPorts	The number of ports of the component or subcomponent.
IpAddress	The IP address of the component or subcomponent.

See also

- ["System tab" \(page 216\)](#)
- ["Base Unit Info tab" \(page 219\)](#)
- ["Agent tab" \(page 224\)](#)
- [" Power Supply tab" \(page 226\)](#)
- [" Fan tab" \(page 227\)](#)
- ["Banner tab" \(page 111\)](#)
- ["Custom Banner tab" \(page 113\)](#)

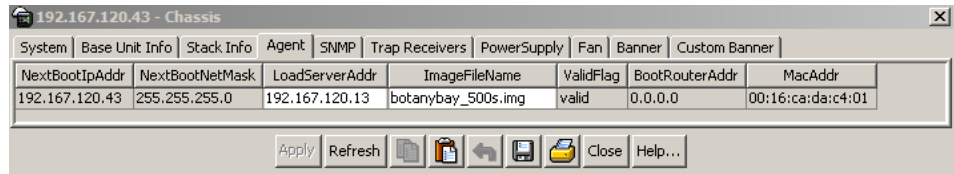
—End—

Agent tab

The **Agent** tab provides read-only information about the addresses that the agent software uses to identify the switch.

Step Action

- 1 Open the **Edit Chassis** screen in the manner detailed at the beginning of this section.
- 2 Select the **Agent** tab, as illustrated in ["Edit Chassis dialog box -- Agent tab" \(page 225\)](#).

Edit Chassis dialog box -- Agent tab

The following table "Agent tab fields" (page 225) describes the Agent tab fields.

Agent tab fields

Field	Description
NextBootpAddr	The IP address of the BootP server to use the next time the switch is booted.
NextBootNetMask	The subnet mask to use the next time the switch is booted.
LoadServerAddr	The IP address of the server from which the device loads the image file.
ImageFileName	The name of the image file.
ValidFlag	Indicates whether the configuration or image files, or both, were downloaded from this interface and if the file names did not change.
BootRouterAddr	The IP address of the boot router for the configuration file or the image file, or both.
MacAddr	The switch MAC address.

See also

- ["System tab" \(page 216\)](#)
- ["Base Unit Info tab" \(page 219\)](#)
- ["Stack Info tab" \(page 221\)](#)
- ["Agent tab" \(page 224\)](#)
- [" Power Supply tab" \(page 226\)](#)
- [" Fan tab" \(page 227\)](#)
- ["Banner tab" \(page 111\)](#)
- ["Custom Banner tab" \(page 113\)](#)

—End—

SNMP tab

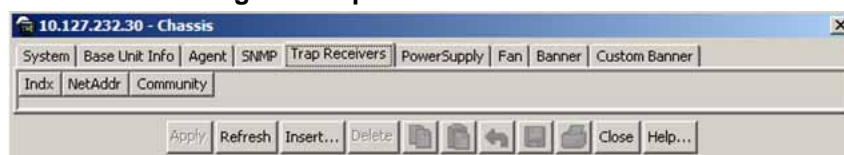
The SNMP tab provides read-only information about the last unauthenticated IP address, the last unauthenticated community string, and the trap receiver entries. For detailed information about SNMP, see *Nortel Ethernet Routing Switch 4500 Series Security Configuration*, NN47205-505.

To open the SNMP tab from the Edit Chassis dialog box, click the SNMP tab.

Trap Receivers tab

The Trap Receivers tab provides read-only information about index, net address, and community trap receivers. For detailed information about Trap Receivers, see *Nortel Ethernet Routing Switch 4500 Series Security Configuration*, NN47205-505.

To open the Trap Receivers tab from the Edit Chassis dialog box, click the Trap Receivers tab.

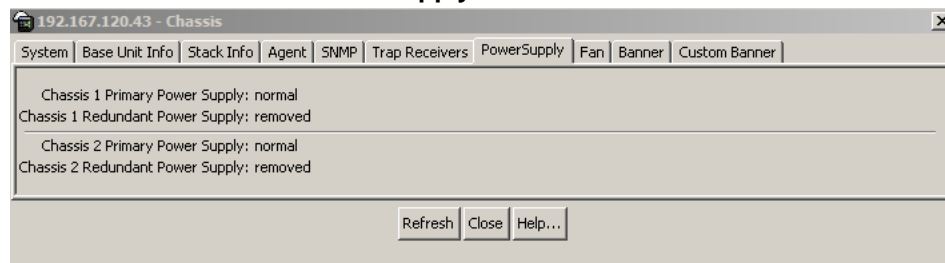
Edit chassis dialog box Trap Receivers tab**Power Supply tab**

The Power Supply tab provides read-only information about the operating status of the switch power supplies.

The power supply parameters for the PoE switches, 4550T-PWR and 4548-GT-PWR, differ slightly because they support Power over Ethernet (PoE).

Step	Action
------	--------

- | | |
|---|--|
| 1 | Open the Edit Chassis screen in the manner detailed at the beginning of this section. |
| 2 | Select the PowerSupply tab, as illustrated in " Edit Chassis screen -- Power Supply tab " (page 226). |

Edit Chassis screen -- Power Supply tab

—End—

The following table "Power Supply status values" (page 227) describes the **Power Supply** status values.

Power Supply status values

Field	Description
OperStat	<p>The operational state of the power supply. Possible values include</p> <ul style="list-style-type: none"> • other: another state. • notAvail: State not available. • removed: Component was removed. • disabled: Operation disabled. • normal: State is in normal operation. • resetInProg: A reset is in progress. • testing: System is performing a self test. • warning: System is operating at a warning level. • nonFatalErr: System is operating at error level. • fatalErr: A fatal error stopped operation. • notConfig: You need to configure a module. The component type determines the allowable values.

See also:

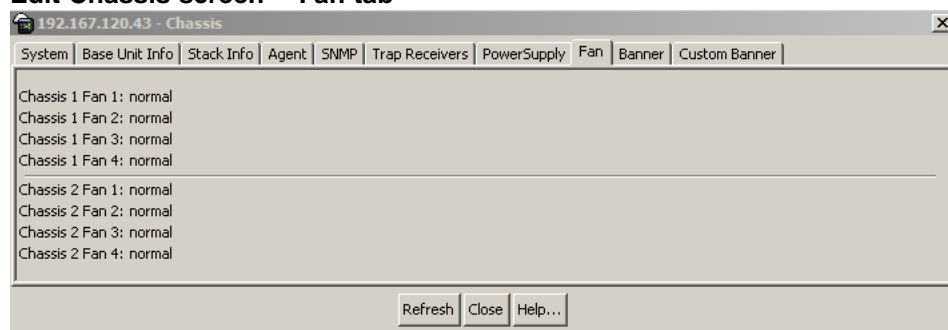
- "System tab" (page 216)
- "Base Unit Info tab" (page 219)
- "Stack Info tab" (page 221)
- "Agent tab" (page 224)
- " Fan tab" (page 227)
- "Banner tab" (page 111)
- "Custom Banner tab" (page 113)

Fan tab

The Fan tab provides read-only information about the operating status of the switch fans.

Step Action

- 1 Open the **Edit Chassis** screen in the manner detailed at the beginning of this section.
- 2 Select the **Fan** tab, as illustrated in "[Edit Chassis screen -- Fan tab](#)" (page 228).

Edit Chassis screen -- Fan tab

—End—

The following table "[Fan operating status](#)" (page 228) describes the Fan operating status.

Fan operating status

Field	Description
OperStat	<p>The operational state of the fan. Values include:</p> <ul style="list-style-type: none"> • other: another state. • notAvail: This state is not available. • removed: Fan was removed. • disabled: Fan is disabled. • normal: Fan is operating in normal operation. • resetInProg: A reset of the fan is in progress. • testing: Fan is performing a self test. • warning: Fan is operating at a warning level. • nonFatalErr: Fan is operating at error level.

Field	Description
	<ul style="list-style-type: none">fatalErr: An error stopped the fan operationnotConfig: You need to reconfigure the fan. The component type determines the allowable values.

See also:

- ["System tab" \(page 216\)](#)
- ["Base Unit Info tab" \(page 219\)](#)
- ["Stack Info tab" \(page 221\)](#)
- ["Agent tab" \(page 224\)](#)
- [" Power Supply tab" \(page 226\)](#)
- ["Banner tab" \(page 111\)](#)
- ["Custom Banner tab" \(page 113\)](#)

Editing and viewing switch ports

Perform port configuration in the Java Device Manager (JDM) on the **Port** screen. Open the **Port** screen by selecting a port in the **Device View** and selecting **Edit > Port** . You can edit multiple ports by selecting ports from the **Device View** while pressing the Control (CTRL) key. Examples of the **Port** screen are illustrated in ["Port screen with one port selected" \(page 230\)](#) and ["Port screen with multiple ports selected" \(page 230\)](#).

Port screen with one port selected

Interface | VLAN | STG | EAPOL | EAPOL Advance | PoE | LACP | Rate Limit

Index: 1
 Name:
 Descr: Nortel Ethernet Routing Switch 4548GT PWR Module - Unit 1 Port 1
 Type: ethernetCsmacd
 Mtu: 9216
 PhysAddress: 00:16:ca:da:c4:01
 AdminStatus: up down
 OperStatus: up
 LastChange: 5 days, 07h:52m:52s
 LinkTrap: enabled disabled

AutoNegotiate

AdminDuplex: half full
 OperDuplex: full
 AdminSpeed: mbps10 mbps100 mbps1000 mbps10000
 OperSpeed: 100 mbps
 AutoNegotiationCapability: 10Half,10Full,100Half,100Full,1000Full,PauseFrame

AutoNegotiationAdvertisements:
 10Half 10Full 100Half
 100Full 1000Half 1000Full
 PauseFrame AsymmPauseFrame

MltId: 0
 IsPortShared: portNotShared
 PortActiveComponent: fixedPort

Apply Refresh Close Help...

As demonstrated in "Port screen with one port selected" (page 230) and "Port screen with multiple ports selected" (page 230), the presentation of the Port screen differs when you select one port or multiple ports. This difference is mainly in presentation although some options are unavailable when you select multiple ports. These exceptions are noted in their descriptions.

Port screen with multiple ports selected

Index	Port	Name	Descr	Type	Mtu	PhysAddress	AdminStatus	OperStatus	LastChange	LinkTrap	AutoNegotiate	AdminDuplex	OperDuplex	AdminSpeed	OperSpeed	AutoNegotiate
1(1/1)	1/1		Nort...	eth...	9216	00:16:ca:d...	up	up	5 days, 07...	enabled	true	full	full	mbps100	100	10Half, 10Full
2(1/2)	1/2		Nort...	eth...	9216	00:16:ca:d...	up	down	5 days, 07...	enabled	true	full	full	mbps1000	1000	10Half, 10Full
3(1/3)	1/3		Nort...	eth...	9216	00:16:ca:d...	up	down	5 days, 07...	enabled	true	full	full	mbps1000	1000	10Half, 10Full
5(1/5)	1/5		Nort...	eth...	9216	00:16:ca:d...	up	down	5 days, 07...	enabled	true	full	full	mbps1000	1000	10Half, 10Full
6(1/6)	1/6		Nort...	eth...	9216	00:16:ca:d...	up	down	5 days, 07...	enabled	true	full	full	mbps1000	1000	10Half, 10Full
7(1/7)	1/7		Nort...	eth...	9216	00:16:ca:d...	up	down	5 days, 07...	enabled	true	full	full	mbps1000	1000	10Half, 10Full
8(1/8)	1/8		Nort...	eth...	9216	00:16:ca:d...	up	down	5 days, 07...	enabled	true	full	full	mbps1000	1000	10Half, 10Full

Apply Refresh Close Help...

The following sections describe some of the tabs on the Port screen:

- " Interface tab" (page 231)

- "PoE tab" (page 235)
- "Configuring Rate Limiting" (page 237)

For information about the **VLAN**, **LACP**, and **STP BPDU-Filtering** tabs, see *Nortel Ethernet Routing Switch 4500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking* (NN47205-501).

Interface tab

The **Interface** tab shows the basic configuration and status of a port.

To view the **Interface** tab, perform the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select the port to edit from the Device View . Select Edit > Port . |
|---|--|

The **Port** screen opens with the **Interface** tab displayed, as illustrated in "Port screen -- Interface tab" (page 231).

Port screen -- Interface tab

To continue, go to:

- " Interface tab" (page 231)

Interface tab items

The following table "Interface tab fields" (page 232) describes the Interface tab fields.

Interface tab fields

Field	Description
Index	A unique value assigned to each interface. The value ranges from 1 to 64 stand-alone. On a stack, the index value of the first port of the second unit is 65. The maximum value is 512.
Name	Enter an optional name for the port.
Descr	The type of switch and number of ports.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	The MAC address assigned to a particular interface.
AdminStatus	<p>The current administrative state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> • up • down <p>When you initialize a managed system, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system.</p>
OperStatus	<p>The current operational state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> • up • down • testing <p>If AdminStatus is up, then OperStatus is also up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus is also down. The interface remains</p>

Field	Description
	in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
LinkTrap	Indicates whether linkUp/linkDown traps are generated for this interface. By default, this object has the value enabled for interfaces that do not operate on top of any other interface (as defined in the ifStackTable).
AutoNegotiate	Indicates whether this port is enabled for autonegotiation.
AdminDuplex	Set the administrative duplex mode of the port (half or full).
OperDuplex	Show the current administrative duplex mode of the port (half or full).
AdminSpeed	Set the port speed.
OperSpeed	The current operating speed of the port.
AutoNegotiation Capability	<p>The port speed and duplex capabilities that hardware can actually support on a port, and which can be advertised by the port using auto negotiation. Bit 7 tells if a port supports pause frame capabilities (for full-duplex links) as a part of the advertisement.</p> <p>bit 0: 10 half duplex advertisements</p> <p>bit 1: 10 full duplex advertisements</p> <p>bit 2: 100 half duplex advertisements</p> <p>bit 3: 100 full duplex advertisements</p> <p>bit 4: 1000 half duplex advertisements</p> <p>bit 5: 1000 full duplex advertisements</p> <p>bit 6: PAUSE frame support advertisements</p>

Field	Description
	<p>bit 7: Asymmetric PAUSE frame support advertisements</p> <p>If the port hardware does not support autonegotiation, then all bits are zero.</p>
AutoNegotiation Advertisements	<p>The port speed and duplex abilities to be advertised during link negotiation.</p> <p>bit 0: 10 half duplex advertised</p> <p>bit 1: 10 full duplex advertised</p> <p>bit 2: 100 half duplex advertised</p> <p>bit 3: 100 full duplex advertised</p> <p>bit 4: 1000 half duplex advertised</p> <p>bit 5: 1000 full duplex advertised</p> <p>bit 6: PAUSE frame support advertised</p> <p>bit 7: Asymmetric PAUSE frame support advertised</p> <p>The abilities specified in this object are used only when auto-negotiation is enabled on the port. If all bits in this object are disabled, and auto negotiation is enabled on the port, then the physical link process on the port is disabled.</p>
MtId	The multilink trunk to which the port is assigned (if any).
IsPortShared	Indicates whether the selected port is a shared port or not.
PortActive Component	Displays the active component of shared ports.

2 After you make changes, click **Apply**.

See also

- "PoE tab" (page 235)
- "Configuring Rate Limiting" (page 237)
- TDR tab

—End—

PoE tab

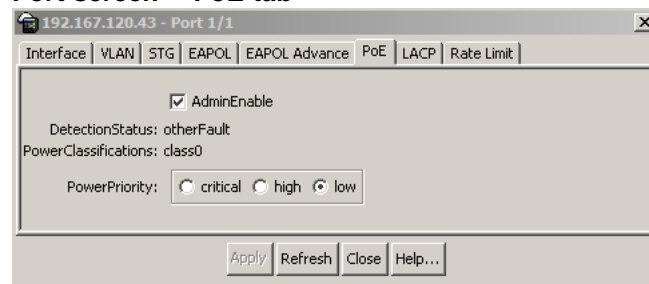
The **PoE** tab enables the configuration of the PoE power settings for a port in the Ethernet Routing Switch 4500. This tab is displayed only for PoE-capable units.

To view the **PoE** tab, perform the following procedure.

Step	Action
------	--------

- 1 Select the port to edit from the **Device View**. Select **Edit > Port**.

The **Port** screen appears. Select the **PoE** tab, as illustrated in "Port screen -- PoE tab" (page 235).

Port screen -- PoE tab

"PoE tab fields" (page 235) describes the **PoE** tab fields.

PoE tab fields

Field	Description
AdminEnable	Enable or disable PoE on this port.

Field	Description
Detection Status	<p>The operational status of the power-device detecting mode on the specified 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 port test: detecting device in test mode otherFault <p>Note: Nortel recommends against using the test operational status.</p>
PowerClassifications	The operational status of the port PD classification.
PowerPriority	<p>Set the power priority for the specified port to:</p> <ul style="list-style-type: none"> critical high low

Note: Use the **PoE** tab to set PoE parameters for each port. The **Power Supply** tab on the **Chassis** screen displays the status of the internal Nortel Ethernet Routing Switch power supply.

—End—

See also

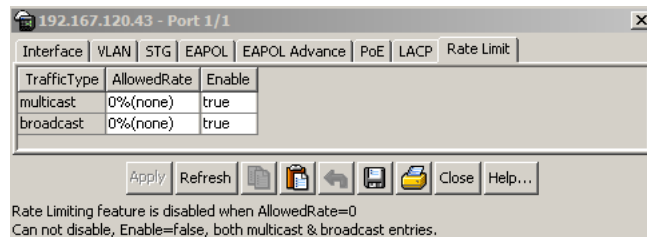
- "Interface tab" (page 231)
- "Configuring Rate Limiting" (page 237)

Configuring Rate Limiting

You can use the **Rate Limit** tab to configure the Rate Limiting for a single port.

- | Step | Action |
|------|--|
| 1 | Select the port to test from the Device View . |
| 2 | Select Edit > Port .
The Port screen appears. |
| 3 | Select the Rate Limit tab.
The Rate Limit tab appears. |

Rate Limit tab



The following table describes the Rate Limit tab items.

Field	Description
TrafficType	Specify the two types of traffic that can be set with rate limiting: broadcast and multicast.
AllowedRate	Set the rate limiting percentage. The available range is from 0 percent (none) to 10 percent.
Enable	Enable and disable rate limiting on the port for the specified traffic type. Options are true (enabled) or false (disabled).

—End—

See also

- [" Interface tab" \(page 231\)](#)
- ["PoE tab" \(page 235\)](#)
- [TDR tab](#)

Editing and viewing switch PoE configurations

You can configure and view the PoE parameters that apply to the whole switch using the Unit screen.

The PowerSupply tab on the Edit Chassis screen displays the status of the internal Nortel Ethernet Routing Switch 4500 Series power supply.

Note: View and edit the PoE parameters for each PoE-capable Ethernet Routing Switch 4500 one by one. If you select more than one unit, the PoE power parameters, such as the PoE tab, are not displayed.

Edit the PoE parameters from the Edit Unit screen on Ethernet Routing Switch 4500 PoE-capable units.

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select the unit. |
| 2 | Open the Edit Unit screen by selecting Edit > Unit . |
-

—End—

Unit tab for a single unit

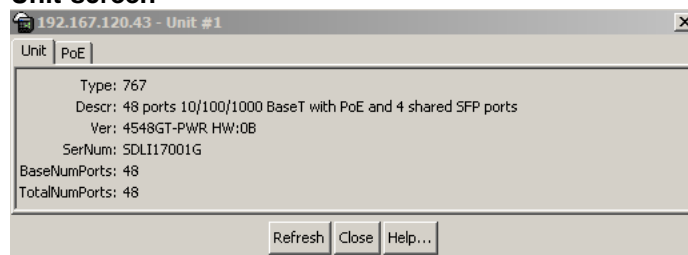
To open the Unit tab for a single unit, perform the following procedure.

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Edit Unit screen using the procedure detailed at the beginning of this section. |
|---|---|

The **Unit** screen appears with the **Unit** tab displayed ("[Unit screen](#)" [page 238](#)).

Unit screen



The following table "[Unit tab items](#)" ([page 238](#)) describes the Unit tab items.

Unit tab items

Item	Description
Type	The switch type.

Item	Description
Descr	A description of the switch hardware including number of ports and transmission speed.
Ver	The switch hardware version.
SerNum	The serial number of this device.
BaseNumPorts	The number of base ports on the switch.
TotalNumPorts	The total number of ports on the switch, including MDA ports.

See also

- ["PoE tab for a single unit" \(page 239\)](#)

—End—

PoE tab for a single unit

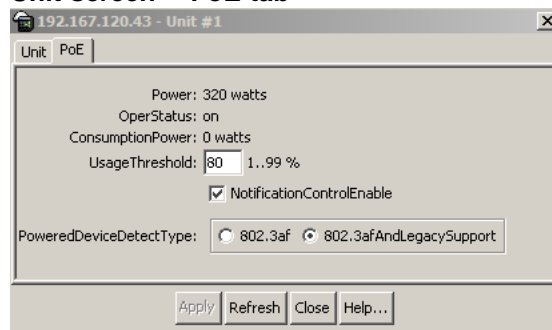
To set the power usage threshold, the power pairs to use, and the power detection method to use, select a *single* Nortel Ethernet Routing Switch 4500 Series switch.

Note: You can view and set these parameters only by selecting one unit. If you select, more than one unit, the **PoE** tab is not displayed.

To open the **PoE** tab for a *single* unit, perform the following procedure.

Step	Action
------	--------

- 1 Select the relevant Ethernet Routing Switch 4500 unit.
- 2 To open the **Unit** screen, select **Edit > Unit**.
- 3 Select the **PoE** tab, as illustrated in "Unit screen -- PoE tab" (page 239).

Unit screen -- PoE tab

The following table "PoE tab items for a single unit" (page 240) describes the PoE tab items for a single unit.

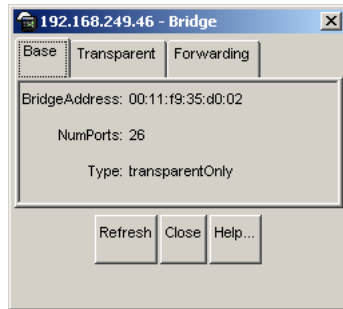
PoE tab items for a single unit

Item	Description
Power	The total power available to the Nortel Ethernet Routing Switch 4500 Series switch.
OperStatus	The power state of the Nortel Ethernet Routing Switch 4500 Series switch.: <ul style="list-style-type: none"> • on • off • faulty
Consumption Power	Displays the power used by the Nortel Ethernet Routing Switch 4500 Series switch.
Usage Threshold	Set a percentage of the total power usage of the Nortel Ethernet Routing Switch 4500 Series switch based on which system sends a trap. <p>Note: You must have the traps enabled (see NotificationControlEnable) to receive a power usage trap.</p>
Notification Control Enable	Enable or disable sending traps if the switch power usage exceeds the percentage set in the UsageThreshold field.
PowerDevice DetectType	Set the power detection method that the switch uses to detect a request for power from a device connected to all ports on the switch: <ul style="list-style-type: none"> • 802.3af • 802.3af and legacy

—End—

Editing Bridging Information

Bridging information displays the MAC Address Table for the switch. To view Bridging information, open the **Bridge** screen by selecting **Edit > Bridge**. This screen is illustrated in "Bridge screen" (page 241).

Bridge screen

For details, see the following topics:

- ["Base tab" \(page 241\)](#)
- ["Transparent tab" \(page 242\)](#)
- ["Forwarding tab" \(page 243\)](#)

Base tab

The Base tab displays basic Bridge information including the MAC address, type, and number of ports participating in the Bridge.

You must uniquely refer to the MAC address used by the bridge. The Mac address must be the smallest MAC address (numerically) of all ports that belong to the bridge. However, the Mac address must be unique only when it is integrated with *dot1dStpPriority*. A unique *BridgeIdentifier* is formed and is used in the Spanning Tree Protocol.

To view the **Base** tab, perform the following procedure.

Step Action

- 1 Open the **Bridge** screen by selecting **Edit > Bridge**.

The **Bridge** screen appears with the **Base** tab selected. This screen and tab are illustrated in ["Bridge screen" \(page 241\)](#).

["Bridge screen -- Base tab fields" \(page 241\)](#) describes the fields on this tab.

Bridge screen -- Base tab fields

Field	Description
BridgeAddress	MAC address of the bridge when it is uniquely referred to. This address must be the smallest MAC address of all ports that belong to the bridge. However, it must be unique. When concatenated with

Field	Description
	dot1dStpPriority, a unique bridge ID is formed that is then used in the Spanning Tree Protocol.
NumPorts	Number of ports controlled by the bridging entity.
Type	The type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this fact is indicated by entries in the port table for the given type.

—End—

See also:

- ["Transparent tab" \(page 242\)](#)
- ["Forwarding tab" \(page 243\)](#)

Transparent tab

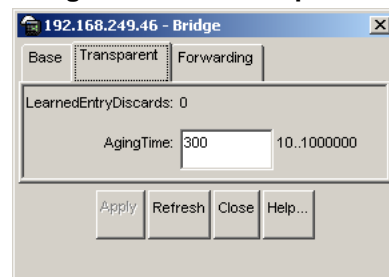
Use the **Transparent** tab to view information about learned forwarding entries.

To view the **Transparent** tab, perform the following procedure.

Step Action

- 1 Open the **Bridge** screen by selecting **Edit > Bridge**.
The **Bridge** screen appears.
- 2 Select the **Transparent** tab, as illustrated in ["Bridge screen -- Transparent tab" \(page 242\)](#).

Bridge screen -- Transparent tab



"Bridge screen -- Transparent tab fields" (page 243) describes the fields on this tab.

Bridge screen -- Transparent tab fields

Field	Description
LearnedEntryDiscards	Number of Forwarding Database entries learned discarded due to insufficient space in the Forwarding Database. If this counter increases, it indicates that the Forwarding Database is becoming full regularly. This condition affects the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has occurred but is not persistent.
AgingTime	Time-out period in seconds for removing old dynamically learned forwarding information. Note: The 802.1D-1990 specification recommends a default of 300 seconds.

- 3 If the **AgingTime** field is modified, click **Apply**.

—End—

See also:

- "Base tab" (page 241)
- "Forwarding tab" (page 243)

Forwarding tab

The **Forwarding** tab displays the current state of the port, as defined by application of the Spanning Tree Protocol.

To view the **Forwarding** tab, perform the following procedure.

Step	Action
1	Open the Bridge screen by selecting Edit > Bridge . The Bridge screen appears.
2	Select the Forwarding tab, as illustrated in "Bridge screen -- Forwarding tab" (page 244).

Bridge screen -- Forwarding tab

The screenshot shows a window titled "192.168.249.46 - Bridge" with three tabs: "Base", "Transparent", and "Forwarding". The "Forwarding" tab is active, displaying a table with three columns: "Status", "Address", and "Port". The table contains 11 rows of data. Below the table are buttons for "Refresh", "Close", and "Help...", along with a status indicator "11 row(s)".

Status	Address	Port
learned	00:03:47:69:64:03	1/5
learned	00:06:29:77:4e:23	1/5
learned	00:06:29:81:c1:0d	1/5
learned	00:06:29:c1:13:01	1/5
learned	00:07:es:40:7a:29	1/5
learned	00:09:97:38:9e:b1	1/5
learned	00:0e:00:63:10:01	1/5
learned	00:0t:ba:1d:3d:81	1/5
mgmt	00:11:19:35:00:00	0
learned	00:50:04:e1:3d:ed	1/5
learned	08:00:87:80:00:78	1/5

To continue, go to:

- ["Forwarding tab fields" \(page 244\)](#)

—End—

See also:

- ["Base tab" \(page 241\)](#)
- ["Transparent tab" \(page 242\)](#)

Forwarding tab fields

The following table ["Forwarding tab fields" \(page 244\)](#) describes the Forwarding tab fields.

Forwarding tab fields

Field	Description
Status	<p>The values for this field include:</p> <ul style="list-style-type: none"> • invalid: Entry is no longer valid, but has not been removed from the table. • learned: Value of the corresponding instance of dot1dTpFdbPort was learned and is being used. • self: Value of the corresponding instance of dot1dTpFdbAddress represents an address of the bridge. The corresponding instance of dot1dTpFdbPort indicates that a specific port on the bridge has this address.

Field	Description
	<ul style="list-style-type: none"> • mgmt(5): Value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress. • other: None of the preceding. This includes instances where another MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is used to determine if frames addressed to the value of dot1dTpFdbAddress are being forwarded.
Address	A unicast MAC address for which the bridge has forwarding or filtering information.
Port	<p>Either the value 0 or the port number on a frame has been seen. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress</p> <p>A value of 0 indicates that the port number has not been learned, so the bridge does not have the forwarding or filtering information for this address (in the dot1dStaticTable). You must assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned.</p>

Configuring SNTP

The **SNTP** screen contains the parameters for configuring Simple Network Time Protocol (SNTP).

Step Action

- 1 Open the **SNTP** screen by selecting **Edit > SNTP** as illustrated in "SNTP screen" (page 246).

SNTP screen

The following table "SNTP dialog box fields" (page 246) describes the **SNTP** screen fields.

SNTP dialog box fields

Field	Description
PrimaryServer Address	The IP address of the primary SNTP server.
SecondaryServer Address	The IP address of the secondary SNTP server.
State	Control whether the device uses SNTP to synchronize the device clock to the Coordinated Universal Time (UTC). If the value is disabled, the device does not synchronize its clock using SNTP. If the value is unicast, the device synchronizes shortly after boot time when network access becomes available, and periodically thereafter.
SynchInterval	Control the frequency, in hours, with which the device attempts to synchronize with the NTP servers.

Field	Description
ManualSynch Request	Specify that the device must immediately attempt to synchronize with the NTP servers.
LastSynch Time	The Coordinated Universal Time when the device last synchronized with an NTP server.
LastSynch Source	The IP source address of the NTP server with which this device last synchronized.
NextSynch Time	The Coordinated Universal Time at which the next synchronization is scheduled.
PrimaryServer SynchFailures	The number of times the switch failed to synchronize with the primary server address. However, synchronization with the secondary server address can still occur.
SecondaryServer SynchFailures	The number of times the switch failed to synchronize with the secondary server address.
CurrentTime	The switch current Coordinated Universal Time.

- 2 Edit the fields in the manner indicated by the table.
- 3 Click **Apply**.

—End—

Viewing topology information using Device Manager

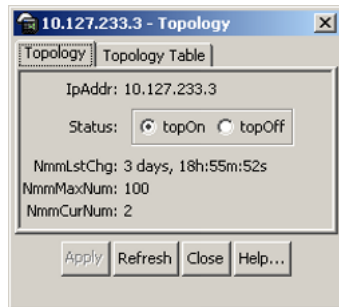
This section describes topology diagnostic information available in Device Manager through the following tabs:

- ["Topology tab" \(page 247\)](#)
- ["Topology Table tab" \(page 248\)](#)

Topology tab

To view topology information, select **Edit > Diagnostics > Topology**.

The **Topology** dialog box appears with the **Topology** tab displayed.

Topology tab

The following table describes the Topology tab fields.

Topology tab fields

Field	Description
IpAddr	The IP address of the device.
Status	Whether Nortel topology is on (topOn) or off (topOff) for the device. The default value is topOn.
NmmLstChg	The value of sysUpTime the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified. If the table has not changed since the last cold or warm start of the agent, then the value is zero.
NmmMaxNum	The maximum number of entries in the NMM topology table.
NmmCurNum	The current number of entries in the NMM topology table.

See also:

- ["Topology Table tab" \(page 248\)](#)

Topology Table tab

To view more topology information, perform the following procedure.

Step	Action
1	From the Device Manager menu bar, select Edit > Diagnostics > Topology . The Topology dialog box appears with the Topology tab displayed.
2	Click the Topology Table tab. The Topology Table tab appears.

Slot	Port	IpAddr	SegId	MacAddr	ChassisType	BkplType	LocalSeg	CurState
0	0	10.127.233.3	0	00:11:f9:34:34:01	mERS5530-24TFD	enetFastGigEnet	true	heartbeat
1	13	10.127.233.2	514	00:13:0a:03:00:41	mPassport8606	enetFastGigEnet	true	heartbeat

The following table describes the Topology Table tab fields

Topology Table tab fields

Field	Description
Slot	The slot number in the chassis in which the topology message was received.
Port	The port on which the topology message was received.
IpAddr	The IP address of the sender of the topology message.
SegId	The segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	The MAC address of the sender of the topology message.
ChassisType	The chassis type of the device that sent the topology message.
BkplType	The backplane type of the device that sent the topology message.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	The current state of the sender of the topology message. The choices are <ul style="list-style-type: none"> topChanged: Topology information recently changed. heartbeat: Topology information is unchanged. new: The sending agent is in a new state.

—End—

See also:

- ["Topology tab" \(page 247\)](#)

Link Layer Discovery Protocol (802.1ab)

This chapter describes the Link Layer Discovery Protocol (LLDP) (IEEE 802.1ab) and contains the following topics:

- "Link Layer Discover Protocol (IEEE 802.1ab) Overview" (page 251)
- "Configuring LLDP using the CLI" (page 255)
- "Configuring LLDP using Device Manager" (page 269)

Link Layer Discover Protocol (IEEE 802.1ab) Overview

Release 5.0 software supports the Link Layer Discovery Protocol (LLDP) (IEEE 802.1ab), which enables stations connected to a LAN to advertise their capabilities to each other, enabling the discovery of physical topology information for network management. LLDP-compatible stations can consist of any interconnection device including PCs, IP Phones, switches, and routers. Each LLDP station stores LLDP information in a standard Management Information Base (MIB), making it possible for a network management system (NMS) or application to access the information.

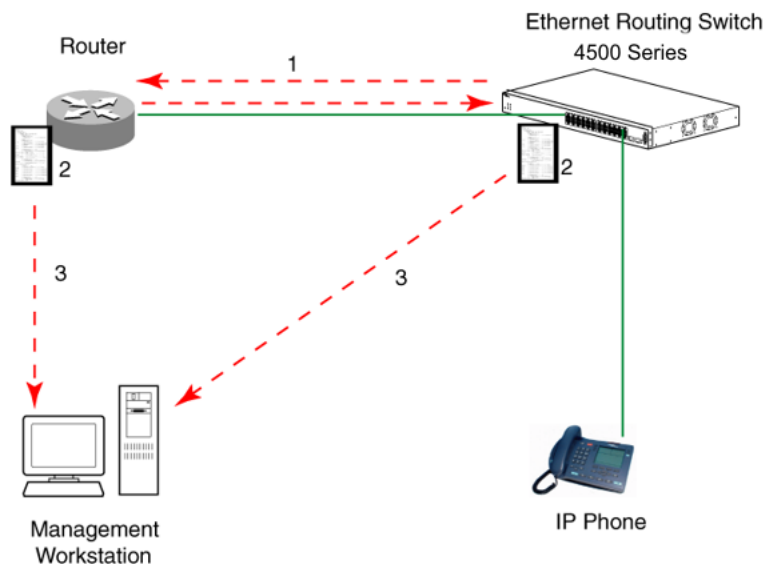
Each LLDP station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN (802.3 Ethernet with 4500 Series).
- receives network management information from adjacent stations on the same LAN.

LLDP also makes it possible to discover certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers. For example, it can be used to discover duplex mismatches between an IP Phone and the connected switch.

LLDP is compatible with IETF PROTO MIB (IETF RFC 2922).

[LLDP: how it works](#) shows an example of how LLDP works in a network.

LLDP How it works

1. The Ethernet Routing Switch and LLDP-enabled router advertise chassis/port IDs and system descriptions to each other.
2. The devices store the information about each other in local MIB databases, accessible by using SNMP.
3. A network management system retrieves the data stored by each device and builds a network topology map.

LLDP operational modes

LLDP is a one-way protocol. An LLDP agent can transmit information about the capabilities and current status of the system associated with its MAC service access point (MSAP) identifier. The LLDP agent also can receive information about the capabilities and current status of the system associated with a remote MSAP identifier. However, LLDP agents cannot solicit information from each other.

You can set the local LLDP agent to transmit only, receive only, or to both transmit and receive LLDP information. You can configure the state for LLDP reception and transmission using SNMP or CLI commands.

Connectivity and management information

The information fields in each LLDP frame are contained in a Link Layer Discovery Protocol Data Unit (LLDPDU) as a sequence of short, variable length information elements known as TLVs (type, length, value).

Each LLDPDU includes the following four mandatory TLVs:

- **Chassis ID TLV**

- **Port ID TLV**
- **Time To Live TLV**
- **End Of LLDPDU TLV**

The chassis ID and the port ID values are concatenated to form a logical MSAP identifier that the recipient uses to identify the sending LLDP agent and port.

A non-zero value in the Time to Live (TTL) field of the TTL TLV indicates to the receiving LLDP agent how long the LLDPDU information from the MSAP identifier remains valid. The receiving LLDP agent automatically discards all LLDPDU information, if the sender fails to update it in a timely manner. A zero value in TTL field of Time To Live TLV tells the receiving LLDP agent to discard the information associated with the LLDPDU MSAP identifier.

In addition to the four mandatory TLVs, Release 5.0 software supports the TLV extension set consisting of Management TLVs and organizationally-specific TLVs. Organizationally-specific TLVs are defined by either the professional organizations or the individual vendors that are involved with the particular functionality being implemented. You can specify which of these optional TLVs to include in the transmitted LLDPDUs for each port.

For more information about the supported TLV extension set, see the following:

- ["Management TLVs" \(page 253\)](#)
- ["IEEE 802.1 organizationally-specific TLVs" \(page 253\)](#)
- ["IEEE 802.3 organizationally-specific TLVs" \(page 254\)](#)

Management TLVs

The optional management TLVs are as follows:

- **Port Description TLV**
- **System Name TLV**
- **System Description TLV**
- **System Capabilities TLV** (indicates both the system supported capabilities and enabled capabilities, such as end station, bridge, or router)
- **Management Address TLV**

IEEE 802.1 organizationally-specific TLVs

The optional IEEE 802.1 organizationally-specific TLVs are:

- **Port VLAN ID TLV** contains the local port PVID.

- **Port And Protocol VLAN ID TLV** contains the VLAN IDs of the port and protocol VLANs that contain the local port.
- **VLAN Name TLV** contains the VLAN names of the VLANs that contain the local port.
- **Protocol Identity TLV** advertises the protocol supported. The following values are used for supported protocols on the 4500 Series:
 - Stp protocol {0x00,0x26,0x42,0x42,0x03, 0x00, 0x00, 0x00}
 - Rstp protocol string {0x00,0x27,0x42,0x42,0x03, 0x00, 0x00, 0x02}
 - Mstp protocol string {0x00,0x69,0x42,0x42,0x03, 0x00, 0x00, 0x03}
 - Eap protocol string {0x88, 0x8E, 0x01}
 - Lldp protocol string {0x88, 0xCC}

IEEE 802.3 organizationally-specific TLVs

The optional IEEE 802.3 organizationally-specific TLVs are:

- **MAC/PHY Configuration/Status TLV** indicates the autonegotiation capability and the speed and duplex status of IEEE 802.3 MAC/PHYs.
- **Power-Via-MDI TLV** indicates the capabilities and current status of IEEE 802.3 PMDs that either require or can provide power over twisted-pair copper links.
- **Link Aggregation TLV** indicates the current link aggregation status of IEEE 802.3 MACs.
- **Maximum Frame Size TLV** indicates the maximum supported 802.3 frame size.

Transmitting LLDPDUs When a transmit cycle is initiated, the LLDP manager extracts the managed objects from the LLDP local system MIB and formats this information into TLVs. TLVs are inserted into the LLDPDU.

LLDPDU are regularly transmitted at a user-configurable transmit interval (*tx-interval*) or when any of the variables contained in the LLDPDU is modified on the local system (such as system name or management address).

Tx-delay is "the minimum delay between successive LLDP frame transmissions."

TLV system MIBs The LLDP local system MIB stores the information for constructing the various TLVs to be sent. The LLDP remote systems MIB stores the information received from remote LLDP agents.

LLDPDU and TLV error handling LLDPDUs and TLVs that contain detectable errors are discarded. TLVs that are not recognized, but that also contain no basic format errors, are assumed to be validated and are stored for possible later retrieval by network management.

Configuring LLDP using the CLI

You can enable and configure LLDP using the CLI. For more information about LLDP, see "[Link Layer Discover Protocol \(IEEE 802.1ab\) Overview](#)" (page 251). This section covers the following commands:

- "lldp command" (page 255)
- "lldp port command" (page 256)
- "lldp tx-tlv command" (page 257)
- "lldp tx-tlv dot1 command" (page 257)
- "lldp tx-tlv dot3 command" (page 258)
- lldp location-identification coordinate-base command
- lldp location-identification civic-address command
- "show lldp command" (page 262)
- "default lldp command" (page 258)
- "default lldp port command" (page 259)
- "default lldp tx-tlv command" (page 259)
- "default lldp tx-tlv dot1 command" (page 260)
- "default lldp tx-tlv dot3 command" (page 261)
- "no lldp port command" (page 261)
- "no lldp tx-tlv command" (page 262)
- "no lldp tx-tlv dot1 command" (page 262)
- "no lldp tx-tlv dot3 command" (page 262)
- "show lldp port command" (page 264)
- "LLDP configuration example" (page 264)

lldp command

The `lldp` command sets the LLDP transmission parameters. The syntax for the `lldp` command is

```
lldp [tx-interval <5-32768>] [tx-hold-multiplier
<2-10>] [reinit-delay <1-10>] [tx-delay <1-8192>]
[notification-interval <5-3600>] ]
```

Run the `lldp` command in Global Configuration command mode.

"[lldp command parameters and variables](#)" (page 256) describes the parameters and variables for the `lldp` command.

lldp command parameters and variables

Parameters and variables	Description
tx-interval <5-32768>	Set the interval between successive transmission cycles.
tx-hold-multiplier <2-10>	Set the multiplier for the tx-interval used to compute the Time To Live value for the TTL TLV.
reinit-delay <1-10>	Set the delay for the reinitialization attempt if the adminStatus is disabled.
tx-delay <1-8192>	Set the minimum delay between successive LLDP frame transmissions.
notification-interval <5-3600>	Set the interval between successive transmissions of LLDP notifications.

lldp port command

The `lldp port` command sets the LLDP port parameters. The syntax for the `lldp port` command is

```
lldp port <portlist> [config notification] [status {rxOnly | txAndRx | txOnly}]
```

Run the `lldp port` command in Interface Configuration command mode.

"[lldp port command parameters and variables](#)" (page 256) describes the parameters and variables for the `lldp port` command.

lldp port command parameters and variables

Parameters and variables	Description
port <portlist>	Specify the ports affected by the command.
config notification	Enable notification when new neighbor information is stored or when existing information is removed.
status {rxOnly txAndRx txOnly}	Set the LLDPDU transmit and receive status on the ports. <ul style="list-style-type: none"> rxonly: enables LLDPDU receive only txAndRx: enables LLDPDU transmit and receive txOnly: enables LLDPDU transmit only

lldp tx-tlv command

The `lldp tx-tlv` command sets the optional Management TLVs to be included in the transmitted LLDPDUs. The syntax for the `lldp tx-tlv` command is

```
lldp tx-tlv [port <portlist>] [port-desc] [sys-name]
[sys-desc] [sys-cap] [local-mgmt-addr]
```

Run the `lldp tx-tlv` command in Interface Configuration command mode.

"[lldp tx-tlv command parameters and variables](#)" (page 257) describes the parameters and variables for the `lldp tx-tlv` command.

lldp tx-tlv command parameters and variables

Parameters and variables	Description
port <portlist>	The ports affected by the command.
port-desc	The port description TLV.
sys-name	The system name TLV.
sys-desc	The system description TLV.
sys-cap	The system capabilities TLV.
local-mgmt-addr	The local management address TLV.

lldp tx-tlv dot1 command

The `lldp tx-tlv dot1` command sets the optional IEEE 802.1 organizationally-specific TLVs to be included in the transmitted LLDPDUs. The syntax for the `lldp tx-tlv dot1` command is

```
lldp tx-tlv [port <portlist>] dot1 [port-vlan-id]
[vlan-name <vlanlist>] [port-protocol-vlan-id <vlanlist>]
[protocol-identity [EAP] [LLDP] [STP] ]
```

The `lldp tx-tlv dot1` command is in the Interface Configuration command mode.

"[lldp tx-tlv dot1 command parameters and variables](#)" (page 257) describes the parameters and variables for the `lldp tx-tlv dot1` command.

lldp tx-tlv dot1 command parameters and variables

Parameters and variables	Description
port <portlist>	The ports affected by the command.
port-vlan-id	The port VLAN ID TLV.
vlan-name	The VLAN name TLV.

Parameters and variables	Description
port-protocol-vlan-id	The port and protocol VLAN ID TLV.
protocol-identity [EAP] [LLDP] [STP]	The protocol identity TLV.

lldp tx-tlv dot3 command

The `lldp tx-tlv dot3` command sets the optional IEEE 802.3 organizationally-specific TLVs to be included in the transmitted LLDPDUs. The syntax for the `lldp tx-tlv dot3` command is

```
lldp tx-tlv [port <portlist>] dot3 [mac-phy-config-status]
[mdi-power-support] [link-aggregation] [maximum-frame-size]
```

Run the `lldp tx-tlv dot3` command in Interface Configuration command mode.

"[lldp tx-tlv dot3 command parameters and variables](#)" (page 258) describes the parameters and variables for the `lldp tx-tlv dot3` command.

lldp tx-tlv dot3 command parameters and variables

Parameters and variables	Description
port <portlist>	The ports affected by the command.
mac-phy-config-status	The MAC/Phy configuration or status TLV.
mdi-power-support	The power via MDI TLV.
link-aggregation	The link aggregation TLV.
maximum-frame-size	The maximum frame size TLV.

default lldp command

The `default lldp` command sets the LLDP transmission parameters to their default values. The syntax for the `default lldp` command is

```
default lldp [tx-interval ] [tx-hold-multiplier ]
[reinit-delay] [tx-delay] [notification-interval]
```

If no parameters are specified, the `default lldp` sets all parameters to their default parameters.

Run the `default lldp` command in Global Configuration command mode.

"[default lldp command parameters and variables](#)" (page 259) describes the parameters and variables for the `default lldp` command.

default lldp command parameters and variables

Parameters and variables	Description
tx-interval	Set the retransmit interval to the default value (30).
tx-hold-multiplier	Set the transmission multiplier to the default value (4).
reinit-delay	Set the reinitialize delay to the default value (2).
tx-delay	Set the transmission delay to the default value (2).
notification-interval	Set the notification interval to the default value (5).

default lldp port command

The `default lldp port` command sets the port parameters to their default values. The syntax for the `default lldp port` command is

```
default lldp port <portlist> [config notification] [status]
```

Run the `default lldp port` command in Interface Configuration command mode.

"[default lldp port command parameters and variables](#)" (page 259) describes the parameters and variables for the `default lldp port` command.

default lldp port command parameters and variables

Parameters and variables	Description
port <portlist>	The ports affected by the command.
config notification	Set the config notification to its default value (disabled).
status	Set the LLDP transmit and receive status to the default value (txAndRx).

default lldp tx-tlv command

The `default lldp tx-tlv` command sets the LLDP Management TLVs to their default values. The syntax for the `default lldp tx-tlv` command is

```
default lldp tx-tlv [port <portlist>] [port-desc] [sys-name]
[sys-desc] [sys-cap] [local-mgmt-addr]
```

Run the `default lldp tx-tlv` command in Interface Configuration command mode.

"[default lldp tx-tlv command parameters and variables](#)" (page 260) describes the parameters and variables for the `default lldp tx-tlv` command.

default lldp tx-tlv command parameters and variables

Parameters and variables	Description
port <portlist>	The ports affected by the command.
port-desc	The port description TLV (default value is false: not included).
sys-name	The system name TLV (default value is false: not included).
sys-desc	The system description TLV (default value is false: not included).
sys-cap	The system capabilities TLV (default value is false: not included).
local-mgmt-addr	The local management address TLV (default value is false: not included).

default lldp tx-tlv dot1 command

The `default lldp tx-tlv dot1` command sets the optional IEEE 802.1 organizationally-specific TLVs to their default values. The syntax for the `default lldp tx-tlv dot1` command is

```
default lldp tx-tlv [port <portlist>] dot1 [port-vlan-id]
[vlan-name ] [port-protocol-vlan-id] [protocol-identity [EAP]
[LLDP] [STP] ]
```

Run the `default lldp tx-tlv dot1` command in Interface Configuration command mode.

"[default lldp tx-tlv dot1 command parameters and variables](#)" (page 260) describes the parameters and variables for the `default lldp tx-tlv dot1` command.

default lldp tx-tlv dot1 command parameters and variables

Parameters and variables	Description
port <portlist>	The ports affected by the command.
port-vlan-id	The port VLAN ID TLV (default value is false: not included).
vlan-name	The VLAN Name TLV (default value is none).

Parameters and variables	Description
port-protocol-vlan-id	The port and protocol VLAN ID TLV (default value is none).
protocol-identity [EAP] [LLDP] [STP]	The protocol identity TLV (default value is none).

default lldp tx-tlv dot3 command

The `default lldp tx-tlv dot3` command sets the optional IEEE 802.3 organizationally-specific TLVs to their default values. The syntax for the `default lldp tx-tlv dot3` command is

```
default lldp tx-tlv [port <portlist>] dot3
[mac-phy-config-status] [mdi-power-support]
[link-aggregation] [maximum-frame-size]
```

Run the `default lldp tx-tlv dot3` command in Interface Configuration command mode.

["default lldp tx-tlv dot3 command parameters and variables" \(page 261\)](#) describes the parameters and variables for the `default lldp tx-tlv dot3` command.

default lldp tx-tlv dot3 command parameters and variables

Parameters and variables	Description
port <portlist>	The ports affected by the command.
mac-phy-config-status	The MAC/Phy Configuration/Status TLV (default value is false: not included).
mdi-power-support	The power via MDI TLV (default value is false: not included).
link-aggregation	The link aggregation TLV (default value is false: not included).
maximum-frame-size	The maximum frame size TLV (default value is false: not included).

no lldp port command

The `no lldp port` command disables LLDP features on the port. The syntax for the `no lldp port` command is

```
no lldp [port <portlist>] [config notification] [status]
```

Run the `no lldp port` command in Interface Configuration command mode.

no lldp tx-tlv command

The `no lldp tx-tlv` command specifies the optional Management TLVs not to include in the transmitted LLDPDUs. The syntax for the `no lldp tx-tlv` command is

```
no lldp tx-tlv [port <portlist>] [port-desc] [sys-name]
[sys-desc] [sys-cap] [local-mgmt-addr]
```

Run the `no lldp tx-tlv` command in Interface Configuration command mode.

no lldp tx-tlv dot1 command

The `no lldp tx-tlv dot1` command specifies the optional IEEE 802.1 TLVs not to include in the transmitted LLDPDUs. The syntax for the `no lldp tx-tlv dot1` command is

```
no lldp tx-tlv [port <portlist>] dot1 [port-vlan-id]
[vlan-name] [port-protocol-vlan-id] [protocol-identity [EAP]
[LLDP] [STP] ]
```

Run the `no lldp tx-tlv dot1` command in Interface Configuration command mode.

no lldp tx-tlv dot3 command

The `no lldp tx-tlv dot3` command specifies the optional IEEE 802.3 TLVs not to include in the transmitted LLDPDUs. The syntax for the `no lldp tx-tlv dot3` command is

```
no lldp tx-tlv [port <portlist>] dot3
[mac-phy-config-status] [mdi-power-support]
[link-aggregation] [maximum-frame-size]
```

Run the `no lldp tx-tlv dot3` command in Interface Configuration command mode.

show lldp command

The `show lldp` command displays the LLDP parameters. The syntax for the `show lldp` command is

```
show lldp [local-sys-data {dot1 | dot3 | detail}]
[mgmt-sys-data]
[rx-stats] [tx-stats] [stats] [pdu-tlv-size]
[tx-tlv {dot1 | dot3 }]
[neighbor { dot1 [vlan-names | protocol-id] } | [dot3] |
[detail] ]
[neighbor-mgmt-addr]
```

Run the `show lldp` command in Privileged EXEC command mode.

The following table describes the `show lldp` command parameters and variables.

show lldp command parameters

Parameters and variables	Description
local-sys-data {dot1 dot3 detail}	<p>The organizationally-specific TLV properties on the local switch:</p> <ul style="list-style-type: none"> dot1: displays the 802.1 TLV properties dot3: displays the 802.3 TLV properties detail: displays all organizationally specific TLV properties <p>To display the properties of the optional management TLVs, include only the local-sys-data parameter in the command.</p>
mgmt-sys-data	The local management system data.
rx-stats	The LLDP receive statistics for the local system.
tx-stats	The LLDP transmit statistics for the local system.
stats	The LLDP table statistics for the remote system.
pdu-tlv-size	The different TLV sizes and the number of TLVs in an LLDPDU.
tx-tlv {dot1 dot3 }	<p>Display which TLVs are transmitted from the local switch in LLDPDUs:</p> <ul style="list-style-type: none"> dot1: displays status for 802.1 TLVs dot3: displays status for 802.3 TLVs <p>To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.</p>
neighbor { dot1 [vlan-names protocol-id] [dot3] [detail]	<p>The neighbor TLVs:</p> <ul style="list-style-type: none"> dot1: displays 802.1 TLVs: <ul style="list-style-type: none"> — vlan-names: VLAN Name TLV — protocol-id: Protocol Identity TLV dot3: displays 802.3 TLVs detail: displays all TLVs
[neighbor-mgmt-addr]	The LLDP neighbor management address.

show lldp port command

The `show lldp port` command displays the LLDP port parameters. The syntax for the `show lldp port` command is

```
show lldp port <portlist> [rx-stats] [tx-stats] [pdu-tlv-size]
[tx-tlv {dot1 | dot3}]
[neighbor {dot1 [vlan-names | protocol-id] } | [dot3]]
```

Run the `show lldp port` command in Privileged EXEC command mode.

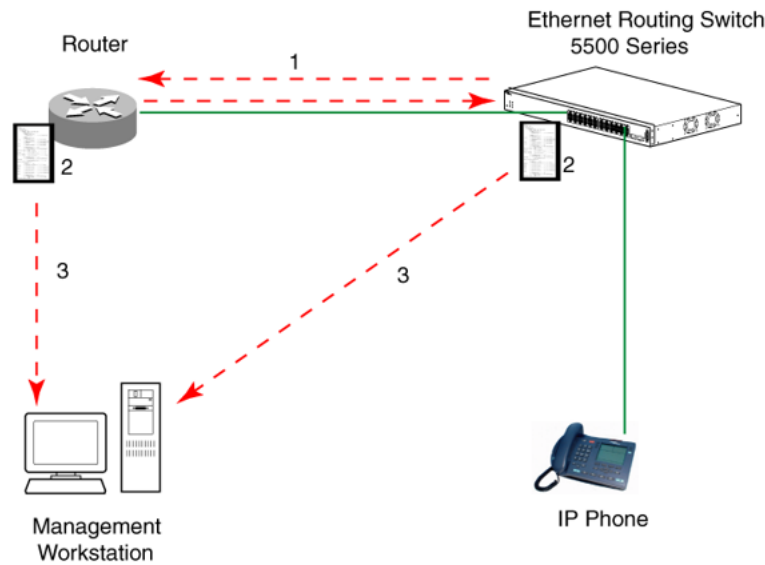
show lldp port command parameters

Parameters and variables	Description
rx-stats	The LLDP receive statistics for the local port.
tx-stats	The LLDP transmit statistics for the local port.
pdu-tlv-size	The different TLV sizes and the number of TLVs in an LLDPDU.
tx-tlv {dot1 dot3 }	<p>Display which TLVs are transmitted from the local port in LLDPDUs:</p> <ul style="list-style-type: none"> dot1: displays status for 802.1 TLVs dot3: displays status for 802.3 TLVs <p>To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.</p>
neighbor { dot1 [vlan-names protocol-id] } [dot3] [detail]	<p>The port neighbor TLVs:</p> <ul style="list-style-type: none"> dot1: displays 802.1 TLVs: <ul style="list-style-type: none"> — vlan-names: VLAN Name TLV — protocol-id: Protocol Identity TLV dot3: displays 802.3 TLVs detail: displays all TLVs.
[neighbor-mgmt-addr]	The port neighbor LLDP management address.

LLDP configuration example

By default, LLDP is enabled for Tx and Rx on all switch ports. The default value for the LLDP Tx interval is 30 seconds (LLDPDUs are sent at 30 seconds). With the default settings, only the mandatory TLVs are sent, but the switch can receive any LLDP Core, DOT1, or DOT3 TLV from its peers.

["LLDP configuration example" \(page 265\)](#)

LLDP configuration example

To configure the example shown above, you must perform the following tasks:

Step	Action
1	Modify the default LLDP Tx interval from (the default 30 second value) to 60 seconds. Note that if any modification is detected in the LLDP local-sys-data before the Tx interval expires, an LLDPDU is immediately sent on all active links in order to update the peers neighbor tables.
2	Enable the Port Description TLV for transmission. (contains the description of the LLDP sending port)
3	Enable the System Name TLV for transmission. (contains the name of the LLDP device)
4	Enable the System Description TLV for transmission. (contains the description of the LLDP device)
5	Enable the System Capabilities TLV for transmission. (contains the capabilities of the LLDP device)
6	Enable the Management Address TLV for transmission. (contains the management address of the LLDP device)
7	Enable the Port VLAN ID TLV for transmission. (contains the PVID of the LLDP sending port)

- 8 Enable the Port And Protocol VLAN ID TLV for transmission. (indicates the Port and Protocol VLANs to which the LLDP sending port belongs to).
- 9 Enable the VLAN Name TLV for transmission. (indicates the names of the VLANs to which the LLDP sending port belongs to)
- 10 Enable the Protocol Identity TLV for transmission. (indicates the supported protocols by the LLDP sending port)
- 11 Enable the MAC/PHY Configuration/Status TLV for transmission. (indicates the IEEE 802.3 duplex and bitrate capabilities and settings of the LLDP sending port)
- 12 Enable the Power Via MDI TLV for transmission. (indicates the MDI power support capabilities of the LLDP sending port)
- 13 Enable the Link Aggregation TLV for transmission. (indicates the link aggregation capability and status of the LLDP sending port)
- 14 Enable the Maximum Frame Size TLV for transmission. (indicates the maximum frame size that could be handled by the LLDP sending port)
- 15 Enable the Location Identification TLV for transmission. (indicates the physical location of the LLDP sending port; three coordinate sets are available to configure and send)
- 16 Enable the Extended Power-via-MDI TLV for transmission. (provides detailed informations regarding the PoE parameters of the LLDP sending device)
- 17 Enable the Inventory – Hardware Revision TLV for transmission. (indicates the hardware revision of the LLDP sending device)
- 18 Enable the Inventory – Firmware Revision TLV for transmission. (indicates the firmware revision of the LLDP sending device)
- 19 Enable the Inventory – Software Revision TLV for transmission. (indicates the software revision of the LLDP sending device)
- 20 Enable the Inventory – Serial Number TLV for transmission. (indicates the serial number of the LLDP sending device)
- 21 Enable the Inventory – Manufacturer Name TLV for transmission. (indicates the manufacturer name of the LLDP sending device)
- 22 Enable the Inventory – Model Name TLV for transmission. (indicates the model name of the LLDP sending device)

—End—

Note: There is currently no ACG support for LLDP.

Detailed configuration commands

The following section describes the detailed CLI commands required to carry out the configuration depicted by "LLDP configuration example" (page 265)

Modifying the default LLDP Tx interval Enter configuration commands, one for each line. End with CNTL/Z.

```
4548GT-PWR-PWR>enable
4548GT-PWR#configure terminal
4548GT-PWR(config)#lldp tx-interval 60
```

Checking the new LLDP global settings

```
4548GT-PWR(config)#show lldp
```

802.1ab configuration:

```
-----
TxInterval:60
TxHoldMultiplier:4
RxInitDelay:2
TxDelay:2
NotificationInterval:5
```

Enabling all LLDP Core TLVs for transmission on the router and IP Phone ports

```
4548GT-PWR(config)#interface fastEthernet 1/13 454
8GT-PWR(config-if)#lldp tx-tlv port 1/13 port-desc
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 sys-name
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 sys-desc
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 sys-cap
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 local-mgmt-addr
```

Checking the LLDP settings of the router and IP Phone ports

```
4548GT-PWR(config-if)#show lldp port 1/13 tx-tlv
```

```
-----
lldp port tlvs
-----
```

PortDesc	SysName	SysDesc	SysCap	MgmtAddr
1	true	true	true	true true
13	true	true	true	true true

Enabling all LLDP DOT1 TLVs for transmission on the router and IP Phone ports

```
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot1 port-vlan-id
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot1
port-protocol-vlan-id
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot1 vlan-name
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot1
protocol-identity EAP LLDP STP
```

Checking the LLDP settings of the router and IP Phone ports

```
4548GT-PWR(config-if)#show lldp port 1/13 tx-tlv dot1
```

```
-----
lldp port dot1 tlvs
-----
```

```
Dot1 protocols: STP,EAP,LLDP
-----
```

```
Port PortVlanId VlanNameList
PortProtocolVlanId ProtocolIdentity
-----
```

```
1      true  1              1
ALL
13     true  1              1
ALL
```

Enabling all LLDP DOT3 TLVs for transmission on the router and IP Phone ports

```
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot3
mac-phy-config-status
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot3
mdi-power-support
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot3
link-aggregation
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot3
maximum-frame-size
```

Checking the LLDP settings of the router and IP Phone ports

```
4548GT-PWR(config-if)#show lldp port 1/13 tx-tlv dot3
```

```
-----
lldp port dot3 tlvs
-----
```

```
-----
Port MacPhy      MdiPower   Link      MaxFrameSize
ConfigStatus Support   Aggregation
-----
```

```
1      true      true      true      true
13     true      true      true      true
```

Configuring LLDP using Device Manager

The following sections describe how to configure and view LLDP information using Device Manager.

- "Viewing and configuring LLDP global and transmit properties" (page 269)
- "LLDP_Port_dot1 dialog box" (page 294)
- "LLDP_Port_dot_3 dialog box" (page 305)

Viewing and configuring LLDP global and transmit properties

Use the following tabs to configure and view LLDP global and transmit properties for local and neighbor systems:

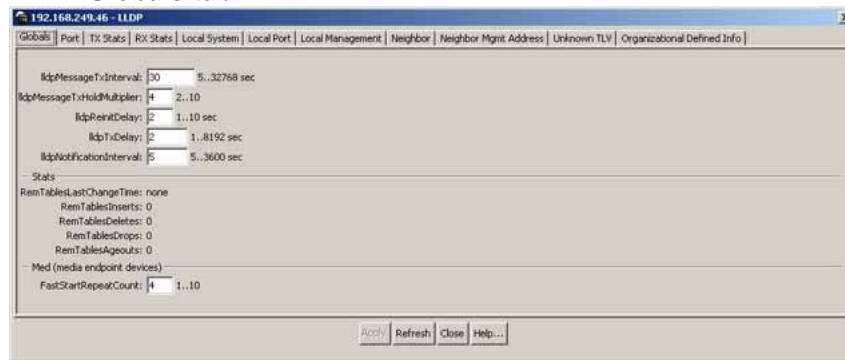
- "Globals tab" (page 269)
- "Port tab" (page 273)
- "TX Stats tab" (page 275)
- "Graphing LLDP transmit statistics" (page 277)
- "RX Stats tab" (page 278)
- "Graphing LLDP receive statistics" (page 280)
- "Local System tab" (page 281)
- "Local Port tab" (page 283)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)
- "Unknown TLV tab" (page 290)
- "Organizational Defined Info tab" (page 292)

Globals tab

With the **Globals** tab, you can configure LLDP transmit properties and view remote table statistics.

To open the Globals tab, perform the following procedure:

Step	Action
1	From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > LLDP . The LLDP dialog box appears with the Globals tab displayed (" LLDP Globals tab " (page 270)).

LLDP Globals tab

"LLDP Globals tab fields" (page 270) describes the Globals tab fields.

LLDP Globals tab fields

Field	Description
lldpMessageTxInterval	The interval, in seconds, at which LLDP frames are transmitted on behalf of this LLDP agent.
lldpMessageTxHoldMultiplier	The time-to-live value expressed as a multiple of the object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, is expressed by the following formula: $TTL = \min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier))$ For example, if the value of lldpMessageTxInterval is 30, and the value of lldpMessageTxHoldMultiplier is 4, the value 120 is encoded in the TTL field in the LLDP header.
lldpReinitDelay	The lldpReinitDelay indicates the delay (in seconds) from when the LLDP Port AdminStatus of a particular port is disabled until reinitialization begins.
lldpTxDelay	The lldpTxDelay indicates the delay (in seconds) between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The recommended value for the lldpTxDelay is set by the following formula: $1 \leq lldpTxDelay \leq (0.25 * lldpMessageTxInterval)$

Field	Description
IldpNotificationInterval	This object controls the transmission of LLDP notifications. The agent must not generate more than one IldpRemTablesChange notification-event in the indicated period, where a <i>notification-event</i> is the "transmission of a single notification PDU type to a list of notification destinations." If additional changes in IldpRemoteSystemsData object groups occur within the indicated throttling period, these trap-events must be suppressed by the agent. An NMS must periodically check the value of IldpStatsRemTableLastChangeTime to detect any missed IldpRemTablesChange notification-events, for example, due to throttling or transmission loss. If notification transmission is enabled for particular ports, the suggested default throttling period is 5 seconds.
RemTablesLastChangeTime	The value of the sysUpTime object (defined in IETF RFC 3418) at the time an entry is created, modified, or deleted in tables associated with the IldpRemoteSystemsData objects, and all LLDP extension objects associated with remote systems. An NMS can use this object to reduce polling of the IldpRemoteSystemsData objects.
RemTablesInserts	The number of times the complete set of information advertised by a particular MSAP is inserted into tables contained in IldpRemoteSystemsData and IldpExtensions objects. The complete set of information received from a particular MSAP is inserted into related tables. If partial information cannot be inserted for a reason such as lack of resources, all of the complete set of information is removed. This counter is incremented only once after the complete set of information is successfully recorded in all related tables. Any failures occurring during insertion of the information set, which result in deletion of previously inserted information, do not trigger any changes in IldpStatsRemTablesInserts because the insert is not completed yet or

Field	Description
	in <code>IldpStatsRemTablesDeletes</code> , because the deletion is only a partial deletion. If the failure is the result of a lack of resources, the <code>IldpStatsRemTablesDrops</code> counter is incremented once.
<code>RemTablesDeletes</code>	The number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in <code>IldpRemoteSystemsData</code> and <code>IldpExtensions</code> objects. This counter is incremented only once when the complete set of information is completely deleted from all related tables. Partial deletions, such as a deletion of rows associated with a particular MSAP, from some tables, but not from all tables, are not allowed, and thus, do not change the value of this counter.
<code>RemTablesDrops</code>	The number of times the complete set of information advertised by a particular MSAP can not be entered into tables contained in <code>IldpRemoteSystemsData</code> and <code>IldpExtensions</code> objects because of insufficient resources.
<code>RemTablesAgeouts</code>	The number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in <code>IldpRemoteSystemsData</code> and <code>IldpExtensions</code> objects because the information timeliness interval has expired. This counter is incremented only once when the complete set of information is completely invalidated (aged out) from all related tables. Partial aging, similar to deletion case, is not allowed, and thus, does not change the value of this counter.

—End—

See also:

- ["Port tab" \(page 273\)](#)
- ["TX Stats tab" \(page 275\)](#)
- ["Graphing LLDP transmit statistics" \(page 277\)](#)

- "RX Stats tab" (page 278)
- "Graphing LLDP receive statistics" (page 280)
- "Local System tab" (page 281)
- "Local Port tab" (page 283)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)
- "Unknown TLV tab" (page 290)
- "Organizational Defined Info tab" (page 292)

Port tab

With the Port tab, you can set the optional TLVs to include in the LLPDUs transmitted by each port.

To open the Port tab, perform the following procedure.

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > LLDP**.
The LLDP dialog box appears with the Globals tab displayed.
- 2 Click the **Port** tab.
The Port tab appears.

LLDP Port tab

The screenshot shows the 'LLDP Port tab' configuration window for IP address 192.168.249.46. The window contains a table with columns for Portnum, AdminStatus, NotificationEnable, TLVTxEnable, MntTxEnable(dot1), TLVStxEnable(dot3), CapSupported(med), TLVStxEnable(med), and NotifyEnable(med). The table lists 26 ports (1/1 to 1/26) with their respective configurations.

Portnum	AdminStatus	NotificationEnable	TLVTxEnable	MntTxEnable(dot1)	TLVStxEnable(dot3)	CapSupported(med)	TLVStxEnable(med)	NotifyEnable(med)
1/1 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/2 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/3 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/4 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/5 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/6 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/7 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/8 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/9 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/10 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/11 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/12 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/13 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/14 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/15 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/16 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/17 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/18 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/19 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/20 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/21 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/22 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/23 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/24 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/25 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false
1/26 tVAndRx	false			false		capabilities, networkPolicy, location, inventory		false

"Port tab fields" (page 274) describes the Port tab fields.

Port tab fields

Field	Description
PortNum	Port number.
AdminStatus	<p>The administratively desired status of the local LLDP agent:</p> <ul style="list-style-type: none"> • txOnly: the LLDP agent transmits LLDP frames on this port and does not store any information about the remote systems to which it is connected. • rxOnly: the LLDP agent receives but does not transmit LLDP frames on this port. • txAndRx: the LLDP agent transmits and receives LLDP frames on this port. • disabled: the LLDP agent does not transmit or receive LLDP frames on this port. If the port receives remote systems information which is stored in other tables before AdminStatus is disabled, the information ages out.
NotificationEnable	<p>Controls, on a per-port basis, whether notifications from the agent are enabled.</p> <ul style="list-style-type: none"> • true: indicates that notifications are enabled • false: indicates that notifications are disabled.
TLVsTxEnable	<p>Sets the optional Management TLVs to be included in the transmitted LLDPDUs:</p> <ul style="list-style-type: none"> • portDesc: Port Description TLV • sysName: System Name TLV • sysDesc: System Description TLV • sysCap: System Capabilities TLV <p>Note: The Local Management tab controls Management Address TLV transmission.</p>

Field	Description
VLANTxEnable(dot1)	Specifies whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is included in the transmitted LLDPDUs.
TLVsTxEnable(dot3)	Sets the optional IEEE 802.3 organizationally defined TLVs to be included in the transmitted LLDPDUs: <ul style="list-style-type: none"> • macPhyConfigStatus: MAC/PHY configuration/status TLV • powerViaMDI: Power over MDI TLV • linkAggregation: Link Aggregation TLV • maxFrameSize: Maximum-frame-size TLV.

—End—

See also:

- ["Globals tab" \(page 269\)](#)
- ["TX Stats tab" \(page 275\)](#)
- ["Graphing LLDP transmit statistics" \(page 277\)](#)
- ["RX Stats tab" \(page 278\)](#)
- ["Graphing LLDP receive statistics" \(page 280\)](#)
- ["Local System tab" \(page 281\)](#)
- ["Local Port tab" \(page 283\)](#)
- ["Local Management tab" \(page 285\)](#)
- ["Neighbor tab" \(page 286\)](#)
- ["Neighbor Mgmt Address tab" \(page 289\)](#)
- ["Unknown TLV tab" \(page 290\)](#)
- ["Organizational Defined Info tab" \(page 292\)](#)

TX Stats tab

With the TX Stats tab, you can view LLDP transmit statistics by port.

To open the TX Stats tab, perform the following procedure.

- | Step | Action |
|------|--|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > LLDP .
The LLDP dialog box appears with the Globals tab displayed. |
| 2 | Click the TX Stats tab.
The TX Stats tab appears ("TX Stats tab" (page 276)). |

TX Stats tab

"TX Stats tab fields" (page 276) describes the TX Stats tab fields.

TX Stats tab fields

Field	Description
PortNum	port number
FramesTotal	the number of LLDP frames transmitted by this LLDP agent on the indicated port

—End—

See also:

- "Globals tab" (page 269)
- "Port tab" (page 273)
- "Graphing LLDP transmit statistics" (page 277)
- "RX Stats tab" (page 278)
- "Graphing LLDP receive statistics" (page 280)
- "Local System tab" (page 281)
- "Local Port tab" (page 283)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)
- "Unknown TLV tab" (page 290)
- "Organizational Defined Info tab" (page 292)

Graphing LLDP transmit statistics

To graph LLDP transmit statistics, perform the following procedure.

- | Step | Action |
|------|--|
| 1 | From the TX Stats tab "TX Stats tab" (page 276)), select the port for which you want to display statistics. |
| 2 | Click Graph .
The TX Stats - Graph dialog box appears. |

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
FramesTotal	9,365	11	0.03	0	0.1	0

- Highlight a data column to graph.
- Click one of the graph buttons.

—End—

See also:

- "Globals tab" (page 269)
- "Port tab" (page 273)
- "TX Stats tab" (page 275)
- "RX Stats tab" (page 278)
- "Graphing LLDP receive statistics" (page 280)
- "Local System tab" (page 281)
- "Local Port tab" (page 283)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)
- "Unknown TLV tab" (page 290)
- "Organizational Defined Info tab" (page 292)

RX Stats tab

With the RX Stats tab, you can view LLDP receive statistics by port.

To open the RX Stats tab, perform the following procedure.

Step	Action
------	--------

- From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > LLDP**.
The LLDP dialog box appears with the Globals tab displayed.
- Click the **RX Stats** tab.
The RX Stats tab appears ("[RX Stats tab](#)" (page 278)).

RX Stats tab

PortNum	FramesDiscardedTotal	FramesErrors	FramesTotal	TLVsDiscardedTotal	TLVsUnrecognizedTotal	AgeoutsTotal
1/1	0	0	0	0	0	0
1/2	0	0	0	0	0	0
1/3	0	0	0	0	0	0
1/4	0	0	0	0	0	0
1/5	0	0	0	0	0	0
1/6	0	0	0	0	0	0
1/7	0	0	0	0	0	0
1/8	0	0	0	0	0	0
1/9	0	0	0	0	0	0
1/10	0	0	0	0	0	0
1/11	0	0	0	0	0	0
1/12	0	0	0	0	0	0
1/13	0	0	0	0	0	0
1/14	0	0	0	0	0	0
1/15	0	0	0	0	0	0
1/16	0	0	0	0	0	0
1/17	0	0	0	0	0	0
1/18	0	0	0	0	0	0
1/19	0	0	0	0	0	0
1/20	0	0	0	0	0	0
1/21	0	0	0	0	0	0
1/22	0	0	0	0	0	0
1/23	0	0	0	0	0	0
1/24	0	0	0	0	0	0
1/25	0	0	0	0	0	0

"[RX Stats tab fields](#)" (page 278) describes the RX Stats tab fields.

RX Stats tab fields

Field	Description
PortNum	Port number.
FramesDiscardedTotal	The number of LLDP frames received on the port and discarded for any reason. This counter provides an indication that LLDP header formatting problems exist with the local LLDP agent in the sending system, or that LLDPDU validation problems exist with the local LLDP agent in the receiving system.
FramesErrors	The number of invalid LLDP frames received on the port, while the LLDP agent is enabled.

Field	Description
FramesTotal	The number of valid LLDP frames received on the port, while the LLDP agent is enabled.
TLVsDiscardedTotal	The number of LLDP TLVs discarded for any reason.
TLVsUnrecognizedTotal	The number of LLDP TLVs received on a given port that are not recognized by this LLDP agent on the indicated port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001 - 111 1110) in Table 9.1 of IEEE 802.1AB-2004. An unrecognized TLV can be a basic management TLV from a later LLDP version.
AgeoutsTotal	This counter represents the number of age-outs that occurred on a given port. An <i>age-out</i> is "the number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in <code>IldpRemoteSystemsData</code> and <code>IldpExtensions</code> objects because the information timeliness interval has expired." This counter is similar to <code>IldpStatsRemTablesAgeouts</code> , except that it is on a per-port basis. This enables NMS to poll tables associated with the <code>IldpRemoteSystemsData</code> objects and all LLDP extension objects associated with remote systems on the indicated port only. This counter is set to zero during agent initialization. When the admin status for a port changes from disabled to <code>rxOnly</code> , <code>txOnly</code> or <code>txAndRx</code> , the counter associated with the same port is reset to 0. The agent also flushes all remote system information associated with the same port. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial aging is not allowed, and thus, does not change the value of this counter.

—End—

See also:

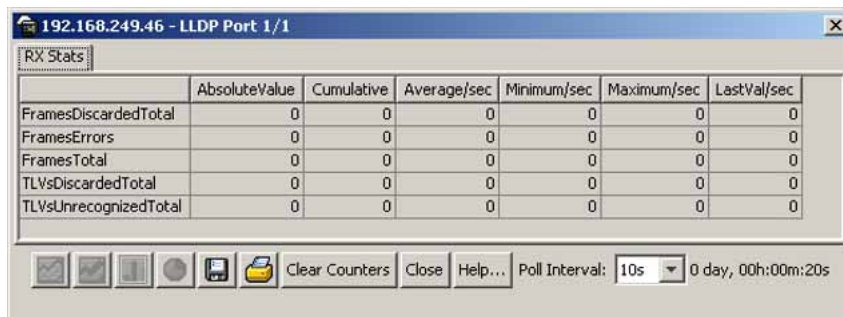
- "Globals tab" (page 269)
- "Port tab" (page 273)
- "TX Stats tab" (page 275)
- "Graphing LLDP transmit statistics" (page 277)
- "Graphing LLDP receive statistics" (page 280)
- "Local System tab" (page 281)
- "Local Port tab" (page 283)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)
- "Unknown TLV tab" (page 290)
- "Organizational Defined Info tab" (page 292)

Graphing LLDP receive statistics

To graph LLDP receive statistics, perform the following procedure.

Step Action

- 1 From the **RX Stats** tab "RX Stats tab" (page 278), select the port for which to display statistics.
- 2 Click **Graph**.
The RX Stats - Graph dialog box appears.



The screenshot shows a window titled "192.168.249.46 - LLDP Port 1/1" with a tab labeled "RX Stats". Inside the window is a table with the following data:

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
FramesDiscardedTotal	0	0	0	0	0	0
FramesErrors	0	0	0	0	0	0
FramesTotal	0	0	0	0	0	0
TLVsDiscardedTotal	0	0	0	0	0	0
TLVsUnrecognizedTotal	0	0	0	0	0	0

Below the table are several icons and buttons: "Clear Counters", "Close", "Help...", and a "Poll Interval" dropdown set to "10s" with a timer showing "0 day, 00h:00m:20s".

- 3 Highlight a data column to graph.
- 4 Click one of the graph buttons.

—End—

See also:

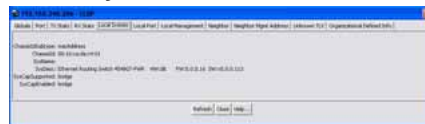
- "Globals tab" (page 269)
- "Port tab" (page 273)
- "TX Stats tab" (page 275)
- "Graphing LLDP transmit statistics" (page 277)
- "RX Stats tab" (page 278)
- "Local System tab" (page 281)
- "Local Port tab" (page 283)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)
- "Unknown TLV tab" (page 290)
- "Organizational Defined Info tab" (page 292)

Local System tab

With the Local System tab, you can view LLDP properties for the local system.

To open the Local System tab, perform the following procedure.

Step	Action
1	From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > LLDP . The LLDP dialog box appears with the Globals tab displayed.
2	Select Local System . The Local System tab appears ("Local System tab" (page 281)).

Local System tab

"Local System tab fields" (page 282) describes the Local System tab fields.

Local System tab fields

Field	Description
ChassisIdSubtype	The type of encoding used to identify the local system chassis: <ul style="list-style-type: none"> • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	The chassis ID.
SysName	The local system name.
SysDesc	The local system description .
SysCapSupported	The system capabilities supported on the local system.
SysCapEnabled	The system capabilities that are enabled on the local system

—End—

See also:

- "Globals tab" (page 269)
- "Port tab" (page 273)
- "TX Stats tab" (page 275)
- "Graphing LLDP transmit statistics" (page 277)
- "RX Stats tab" (page 278)
- "Graphing LLDP receive statistics" (page 280)
- "Local Port tab" (page 283)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)

- "Unknown TLV tab" (page 290)
- "Organizational Defined Info tab" (page 292)

Local Port tab

With the Local Port tab, you can view LLDP port properties for the local system.

To open the Local Port tab, perform the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > LLDP .
The LLDP dialog box appears with the Globals tab displayed. |
| 2 | Click the Local Port tab.
The Local Port tab appears ("Local Port tab" (page 283)). |

Local Port tab

PortNum	PortIdSubtype	PortId	PortDesc
1/1	macAddress	00:11:f9:35:d0:01	Port 1
1/2	macAddress	00:11:f9:35:d0:02	Port 2
1/3	macAddress	00:11:f9:35:d0:03	Port 3
1/4	macAddress	00:11:f9:35:d0:04	Port 4
1/5	macAddress	00:11:f9:35:d0:05	Port 5
1/6	macAddress	00:11:f9:35:d0:06	Port 6
1/7	macAddress	00:11:f9:35:d0:07	Port 7
1/8	macAddress	00:11:f9:35:d0:08	Port 8
1/9	macAddress	00:11:f9:35:d0:09	Port 9
1/10	macAddress	00:11:f9:35:d0:0a	Port 10
1/11	macAddress	00:11:f9:35:d0:0b	Port 11
1/12	macAddress	00:11:f9:35:d0:0c	Port 12
1/13	macAddress	00:11:f9:35:d0:0d	Port 13
1/14	macAddress	00:11:f9:35:d0:0e	Port 14
1/15	macAddress	00:11:f9:35:d0:0f	Port 15
1/16	macAddress	00:11:f9:35:d0:10	Port 16
1/17	macAddress	00:11:f9:35:d0:11	Port 17
1/18	macAddress	00:11:f9:35:d0:12	Port 18
1/19	macAddress	00:11:f9:35:d0:13	Port 19
1/20	macAddress	00:11:f9:35:d0:14	Port 20
1/21	macAddress	00:11:f9:35:d0:15	Port 21
1/22	macAddress	00:11:f9:35:d0:16	Port 22
1/23	macAddress	00:11:f9:35:d0:17	Port 23
1/24	macAddress	00:11:f9:35:d0:18	Port 24

"Local Port tab fields" (page 283) describes the **Local Port** tab fields.

Local Port tab fields

Field	Description
PortNum	Port number.

Field	Description
PortIdSubtype	The type of port identifier encoding used in the associated PortId object. <ul style="list-style-type: none"> • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local.
PortId	The string value used to identify the port component associated with a given port in the local system.
PortDesc	The string value used to identify the 802 LAN station port description associated with the local system. If the local agent supports IETF RFC 2863, the PortDesc object has the same value as the ifDescr object.

—End—

See also:

- "Globals tab" (page 269)
- "Port tab" (page 273)
- "TX Stats tab" (page 275)
- "Graphing LLDP transmit statistics" (page 277)
- "RX Stats tab" (page 278)
- "Graphing LLDP receive statistics" (page 280)
- "Local System tab" (page 281)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)
- "Unknown TLV tab" (page 290)
- "Organizational Defined Info tab" (page 292)

Local Management tab

With the Local Management tab, you can view LLDP management properties for the local system.

To open the Local Management tab, perform the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > LLDP .
The LLDP dialog box appears with the Globals tab displayed. |
| 2 | Click the Local Management tab.
The Local Management tab appears (" Local Management tab " (page 285)). |

Local Management tab



"Local Management tab fields" (page 285) describes the Local Management tab fields.

Local Management tab fields

Field	Description
AddrSubtype	The type of management address identifier encoding used in the associated Addr object.
Addr	The string value used to identify the management address component associated with the local system. This address is used to contact the management entity.
AddrLen	The total length of the management address subtype and the management address fields in LLDPDUs transmitted by the local LLDP agent. The management address length field is needed so that the receiving systems that do not implement SNMP are not required to implement an iana family numbers/address length equivalency table to decode the management address.

Field	Description
AddrIfSubtype	Identifies the numbering method used to define the interface number associated with the remote system. <ul style="list-style-type: none"> unknown ifIndex systemPortNumber
AddrIfId	The integer value used to identify the interface number of the management address component associated with the local system.
AddrOID	The value used to identify the type of hardware component or protocol entity associated with the management address advertised by the local system agent.
AddrPortsTxEnable	Identifies the ports on which the local system management address TLVs are transmitted in the LLPDUs.

—End—

See also:

- ["Globals tab" \(page 269\)](#)
- ["Port tab" \(page 273\)](#)
- ["TX Stats tab" \(page 275\)](#)
- ["Graphing LLDP transmit statistics" \(page 277\)](#)
- ["RX Stats tab" \(page 278\)](#)
- ["Graphing LLDP receive statistics" \(page 280\)](#)
- ["Local System tab" \(page 281\)](#)
- ["Local Port tab" \(page 283\)](#)
- ["Neighbor tab" \(page 286\)](#)
- ["Neighbor Mgmt Address tab" \(page 289\)](#)
- ["Unknown TLV tab" \(page 290\)](#)
- ["Organizational Defined Info tab" \(page 292\)](#)

Neighbor tab

With the Neighbor tab, you can view LLDP properties for the remote system.

To open the Neighbor tab, perform the following procedure.

- | Step | Action |
|------|--|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > LLDP .
The LLDP dialog box appears with the Globals tab displayed. |
| 2 | Click the Neighbor tab.
The Neighbor tab appears (" Neighbor tab " (page 287)). |

Neighbor tab



"[Neighbor tab fields](#)" (page 287) describes the **Neighbor** tab fields.

Neighbor tab fields

Field	Description
TimeMark	The TimeFilter for this entry. See the TimeFilter textual convention in IETF RFC 2021 for details about TimeFilter.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ChassisIdSubtype	The type of encoding used to identify the remote system chassis: <ul style="list-style-type: none"> chassisComponent interfaceAlias portComponent macAddress networkAddress interfaceName local.
ChassisId	Remote chassis ID.

Field	Description
SysCapSupported	Identifies the system capabilities supported on the remote system.
SysCapEnabled	Identifies the system capabilities that are enabled on the remote system.
SysName	Remote system name.
SysDesc	Remote system description.
PortIdSubtype	The type of encoding used to identify the remote port. <ul style="list-style-type: none"> • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local
PortId	Remote port ID.
PortDesc	Remote port description.

—End—

See also:

- ["Globals tab" \(page 269\)](#)
- ["Port tab" \(page 273\)](#)
- ["TX Stats tab" \(page 275\)](#)
- ["Graphing LLDP transmit statistics" \(page 277\)](#)
- ["RX Stats tab" \(page 278\)](#)
- ["Graphing LLDP receive statistics" \(page 280\)](#)
- ["Local System tab" \(page 281\)](#)
- ["Local Port tab" \(page 283\)](#)
- ["Local Management tab" \(page 285\)](#)
- ["Neighbor Mgmt Address tab" \(page 289\)](#)
- ["Unknown TLV tab" \(page 290\)](#)
- ["Organizational Defined Info tab" \(page 292\)](#)

Neighbor Mgmt Address tab

With the Neighbor Mgmt Address tab, you can view LLDP management properties for the remote system.

To open the Neighbor Mgmt Address tab, perform the following procedure.

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > LLDP . |
|---|---|

The LLDP dialog box appears with the Globals tab displayed.

- | | |
|---|---|
| 2 | Click the Neighbor Mgmt Address tab. |
|---|---|

The Neighbor Mgmt Address tab appears ("[Neighbor Mgmt Address tab](#)" (page 289)).

Neighbor Mgmt Address tab



"[Neighbor Mgmt Address tab fields](#)" (page 289) describes the Neighbor Mgmt Address tab fields.

Neighbor Mgmt Address tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	The local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
AddrSubtype	The type of encoding used in the associated Addr object.
Addr	The management address associated with the remote system.

Field	Description
AddrIfSubtype	The numbering method used to define the interface number associated with the remote system. <ul style="list-style-type: none"> unknown ifIndex systemPortNumber
AddrIfId	The integer value used to identify the interface number of the management address component associated with the remote system.
AddrOID	The value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.

—End—

See also:

- ["Globals tab" \(page 269\)](#)
- ["Port tab" \(page 273\)](#)
- ["TX Stats tab" \(page 275\)](#)
- ["Graphing LLDP transmit statistics" \(page 277\)](#)
- ["RX Stats tab" \(page 278\)](#)
- ["Graphing LLDP receive statistics" \(page 280\)](#)
- ["Local System tab" \(page 281\)](#)
- ["Local Port tab" \(page 283\)](#)
- ["Local Management tab" \(page 285\)](#)
- ["Neighbor tab" \(page 286\)](#)
- ["Unknown TLV tab" \(page 290\)](#)
- ["Organizational Defined Info tab" \(page 292\)](#)

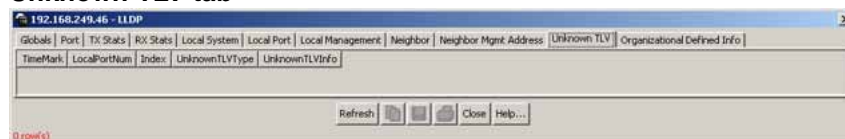
Unknown TLV tab

With the Unknown TLV tab, you can view details about unknown TLVs received on the local system.

To open the Unknown TLV tab, perform the following procedure.

- | Step | Action |
|------|--|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > LLDP .
The LLDP dialog box appears with the Globals tab displayed. |
| 2 | Click the Unknown TLV tab.
The Unknown TLV tab appears (" Unknown TLV tab " (page 291)). |

Unknown TLV tab



"[Unknown TLV tab fields](#)" (page 291) describes the Unknown TLV tab fields.

Unknown TLV tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	The local port which receives the remote system information.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
UnknownTLVType	The value extracted from the type field of the unknown TLV.
UnknownTLVInfo	The value extracted from the value field of the unknown TLV.

—End—

See also:

- "[Globals tab](#)" (page 269)
- "[Port tab](#)" (page 273)
- "[TX Stats tab](#)" (page 275)
- "[Graphing LLDP transmit statistics](#)" (page 277)
- "[RX Stats tab](#)" (page 278)

- "Graphing LLDP receive statistics" (page 280)
- "Local System tab" (page 281)
- "Local Port tab" (page 283)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)
- "Organizational Defined Info tab" (page 292)

Organizational Defined Info tab

With the Organizational Defined Info tab, you can view Organizationally-specific properties for the remote system.

To open the Organizational Defined Info tab, perform the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > LLDP .
The LLDP dialog box appears with the Globals tab displayed. |
| 2 | Click the Organizational Defined Info tab.
The Organizational Defined Info tab appears (" Organizational Defined Info tab " (page 292)). |

Organizational Defined Info tab



"Organizational Defined Info tab fields" (page 292) describes the Organizational Defined Info tab fields.

Organizational Defined Info tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	The local port that receives the remote system information.

Field	Description
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
OrgDefInfoOUI	The Organizationally Unique Identifier, as defined in IEEE 802-2001, is a 24 bit (three octets) globally unique assigned number referenced by various standards, of the information received from the remote system.
OrgDefInfoSubtype	The integer value used to identify the subtype of the organizationally defined information received from the remote system. The subtype value is required to identify different instances of organizationally defined information that cannot be retrieved without a unique identifier that indicates the particular type of information contained in the information string.
OrgDefInfoIndex	This object represents an arbitrary local integer value used by this agent to identify a particular unrecognized organizationally defined information instance, unique only for the OrgDefInfoOUI and lldpRemOrgDefInfoSubtype of the same remote system. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot. It is unlikely that the lldpRemOrgDefInfoIndex will wrap between reboots.
OrdDefInfo	The string value used to identify the organizationally defined information of the remote system. The encoding for this object is the same as that defined for SnmpAdminString TC.

—End—

See also:

- "Globals tab" (page 269)

- "Port tab" (page 273)
- "TX Stats tab" (page 275)
- "Graphing LLDP transmit statistics" (page 277)
- "RX Stats tab" (page 278)
- "Graphing LLDP receive statistics" (page 280)
- "Local System tab" (page 281)
- "Local Port tab" (page 283)
- "Local Management tab" (page 285)
- "Neighbor tab" (page 286)
- "Neighbor Mgmt Address tab" (page 289)
- "Unknown TLV tab" (page 290)

LLDP_Port_dot1 dialog box

You can use the **LLDP_Port_dot1** dialog box to configure and view IEEE 802.1 LLDP information. For more information, see the following sections:

- "Local VLAN Id tab" (page 294)
- "Local Protocol VLAN tab" (page 295)
- "Local VLAN Name tab" (page 297)
- "Local Protocol tab" (page 298)
- "Neighbor VLAN Id tab" (page 300)
- "Neighbor Protocol VLAN tab" (page 301)
- "Neighbor VLAN Name tab" (page 303)
- "Neighbor Protocol tab" (page 304)

Local VLAN Id tab

With the Local VLAN Id tab, you can view LLDP VLAN ID properties for the local system.

To open the Local VLAN Id tab, perform the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port dot1 .
The LLDP_Port_dot1 dialog box appears with the Local VLAN Id tab displayed ("Local VLAN Id tab" (page 295)). |
|---|--|

Local VLAN Id tab

PortNum	VlanId	Local Protocol VLAN	Local VLAN Name	Local Protocol	Neighbor VLAN Id	Neighbor Protocol VLAN	Neighbor VLAN Name	Neighbor Protocol
1/1	1							
1/2	1							
1/3	1							
1/4	1							
1/5	1							
1/6	1							
1/7	1							
1/8	1							
1/9	1							
1/10	1							
1/11	1							
1/12	1							
1/13	1							
1/14	1							

"Local VLAN Id tab fields" (page 295) describes the Local VLAN Id tab fields.

Local VLAN Id tab fields

Field	Description
PortNum	The port number.
VlanId	The local port VLAN ID. A value of zero is used if the system does not know the PVID.

—End—

See also:

- "Local Protocol VLAN tab" (page 295)
- "Local VLAN Name tab" (page 297)
- "Local Protocol tab" (page 298)
- "Neighbor VLAN Id tab" (page 300)
- "Neighbor Protocol VLAN tab" (page 301)
- "Neighbor VLAN Name tab" (page 303)
- "Neighbor Protocol tab" (page 304)

Local Protocol VLAN tab

With the Local Protocol VLAN tab, you can view LLDP Protocol VLAN properties for the local system.

To open the Local Protocol VLAN tab, perform the following procedure.

Step	Action
------	--------

- From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot1**.
The LLDP_Port_dot1 dialog box appears with the Local VLAN Id tab displayed.
- Click the **Local Protocol VLAN** tab.
The Local Protocol VLAN tab appears ("**Local Protocol VLAN tab**" (page 296)).

Local Protocol VLAN tab

PortNum	ProtoVlanId	ProtoVlanSupported	ProtoVlanEnabled	ProtoVlanTxEnable
1/1	1	true	true	false
1/2	1	true	true	false
1/3	1	true	true	false
1/4	1	true	true	false
1/5	1	true	true	false
1/6	1	true	true	false
1/7	1	true	true	false
1/8	1	true	true	false
1/9	1	true	true	false
1/10	1	true	true	false
1/11	1	true	true	false
1/12	1	true	true	false
1/13	1	true	true	false
1/14	1	true	true	false
1/15	1	true	true	false
1/16	1	true	true	false
1/17	1	true	true	false
1/18	1	true	true	false
1/19	1	true	true	false
1/20	1	true	true	false
1/21	1	true	true	false
1/22	1	true	true	false

"Local Protocol VLAN tab fields" (page 296) describes the Local Protocol VLAN tab fields.

Local Protocol VLAN tab fields

Field	Description
PortNum	The port number.
ProtoVlanId	The ID of the port and protocol VLANs associated with the local port. A value of zero is used if the system does not know the protocol VLAN ID (PPVID).
ProtoVlanSupported	Indicate whether the local port supports port and protocol VLANs.
ProtoVlanEnabled	Indicate whether the port and protocol VLANs are enabled on the local port.
ProtoVlanTxEnable	Indicate whether the corresponding local port and protocol VLAN information are transmitted from the port.

—End—

See also:

- "Local VLAN Id tab" (page 294)
- "Local VLAN Name tab" (page 297)
- "Local Protocol tab" (page 298)
- "Neighbor VLAN Id tab" (page 300)
- "Neighbor Protocol VLAN tab" (page 301)
- "Neighbor VLAN Name tab" (page 303)
- "Neighbor Protocol tab" (page 304)

Local VLAN Name tab

With the Local VLAN Name tab, you can view LLDP VLAN Name properties for the local system.

To open the Local VLAN Name tab, perform the following procedure.

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot1**.
The LLDP_Port_dot1 dialog box appears with the Local VLAN Id tab displayed.
- 2 Click the **Local VLAN Name** tab.
The Local VLAN Name tab appears ("Local VLAN Name tab" (page 297)).

Local VLAN Name tab

PortNum	VlanId	VlanName	VlanNameTxEnable
1/1	1	VLAN #1	false
1/2	1	VLAN #1	false
1/3	1	VLAN #1	false
1/4	1	VLAN #1	false
1/5	1	VLAN #1	false
1/6	1	VLAN #1	false
1/7	1	VLAN #1	false
1/8	1	VLAN #1	false
1/9	1	VLAN #1	false
1/10	1	VLAN #1	false
1/11	1	VLAN #1	false
1/12	1	VLAN #1	false
1/13	1	VLAN #1	false
1/14	1	VLAN #1	false
1/15	1	VLAN #1	false
1/16	1	VLAN #1	false
1/17	1	VLAN #1	false
1/18	1	VLAN #1	false
1/19	1	VLAN #1	false
1/20	1	VLAN #1	false
1/21	1	VLAN #1	false
1/22	1	VLAN #1	false
1/23	1	VLAN #1	false

"Local VLAN Name tab fields" (page 298) describes the Local VLAN Name tab fields.

Local VLAN Name tab fields

Field	Description
PortNum	The port number.
VlanId	The integer value used to identify the IEEE 802.1Q VLAN IDs with which the given port is compatible.
VlanName	The string value used to identify the VLAN name identified by the VLAN ID associated with the given port on the local system. This object contains the value of the dot1QVLANStaticName object (defined in IETF RFC 2674) identified with the given lldpXdot1LocVlanId.
VlanNameTxEnable	Indicates whether the corresponding Local System VLAN name instance is transmitted from the port.

—End—

See also:

- "Local VLAN Id tab" (page 294)
- "Local Protocol VLAN tab" (page 295)
- "Local Protocol tab" (page 298)
- "Neighbor VLAN Id tab" (page 300)
- "Neighbor Protocol VLAN tab" (page 301)
- "Neighbor VLAN Name tab" (page 303)
- "Neighbor Protocol tab" (page 304)

Local Protocol tab

With the **Local Protocol** tab, you can view LLDP protocol properties for the local system.

To open the Local Protocol tab, perform the following procedure.

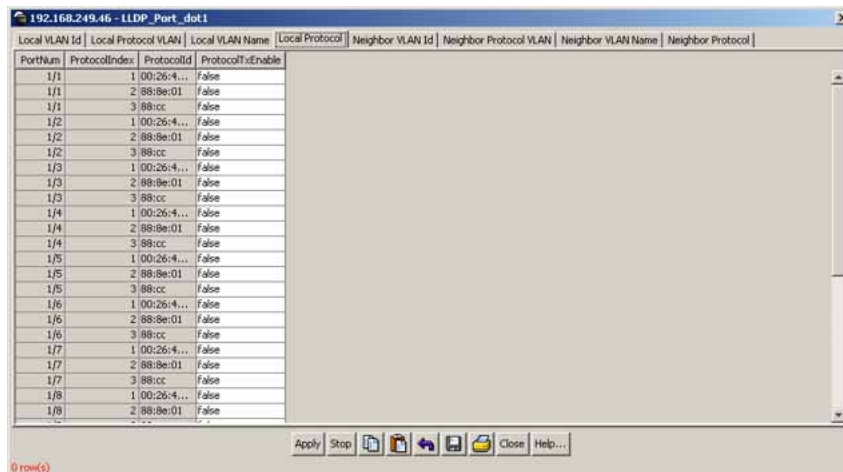
Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot1**.

The LLDP_Port_dot1 dialog box appears with the Local VLAN Id tab displayed.

- 2 Click the **Local Protocol** tab.
The Local Protocol tab appears ("Local Protocol tab" (page 299)).

Local Protocol tab



"Local Protocol tab fields" (page 299) describes the Local Protocol tab fields.

Local Protocol tab fields

Field	Description
PortNum	The port number.
ProtocollIndex	An arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocollId	The octet string value used to identify the protocols associated with the given port of the local system.
ProtocolTxEnable	Indicate whether the corresponding Local System Protocol Identity instance is transmitted on the port.

—End—

See also:

- "Local VLAN Id tab" (page 294)
- "Local Protocol VLAN tab" (page 295)

- "Local VLAN Name tab" (page 297)
- "Neighbor VLAN Id tab" (page 300)
- "Neighbor Protocol VLAN tab" (page 301)
- "Neighbor VLAN Name tab" (page 303)
- "Neighbor Protocol tab" (page 304)

Neighbor VLAN Id tab

With the **Neighbor VLAN Id** tab, you can view LLDP VLAN ID properties for the remote system.

Step Action

To open the **Neighbor VLAN Id** tab:

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot1**.
The LLDP_Port_dot1 dialog box appears with the Local VLAN Id tab displayed.
- 2 Click the **Neighbor VLAN Id** tab.
The Neighbor VLAN Id tab appears ("[Neighbor VLAN Id tab](#)" (page 300)).

Neighbor VLAN Id tab



"[Neighbor VLAN Id tab fields](#)" (page 300) describes the Neighbor VLAN Id tab fields.

Neighbor VLAN Id tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.

Field	Description
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
VlanId	The port VLAN identifier associated with the remote system. If the remote system does not know the PVID or does not support port-based VLAN operation, the value is zero.

—End—

See also:

- ["Local VLAN Id tab" \(page 294\)](#)
- ["Local Protocol VLAN tab" \(page 295\)](#)
- ["Local VLAN Name tab" \(page 297\)](#)
- ["Local Protocol tab" \(page 298\)](#)
- ["Neighbor Protocol VLAN tab" \(page 301\)](#)
- ["Neighbor VLAN Name tab" \(page 303\)](#)
- ["Neighbor Protocol tab" \(page 304\)](#)

Neighbor Protocol VLAN tab

With the Neighbor Protocol VLAN tab, you can view LLDP Protocol VLAN properties for the remote system.

To open the Neighbor Protocol VLAN tab, perform the following procedure.

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot1**.
The LLDP_Port_dot1 dialog box appears with the Local VLAN Id tab displayed.
- 2 Click the **Neighbor Protocol VLAN** tab.
The Neighbor Protocol VLAN tab appears ("[Neighbor Protocol VLAN tab" \(page 302\)](#)").

Neighbor Protocol VLAN tab

"Neighbor Protocol VLAN tab fields" (page 302) describes the Neighbor Protocol VLAN tab fields.

Neighbor Protocol VLAN tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identify the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ProtoVlanId	The ID of the port and protocol VLANs associated with the remote port. A value of zero is used if the system does not know the protocol VLAN ID (PPVID).
ProtoVlanSupported	Indicate whether the remote port supports port and protocol VLANs.
ProtoVlanEnabled	Indicate whether the port and protocol VLANs are enabled on the remote port.

—End—

See also:

- "Local VLAN Id tab" (page 294)
- "Local Protocol VLAN tab" (page 295)
- "Local VLAN Name tab" (page 297)
- "Local Protocol tab" (page 298)
- "Neighbor VLAN Id tab" (page 300)
- "Neighbor VLAN Name tab" (page 303)
- "Neighbor Protocol tab" (page 304)

Neighbor VLAN Name tab

With the Neighbor VLAN Name tab, you can view LLDP VLAN Name properties for the remote system.

To open the Neighbor VLAN Name tab, perform the following procedure.

Step	Action
1	From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port dot1 . The LLDP_Port_dot1 dialog box appears with the Local VLAN ID tab displayed.
2	Click the Neighbor VLAN Name tab. The Neighbor VLAN Name tab appears (" Neighbor VLAN Name tab " (page 303)).

Neighbor VLAN Name tab



"[Neighbor VLAN Name tab fields](#)" (page 303) describes the **Neighbor VLAN Name** tab fields.

Neighbor VLAN Name tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	Identify the local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
VlanId	The integer value used to identify the IEEE 802.1Q VLAN IDs with which the remote port is compatible.
VlanName	The VLAN name identified by the VLAN ID associated with the remote system.

—End—

See also:

- "Local VLAN Id tab" (page 294)
- "Local Protocol VLAN tab" (page 295)
- "Local VLAN Name tab" (page 297)
- "Local Protocol tab" (page 298)
- "Neighbor VLAN Id tab" (page 300)
- "Neighbor Protocol VLAN tab" (page 301)
- "Neighbor Protocol tab" (page 304)

Neighbor Protocol tab

With the Neighbor Protocol tab, you can view LLDP Protocol properties for the remote system.

To open the Neighbor Protocol tab, perform the following procedure.

Step	Action
------	--------

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot1**.
The LLDP_Port_dot1 dialog box appears with the Local VLAN Id tab displayed.
- 2 Click the **Neighbor Protocol** tab.
The Neighbor Protocol tab appears ("[Neighbor Protocol tab](#)" (page 304)).

Neighbor Protocol tab

"[Neighbor Protocol tab fields](#)" (page 304) describes the Neighbor Protocol tab fields.

Neighbor Protocol tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	The local port on which the remote system information is received.

Field	Description
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ProtocolIndex	This object represents an arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocolId	The protocols associated with the remote port.

—End—

See also:

- "Local VLAN Id tab" (page 294)
- "Local Protocol VLAN tab" (page 295)
- "Local VLAN Name tab" (page 297)
- "Local Protocol tab" (page 298)
- "Neighbor VLAN Id tab" (page 300)
- "Neighbor Protocol VLAN tab" (page 301)
- "Neighbor VLAN Name tab" (page 303)

LLDP_Port_dot_3 dialog box

You can use the LLDP_Port_dot3 dialog box to configure and view IEEE 802.3 LLDP information. For more information, see the following tabs:

- "Local Port Auto-negotiation tab" (page 306)
- "Local PoE tab" (page 307)
- "Local Link Aggregate tab" (page 309)
- "Local Max Frame tab" (page 311)
- "Neighbor Port Auto-negotiation tab" (page 312)
- "Neighbor PoE tab" (page 313)
- "Neighbor Link Aggregate tab" (page 315)
- "Neighbor Max Frame tab" (page 317)

Local Port Auto-negotiation tab

With the Local Port Auto-negotiation tab, you can view LLDP auto-negotiation properties for the local system.

To open the Local Port Auto-negotiation tab, perform the following procedure.

Step	Action
------	--------

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot3**.

The LLDP_Port_dot3 dialog box appears with the Local Port Auto-negotiation tab displayed ("[Local Port Auto-negotiation tab](#)" ([page 306](#))).

Local Port Auto-negotiation tab

PortNum	AutoNegSupported	AutoNegEnabled	AutoNegAdvertisedCap	OperMauType
1/1	true			30
1/2	true			30
1/3	true			30
1/4	true			30
1/5	true			30
1/6	true			30
1/7	true			30
1/8	true			30
1/9	true			30
1/10	true			30
1/11	true			30
1/12	true			30
1/13	true			30
1/14	true			30
1/15	true			30
1/16	true			30
1/17	true			30
1/18	true			30
1/19	true			30
1/20	true			30
1/21	true			30
1/22	true			30

"[Local Port Auto-negotiation tab fields](#)" ([page 306](#)) describes the Local Port Auto-negotiation tab fields.

Local Port Auto-negotiation tab fields

Field	Description
PortNum	The port number.
AutoNegSupported	Indicate whether the local port supports Auto-negotiation.
AutoNegEnabled	Indicate whether Auto-negotiation is enabled on the local port.

Field	Description
AutoNegAdvertisedCap	This object contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the local port on the system.
OperMauType	A value that indicates the operational MAU type of the given port on the local system.

—End—

See also:

- "Local PoE tab" (page 307)
- "Local Link Aggregate tab" (page 309)
- "Local Max Frame tab" (page 311)
- "Neighbor Port Auto-negotiation tab" (page 312)
- "Neighbor PoE tab" (page 313)
- "Neighbor Link Aggregate tab" (page 315)
- "Neighbor Max Frame tab" (page 317)

Local PoE tab

With the Local PoE tab, you can view LLDP PoE properties for the local system.

To open the Local PoE tab, perform the following procedure.

Step	Action
1	From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port dot3 . The LLDP_Port_dot3 dialog box appears with the Local Port Auto-negotiation tab displayed.
2	Click the Local PoE tab. The Local PoE tab appears.

Local PoE tab

PortNum	PowerPortClass	PowerMDISupported	PowerMDIEnabled	PowerPairControlable	PowerPairs	PowerClass
1/1 pClassPSE	false	false	false	false	spare	class0
1/2 pClassPSE	false	false	false	false	spare	class0
1/3 pClassPSE	false	false	false	false	spare	class0
1/4 pClassPSE	false	false	false	false	spare	class0
1/5 pClassPSE	false	false	false	false	spare	class0
1/6 pClassPSE	false	false	false	false	spare	class0
1/7 pClassPSE	false	false	false	false	spare	class0
1/8 pClassPSE	false	false	false	false	spare	class0
1/9 pClassPSE	false	false	false	false	spare	class0
1/10 pClassPSE	false	false	false	false	spare	class0
1/11 pClassPSE	false	false	false	false	spare	class0
1/12 pClassPSE	false	false	false	false	spare	class0
1/13 pClassPSE	false	false	false	false	spare	class0
1/14 pClassPSE	false	false	false	false	spare	class0
1/15 pClassPSE	false	false	false	false	spare	class0
1/16 pClassPSE	false	false	false	false	spare	class0
1/17 pClassPSE	false	false	false	false	spare	class0
1/18 pClassPSE	false	false	false	false	spare	class0
1/19 pClassPSE	false	false	false	false	spare	class0
1/20 pClassPSE	false	false	false	false	spare	class0
1/21 pClassPSE	false	false	false	false	spare	class0
1/22 pClassPSE	false	false	false	false	spare	class0
1/23 pClassPSE	false	false	false	false	spare	class0
1/24 pClassPSE	false	false	false	false	spare	class0
1/25 pClassPSE	false	false	false	false	spare	class0

"Local PoE tab fields" (page 308) describes the Local PoE tab fields.

Local PoE tab fields

Field	Description
PortNum	The port number.
PowerPortClass	The port Class of the local port.
PowerMDISupported	Indicate whether MDI power is supported on the local port.
PowerMDIEnabled	Indicate whether MDI power is enabled on the local port.
PowerPairControlable	Derived from the value of the pethPsePortPowerPairsControlAbility object (defined in IETF RFC 3621), this value is used to indicate whether pair selection can be controlled on the local port.
PowerPairs	This object contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the local port: <ul style="list-style-type: none"> • signal • spare
PowerClass	This object contains the value of the pethPsePortPowerClassifications object (defined in IETF RFC 3621) for the local port: <ul style="list-style-type: none"> • class0 • class1

Field	Description
	<ul style="list-style-type: none"> • class2 • class3 • class4

—End—

See also:

- "Local Port Auto-negotiation tab" (page 306)
- "Local Link Aggregate tab" (page 309)
- "Local Max Frame tab" (page 311)
- "Neighbor Port Auto-negotiation tab" (page 312)
- "Neighbor PoE tab" (page 313)
- "Neighbor Link Aggregate tab" (page 315)
- "Neighbor Max Frame tab" (page 317)

Local Link Aggregate tab

With the Local Link Aggregate tab, you can view LLDP link aggregation properties for the local system.

To open the Local Link Aggregate tab, perform the following procedure.

Step	Action
1	From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port dot3 . The LLDP_Port_dot3 dialog box appears with the Local Port Auto-negotiation tab displayed.
2	Click the Local Link Aggregate tab. The Local Link Aggregate tab appears ("Local Link Aggregate" (page 310)).

Local Link Aggregate

PortNum	LinkAggStatus	LinkAggPortId
1/1	0	
1/2	0	
1/3	0	
1/4	0	
1/5	0	
1/6	0	
1/7	0	
1/8	0	
1/9	0	
1/10	0	
1/11	0	
1/12	0	
1/13	0	
1/14	0	
1/15	0	
1/16	0	
1/17	0	
1/18	0	
1/19	0	
1/20	0	
1/21	0	

"Local Link Aggregate tab fields" (page 310) describes the Local Link Aggregate tab fields.

Local Link Aggregate tab fields

Field	Description
PortNum	The port number.
LinkAggStatus	Specify the link aggregation capabilities and the current aggregation status of the link.
LinkAggPortId	Contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component in link aggregation. If the port is not in a link aggregation state or does not support link aggregation, this value is set to zero.

—End—

See also:

- "Local Port Auto-negotiation tab" (page 306)
- "Local PoE tab" (page 307)
- "Local Max Frame tab" (page 311)
- "Neighbor Port Auto-negotiation tab" (page 312)
- "Neighbor PoE tab" (page 313)
- "Neighbor Link Aggregate tab" (page 315)

- "Neighbor Max Frame tab" (page 317)

Local Max Frame tab

With the Local Max Frame tab, you can view LLDP maximum frame size properties for the local system.

To open the Local Max Frame tab, perform the following procedure.

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot3**.
The LLDP_Port_dot3 dialog box appears with the Local Port Auto-negotiation tab displayed.
- 2 Click the **Local Max Frame** tab.
The Local Max Frame tab appears ("Local Max Frame tab" (page 311)).

Local Max Frame tab



"Local Max Frame tab fields" (page 311) describes the Local Max Frame tab fields.

Local Max Frame tab fields

Field	Description
PortNum	The port number.
MaxFrameSize	The maximum frame size for the port.

—End—

See also:

- "Local Port Auto-negotiation tab" (page 306)
- "Local PoE tab" (page 307)
- "Local Link Aggregate tab" (page 309)
- "Neighbor Port Auto-negotiation tab" (page 312)
- "Neighbor PoE tab" (page 313)
- "Neighbor Link Aggregate tab" (page 315)
- "Neighbor Max Frame tab" (page 317)

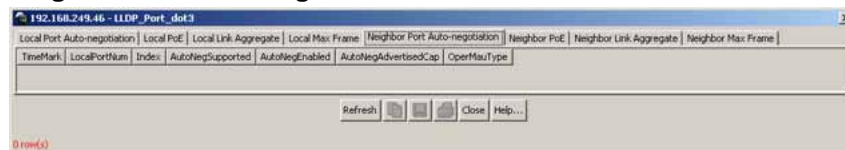
Neighbor Port Auto-negotiation tab

With the Neighbor Port Auto-Negotiation tab, you can view LLDP auto-negotiation properties for the remote system.

To open the Neighbor Port Auto-Negotiation tab, perform the following procedure.

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot3**.
The LLDP_Port_dot3 dialog box appears with the Local Port Auto-negotiation tab displayed.
- 2 Click the **Neighbor Port Auto-negotiation** tab.
The Neighbor Port Auto-negotiation tab appears ("[Neighbor Port Auto-negotiation tab](#)" (page 312)).

Neighbor Port Auto-negotiation tab

"[Neighbor Port Auto-negotiation tab fields](#)" (page 312) describes the Neighbor Port Auto-negotiation tab fields.

Neighbor Port Auto-negotiation tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	The local port on which the remote system information is received.

Field	Description
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
AutoNegSupported	The truth value used to indicate whether the given port (associated with a remote system) supports Auto-negotiation.
AutoNegEnabled	Indicate whether Auto-negotiation is enabled on the remote port.
AutoNegAdvertisedCap	This object contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the remote port.
OperMauType	A value that indicates the operational MAU type of the given port on the remote system.

—End—

See also:

- ["Local Port Auto-negotiation tab" \(page 306\)](#)
- ["Local PoE tab" \(page 307\)](#)
- ["Local Link Aggregate tab" \(page 309\)](#)
- ["Local Max Frame tab" \(page 311\)](#)
- ["Neighbor PoE tab" \(page 313\)](#)
- ["Neighbor Link Aggregate tab" \(page 315\)](#)
- ["Neighbor Max Frame tab" \(page 317\)](#)

Neighbor PoE tab

With the Neighbor PoE tab, you can view LLDP PoE properties for the remote system.

To open the Neighbor PoE tab, perform the following procedure.

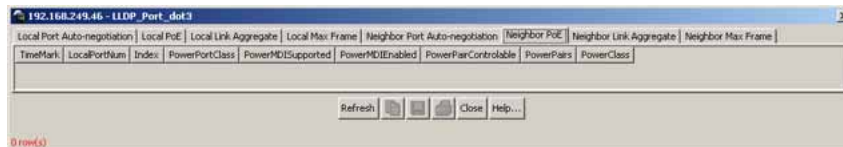
Step	Action
------	--------

- | | |
|----------|--|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port dot3 . |
|----------|--|

The LLDP_Port_dot3 dialog box appears with the Local Port Auto-negotiation tab displayed.

- 2 Click the **Neighbor PoE** tab.
The Neighbor PoE tab appears ("[Neighbor PoE tab](#)" (page 314)).

Neighbor PoE tab



"[Neighbor PoE tab fields](#)" (page 314) describes the Neighbor PoE tab fields.

Neighbor PoE tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	The local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PowerPortClass	The port Class of the remote port.
PowerMDISupported	Indicate whether MDI power is supported on the remote port.
PowerMDIEnabled	Indicate whether MDI power is enabled on the remote port.
PowerPairControlable	Derived from the value of the pethPsePortPowerPairsControlAbility object (defined in IETF RFC 3621), this value is used to indicate whether pair selection can be controlled on the remote port.

Field	Description
PowerPairs	This object contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the remote port. <ul style="list-style-type: none"> • signal • spare
PowerClass	This object contains the value of the pethPsePortPowerClassifications object (defined in IETF RFC 3621) for the remote port. <ul style="list-style-type: none"> • class0 • class1 • class2 • class3 • class4

—End—

See also:

- "Local Port Auto-negotiation tab" (page 306)
- "Local PoE tab" (page 307)
- "Local Link Aggregate tab" (page 309)
- "Local Max Frame tab" (page 311)
- "Neighbor Port Auto-negotiation tab" (page 312)
- "Neighbor Link Aggregate tab" (page 315)
- "Neighbor Max Frame tab" (page 317)

Neighbor Link Aggregate tab

With the Neighbor Link Aggregate tab, you can view LLDP link aggregation properties for the remote system.

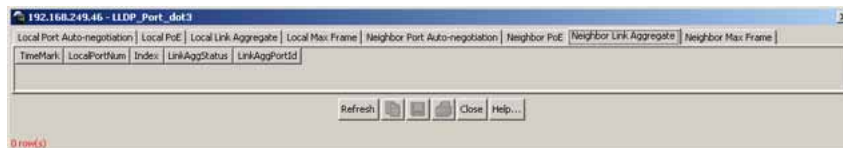
To open the Neighbor Link Aggregate tab, perform the following procedure.

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port dot3**.
The LLDP_Port_dot3 dialog box appears with the Local Port Auto-negotiation tab displayed.

- 2 Click the **Neighbor Link Aggregate** tab.
The Neighbor Link Aggregate tab appears ("Neighbor Link Aggregate tab fields" (page 316)).

Neighbor Link Aggregate tab fields



"Neighbor Link Aggregate tab fields" (page 316) describes the Neighbor Link Aggregate tab fields.

Neighbor Link Aggregate tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	The local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
LinkAggStatus	Specify the link aggregation capabilities and the current aggregation status of the remote link.
LinkAggPortId	Contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component in link aggregation. If the port is not in a link aggregation state or does not support link aggregation, this value is set to zero.

—End—

See also:

- "Local Port Auto-negotiation tab" (page 306)
- "Local PoE tab" (page 307)
- "Local Link Aggregate tab" (page 309)
- "Local Max Frame tab" (page 311)

- "Neighbor Port Auto-negotiation tab" (page 312)
- "Neighbor PoE tab" (page 313)
- "Neighbor Link Aggregate tab" (page 315)
- "Neighbor Max Frame tab" (page 317)

Neighbor Max Frame tab

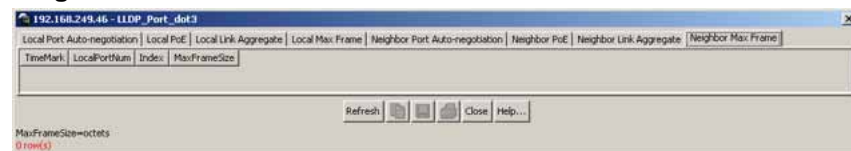
With the Neighbor Max Frame tab, you can view LLDP maximum frame size properties for the remote system.

To open the Neighbor Max Frame tab, perform the following procedure.

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port dot3 .
The LLDP_Port_dot3 dialog box appears with the Local Port Auto-negotiation tab displayed. |
| 2 | Click the Neighbor Max Frame tab.
The Neighbor Max Frame tab appears (" Neighbor Max Frame tab " (page 317)). |

Neighbor Max Frame tab



"[Neighbor Max Frame tab fields](#)" (page 317) describes the Neighbor Max Frame tab fields.

Neighbor Max Frame tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
LocalPortNum	The local port on which the remote system information is received.
Index	An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
MaxFrameSize	The maximum frame size for the remote port.

—End—

See also:

- "Local Port Auto-negotiation tab" (page 306)
- "Local PoE tab" (page 307)
- "Local Link Aggregate tab" (page 309)
- "Local Max Frame tab" (page 311)
- "Neighbor Port Auto-negotiation tab" (page 312)
- "Neighbor PoE tab" (page 313)
- "Neighbor Link Aggregate tab" (page 315)

Nortel Ethernet Routing Switch 4500 Series

Overview — System Configuration

Copyright © 2007, Nortel Networks
All Rights Reserved.

Publication: NN47205-500
Document status: Standard
Document version: 02.01
Document date: 23 February 2007

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

Sourced in Canada and the United States of America

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

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Java is a trademark of Sun Microsystems, Inc.

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

