



Nortel Ethernet Routing Switch 5500 Series

Configuration — System

Document status: Standard
Document version: 03.01
Document date: 27 August 2007

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

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

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

Trademarks

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks. All other products or services may be trademarks, registered trademarks, service marks, or registered service marks of their respective owners. The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice.

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

Revision History

Date Revised	Version	Reason for revision
July 2005	1.00	New document for Software Release 4.2.
June 2006	2.00	Document updated for Software Release 5.0.
June 2006	2.01	Minor revision for Software Release 5.0.
June 2006	2.02	Minor revision for Software Release 5.0.
July 2006	2.03	Minor revision for Software Release 5.0.
August 2007	3.01	Document updated for Software Release 5.1.

4 Revision History

Contents

Preface	11
Nortel Ethernet Routing Switch 5500 Series	12
Related publications	12
How to get help	13
Getting help from the Nortel web site	14
Getting help over the phone from a Nortel Solutions Center	14
Getting help from a specialist using an Express Routing Code	14
Getting help through a Nortel distributor or reseller	14
5500 Series user interfaces	15
Command line interface	15
Accessing the CLI	15
CLI command modes	17
Java Device Manager	20
Obtaining the Java Device Manager	20
Installing the Java Device Manager	21
Starting the Java Device Manager	33
Configuring Device Manager properties	34
Opening a Switch with the Java Device Manager	39
Device Manager interface components	41
Shortcut menus	46
Status bar	48
Using the buttons in Device Manager screens	48
Editing objects	48
Telneting to a switch	54
Opening an SSH connection to the switch	54
Trap log	55
Accessing the Web-based Management Interface	55
Device Manager Online Help	55
Web-based Management Interface	56
Accessing the Web-based Management Interface	56
Web-based Management Interface layout	57
Basic configuration tasks	65
Feature licensing	66

Demo license	66
Working with feature license files using the CLI	67
Copying the license file using the Java Device Manager	68
Factory default configuration	69
Setting user access limitations	75
Setting user access limitations using the CLI	75
Setting user access limitations using the Web-based Management Interface	79
Updating switch software	85
Changing switch software in the CLI	86
Changing switch software in the Java Device Manager	88
Changing switch software in the Web-based Management Interface	91
LED activity during software download	94
Setting TFTP parameters	94
Setting a default TFTP server	94
Displaying the default TFTP server	94
Clearing the default TFTP server	95
Working with configuration files	95
Configuration files in the CLI	95
Configuration files in the JDM	97
Configuration files in the Web-based Management Interface	102
Automatically downloading a configuration file	107
Terminal setup	109
Setting the default management interface	109
Setting Telnet access	110
telnet-access command	110
no telnet-access command	111
default telnet-access command	112
Setting server for Web-based management	112
web-server command	112
no web-server command	113
Setting boot parameters	113
boot command	113
Defaulting to BootP-when-needed	114
Configuring with the command line interface	114
Configuring and enabling DHCP	115
ip dhcpc server command	115
no ip dhcpc server command	116
show ip dhcpc command	116
Customizing the CLI banner	117
show banner command	117
banner command	118
no banner command	118
Displaying complete GBIC information	121

Displaying hardware information	121
Shutdown command	121
CLI Help	122
<hr/>	
About the Nortel Ethernet Routing Switch 5500 Series	123
Hardware features	123
Nortel Ethernet Routing Switch 5510	123
Nortel Ethernet Routing Switch 5520	124
User interface button	124
Cooling fans	130
Redundant power supply and uninterruptible power supply	130
DC-DC Converter Module	131
Stacking capabilities	131
Auto Unit Replacement	132
AUR function	133
Configuring AUR using the CLI	139
Configuring AUR using Device Manager	140
Agent Auto Unit Replacement (AAUR)	141
Features of the Nortel Ethernet Routing Switch 5500 Series	142
Flash memory storage	143
Policy-enabled networking	144
Power over Ethernet	144
Virtual Local Area Networks	144
Spanning Tree Protocol groups	145
Rapid Spanning Tree Protocol	146
Multiple Spanning Tree Protocol	146
Trunk groups	147
Security	147
Port mirroring	148
Auto-MDI X	148
Auto-polarity	149
Autosensing and autonegotiation	149
ASCII configuration file	153
Displaying unit uptime	155
Port naming	155
Port error summary	155
IP address for each unit in a stack	156
BootP mode	156
Dynamic Host Configuration Protocol (DHCP)	156
Web quick start	157
Simple Network Time Protocol	157
Supported standards and RFCs	158
Standards	158
RFCs	159

Power over Ethernet	161
PoE overview	162
Port power priority	163
External power source	164
Stacking	164
Power pairs	164
Power availability	165
Internal power source only option	165
External power source only option	166
Power sharing option	167
Power Supply Unit (PSU) option	168
Diagnosing and correcting PoE problems	169
Messages	169
Connecting the PSU	169
Power management	171
Configuring PoE using the CLI	172
Set port power enable or disable	172
Set port power priority	173
Set power limit for channels	173
Set traps control	174
Show main power status	174
Set power usage threshold	174
Setting PoE detection method	175
Show port power status	175
Show port power measurement	175
Viewing PoE ports using the JDM	175
Configuring PoE using the JDM	176
Configuring PoE using the Web-based Management Interface	176
Configuring power management on the switch	177
Configuring power management for the ports	178

Switch administration tasks	183
General switch administration using the CLI	183
Multiple switch configurations	184
New Unit Quick Configuration	185
IP blocking	186
Assigning and clearing IP addresses	187
Assigning and clearing IP addresses for specific units	190
Displaying interfaces	192
Setting port speed	192
Testing cables with the Time Domain Reflectometer	195
Enabling Autotopology	196
Enabling flow control	198

Enabling rate-limiting	200
Using Simple Network Time Protocol	202
Real time clock configuration	207
Custom Autonegotiation Advertisements	209
Connecting to Another Switch	210
Domain Name Server (DNS) Configuration	212
General Switch Administration using the Web-based Management Interface	214
Viewing stack information	214
Viewing summary switch information	216
Changing stack numbering	218
Identifying unit numbers	220
Configuring BootP, DHCP, IP, and gateway settings	220
Modifying system settings	230
Managing remote access by IP address	231
Configuring the Real-Time Clock	234
General Switch Administration using the JDM	235
Viewing Unit information	235
Viewing SFP GBIC ports	236
Editing the chassis configuration	236
Editing and viewing switch ports	250
Editing and viewing switch PoE configurations	262
Editing Bridging Information	265
Configuring SNTP	270
Configuring local time zone	272
Configuring daylight savings time	273
Viewing topology information using Device Manager	274
Topology tab	275
Topology Table tab	275
Link Layer Discovery Protocol (802.1ab)	279
Link Layer Discover Protocol (IEEE 802.1ab) Overview	279
LLDP operational modes	280
Connectivity and management information	280
Configuring LLDP using the CLI	284
lldp command	285
lldp port command	285
lldp tx-tlv command	286
lldp tx-tlv dot1 command	286
lldp tx-tlv dot3 command	287
lldp tx-tlv med command	287
lldp location-identification coordinate-base command	288
lldp location-identification civic-address command	289
lldp location-identification ecs-elin command	290
default lldp command	290

- default lldp port command 291
- default lldp tx-tlv command 292
- default lldp tx-tlv dot1 command 292
- default lldp tx-tlv dot3 command 293
- default lldp tx-tlv med command 293
- no lldp port command 294
- no lldp tx-tlv command 294
- no lldp tx-tlv dot1 command 294
- no lldp tx-tlv dot3 command 295
- no lldp tx-tlv med command 295
- show lldp command 295
- show lldp port command 297
- Configuring LLDP using Device Manager 304
 - Viewing and configuring LLDP global and transmit properties 304
 - LLDP_Port_dot1 dialog box 331
 - LLDP_Port_dot_3 dialog box 342
 - LLDP_Port_med dialog box 354

Index

Preface

This guide provides information and instructions about the basic system configuration on the Nortel* Ethernet Routing Switch 5500 Series. Please consult any documentation included with the switch and the product release notes (see "[Related publications](#)" (page 12)) for any errata before beginning the configuration process.

The topics listed in "[Related topics](#)" (page 11) are related to the system configuration process but are not covered in depth in this book. Consult the book listed for specific information about that topic.

Related topics

Topic	Book
Switch security	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Security</i> (NN47200-501)
VLANs	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and Link Aggregation</i> (NN47200-502)
Spanning Trees and Spanning Tree Groups	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and Link Aggregation</i> (NN47200-502)
MultiLink Trunking	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and Link Aggregation</i> (NN47200-502)
IP Routing	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols</i> (NN47200-503)
Quality of Service	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service</i> (NN47200-504)
IP Filtering	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Security</i> (NN47200-501)
IPFIX	<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Monitoring</i> (NN47200-505)

Nortel Ethernet Routing Switch 5500 Series

"5500 Series Switch platforms" (page 12) outlines the switches that are part of the 5500 Series of Nortel Ethernet Routing Switches

5500 Series Switch platforms

5500 Series Switch Model	Key Features
Nortel Ethernet Routing Switch 5510-24T	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5510-48T	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5520-24T-PWR	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5520-48T-PWR	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5530-24TFD	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains twelve shared SFP ports and two XFP ports.

Related publications

For more information about the management, configuration, and usage of the Nortel Ethernet Routing Switch 5500 Series, refer to the publications listed in "[Nortel Ethernet Routing Switch 5500 Series documentation](#)" (page 12).

Nortel Ethernet Routing Switch 5500 Series documentation

Title	Description	Part Number
<i>Nortel Ethernet Routing Switch 5500 Series Installation</i>	Instructions for the installation of a switch in the Nortel Ethernet Routing Switch 5500 Series. It also provides an overview of hardware key to the installation, configuration, and maintenance of the switch.	NN47200-300
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — System</i>	Instructions for the general configuration of switches in the 5500 Series that are not covered by the other documentation.	NN47200-500

Title	Description	Part Number
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Security</i>	Instructions for the configuration and management of security for switches in the 5500 Series.	NN47200-501
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and Link Aggregation</i>	Instructions for the configuration of spanning and trunking protocols on 5500 Series switches.	NN47200-502
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — IP Routing Protocols</i>	Instructions for the configuration of IP routing protocols on 5500 Series switches.	NN47200-503
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service</i>	Instructions for the configuration and implementation of QoS on 5500 Series switches.	NN47200-504
<i>Nortel Ethernet Routing Switch 5500 Series Configuration — System Monitoring</i>	Instructions for the configuration, implementation, and use of system monitoring and IPFIX on 5500 Series switches.	NN47200-505
<i>Nortel Ethernet Routing Switch 5500 Series Release Notes — Software Release 5.0</i>	Provides an overview of new features, fixes, and limitations of the 5500 Series switches. Also included are any supplementary documentation and document errata.	NN47200-400
<i>Installing the Nortel Ethernet Redundant Power Supply Unit 15</i>	Instructions for the installation and use of the Nortel Ethernet RPSU 15.	217070-A
<i>DC-DC Converter Module for the Baystack 5000 Series Switch</i>	Instructions for the installation and use of the DC-DC power converter.	215081-A
<i>Nortel Ethernet Routing Switch 5500 Series Installation — SFP</i>	Instructions for the installation and use of small form-factor pluggable transceivers and gigabit interface converters.	318034-C

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.

5500 Series user interfaces

The 5500 Series of the Nortel Ethernet Routing Switch provides three distinct user interfaces that the switch administrator can use to perform switch configuration. This chapter provides an introduction to each user interface, how it is used, and instructions for installation if applicable.

This chapter contains the following topics:

- ["Command line interface" \(page 15\)](#)
- ["Java Device Manager" \(page 20\)](#)
- ["Web-based Management Interface" \(page 56\)](#)

Command line interface

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

The following sections highlight the CLI as the primary means of using the textual configuration interface in the 5500 Series switches:

- ["Accessing the CLI" \(page 15\)](#)
- ["CLI command modes" \(page 17\)](#)

Accessing the CLI

The command line interface is accessed through either a direct console connection to the switch or by using the Telnet protocol to connect to the switch remotely.

To connect to the CLI, follow this procedure:

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

- | | |
|---|---|
| 1 | Connect to the switch through either an appropriate Telnet application or by connecting a console cable to the console port on the switch and using a terminal emulation program to initiate communication. |
|---|---|

- 4 From the Command Line Interface main menu illustrated in "[CLI Main Menu](#)" (page 17), press **c** or select the menu item **Command Line Interface** and press **Enter** to access the CLI.

CLI Main Menu

```

Ethernet Routing Switch 5530-24TFD Main Menu

IP Configuration/Setup...
SNMP Configuration...
System Characteristics...
Switch Configuration...
Console/Comm Port Configuration...
Display Hardware Units...
Spanning Tree Configuration...
TELNET/SNMP/Web Access Configuration...
Software Download...
Configuration File...
Display System Log...
Reset...
Reset to Default Settings...
Shutdown Command...
Command Line Interface...
Logout...

Use arrow keys to highlight option, press <Return> or <Enter> to select option.

```

Depending on whether the switch is in a stand-alone or stacked configuration, the menu illustrated in "[CLI Main Menu](#)" (page 17) may change. For this procedure, the menu displayed is for a switch in stand-alone configuration. Whether the switch is in one configuration or another does not affect how you access the CLI.

- 5 The CLI prompt is now displayed.

—End—

CLI command modes

The CLI has four different command modes based on the level of permissions a particular user has when logging in to the switch. This level of permission is determined by the password used at login. The five command modes 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 the switch is first turned on and provides a limited subset of CLI commands. This mode is the most restrictive CLI mode and has few commands available.

- **Privileged EXEC Mode**

The Privileged EXEC mode (also referred to as *privExec* mode) enables the user to perform basic switch-level management tasks, such as downloading software images, setting passwords, and booting the switch. *privExec* is an unrestricted mode that allows you to view all settings on the switch, and if you are logged in with write access, it also allows you to access all configuration modes and commands that affect operation of the switch (such as downloading images, rebooting, etc.).

- **Global Configuration Mode**

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

- **Interface Configuration Mode**

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

- **Router Configuration Mode**

The Router Configuration mode (also referred to as *config-router* mode) enables the user to configure routing parameters for RIP, OSPF, and VRRP.

It is possible to move between command modes on a limited basis. You must use the Global Configuration mode to move to another mode. The following rules apply when moving between command modes:

- It is possible to move from User EXEC mode to Privileged EXEC mode by using the **enable** command at the command prompt.
- If a user is currently in Privileged EXEC mode, it is possible to move into Global Configuration mode using the **configure** command. The user enters the Interface Configuration by entering the **interface fastethernet <port number>** command to configure a port, or **interface vlan <vlan number>** command to configure a VLAN.
- From the Global Configuration mode, the user can enter the Router Configuration Mode by entering one of the following commands

```
— router rip
— router ospf
— router vrrp
```

"[Command Mode prompts and Usage Commands](#)" (page 19) lists the four command modes, the prompt particular to each, and the CLI commands used to enter and exit the different modes. Each switch displays a prompt

specific to the switch type. In "[Command Mode prompts and Usage Commands](#)" (page 19), the prompts displayed are for a Nortel Ethernet Routing Switch 5530-24TFD.

Command Mode prompts and Usage Commands

Command Mode	CLI Prompt	Entrance and Exit Commands
User EXEC (exec)	5530-24TFD>	This is the default command mode and does not require an entrance command. To exit the CLI, type the exit or logout command.
Privileged EXEC (privExec)	5530-24TFD#	To enter this command mode from User EXEC mode, type the enable command. To exit the CLI, type the exit or logout command.
Global Configuration (config)	5530-24TFD(config)#	To enter this command mode, from Privileged EXEC mode type the configure command. To exit the CLI completely, type the logout command. To return to Privileged EXEC mode, use the end or exit commands.
Interface Configuration (config-if)	5530-24TFD(config-if)#	Entry into this command mode is dependent on the type of interface being configured. Use the interface fastethernet <port number> command to enter this mode to configure a port, and the interface vlan <vlan number> command to enter this mode to configure a VLAN. To exit the CLI completely, use the logout command. To return to Global Configuration mode, use the exit command. To return to Privileged EXEC mode, use the end command.
Router Configuration (config-router)	5530-24TFD(config-router)#	Entry into this command mode is dependent on the protocol being configured. Use the router rip command to enter this mode to configure RIP, the router ospf command to enter this mode to configure OSPF, and the router vrrp command to enter this mode to configure VRRP. To exit the CLI completely, use the logout command. To return to Global Configuration

Command Mode	CLI Prompt	Entrance and Exit Commands
		mode, use the <code>exit</code> command. To return to Privileged EXEC mode, use the <code>end</code> command.

Java Device Manager

The Java Device Manager (JDM) is a graphical user interface 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, all switch configuration tasks can be performed.

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 wishing to access a Nortel Ethernet Routing Switch 5500 Series through the JDM must install the application on an appropriate computer.

This section contains the following topics:

- "Obtaining the Java Device Manager" (page 20)
- "Installing the Java Device Manager" (page 21)
- "Starting the Java Device Manager" (page 33)
- "Configuring Device Manager properties" (page 34)
- "Opening a Switch with the Java Device Manager" (page 39)
- "Device Manager interface components" (page 41)

Obtaining the Java Device Manager

If the JDM is not already installed on the computer to be used for switch management, it may be obtained through a download from the Nortel web site.

To obtain the JDM, follow this procedure:

Step	Action
1	Open a new web browser window and type http://www.nortel.com/support in the Address area.
2	If the Browse product support tab is not already selected, click on it.
3	From the list provided in the product family box, select Nortel Ethernet Routing Switch .

- 4 From the product list, select the family of Nortel Ethernet Routing Switch that the JDM will be used to connect to.
- 5 From the content list, select **Software**.
- 6 Click **Go**.
- 7 The resulting list displays all software associated with the switch family that was selected in descending chronological order. Select the latest version of the JDM software in the list (the version that appears first in the list) by clicking on the associated link.
- 8 The screen displayed lists the version of software specific to each operating system environment. Select the operating system environment running on the computer selected for switch administration by clicking on the associated link.
- 9 A screen appears, prompting the user to either open the file or save it to a location on the local file system. Save the file to the local file system.
- 10 File download now commences. After the download is complete, refer to "[Installing the Java Device Manager](#)" (page 21) for procedures on installing the software.

—End—

Installing the Java Device Manager

After obtaining the latest version of the JDM, it must be installed 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 21)
- "[Installing the JDM in a UNIX Environment](#)" (page 27)

Before beginning the installation procedure in any operating system environment, ensure that all previous versions of the software have been uninstalled and that the new version of the application is installed to 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:

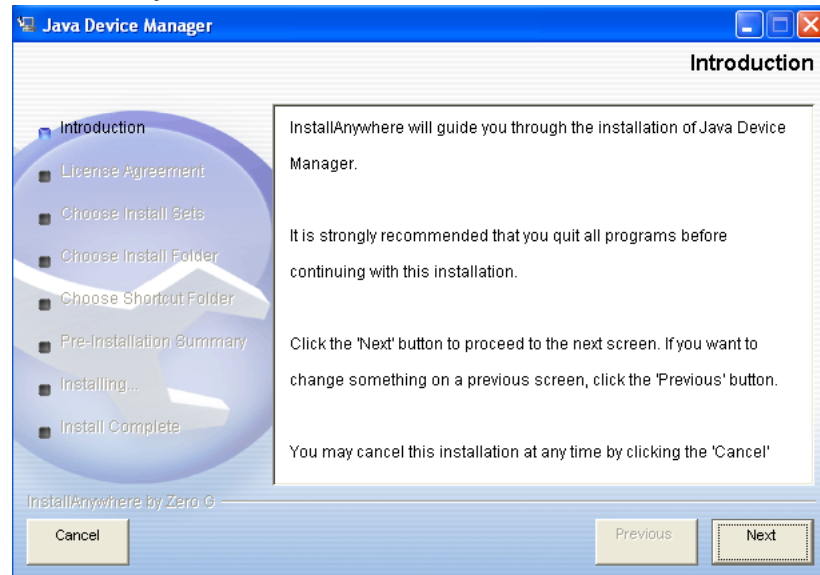
- **Operating System Version**

- Windows NT, Windows 95, Windows 98, Windows 2000, Windows XP, Windows 2003, or Windows Vista
- **CPU Requirements**
 - Pentium II 350 MHz or above
- **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, follow this procedure:

Step	Action
1	Close all programs.
2	Locate the downloaded executable file on the local computer.
3	Double-click the executable <code>jdm_XXX.exe</code> 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 now loads. When the program is ready to proceed with the installation, a screen similar to the one illustrated in " Introductory Windows installation screen " (page 23) is displayed. Follow all instructions on this screen before proceeding with the installation. Click Next when ready.

Introductory Windows installation screen



- 5 The next screen requests acceptance of the license agreement that governs the JDM software. Acceptance of this license agreement is mandatory for installation of the JDM. Read the license agreement fully and indicate acceptance by selecting the option button labeled **I accept the terms of the License Agreement**. To proceed, click **Next**. "Windows License Agreement screen" (page 23) illustrates an example of this screen.

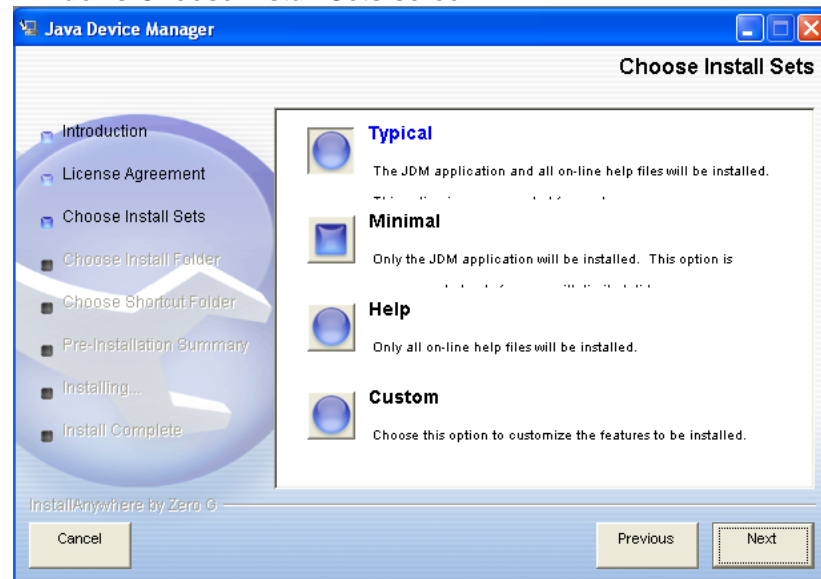
Windows License Agreement screen



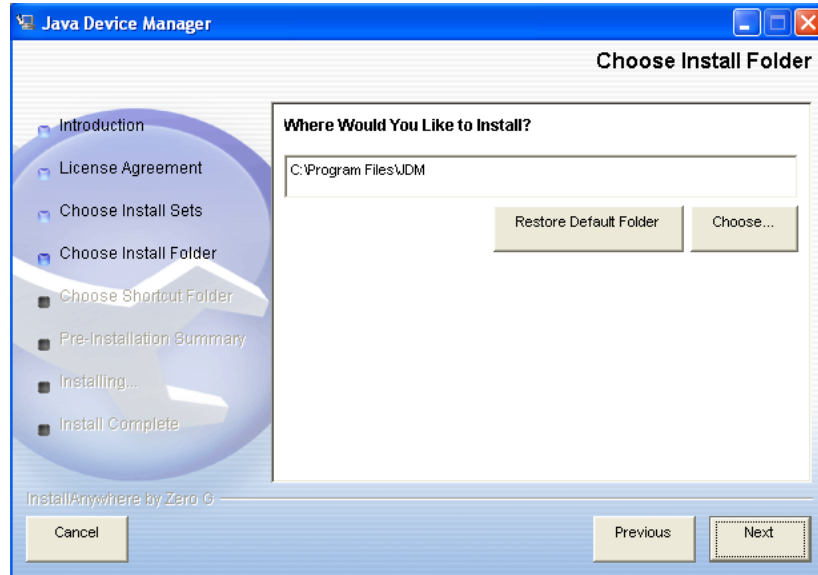
- 6 After accepting the license agreement, the next screen (shown in "[Windows Choose Install Sets screen](#)" ([page 24](#))) prompts for an installation set. Although four options are present, Nortel recommends selecting the **Typical** option, as this ensures all application components are installed. If a more specialized installation is required, select one of the other options. The four options are as follows:
- **Typical** -- All software components and online Help is installed.
 - **Minimal** -- Installs only the software. Online Help is not installed.
 - **Help** -- Installs the online Help files only.
 - **Custom** -- enables the selection of software components and online Help to be installed.

Click **Next** to proceed.

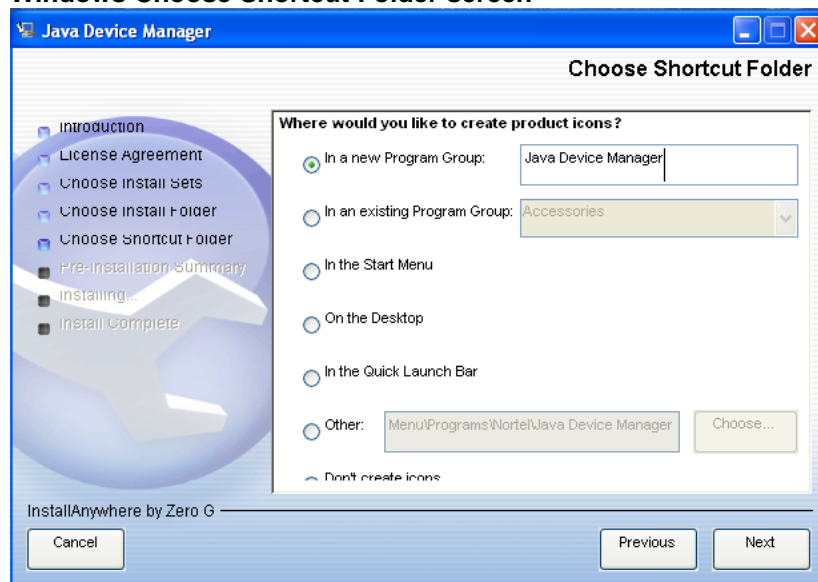
Windows Choose Install Sets screen



- 7 On the next screen (shown in "[Windows Choose Install Folder screen](#)" ([page 25](#))), 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.

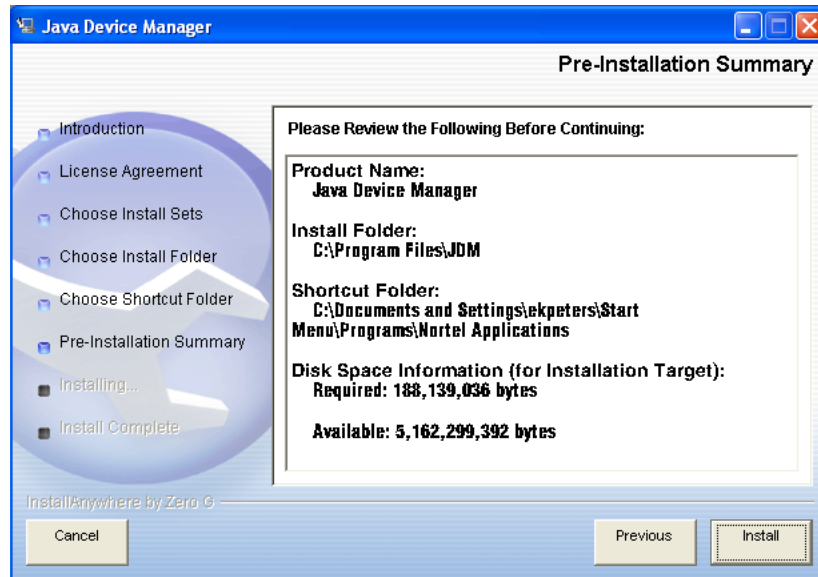
Windows Choose Install Folder screen

- 8 On the screen pictured in "[Windows Choose Shortcut Folder screen](#)" ([page 25](#)), select a location for the placement of icons in the Start menu. After making this selection, click **Next** to proceed.

Windows Choose Shortcut Folder screen

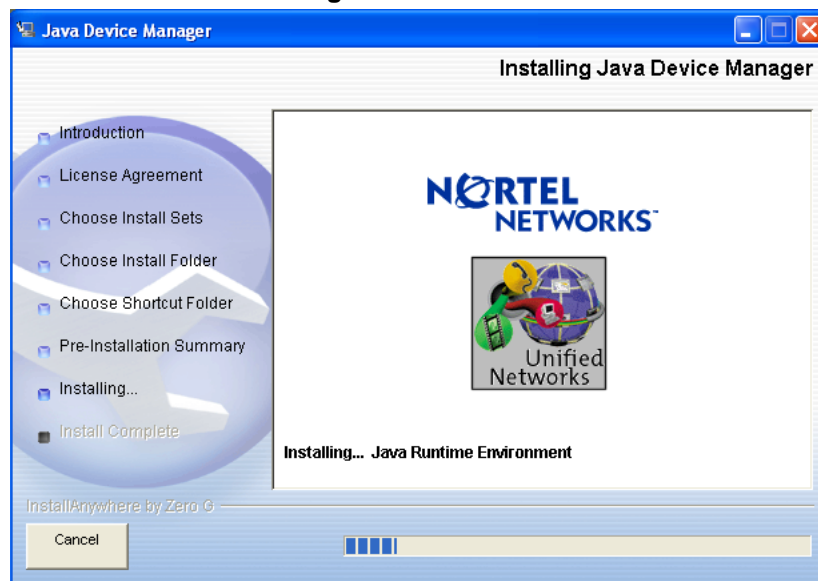
- 9 Confirm the previous selections on the Pre-Installation Summary screen ("[Windows Pre-Installation Summary screen](#)" ([page 26](#))). If all selections are accurate, click **Install** to begin installing the JDM to the local computer. If changes are necessary, click **Previous** to return to the screens in question.

Windows Pre-Installation Summary screen

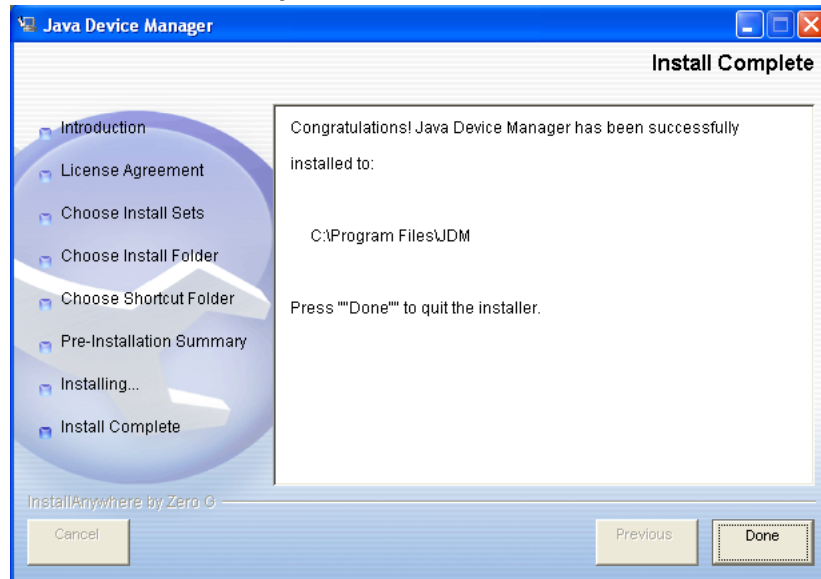


- 10 During the installation process, the screen illustrated in "Windows Installation Progress screen" (page 26) is displayed to show the progress of the installation.

Windows Installation Progress screen



- 11 When the installation process is finished, the screen displayed in "Windows Install Complete screen" (page 27) is shown. Click **Done** to complete the installation process.

Windows Install Complete screen

—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 2.8.x (or higher) or Linux Kernel 2.2 (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 the JDM is being installed uses the Sun Solaris operating system, refer to the section "[Installing Solaris Patches](#)" (page 32) before beginning the installation process. 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 process. Depending on the UNIX operating system in use, the file name takes one of three forms. "UNIX JDM installation files" (page 28) outlines the form each file name takes.

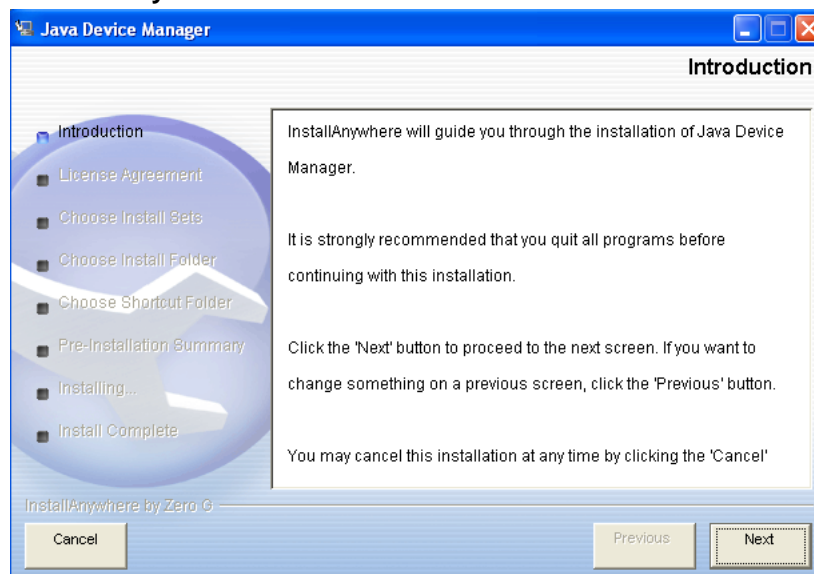
UNIX JDM installation files

Operating System	File Name
Sun Solaris	jdm_XXXX_solaris_sparc.sh
Linux	jdm_XXXX_linux.sh

In the downloaded file, XXXX in the table is substituted with the version number of the JDM being downloaded.

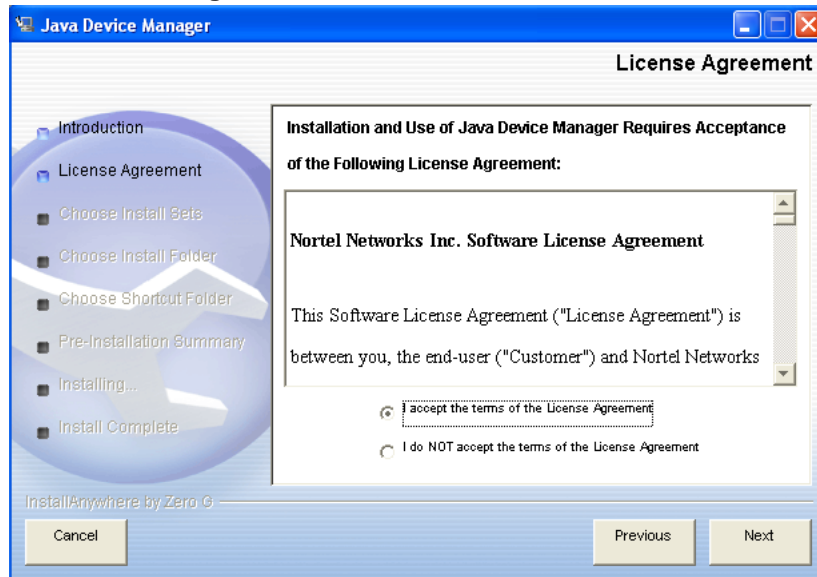
- 4 The installation program now loads. When the program is ready to proceed with the installation, a screen similar to the one illustrated in "Introductory UNIX installation screen" (page 28) is displayed. Follow all instructions on this screen before proceeding with the installation. Click **Next** when ready.

Introductory UNIX installation screen



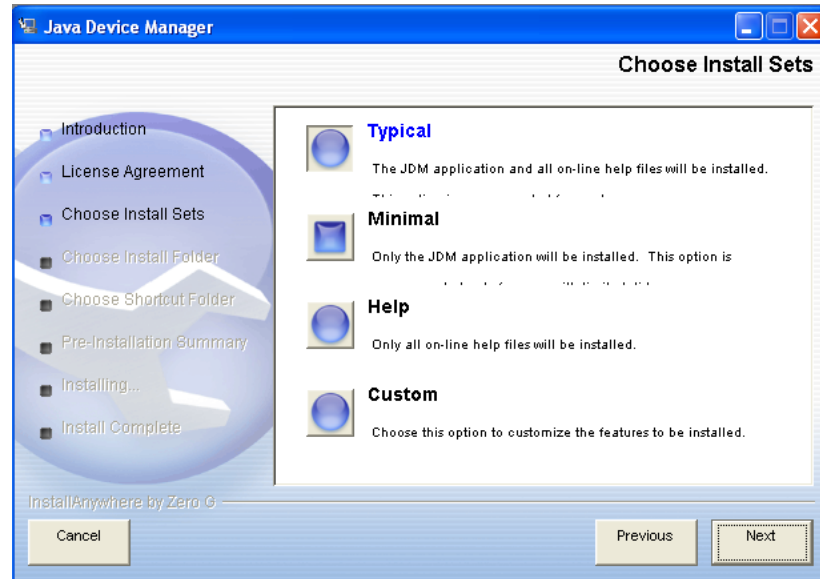
- 5 The next screen requests acceptance of the license agreement that governs the JDM software. Acceptance of this software license is mandatory for installation of the JDM. Read the license agreement fully and indicate acceptance by selecting the option button labeled **I accept the terms of the License Agreement**. To proceed, click **Next**. "UNIX License Agreement screen" (page 29) illustrates an example of this screen.

UNIX License Agreement screen

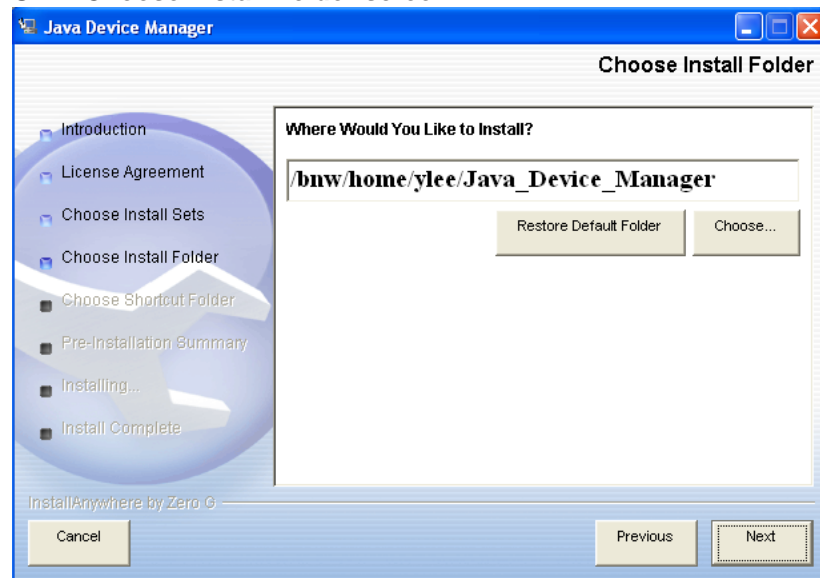


- 6 After accepting the license agreement, the next screen (shown in "UNIX Choose Install Sets screen" (page 30)) prompts for an installation set. Although four options are present, Nortel recommends selecting the **Typical** option, as this ensures all application components are installed. If a more specialized installation is required, select one of the other options. The four options are as follows:
- **Typical** -- All software components and online Help is installed.
 - **Minimal** -- Installs only the software. Online Help is not installed.
 - **Help** -- Installs the online Help files only.
 - **Custom** -- enables the selection of software components and online Help to be installed.

Click **Next** to proceed.

UNIX Choose Install Sets screen

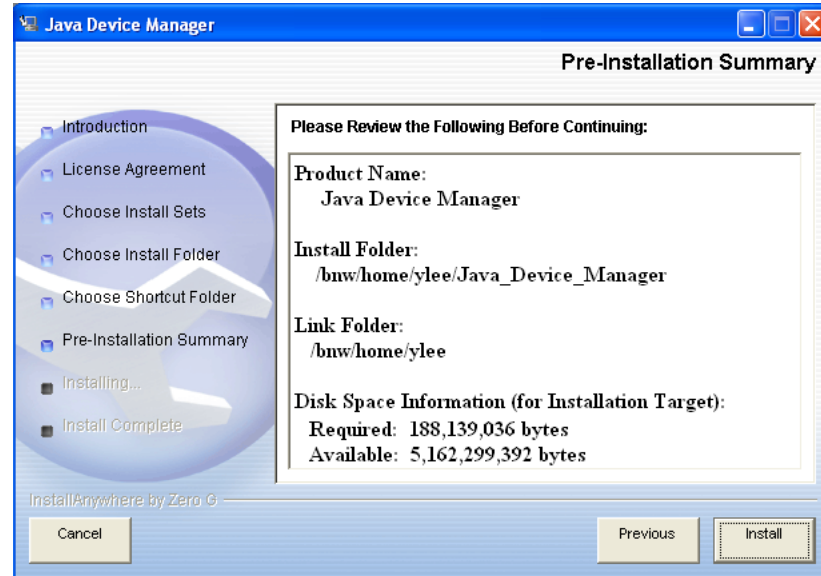
- 7 On the next screen (shown in "UNIX Choose Install Folder screen" (page 30)), type a location on the local file system to install the JDM, or select a location by clicking **Choose**. Click **Restore Folder Default** to restore the default installation location at any time. Click **Next** to proceed.

UNIX Choose Install Folder screen

- 8 Confirm the previous selections on the Pre-Installation Summary Screen (shown in "UNIX Pre-Installation Summary screen" (page 31)). If all selections are accurate, click **Install** to begin installing the

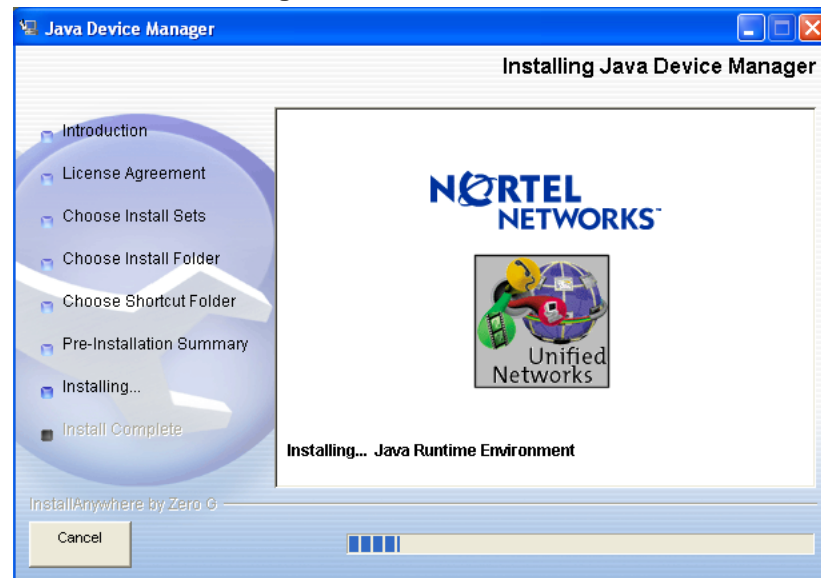
JDM to the local computer. If changes are necessary, click **Previous** to return to the screens in question.

UNIX Pre-Installation Summary screen

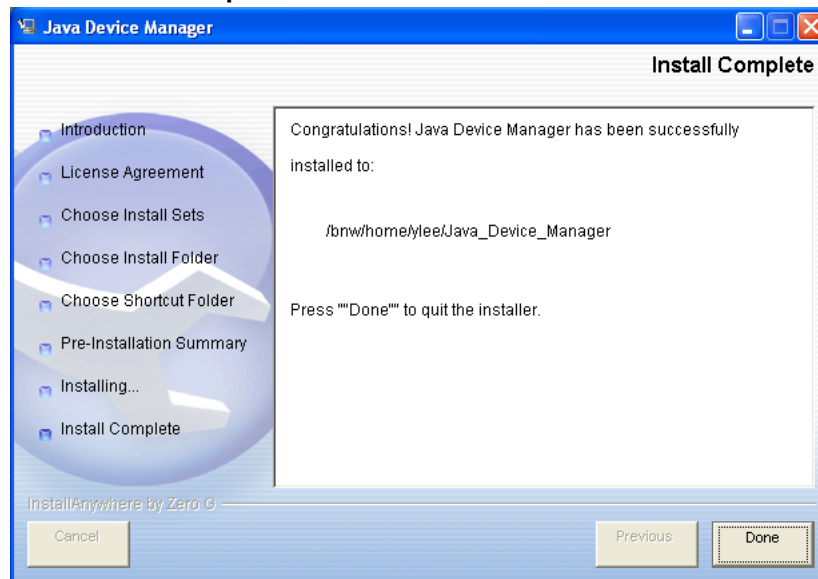


- 9 During the installation process, the screen illustrated in "UNIX Installation Progress screen" (page 31) is displayed to show the progress of the installation.

UNIX Installation Progress screen



- 10 When the installation process is finished, the screen displayed in "UNIX Install Complete screen" (page 32) is shown. Click **Done** to complete the installation process.

UNIX Install Complete screen

—End—

Installing Solaris Patches For SPARC versions 5.8, 5.9, and 5.10, it is necessary to install operating system patches for Sun Solaris before beginning the installation of the JDM. Consult the system administrator or a network technician if it is not known whether these patches are installed on the workstation being used. These patches only need to be applied to the workstation once.

To proceed with patch installation, follow this procedure:

Step Action

- 1 Use the `uname -a` command on the Solaris workstation to determine the version of Solaris that is installed.
- 2 Open a new web browser window and type `http://sunsolve.sun.com` 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 for executing the JDM is dependent on the operating system environment in which it was installed. "JDM execution options" (page 33) outlines 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 the installation defaults were selected, from the Windows taskbar select Start > Programs > Nortel > Java Device Manager > DM. • Otherwise, select the menu options 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 enables the execution of the JDM from any directory on the computer. Consult the operating system documentation for the steps to complete this process.

After the JDM is successfully started, the JDM main window ("JDM main window" (page 33)) is displayed.

JDM main window



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

- Before you access a device, select **Device > Properties > Current**.
- After you access a device, select **Device > Properties > Devices**.

Configuring Device Manager properties

Device Manager uses the Simple Network Management Protocol (SNMP) to configure and manage Ethernet Routing Switch 5500 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.

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.

Setting the Device Manager properties before accessing a device

To set the Device Manager properties before you access a device, perform the following procedure.

Step Action

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

The **Properties** dialog box appears.

- 2 Configure the properties.

Area	Item	Description
Polling	Status Interval	Interval at which statistics and status information is gathered. For a full stack, set this interval to between 120 and 300 seconds.
	Hotswap Detect every	The frequency at which Device Manager polls for hot swap module information. This value is in relation to the Status Interval value. For example, if the Status Interval is set to 120, and the value for Hotswap Detect every is 2, Device Manager polls the hot swap modules every 240 seconds. If less frequent hot swap polling is desired, 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 Device > Refresh Status .
SNMP	Retry Count	Number of times Device Manager sends the same polling request if a response is not returned to Device Manager. You may want to 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 may want to increase the timeout interval and then change the Retransmission Strategy to superlinear.
	Trace	If checked, you have the ability to perform trace routes.
	Listen for traps	When selected (enabled), Device manager listens for traps from the device.
	Max Traps in Log	The specified number of traps that may exist in the trap log. The default is 500.
	Trap Port	Specifies the UDP port that Device Manager uses to listen for SNMP traps.
	Listen for Syslogs	Enables the Device Manager to listen to the syslog.
	Confirm row deletion	When selected (enabled), Device Manager displays a dialog box for confirmation before deleting a row or entry from any table.
	Default Read Community	Default Read Community string. You can edit this field by highlighting the current value and typing over it.
Default Write Community	Default Write Community string. You can 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.
Web Management	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.
Application Launch from JDM	Telnet	Default Telnet is the one that comes with the operating system. To define a specific Telnet, select User-Defined and specify the Telnet path and parameters.
	SSH	Default SSH is the one bundled with in the JDM. To define a specific SSH, select User-Defined and specify the SSH client path and parameters.

3 Click **OK**.

—End—

Enabling Save SNMPv3 Devices to Open Last

When you enable **Save SNMPv3 Devices to Open Last**, the JDM displays a warning message.

When you enable **Save SNMPv3 Devices to Open Last**, a user can use **Device > Open Last by SNMPv3** and select the device to open without reentering the v3 required information.

The main purpose for SNMPv3 is security, so if you enable **Save SNMPv3 Devices to Open Last**, then any other user can access the device without the need to reenter all v3 required information.

When you disable **Save SNMPv3 Devices to Open Last**, all previously saved SNMPv3 device data is erased, and the JDM displays a warning message.

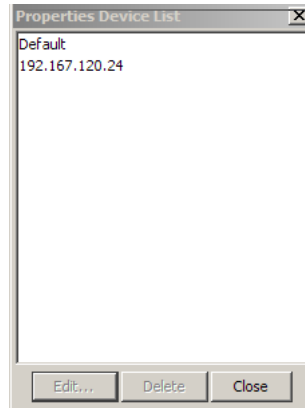
Setting Device Manager properties for a device

To set the Device Manager properties after you access a device, perform the following procedure.

Step Action

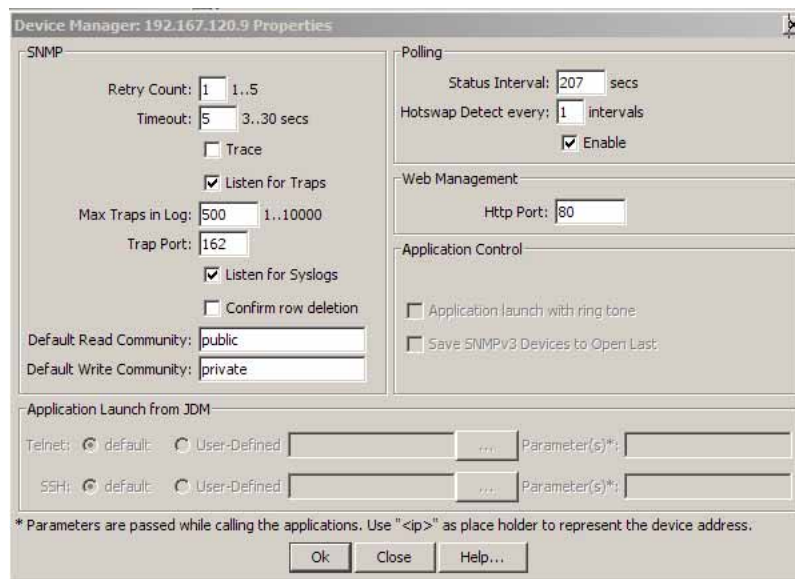
- 1 From the Device Manager menu bar, choose **Device > Properties > Devices**.

The Properties Device List appears.



- 2 Select the IP address of a device from the Properties Device List.
- 3 Click **Edit**.

The **Device Manager: xxx.xxx.xxx.xxx Properties** dialog box appears.



4 Configure the properties.

Area	Item	Description
Polling	Status Interval	Interval at which statistics and status information is gathered. For a full stack, set this interval to between 120 and 300 seconds.
	Hotswap Detect every	The frequency at which Device Manager polls for hot swap module information. This value is in relation to the Status Interval value. For example, if the Status Interval is set to 120, and the value for Hotswap Detect every is 2, Device Manager polls the hot swap modules every 240 seconds. If less frequent hot swap polling is desired, 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 Device > Refresh Status .
SNMP	Retry Count	Number of times Device Manager sends the same polling request if a response is not returned to Device Manager. You may want to 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 may want to increase the timeout interval and then change the Retransmission Strategy to superlinear.
	Trace	If checked, you have the ability to perform trace routes.
	Listen for traps	When selected (enabled), Device manager listens for traps from the device.
	Max Traps in Log	The specified number of traps that may exist in the trap log. The default is 500.
	Trap Port	Specifies the UDP port that Device Manager uses to listen for SNMP traps.
	Listen for Syslogs	Enables the Device Manager to listen to the syslog.
	Confirm row deletion	When selected (enabled), Device Manager displays a dialog box for confirmation before deleting a row or entry from any table.
	Default Read Community	Default Read Community string. You can edit this field by highlighting the current value and typing over it.
	Default Write Community	Default Write Community string. You can 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.
Web Management	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.
Application Launch from JDM	Telnet	Default Telnet is the one that comes with the operating system. To define a specific Telnet, select User-Defined and specify the Telnet path and parameters.
	SSH	Default SSH is the one bundled with in the JDM. To define a specific SSH, select User-Defined and specify the SSH client path and parameters.

5 Click **OK**.

—End—

Opening a Switch with the Java Device Manager

To open, or connect, to a switch, the following information is required:

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

These pieces of information can be obtained from the switch administrator.

After this information is obtained, follow this procedure to connect to a switch:

Step Action

- 1 Start the **Java Device Manager** as outlined in the section "[Starting the Java Device Manager](#)" (page 33).

- 2 Select **Open > Device** from the JDM menu, or press **CTRL+O**. The screen depicted in the following figure is displayed.

- 3 Enter the information necessary to make a connection to the switch. The following table describes each of the fields on the **Open Device** screen.

Field	Description
Device Name	Either an IP address or 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.
Use default community strings in properties	When selected, the Device Manager uses the default community string. Set the default community strings in Device > Properties .
v3 Enabled	When selected, the Open Device dialog box displays SNMPv3 options.
User Name	The name of the user.
Context Name	Specify the context name.
Authentication Protocol	Identify the authentication protocol used.
Authentication Password	Specify the current authentication password.
Privacy Protocol	Identify the privacy protocol.
Privacy Password	Specify the current privacy password.

Not all information is required for connection to a switch.

If the **v3 Enabled** check box is not selected, only a **Device Name**, **Read Community**, and **Write Community** value are needed. If you enable **Use default community strings in properties**, the Device Manager uses the default values specified in the device properties for **Read Community**, and **Write Community**.

If **v3 Enabled** is selected, then **Device Name**, **User Name**, **Authentication Protocol**, **Authentication Password**, **Privacy Protocol**, and **Privacy Password** are required. Some devices require a value in **Context Name**.

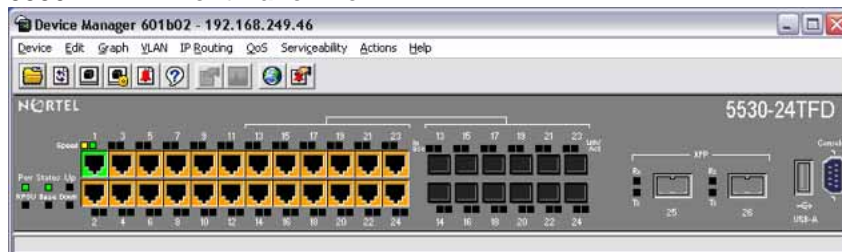
Consult the switch administrator to determine if SNMP version 3 is used for switch connectivity and administration in the network.

4 Click **Open**.

—End—

If the proper information was entered, a connection with the switch is established and a graphical representation of the switch front panel is displayed. "[5530-24TFD Front Panel View](#)" (page 41) displays the result of a successful connection to a Nortel Ethernet Routing Switch 5530-24TFD.

5530-24TFD Front Panel View



Note: After a switch has been connected to successfully once, the connection information is stored. Subsequent connections to the switch can be made by selecting **Device > Open Last by SNMPv1/v2** or **Device > Open Last by SNMPv3** from the JDM menu and selecting the IP address of the switch.

Device Manager interface components

The Java Device Manager consists of several user interface components that make up the application. 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 46)
- "Status bar" (page 48)
- "Using the buttons in Device Manager screens" (page 48)
- "Editing objects" (page 48)
- "Telneting to a switch" (page 54)
- "Opening an SSH connection to the switch" (page 54)
- "Trap log" (page 55)
- "Accessing the Web-based Management Interface" (page 55)
- "Device Manager Online Help" (page 55)

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	Opens a device, refreshes the device view, rediscovers a device, and sets the polling and SNMP properties. This menu also enables you to open and view the Trap Log, SysLog, and Log. It also enables the establishment of a Telnet or SSH connection to the device that is currently open.
Edit	Opens edit dialog boxes for the objects selected in the device view. It opens dialog boxes for managing files and running diagnostic tests. This command also enables SNMP, SNMP v3 and related configurations to be set.
Graph	Opens statistics dialog boxes for the selected object.
VLAN	Opens dialog boxes for managing VLANs, Spanning Tree Groups (STG), and MultiLink Trunking (MLT), and Link Aggregation Control Protocol (LACP).
IP Routing	Opens configuration dialog boxes to set up IP routing functions for the switch, including ARP, OSPF, RIP, VRRP, DHCP, UDP Forwarding, and Policies.
QoS	Opens configuration and monitoring dialog boxes for Quality of Service or Differentiated Services.
Serviceability	Opens configuration dialog boxes for IPFIX and RMON .

Command	Description
Actions	enables you to open the Home page for the Web-based management session.
Help	Opens online Help topics for Device Manager and provides 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 some additional actions.

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

Toolbar buttons

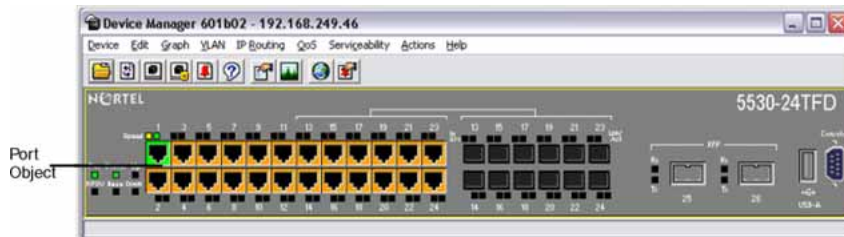
Button	Name	Description	Menu bar equivalent
	OpenDevice	Opens the Open Device dialog box.	Device > Open
	Refresh Device Status	Refreshes the device view information.	Device > Refresh Status
	Trap Log	Opens the trap log.	Device > Trap Log
	Help	Opens online Help in a Web browser.	Help > Device
	Edit Selected	Displays configuration data for the selected chassis object.	Edit > Unit Edit > Chassis Edit > Port
	Graph Selected	Opens statistics and graphing dialog boxes for the selected object.	Graph > Chassis Graph > Port
	Globe	Opens a Web-based management session.	Actions > Open Home Page
	Telnet	Opens a Telnet session.	Device > Telnet
	SSH	Opens a SSH session.	Device > SSH Connection
	Alarm Manager	Opens the Rmon Alarm Manager.	Serviceability > Rmon > Alarm Manager

Device view

The device view gives a visual determination of the operating status of the various units and ports in the hardware configuration. The device view also can be used 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

See also

"Device view" (page 44)

Selecting a single object To select a single object:

- Click the edge of the object.

The object is outlined in yellow, indicating that it is selected. 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):

- Do one of the following:
 - For a block of contiguous ports, drag to select the group of ports.
 - For multiple ports, or switches in the stack, **Ctrl+click** on the objects.

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

- Select **Edit > Select > Ports** from the menu.

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

- Select **Edit > Select > Units** from the menu.

To select an entire stack:

- Select **Edit > Select > Chassis** from the menu.

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 activity of the LEDs.

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

The following table ["Port color codes" \(page 45\)](#) shows the status assigned to each color.

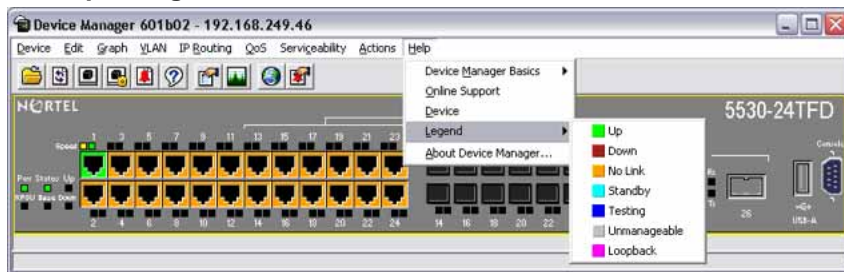
Port color codes

Color	Description
Green	Port is operating.
Red	Port has been 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 5500 Series.
Dark Blue	Port is being tested. Note: This is not supported on the Nortel Ethernet Routing Switch 5500 Series.

Color	Description
Gray	Port is unmanageable.
Purple	Port is in loopback testing mode.
	Note: This is not supported on the Nortel Ethernet Routing Switch 5500 Series.

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

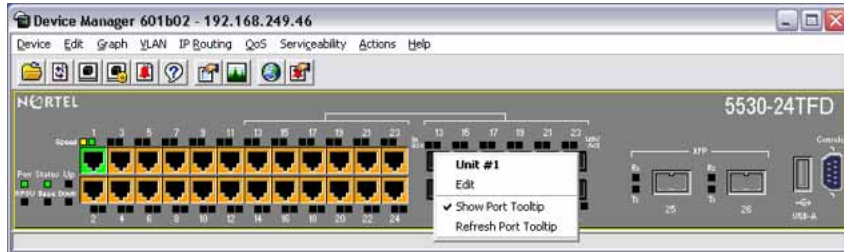
Color port legend



Shortcut menus

Each object in the device view has a shortcut menu that appears when the object is right-clicked. 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 46).

Switch unit shortcut menu



The following table "Switch unit shortcut menu commands" (page 46) describes the commands on the switch unit shortcut menu.

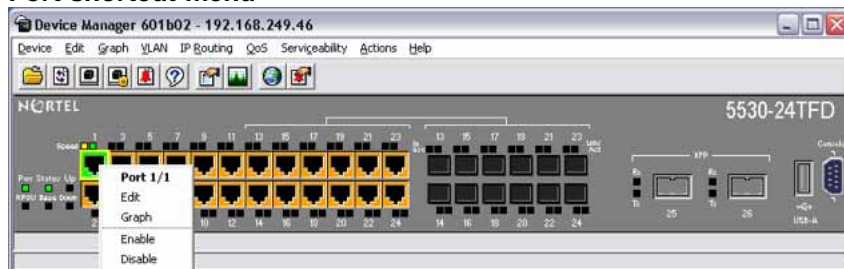
Switch unit shortcut menu commands

Command	Description
Unit #	Displays the unit number.

Command	Description
Edit	Opens a read-only dialog box that provides basic hardware information about the switch.
Show Port Tooltip	Displays a pop-up window or a "tooltip" that contains the name of the port and the port speed when the mouse is moved 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	Refreshes the port "tooltip" information after a new port name is assigned to it, or the port speed is reconfigured. You can update the information that is displayed in the tooltip from Edit > Port. Click on Refresh Port Tooltip to view the updated information.
Refresh PoE Status	Refreshes the status of PoE ports on the switch (available only on 5500-PWR switches).

The port shortcut menu provides a faster path for editing and graphing a single port; however, the same options can be accessed using the menu bar or the toolbar. The port shortcut menu is illustrated in "Port shortcut menu" (page 47).

Port shortcut menu



The following table "Port shortcut menu commands" (page 47) describes the commands on the port shortcut menu.

Port shortcut menu commands

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








Status bar

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

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	Opens a dialog box to create a new entry for a table; and then from the dialog box, inserts the new entry in the table.
	Copy	Copies selected cells from a table.
	Paste	Pastes copied values to a currently selected table cell.
	Reset Changes	Causes changed (but not applied) fields to revert to their previous values.
	Print Table or Print Graph	Prints a table or graph.
	Stop	Stops the current action (compiling, saving, and so forth). If you are updating or compiling a large data table, the Refresh button changes to a Stop button while this action is taking place. Clicking the Stop button interrupts the polling process.
	Export Data	Exports information to a file you specify. You can then import this file into a text editor or spreadsheet for further analysis.

Editing objects

Objects and values in the Device Manager device view can be edited 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 a screen value is changed, the changed value is shown in **bold**. However, changes are not applied to the running configuration until **Apply** is clicked.

Note: Many dialog boxes contain a **Refresh** button. After changes are applied 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. Statistics can be viewed and graphed for a single object or multiple objects.

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

Types of statistics The data tables in the statistics dialog boxes list the counters, or categories of statistics being 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.

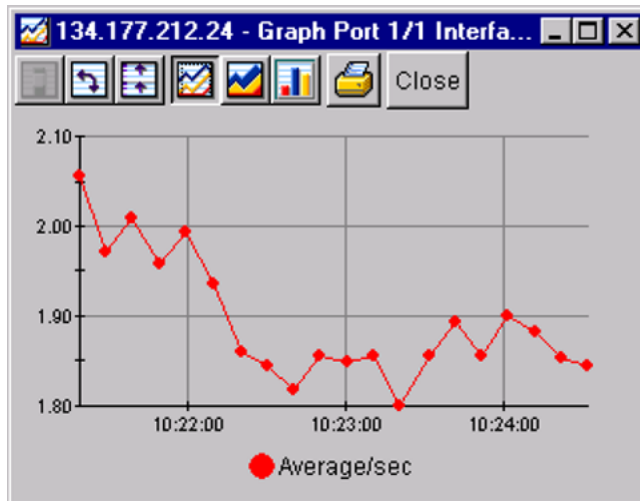
"Types of statistics" (page 49) The following table describes the types of statistics shown in the statistics dialog boxes.

Types of statistics

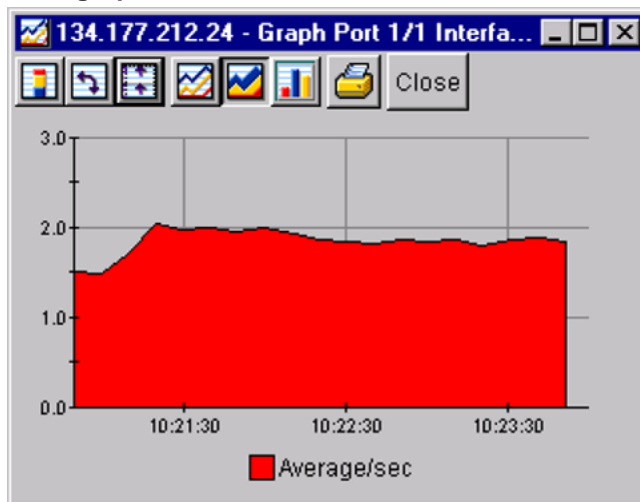
Statistic	Description
AbsoluteValue	The total count since the last time counters were reset. A system reboot resets all counters.
Cumulative	The total count since the statistics window was first opened. The elapsed time for the cumulative counter is shown at the bottom of the graph window.
Average/sec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

Types of graphs With Device Manager, line, area, bar, and pie graphs can be created. "Line graph" (page 50), "Area graph" (page 50), "Bar graph" (page 51), and "Pie graph" (page 51) illustrate the different graph styles, respectively.

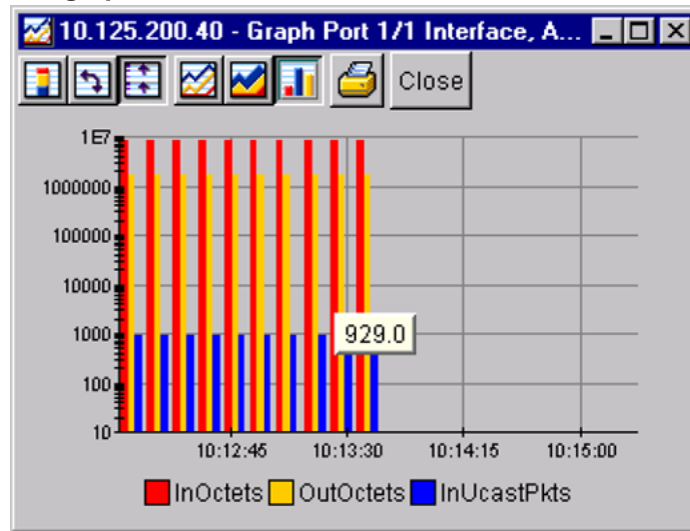
Line graph



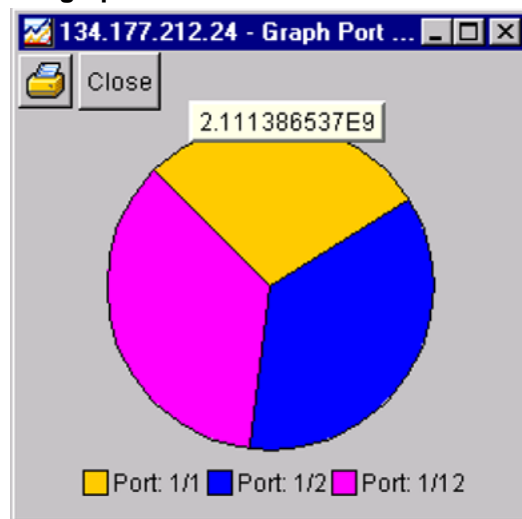
Area graph



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

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
InOctets	58,670,767	13,001	260.02	84.9	417.3	235.9
OutOctets	25,634,465	11,217	224.34	40.9	496.3	47.3
InUcastPkts	70,404	16	0.32	0.1	0.6	0.2
OutUcastPkts	97,500	25	0.5	0.2	0.9	0.3
InMulticastPkts	312,869	35	0.7	0.7	0.7	0.7
OutMulticastPkts	58,438	7	0.14	0.1	0.2	0.1
InBroadcastPkts	140,404	23	0.46	0.1	1	1
OutBroadcastPkts	375	0	0	0	0	0
InDiscards	35,381	0	0	0	0	0
OutDiscards	0	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 49)) for the selected objects. For example, "Interface statistics for multiple ports" (page 52) shows LastValue statistics for the selected ports.

Interface statistics for multiple ports

Interface	InOctets	OutOctets	InUcastPkts	OutUcastPkts	InMulticastPkts	OutMulticastPkts	InBroadcastPkts	OutBroadcastPkts	InDiscards	OutDiscards	InErrors	OutErrors	InUnknownProtos
Port: 1/1	39,066,...	10,115,236	39,305	56,197	233,014	44,141	107,742	261	28,209	0	0	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

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

The statistics are updated based on the poll interval shown at the bottom of the dialog box. A different polling interval can be selected.

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

Statistics can be exported to a tab-separated file format and the file imported 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 Do one of the following:
 - On the toolbar, click **Graph Selected**.
 - From the shortcut menu for the object, choose **Graph**.
 - From the menu, choose **Graph > Chassis** or **Graph > Port**.

A statistics dialog box appears with tabs for different categories of statistics for the selected object ("[Statistics dialog box for a port](#)" (page 53)).

Statistics dialog box for a port







	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
InOctets	58,670,767	13,001	260.02	84.9	417.3	235.9
OutOctets	25,634,465	11,217	224.34	40.9	496.3	47.3
InUcastPkts	70,404	16	0.32	0.1	0.6	0.2
OutUcastPkts	97,500	25	0.5	0.2	0.9	0.3
InMulticastPkts	312,869	35	0.7	0.7	0.7	0.7
OutMulticastPkts	58,438	7	0.14	0.1	0.2	0.1
InBroadcastPkts	140,404	23	0.46	0.1	1	1
OutBroadcastPkts	375	0	0	0	0	0
InDiscards	35,381	0	0	0	0	0
OutDiscards	0	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

- 3 Select a tab for the group of statistics to view.
- 4 On the displayed data table, drag to select the cells to graph. (They 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 a copy of the graph, click **Print**.
- 7 Buttons at the top of the graph screen for line, area, and bar graphs change the orientation of the graph, change the scale, or 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	"Stacks" data quantities instead of displaying them side-by-side.
	Horizontal	Rotates the graph 90 degrees.
	Log Scale	Changes the scale of the x-axis (of an unrotated graph) from numeric to logarithmic.
	Line Chart	Converts an area graph or bar graph to a line graph.
	Area Chart	Converts a line graph or bar graph to an area graph.
	Bar Chart	Converts a line graph or area graph to a bar graph.

Telnetting to a switch

From Device Manager, a Telnet session can be initiated to the console interface for the switch or stack being accessed.

To Telnet to a switch, do one of the following:

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

Opening an SSH connection to the switch

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

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

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

An SSH window to the switch appears.

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

Trap log

The Nortel Ethernet Routing Switch 5500 Series can be configured to send SNMP generic traps. When Device Manager is running, any traps received are recorded in the trap log. The maximum number of entries in the trap log can be set using the **Properties** screen. The default number of trap log entries is 500.

To view the trap log:

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

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

Using the **Export** button at the bottom of the screen, trap logs can be exported to a file.

By default, the Device Manager receives traps on port 162. If this port is being used by another application, the trap log cannot be viewed until the other application is disabled and Device Manager is restarted.

You can configure another port, other than port 162, as the trap port from the Properties dialog box.

By default, traps are sent in SNMP V2c format. However, if an older Network Management System (NMS) is being used (one that supports only SNMP v1 traps), traps are sent in v1 format.

Accessing the Web-based Management Interface

The Web-based Management Interface for the Nortel Ethernet Routing Switch 5500 Series can be accessed from the Device Manager.

To view the Web-based Management Interface, select **Actions > Open Home Page** from the menu. 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 displayed in the computer's default web browser. The web browser launches automatically when the **Help** button is clicked.

The default locations of the Help files are the directories listed in the following table.

Help file locations

Platform	Default path
Windows 95, Windows 98, Windows NT, Windows XP, UNIX, Windows 2003, and Windows Vista	<p><JDM Installation directory> /help/ flagship/v510.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, no installation is needed as 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 being used and the switch CPU are on the same virtual local area network (VLAN). Use the Command Line Interface and verify the VLAN assignments to confirm that the VLANs are the same. If the switch and computer are not on the same VLAN, the Web-based Management Interface cannot be accessed.

After VLAN verification has taken place, the Web-based Management Interface can be accessed by performing the following procedure:

Step	Action
1	Open a new 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 <i>http://10.30.31.105</i> is entered in the Address field. The IP address of the switch or stack can be obtained 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 that is required or has been assigned. For read-only access the user name is RO and for read-write access it is RW . These user names are case-sensitive. The password can be obtained from the switch administrator.

- 4 If all information is correct, the main switch page appears. "5530-24TFD Main Page" (page 57) displays an example of the main switch page for a Nortel Ethernet Routing Switch 5530-24TFD.

—End—

5530-24TFD Main Page

Administration > System Information

Ethernet Routing Switch 5530 - 24TFD

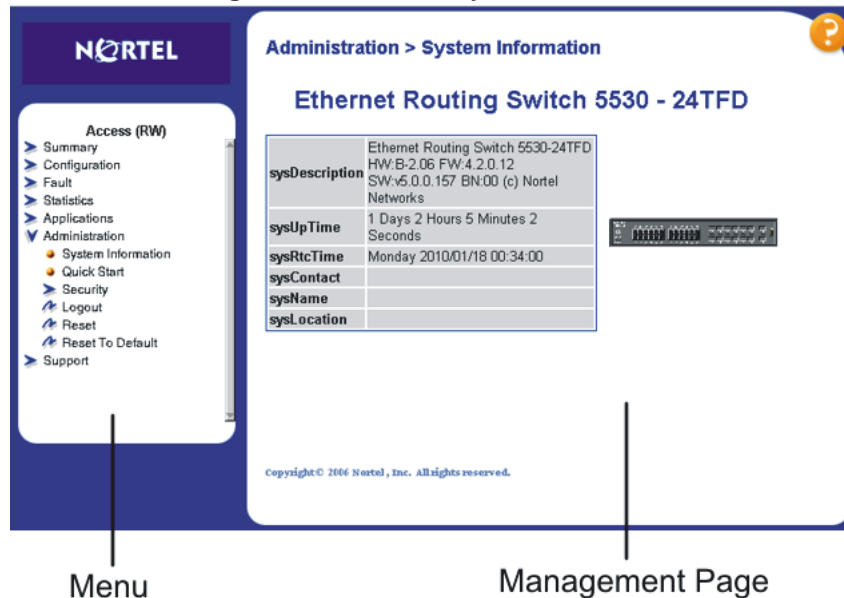
sysDescription	Ethernet Routing Switch 5530-24TFD HW: B-2.06 FW: 4.2.0.12 SW: v5.0.0.157 BN:00 (c) Nortel Networks
sysUpTime	1 Days 2 Hours 5 Minutes 2 Seconds
sysRtcTime	Monday 2010/01/18 00:34:00
sysContact	
sysName	
sysLocation	

Copyright © 2006 Nortel, Inc. All rights reserved.

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. "Web-based Management Interface layout" (page 58) illustrates this layout.

Web-based Management Interface layout



Menu

The menu, as illustrated in "[Web-based Management Interface layout](#)" ([page 58](#)), contains the seven main units of work that can be done through the Web-based Management Interface, and their corresponding options. To navigate through the menu, click on one of the main headers and the corresponding options are displayed below it. Click one of the options to display the associated management page. Some options are only available when the switch is part of a stack configuration and are not displayed when the switch is in a stand-alone configuration.

"[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 Identify Unit Numbers* Stack Numbering*	This menu provides information about the current state of the individual switch or stack.
<p>* These menu options are only available when the switch is part of a stacked configuration. ** These menu options have additional menu options associated with them.</p>		

Main Heading	Options	Description
Configuration	IP System Remote Access SNMPv1 SNMPv3** SNMP Trap MAC Address Table Find MAC Address Port Management High Speed Flow Control Software Download Ascii Config Download Configuration File Console/Comm Port RTC Time Configuration Load License	This menu enables the user to configure aspects of the switch or stack operation.
Fault	RMON Threshold RMON Event Log System Log	This menu enables the user to configure fault thresholds and view event logs.
Statistics	Port Port Error Summary Interface Ethernet Errors Transparent Bridging RMON Ethernet RMON History	This menu enables the user to view statistics on a variety of switch functions.
* These menu options are only available when the switch is part of a stacked configuration. ** These menu options have additional menu options associated with them.		

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









CAUTION

Nortel recommends the use of the navigation tools provided in the interface instead of those provided by the web browser, such as page forward and back and page refresh. Web browser functions do not enhance the use of the interface and may cause interference 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 on 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 it. Click on the icon to collapse the menu and hide all associated options.
	This icon identifies a menu option. Click on 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 on the icon to see the management page associated with this menu option and any related page hyperlinks it contains.
	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. Clicking on this icon opens a new web browser window and loads the Nortel corporate home page.

Management Page

The Management Page, as illustrated in "Web-based Management Interface layout" (page 58), is the main work area in the Web-based Management Interface. As different items and options are selected from the menu the associated Management Page is loaded. "Quick Start Management page" (page 62) illustrates the Quick Start Management Page which is accessed by selecting **Administration > Quick Start** from the menu.

Quick Start Management page

Administration > Quick Start

IP

	Configurable	In Use
In-Band Switch IP Address	192.168.249.46	192.168.249.46
In-Band Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.249.1	192.168.249.1

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

Every Management Page is comprised of one or more of the following elements:

- **Display Field**

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

- **Input Field**

Input fields allow the user to enter or change information. Input fields have a white background and can be edited.







- **Check Box**

Check boxes are used 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) and when it does not, it is disabled (off). Click in the check box to either enter a check mark or remove it.

- **Icons and Buttons**

Icons and buttons on a Management Page represent an action that can be performed on the page. Clicking the icon or button initiates 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	Submits entered information to the switch. If present, ensure that this button is clicked every time new information is entered on the Management Page.
	Modify	Opens a modification page for the data row in which it appears.
	View	Opens a read-only statistics page for the data row in which it appears.
	Delete	Deletes the data row in which it appears.
	Help	Opens the Help for the current Management Page in a new web browser window.
	Item-Specific Help	Opens the help for the current data item in a new web browser window.

Basic configuration tasks

This chapter outlines basic configuration tasks that can be performed on a Nortel Ethernet Routing Switch 5500 Series. After a switch is successfully installed, the following tasks can be performed to enable basic switch functionality.

This chapter contains the following topics:

- "Feature licensing" (page 66)
- "Factory default configuration" (page 69)
- "Setting user access limitations" (page 75)
- "Updating switch software" (page 85)
- "Setting TFTP parameters" (page 94)
- "Working with configuration files" (page 95)
- "Terminal setup" (page 109)
- "Setting the default management interface" (page 109)
- "Setting Telnet access" (page 110)
- "Setting server for Web-based management" (page 112)
- "Setting boot parameters" (page 113)
- "Defaulting to BootP-when-needed" (page 114)
- "Customizing the CLI banner" (page 117)
- "Displaying complete GBIC information" (page 121)
- "Displaying hardware information" (page 121)
- "Shutdown command" (page 121)
- "CLI Help" (page 122)

Feature licensing

With Release 5.1 software, you must have an Advanced Routing License or a Demo license to enable certain features. These software licenses support the following five features:

- IP Flow Information eXport (IPFIX)
- Split MultiLink Trunking (SMLT)
- Open Shortest Path First (OSPF)
- Virtual Router Redundancy Protocol (VRRP)
- Equal Cost Multi Path (ECMP)

The software license file is based on authorized MAC address(es). A software license file can support up to 1,000 MAC addresses.

A software license file is generated from one or more MAC addresses. The MAC address of the base unit is required and Nortel recommends including the MAC address of the temporary base in file generation. This measure ensures that the licensed features continue to operate if the base unit fails.

A ERS 5500 Series switch supports up to ten valid license files. For example, you install License File 1 to cover your network of ERS 5500 Series switches, but the base unit fails and is replaced. You install a new license file (License File 2) to cover the replacement unit. The two separate license files are required to support the network.

You can contact Nortel to order the Advanced Routing License Features Activation Kit (part number 322515-A). The kit contains the Software License Certificate. Follow the instructions on this certificate to obtain your software license file.

Demo license

Release 5.1 introduces a Demo License, which enables OSPF, ECMP, VRRP, SMLT, and IPFIX, or any combination thereof for a period of 30 days. At the end of the 30 day trial period, the features will be disabled, with the exception of SMLT. Due to the manner in which SMLT is implemented through cabling, and the fact that Spanning Tree Protocol needs to be disabled, a loop would be formed on the network if SMLT was disabled as a feature. Therefore, the following actions will take place to minimize the potential network impact.

Three traps are sent.

- The first trap is sent five days prior to expiration of the license.

```
Trap: bsnTrialLicenseExpiration: Trial license 1  
will expire in 5 day(s).
```

- The second trap is sent one day prior to the expiration of the license.

```
Trap: bsnTrialLicenseExpiration: Trial license 1
will expire in 1 day(s).
```

- The last trap is sent upon termination of the license.

```
Trap: bsnTrialLicenseExpiration: Trial license 1
has expired.
```

At this point, all license features are disabled except SMLT. SMLT will remain enabled until there is a stack/unit reset. Once the stack/unit is reset, the feature will be disabled, and a loop will be formed if there has been no intervention to remove/disable the ports participating in the IST.

Therefore, it is recommended that upon receiving the first trap that the administrator begin to manually disable that feature and ensure that any cabling loop is removed.

Working with feature license files using the CLI

With the following commands, you can copy the software license file to your switch and display or clear the existing license information:

- ["copy tftp license command" \(page 67\)](#)
- ["show license command" \(page 68\)](#)
- ["clear license command" \(page 68\)](#)

copy tftp license command

With the `copy tftp license` command, you can copy the features software license file from a TFTP server to your switch. After you copy the license to the switch, you must perform a reboot to activate the license.

Note: The software license is copied to NVRAM. If you reset the switch to default, this removes the software license from the switch. In this case, you must recopy the license file to the switch and reboot to reactivate the licensed features.

The syntax for the `copy tftp license` command is:

```
copy tftp license <A.B.C.D> <WORD>
```

The `copy tftp license` command is in the `privExec` command mode.

["copy tftp license command parameters" \(page 68\)](#) describes the parameters and variables for the `copy tftp license` command.

copy tftp license command parameters

Parameter	Description
<A.B.C.D>	The TFTP server address.
<WORD>	The software license filename on the TFTP server.

show license command

With the `show license` command, you can display the existing software licenses on your switch.

The syntax for the `show license` command is:

```
show license { <1-10> | all }
```

The `show license` command is in the `privExec` command mode.

clear license command

With the `clear license` command, you can delete the existing software licenses on your switch.

The syntax for the `clear license` command is:

```
clear license { <1-10> | all }
```

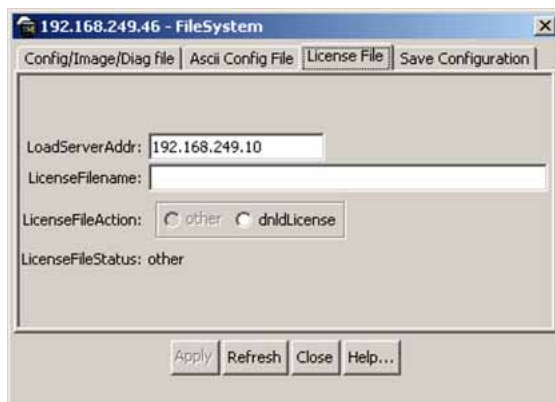
The `clear license` command is in the `privExec` command mode.

Copying the license file using the Java Device Manager

Use the Java Device Manager to copy the license file to the 5500 Series Nortel Ethernet Routing Switch.

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

- | | |
|---|---|
| 1 | From the JDM menu select Edit > File System .
The FileSystem dialog box appears. |
| 2 | Click the License File tab.
The License File tab appears. |



- 3 In the **LoadServerAddr** field, enter the TFTP server address.
- 4 In the **LicenseFileName** field, enter the software license filename for the TFTP server.
- 5 In the **LicenseFileAction** field, select **dnldLicense**.
- 6 Click **Apply**.
- 7 Click **Refresh**.
The LicenceFileStatus field displays the file copy progress. After the file copy completes, a warning message appears prompting you to reboot the switch and activate the license.
- 8 To reboot the switch, choose **Edit > Chassis**
- 9 Under the **System** tab, select the **reboot** option and click **Apply**.

—End—

Factory default configuration

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

"[Factory default configuration settings](#)" (page 69) 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

Setting	Factory Default Configuration Value
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
Clear by Ports	NONE
Learn by Ports	NONE
Current Learning Mode	Not Learning
Trunk	blank field
Security	Disabled
Port List	blank field

Setting	Factory Default Configuration Value
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)
Unit	1
Status	Enabled (for all ports)
Linktrap	On
Autonegotiation	Enabled (for all ports)
Speed/Duplex	(Refer to Autonegotiation)
Trunk	1 to 32 (depending on configuration status)
Trunk Members (Unit/Port)	Blank field

Setting	Factory Default Configuration Value
STP Learning	Normal
Trunk Mode	Basic
Trunk Status	Disabled
Trunk Name	Trunk #1 to Trunk #32
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
Console Switch Password	None
Console Stack Password	None
Telnet/Web Stack Password	None
Telnet/Web Switch Password	None
Console Read-Only Switch Password	user

Setting	Factory Default Configuration Value
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	<ul style="list-style-type: none"> • STP Group 1--No • Other STP Groups--Yes
STP Group State	<ul style="list-style-type: none"> • 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
STP Group	1
TELNET Access/SNMP/Web	<p>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.</p> <p>Use list: Yes</p>
Login Timeout	1 minute
Login Retries	3

Setting	Factory Default Configuration Value
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
Auto Configuration on Reset	Disabled
EAPOL Security Configuration	
High Speed Flow Control Configuration	
VLAN Configuration Control	Strict
Agent Auto Unit Replacement	Enabled

Setting user access limitations

By default, a 5500 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 must not be ignored during the initial configuration process.

For more information about switch user interfaces, consult ["5500 Series user interfaces" \(page 15\)](#).

The following procedures for setting user access limitations are covered in this section:

- ["Setting user access limitations using the CLI" \(page 75\)](#)
- ["Setting user access limitations using the Web-based Management Interface" \(page 79\)](#)

Setting user access limitations using the CLI

The CLI enables the administrator to limit user access through the creation and maintenance of passwords for Web, Telnet and Console access. This is a two-step process that requires first creating the password and then enabling it.

Ensure that **Global Configuration** mode is entered in the CLI before beginning 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 set the read-only and read-write passwords, perform the following procedure.

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 15) .
2	From the command prompt, use the <code>cli password</code> command to change the desired password. <pre>cli password {read-only read-write} <password></pre> "cli password parameters" (page 76) explains the parameters for the <code>cli password</code> command.

cli password parameters

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 the read-only and read-write passwords are set, they can be individually enabled or disabled for the various switch access methods. When enabled, password security prompts you for a password and the value is hidden. To enable or disable passwords, perform the following procedure:

Step Action

- 1** Access the CLI through the Telnet protocol or a Console connection. For detailed information about this subject, refer to ["Accessing the CLI" \(page 15\)](#).
- 2** From the command prompt, use the `[no] password` command to enable or disable the desired password.


```
[no] password {telnet | serial} {none | local | radius | tacacs}
```

["cli password parameters" \(page 76\)](#) explains the parameters for the `cli password` command.

cli password parameters

Parameter	Description
{telnet serial}	This parameter specifies if the password is enabled or disabled for telnet or the console. Telnet and web access are tied

Parameter	Description
	together so that enabling or disabling passwords for one enables or disables it for the other.
{none local radius tacacs}	This parameter specifies if the password is to be disabled (none), or if the password to be used is the locally stored password created in " Setting the read-only and read-write passwords " (page 75), or if RADIUS authentication or TACACS +AAA services 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 the use of a dedicated network resource. This network resource contains a listing 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, when prompted, a password. The password value is hidden when entered. This information is checked against the preexisting list. If the user credentials are valid they can access the switch.

If RADIUS Authentication was selected when enabling passwords through the CLI, the RADIUS server settings must be specified to complete the process. Ensure that **Global Configuration** mode is entered in the CLI before beginning 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, refer to "[Accessing the CLI](#)" (page 15) .
- 2 From the command prompt, use the `radius-server` command to configure the server settings.


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

"[radius-server parameters](#)" (page 78) explains the parameters for the `radius-server` command.

radius-server parameters

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

3 Press **Enter**.

—End—

Related RADIUS Commands During the process of configuring RADIUS authentication, there are three other CLI commands that can be useful to the process. These commands are:

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

1 `show radius-server`

The command takes no parameters and displays the current RADIUS server configuration.

2 `no radius-server`

This command takes no parameters and clears any previously configured RADIUS server settings.

3 `radius-server password fallback`

This command takes no parameters and enables the password fallback RADIUS option if it was not done when the RADIUS server was configured initially.

—End—

Setting user access limitations using the Web-based Management Interface

The Web-based Management Interface enables the administrator to limit user access through the creation and maintenance of passwords for Web, Telnet, and Console access. The following sections outline the procedures for performing these tasks:

- "Setting the Web password" (page 79)
- "Setting the Telnet password" (page 81)
- "Setting the Console password" (page 82)
- "Configuring RADIUS authentication" (page 84)

Setting the Web password

To require password authentication when the user logs in to the switch through the Web-based Management Interface, it is necessary to edit the Web password. To do this, select **Administration > Security > Web** from the main menu and follow this procedure:

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

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

- **None**

This selection indicates that no password is required for users accessing the switch through the Web-based Management Interface.



CAUTION

Using the **None** setting means that any user with knowledge of the IP address of the switch and the appropriate network access can make changes to the switch configuration.

- **Local Password**

This selection indicates that the user is required to 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 between 1 and 15 characters in length.

- **RADIUS Authentication**

This selection indicates that the user is authenticated by a RADIUS server present on the local area network. See the section "[Configuring RADIUS authentication](#)" (page 84) for information about configuring the parameters for RADIUS server authentication.

- 2 If the Local Password option was selected in step 1, specify a password to grant read-only access to the switch in the **Read-Only Switch Password** field.
- 3 If the Local Password option was selected 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** drop-down list always overrides the values in the **Read-Only Switch Password** and **Read-Write Switch Password** fields.

- 4 Click **Submit**.

Note: The **Web Stack Password** settings cannot be changed on this screen and only appear here for informational purposes. Refer to "[Setting user access limitations using the CLI](#)" (page 75) for procedures to change this password.

—End—

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

Web Password Management page

The screenshot shows the Nortel Web Password Management page. The page title is "Administration > Security > Web". The page contains two sections: "Web Switch Password Setting" and "Web Stack Password Setting". The "Web Switch Password Setting" section has a dropdown menu for "Web Switch Password Type" set to "None", and text input fields for "Read-Only Switch Password" (value: user) and "Read-Write Switch Password" (value: secure). The "Web Stack Password Setting" section has a dropdown menu for "Web Stack Password Type" set to "None", and text input fields for "Read-Only Stack Password" (value: user) and "Read-Write Stack Password" (value: secure). A "Submit" button is located at the bottom of the form. A navigation menu on the left shows "Security" expanded with "Web" selected.

Setting the Telnet password

To require password authentication when the user logs into the switch through the Telnet protocol, it is necessary to edit the Telnet password. To do this, select **Administration > Security > Telnet** from the main menu and follow this procedure:

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

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

- **None**

This selection indicates that no password is required for users accessing the switch through the Telnet protocol.



CAUTION

Using this setting means that any user with knowledge of the IP address of the switch and the appropriate network access can make changes to the switch configuration.

- **Local Password**

This selection indicates that the user is required to 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 between 1 and 15 characters in length.

- **RADIUS Authentication**

This selection indicates that the user is authenticated by a RADIUS server present on the local area network. See the section "[Configuring RADIUS authentication](#)" (page 84) for information about configuring the parameters for RADIUS server authentication.

- | | |
|---|--|
| 2 | If the Local Password option was selected in Step 1, specify a password to grant read-only access to the switch in the Read-Only Telnet Password field. |
| 3 | If the Local Password option was selected in Step 1, specify a password to grant read-write access to the switch in the Read-Write Telnet Password field. |

Note: A value of **None** or **RADIUS Authentication** in the **Telnet Switch Password Type** drop-down list always overrides the

values in the **Read-Only Telnet Password** and **Read-Write Telnet Password** fields.

4 Click **Submit**.

Note: The **Telnet Stack Password** settings cannot be changed on this screen and only appear here for information purposes. Refer to "Setting user access limitations using the CLI" (page 75) for procedures to change this password.

—End—

"Telnet Password Management page" (page 82) 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, it is necessary to edit the Console password. To do this, select **Administration > Security > Console** from the main menu and follow this 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**

This selection indicates that no password is required for users accessing the switch through the Console.

**CAUTION**

Using the **None** setting means that any user with access to a switch Console connection can make changes to the switch configuration.

- **Local Password**

This selection indicates that the user is required to 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 between 1 and 15 characters in length.

- **RADIUS Authentication**

This selection indicates that the user is authenticated by a RADIUS server present on the local area network. See the section "[Configuring RADIUS authentication](#)" (page 84) for information about configuring the parameters for RADIUS server authentication.

- 2 If the Local Password option was selected in step 1, specify a password to grant read-only access to the switch in the **Read-Only Console Password** field.
- 3 If the Local Password option was selected 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** drop-down list always overrides the values in the **Read-Only Console Password** and **Read-Write Console Password** fields.

- 4 Click **Submit**.

Note: The **Console Stack Password** settings cannot be changed on this screen and only appear here for informational purposes. Refer to "[Setting user access limitations using the CLI](#)" (page 75) for procedures to change this password.

—End—

"Console Password Management page" (page 84) shows an example of the Console Password Management Page in the Web-based Management Interface.

Console Password Management page

The screenshot shows the 'Console Password Management' page in the Nortel Web-based Management Interface. The breadcrumb navigation is 'Administration > Security > Console'. The page is divided into two main sections: 'Console Switch Password Setting' and 'Console Stack Password Setting'. Each section contains three input fields: 'Console Password Type' (a dropdown menu set to 'None'), 'Read-Only Password' (a text box containing 'user'), and 'Read-Write Password' (a text box containing 'secure'). A 'Submit' button is located at the bottom of the form. On the left side, there is a navigation menu with options like 'Access (RW)', 'Summary', 'Configuration', 'Fault', 'Statistics', 'Applications', 'Administration', 'System Information', 'Quick Start', 'Security', 'Web', 'Telnet', 'Console', 'RADIUS', 'Logout', and 'Reset'.

Configuring RADIUS authentication

The *Remote Authentication Dial-In User Service* (RADIUS) protocol is a means to authenticate users through the use of a dedicated network resource. This network resource contains a listing 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 preexisting list. If the user credentials are valid they can access the switch.

If RADIUS Authentication was selected for any of the switch authentication options in the previous three sections, the RADIUS server settings must be specified to complete the process. To set the RADIUS Authentication parameters, select **Administration > Security > RADIUS** from the menu and follow this 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 uses to listen for RADIUS authentication requests.

- 4 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.
- 5 Click **Submit**.

—End—

"RADIUS Authentication Management page" (page 85) 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	0.0.0.0
Secondary RADIUS Server	0.0.0.0
UDP RADIUS Port	1812
RADIUS Timeout Period	2 seconds
RADIUS Shared Secret	•••••••••• Re-enter to verify

Submit

Updating switch software

Updating switch software is a necessary part of switch configuration and maintenance. Updating the version of software running on the switch can be accomplished through either the Web-based Management Interface or the CLI.

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

- The switch has been given a valid IP address.
- A Trivial File Transfer Protocol (TFTP) server is present on the network that is accessible by the switch and that has the desired software version loaded.
- If changing the switch software on a Nortel Ethernet Routing Switch 5530-24TFD using a USB Mass Storage Device, ensure that the Mass Storage Device has the desired software version loaded on it and is inserted into the front panel USB port.
- If the CLI is to be used, ensure that the CLI is in **Privileged EXEC** mode.
- If the Web-based Management Interface is to be used, ensure that **read-write** access is being used.

For details on updating switch software, refer to the following sections

- "Changing switch software in the CLI" (page 86)
- "Changing switch software in the Java Device Manager" (page 88)
- "Changing switch software in the Web-based Management Interface" (page 91)
- "LED activity during software download" (page 94)

Changing switch software in the CLI

To change the software version running on the switch using the CLI, follow this procedure:

Step	Action
1	Access the CLI through the Telnet protocol or a Console connection. For detailed information about this subject refer to " Accessing the CLI " (page 15).
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 86) explains the parameters for the <code>download</code> command.</p>

download parameters

Parameter	Description
address <ip>	This parameter is the IP address of the TFTP server to be used. The address <ip> parameter is optional and if omitted the switch defaults to the TFTP server specified by the <code>tftp-server</code> command unless software download is to take place using a USB Mass Storage Device.
image <image name>	This parameter is 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 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 and only one can be executed at a time.	

Parameter	Description
diag <image name>	This parameter is the name of the diagnostic image to be downloaded from the TFTP server.
poe_module_image <image name>	This parameter is the name of the PoE module image to be downloaded from the TFTP server. This option is only available in 5500 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 5530-24TFD switch this parameter specifies that the software download is performed using a USB Mass Storage Device and the front panel USB port.
The <code>image</code> , <code>image-if-newer</code> , <code>diag</code> , and <code>poe_module_image</code> parameters are mutually exclusive and only one can be executed at a time.	

3 Press **Enter**.

—End—

The software download process 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 process. Depending on network conditions, this process may take up to 10 minutes.

When the download process is complete, the switch automatically resets unless the `no-reset` parameter was used. 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 87).

Software download message output

```
Download Image [/]

Saving Image [-]

Finishing Upgrading Image
```

During the download process the switch is not operational.

The progress of the download process can be tracked by observing the front panel LEDs. For more information about this topic, refer to "[LED activity during software download](#)" (page 94).

Changing switch software in the Java Device Manager

To change the software version running on the switch using the Java Device Manager, follow this procedure:

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

- | | |
|---|--|
| 1 | Connect to the switch using the Java Device Manager (JDM). For specific information about this topic, refer to " Opening a Switch with the Java Device Manager " (page 39). |
| 2 | From the JDM menu select Edit > File System . |

The File System screen appears. "[Java Device Manager File System screen](#)" (page 88) illustrates an example of this screen.

Java Device Manager File System screen

- | | |
|---|--|
| 3 | Select the Config/Image/Diag file tab if it is not already selected. |
| 4 | In the fields provided, specify the information necessary to perform the download process. " File System screen fields " (page 88) outlines each of the fields present 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. This field is used when working with configuration files and is not used when downloading a software image. For further information about this topic, refer to "Working with configuration files" (page 95) .
BinaryConfigUnit Number	The unit number of the portion of the configuration file that has to be extracted and used for the stand-alone unit configuration. If this value is 0 it is ignored. This field is used when working with configuration files and is not used when downloading a software image. For further information about this topic, refer to "Working with configuration files" (page 95) .
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	This field indicates the unit number of the USB port to be used in file upload or download operation.
Action	<p>This group of option buttons represents the actions that are to be taken during this file system operation. The options applicable to a software download are:</p> <ul style="list-style-type: none"> • dnldImg - Select this option to 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. • dnldFw - Select this option to 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. • dnldImgIfNewer - Select this option to download a new software image to the switch only if it is newer than the one currently in use.

Field	Description
	<ul style="list-style-type: none"> • dnldImgFromUsb - Select this option to 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. This option is only available on the Nortel Ethernet Routing Switch 5530-24TFD. • dnldFwFromUsb - Select this option to 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. This option is only available on the Nortel Ethernet Routing Switch 5530-24TFD. • dnldImgNoReset - Select this option to 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. After the download is complete, the switch is not reset. • dnldFwNoReset - Select this option to 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. <p>Note: For information about additional options, refer to "Working with configuration files" (page 95).</p>
Status	<p>Displays the status of the last action that occurred since the switch was last booted. The values that are displayed are:</p> <ul style="list-style-type: none"> • other - No action has taken place since the last boot. • inProgress - The selected operation is currently in progress.

Field	Description
	<ul style="list-style-type: none"> • success - The selected operation was successful. • fail - The selected operation failed.

5 Click **Apply**.

—End—

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

Changing switch software in the Web-based Management Interface

To change the software version running on the switch using the Web-based Management Interface, follow this procedure:

Step	Action
1	Log in to the Web-based Management Interface. For specific information about this topic, refer to " Accessing the Web-based Management Interface " (page 56).
2	Navigate to the Software Download Management page by selecting Configuration > Software Download from the menu. The Software Download Management page appears. " Software Download Management page " (page 92) illustrates an example of this page.

Software Download Management page

- 3 In the provided fields, specify the information needed to complete the software download procedure. "Software download page fields" (page 92) outlines each of the fields present 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 on to the switch. This field is optional if performing a diagnostics image download only and can be between 1 and 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 performing a software image download only and can be between 1 and 30 characters in length.
Select Target (5530-24TFD Only)	The target from which the software images are downloaded. Select either TFTP Server or USB as the download target. This field is only present for 5530-24TFD switches.

Field	Description
TFTP Server IP Address	The IP address of the TFTP Server to be used in the software download. If a 5530-24TFD switch is being used, and USB was selected in the Select Target list, this field is optional.
Start TFTP Load of New Image	<p>The type of software download to perform. Select the appropriate option from the list. The options are:</p> <ul style="list-style-type: none"> • No - Do not perform a software download of any kind. • 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. • 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 process occurs automatically after clicking **Submit**. This process erases the contents of flash memory and replaces it with the new software image. Do not interrupt the download process. Depending on network conditions this process can take up to 10 minutes. When the download process is complete, the switch automatically resets and the new software image initiates a self-test. During the download process, the switch is not operational.

LED activity during software download

During the software download process, the port LEDs light one after another in a chasing pattern except for ports 11, 12, 23, and 24 on a Nortel Ethernet Routing Switch 5510-24T and ports 35, 36, 47, and 48 on a Nortel Ethernet Routing Switch 5510-48T.

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 of the processes in the switch can make use of a Trivial File Transfer Protocol (TFTP) server. The following sections detail how to set a default TFTP server for the switch and to clear these defaults through the command line interface:

- ["Setting a default TFTP server" \(page 94\)](#)
- ["Displaying the default TFTP server" \(page 94\)](#)
- ["Clearing the default TFTP server" \(page 95\)](#)

Setting a default TFTP server

The switch processes that make use of a TFTP server often give the switch administrator the option of specifying the IP address of a TFTP server to be used. Instead of entering this address every time it is needed, a default IP address can be stored on the switch.

A default TFTP server for the switch is specified with the `tftp-server` command. The syntax of this command is:

```
tftp-server <A.B.C.D>
```

To complete the command, replace the `<A.B.C.D>` with the IP address of the default TFTP server. This command must be executed in the Privileged EXEC command mode.

Displaying the default TFTP server

The default TFTP server configured for the switch can be displayed in the CLI at any time by using the `show tftp-server` command. This command has no parameters and is executed in the Privileged EXEC mode.

Clearing the default TFTP server

The default TFTP server can be cleared from the switch and reset to 0.0.0.0 with the following two commands:

- `no tftp-server`

This command has no parameters and is executed from the Global Configuration command mode.

- `default tftp-server`

This command has no parameters and is executed from the Global Configuration command mode.

Working with configuration files

This section details working with configuration files through the various switch interfaces. Configuration files are ASCII text files that allow the administrator to quickly change the configuration of a switch.

This section contains information about the following topics:

- ["Configuration files in the CLI" \(page 95\)](#)
- ["Configuration files in the JDM" \(page 97\)](#)
- ["Configuration files in the Web-based Management Interface" \(page 102\)](#)
- ["Automatically downloading a configuration file" \(page 107\)](#)

Configuration files in the CLI

The CLI provides many options for working with configuration files. Through the CLI, configuration files can be displayed, stored, and retrieved.

For details, refer to the following:

- ["Displaying the current configuration" \(page 95\)](#)
- ["Storing the current configuration" \(page 96\)](#)
- ["Restoring a system configuration" \(page 96\)](#)
- ["Saving the current configuration" \(page 97\)](#)

Displaying the current configuration

The `show running-config` command displays the current configuration of switch or a stack.

The syntax for the `show running-config` command is:

- `show running-config`

This command only can be executed in the Privileged EXEC mode and takes no parameters.

Storing the current configuration

The `copy running-config` command copies the contents of the current configuration file to another location for storage. For all switches in the 5500 Series, the configuration file can be saved to a TFTP server. The Nortel Ethernet Routing Switch 5530-24TFD also provides the ability to save the configuration file to a USB Mass Storage Device through the front panel USB drive.

The syntax for the `copy running-config` command is:

- `copy running-config {tftp | (usb) [u2]} address <A.B.C.D> filename <name>`

"[copy running-config parameters](#)" (page 96) outlines the parameters for using this command.

copy running-config parameters

Parameter	Description
{tftp usb}	This parameter specifies the general location in which the configuration file is saved. On 5510 and 5520 Nortel Ethernet Routing Switches, TFTP is always used. On a 5530-24TFD the option is available to use the provided USB port.
address <A.B.C.D>	If a TFTP server is to be used, this parameter signifies the IP address of the server to be used.
filename <name>	The name of the file that is created when the configuration is saved to the TFTP server or USB Mass Storage Device.

The `copy running-config` command only can be executed in the Privileged EXEC mode.

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 stored on a TFTP server. The syntax is:

— `copy tftp config address <A.B.C.D> filename <name>`

"[copy tftp config parameters](#)" (page 97) outlines the parameters for this command.

copy tftp config parameters

Parameter	Description
address <A.B.C.D>	The IP address of the TFTP server to be used.
filename <name>	The name of the file to be retrieved.

- **copy usb config**

On the Nortel Ethernet Routing Switch 5530-24TFD, use this command to restore a configuration file stored on 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 unit**

This command enables the configuration of a switch in a stack to be copied to a stand-alone switch for the purpose of replacing units in a stack. The syntax is:

— **copy tftp config unit address <A.B.C.D> filename <name> unit <unit number>**

"[copy tftp config unit parameters](#)" (page 97) outlines the parameters for this command.

copy tftp config unit parameters

Parameter	Description
address <A.B.C.D>	The IP address of the TFTP server to be used.
filename <name>	The name of the file to be used.
unit <unit number>	The number of the stack unit to be used.

Saving the current configuration

The configuration currently in use on a switch is regularly saved to the flash memory automatically. However, this process can be manually initiated using the **copy config nvram** command. This command takes no parameters and must be issued from the Privileged EXEC mode.

Configuration files in the JDM

The Java Device Manager (JDM) provides tools for the storage and retrieval of configuration files.

For details, refer to the following topics:

- "Storing the current ASCII configuration" (page 98)
- "Retrieving an ASCII configuration file" (page 99)
- "Storing a binary configuration file" (page 100)
- "Retrieving a binary configuration file" (page 101)

Storing the current ASCII configuration

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

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 100).
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 the configuration file is stored.
5	If the configuration file is saved to a USB storage device, enter the stack unit number in which the USB device is inserted in the UsbTargetUnit field.
6	Select the uploadNow option button in the AsciiConfigManualUpload field to transfer the file to a TFTP server or select the uploadToUsb option button 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 shown as inProgress , wait for up to two minutes and then click Refresh to see any new status that has been 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 USB storage device and apply it to the switch, perform the following tasks:

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 100).
3	In the LoadServer Addr field, type the IP address of the desired TFTP server. If the configuration file is retrieved from a USB storage device, skip this step.
4	In the AsciiConfigFilename field, type the name under which the configuration file is stored.
5	If the configuration file is retrieved from a USB storage device, enter the stack unit number in which the USB device is inserted in the UsbTargetUnit field.
6	Select the downloadNow option button in the AsciiConfigManual-Download field to transfer the file from a TFTP server, or select the downloadFromUsb option button in the AsciiConfigManualDownload field to transfer the file from a USB mass storage device.
7	Click Apply .
8	Check the AsciiConfigManualDldStatus field for the file transfer status. If the status of the file download is shown as inProgress , wait for up to two minutes and then click Refresh to see any new status that has been applied to the download. The file download is complete when the status displays either Passed or Failed .

—End—

AsciiConfigFile tab

192.168.249.46 - FileSystem

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

LoadServerAddr: 192.168.249.10

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...

Storing a binary configuration file

To store the current binary configuration file to a TFTP server or USB storage device, follow this 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 88).
- 3 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. If the file is stored on a USB storage device, skip this step.
- 4 Enter the name to assign to the configuration file in the **BinaryConfigFilename** field.
- 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 the configuration file is saved 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 the **upldConfig** option to upload to a TFTP server or **upldConfigtoUsb** to upload it to a USB storage device.
- 8 Click **Apply**.

—End—

Retrieving a binary configuration file

To retrieve a binary configuration file from a TFTP server, follow this 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 88).
3	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. If the file is retrieved from a USB storage device, skip this step.
4	Enter the name of the configuration file to retrieve in the BinaryConfigFilename field.
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 the configuration file is retrieved 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 the dnldConfig option to download the file from a TFTP server or dnldConfigFromUsb to download it from a USB storage device.
8	Click Apply .

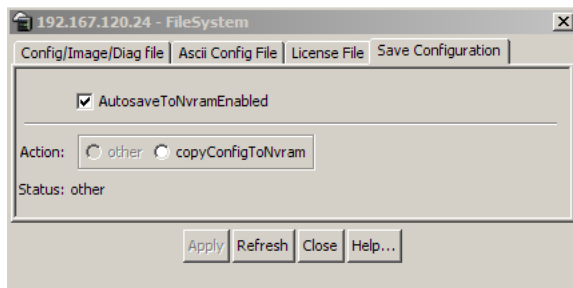
—End—

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.

To save the current configuration:

Step	Action
1	From the JDM menu, select Edit > File System . 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, choose **copyConfigToNvram**.
- 4 Click **Apply**.
- 5 Click **Refresh**
The Status field displays the file copy progress.

—End—

Autosaving the current configuration

If you enable **AutosaveToNvramEnabled**, the configuration currently in use on a switch is regularly saved to the flash memory. You can enable or disable **AutosaveToNvramEnabled** from the **Edit > File System > Save Configuration** tab.

Configuration files in the Web-based Management Interface

The Web-based Management Interface provides tools for the storage and retrieval of configuration files.

For details, refer to the following topics:

- ["Storing and retrieving a configuration file through TFTP or USB" \(page 103\)](#)
- ["Retrieving a configuration file through HTTP or USB" \(page 105\)](#)

Storing and retrieving a configuration file through TFTP or USB

The **Configuration File Download/Upload** page in the Web-based Management Interface is used to store or retrieve a configuration file. This page is illustrated in "Configuration File Download/Upload page" (page 103).

Configuration File Download/Upload page

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 that are relevant to the file upload process. "File upload fields" (page 103) outlines the relevant fields.

File upload fields

Field	Description
Configuration Image Filename	The name of the file to be created during the upload process.
Select Target	The location to which the file is uploaded. On the Nortel Ethernet Routing Switch 5530-24TFD, this can be either TFTP (TFTP Server) or USB (USB Mass Storage Device). On all other switches in the 5500 Series only the TFTP option is available.
TFTP Server IP Address	The IP address of the TFTP server to be used if applicable.
Copy Configuration Image To Target	To perform a file upload, ensure that YES is selected from this list.
Retrieve Configuration Image From Target	To perform a file upload, ensure that NO is selected 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 that are relevant to the file download process. "[File download fields](#)" (page 104) outlines the relevant fields.

File download fields

Field	Description
Configuration Image Filename	The name of the file to be retrieved during the download process.
Select Target	The location from which the file is downloaded from. On the Nortel Ethernet Routing Switch 5530-24TFD, this can be either TFTP (TFTP Server) or USB (USB Mass Storage Device). On all other switches in the 5500 Series, only the TFTP option is available.
TFTP Server IP Address	The IP address of the TFTP server to be used if applicable.
Copy Configuration Image To Target	To perform a file download, ensure that NO is selected from this list.
Retrieve Configuration Image From Target	To perform a file upload, ensure that YES is selected from this list.
Target Unit For Retrieve	This field is only available in stand-alone switches. Instead of downloading a fixed configuration file, it is possible to download the configuration from another switch in stack when replacing 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

The **Configuration File Download/Upload** page requires the usage of a TFTP server when working with 5500 Series switches that have no USB port present. The **Ascii Configuration File Download** page, however, enables the administrator to download an ASCII text configuration file to the switch directly without the need of a TFTP server.

"[Ascii Configuration File Download page](#)" (page 105) illustrates the **Ascii Configuration File** download page.

Ascii Configuration File Download page

On the Nortel Ethernet Routing Switch 5530-24TFD an ASCII configuration file can be downloaded from either a computer or through the switch USB port. On other switches in the 5500 Series this process only can be done through a computer.

To download an ASCII configuration file from a computer, perform these tasks:

Step	Action
1	Open the page by selecting Configuration > Ascii Config Download from the Web-based Management Interface.
2	In the table entitled Ascii Configuration File Download Setting , type the name of the file, including the full local path, in the Ascii Configuration File field. Alternately, 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.

As noted, on the 5530-24TFD switch the option also exists to download an ASCII configuration file through the provided USB port. To download the configuration file through the USB port, follow this procedure:

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

- | | |
|---|---|
| 1 | Open the page by selecting Configuration > Ascii Config Download from the Web-based Management Interface. |
| 2 | In the table entitled Ascii Configuration USB File Download Setting (present only on 5530-24TFD switches), supply the necessary information in the fields provided to complete the file download. " Ascii USB file download fields " (page 106) outlines the fields present. |

Ascii USB file download fields

Field	Description
Select Target	The target from which the file is downloaded. The only selectable option in this case is USB .
Ascii Configuration File	The name of the configuration file to be downloaded to the switch.
Retrieve Configuration File from Target	To proceed with the file transfer, change the value in the drop-down 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

The switch also can be configured to automatically download a configuration when it boots. This section covers how to configure a switch to perform this task:

- ["Using the CLI" \(page 107\)](#)
- ["Using the JDM" \(page 108\)](#)

Using the CLI

This feature is enabled through the CLI by using the `configure network` command. This command enables a script to be loaded and executed immediately as well as 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 <A.B.C.D> filename <name>
```

["configure network parameters" \(page 107\)](#) outlines the parameters for this command.

configure network parameters

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

Parameter	Description
address <A.B.C.D>	The IP address of the desired TFTP server.
filename <name>	The name of the configuration file to use in this process

This command must be run in the Privileged EXEC mode.

The current switch settings relevant to this process can be viewed using the **show config-network** command. This command takes no parameters and must be executed in Privileged EXEC mode.

Using the JDM

This feature is enabled through the Java Device Manager (JDM) by using the **File System** screen. To enable the automatic downloading of a configuration file, follow this 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 100).
3	Type the IP address of the desired TFTP server in the LoadServerAddr field.
4	Type the name of the configuration file to be used in the AsciiConfigFilename field.
5	From the AsciiConfigAutoDownload field, select the option button that represents how the configuration file is to be downloaded. The options are: <ul style="list-style-type: none"> • disabled - Automatic downloading is disabled. • useBootp - Use BootP to 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 .

—End—

Terminal setup

Switch terminal settings can be customized to suit the preferences of a switch administrator. This operation must be performed in the Command Line Interface.

The `terminal` command configures terminal settings. These settings are transmit and receive speeds, terminal length, and terminal width.

The syntax of the `terminal` command is:

```
terminal speed {2400|4800|9600|19200|38400} length
<0-132> width <1-132>
```

The terminal command is executed in the User EXEC command mode. "[terminal parameters](#)" (page 109) describes the parameters and variables for the terminal command.

terminal parameters

Parameter	Description
speed {2400 4800 9600 19200 38400}	Sets the transmit and receive baud rates for the terminal. The speed can be set at one of the five options shown; the default is 9600.
length	Sets the length of the terminal display in lines; the default is 23. Note: If the terminal length is set to a value of 0, the pagination is disabled and the display continues to scroll without stopping.
width	Sets the width of the terminal display in characters; the default is 79.

The `show terminal` command can be used at any time to display the current terminal settings. This command takes no parameters and is executed in the EXEC command mode.

Setting the default management interface

The default management interface can be set using the command line interface to suit the preferences of the switch administrator. This selection is stored in NVRAM and propagated to all units in a stack configuration. When the system is started, the banner displays and prompts the user to enter **Ctrl+Y**. After these characters are entered, the system displays either a menu or the command line interface prompt, depending on previously configured defaults. When using the console port, you must log out for the new mode to display. When using Telnet, all subsequent Telnet sessions display the selection.

To change the default management interface, use the `cmd-interface` command. The syntax of this command is:

```
cmd-interface {cli | menu}
```

The `cmd-interface` command must be executed in the Privileged EXEC command mode.

Setting Telnet access

The CLI can be accessed 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 access the CLI system simultaneously, through the serial port, Telnet, and modems. The maximum number of simultaneous users is four, plus, one each at the serial port for a total of 12 users on the stack. All users can configure simultaneously.

For details on viewing and changing the Telnet-allowed IP addresses and settings, refer to the following:

- ["telnet-access command" \(page 110\)](#)
- ["no telnet-access command" \(page 111\)](#)
- ["default telnet-access command" \(page 112\)](#)

telnet-access command

The `telnet-access` command configures the Telnet connection that is used to manage the switch. The `telnet-access` command is executed 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>
<A.B.C.D> [mask <A.B.C.D>]
```

The `telnet-access` command is executed in the Global Configuration command mode.

["telnet-access parameters" \(page 110\)](#) describes the parameters for the `telnet-access` command.

telnet-access parameters

Parameters	Description
enable disable	Enables or disables Telnet connection.

Parameters	Description
login-timeout <1-10>	Specify in minutes the time for the Telnet connection to be established after connecting to the switch. Enter an integer between 1 and 10.
retry <1-100>	Specify the number of times the user can enter an incorrect password before closing the connection. Enter an integer between 1 and 100.
inactive-timeout <0-60>	Specify in minutes the duration for an inactive session to be terminated.
logging {none access failures all}	Specify the events whose details you want to store 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> <A.B.C.D> [mask <A.B.C.D>]	Specify the source IP address from which connections are allowed. Enter the IP address in dotted-decimal notation. Mask specifies the subnet mask from which connections are allowed; 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>]]
```

The `no telnet-access` command is executed in the Global Configuration command mode.

"[no telnet-access parameters](#)" (page 112) describes the parameters and variables for the `no telnet-access` command.

no telnet-access parameters

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

The `default telnet-access` command is executed in the 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, refer to the following:

- ["web-server command" \(page 112\)](#)
- ["no web-server command" \(page 113\)](#)

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}
```

The `web-server` command is executed in the Global Configuration command mode.

"[web-server parameters](#)" (page 113) describes the parameters and variables for the `web-server` command.

web-server parameters

Parameters and variables	Description
enable disable	Enables or disables 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
```

The `no web-server` command is executed in the Global Configuration command mode.

Setting boot parameters

The command outlined in this section is used for booting the switch or stack as well as setting 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] [partial default] [unit <unitno>]
```

The `boot` command is executed in the Privileged EXEC command mode.

"[boot parameters](#)" (page 113) describes the parameters for the `boot` command.

boot parameters

Parameters and variables	Description
default	Reboot the stack or switch and use the factory default configurations
partial-default	Reboot the stack or switch and use partial factory default configurations
unit <unitno>	Unit number

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

Defaulting to BootP-when-needed

The BootP default value is BootP-when-needed. This enables the switch to be booted and the system to automatically seek a BootP server for the IP address.

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

However, if the device does not have an assigned IP address 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 rebooting the device.

When the system is upgraded, the switch retains the previous BootP value. When the switch is defaulted 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" \(page 114\)](#)
- ["no ip bootp server command" \(page 115\)](#)
- ["default ip bootp server command" \(page 115\)](#)

ip bootp server command

The `ip bootp server` command configures BootP on the current instance of the switch or server. This command is used 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}
```

The `ip bootp server` command is executed in the Global Configuration command mode.

["ip bootp server parameters" \(page 115\)](#) describes the parameters for the `ip bootp server` command.

ip bootp server parameters

Parameters and variables	Description
always disable last needed	<p>Specifies 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
```

The `no ip bootp server` command is executed in the 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
```

The `default ip bootp server` command is executed in the Global Configuration command mode.

Configuring and enabling DHCP

Use the `ip dhcp` commands to enable, disable and view the state of the DHCP client. When configuring DHCP on a stack, changes affect only the base unit.

- ["ip dhcp server command" \(page 115\)](#)
- ["no ip dhcp server command" \(page 116\)](#)
- ["show ip dhcp command" \(page 116\)](#)

ip dhcp server command

The `ip dhcp server` command enables the DHCP client and starts the autoconfiguration process. This command can also be used to set the lease time and renew the lease.

The syntax of the `ip dhcpc server` command is:

```
ip dhcpc server [always | disable | last | needed | renew |
lease <seconds>]
```

The `ip dhcpc server` command is executed in config mode.

"[ip dhcpc server command parameters and variables](#)" (page 116) shows the parameters and variable for use with the `ip dhcpc server` command.

ip dhcpc server command parameters and variables

Parameters and variables	Description
always	Always use the dhcpc server.
disable	Never use the dhcpc server.
last	Use dhcp or the last address.
needed	Use the dhcpc server when needed.
renew	Renew the IP lease.
lease <seconds>	Modify the lease interval for an IP address. <seconds>: the number of seconds duration for the modified lease.

Modify the DHCP client lease time after lease has already been acquired example

```
ip dhcpc server lease 600
ip dhcpc server renew
```

no ip dhcpc server command

The `no ip dhcpc server` server command disables use of the DHCP client. The syntax of the `no ip dhcpc server` command is:

```
no ip dhcpc server
```

The `ip dhcpc server` command is executed in config mode.

show ip dhcpc command

The `show ip dhcpc` command displays the status of the DHCP client. The syntax of the `show ip dhcpc` command is:

```
show dhcpc [address | default-gateway | lease | dns]
```

The four possible results (modes) of the status command are Always, Disabled, Last, and Needed.

The `ip dhcpc server` command is executed in config mode.

"[show ip dhcp command parameters and variables](#)" (page 117) shows the parameters and variable for use with the `show ip dhcpc` command.

show ip dhcp command parameters and variables

Parameters and variables	Description
address	Displays the DHCP client mode and the IP address acquired.
default-gateway	Displays the DHCP client mode and the IP address of the gateway.
lease	Displays the DHCP client mode and the lease time of the IP address obtained from the DHCP server.
dns	Displays the DHCP client mode and the IP address of the DNS server obtained from the DHCP server.

Customizing the CLI banner

The banner presented when a user logs in to the switch through the CLI can be configured 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, refer to the following commands:

- ["show banner command" \(page 117\)](#)
- ["banner command" \(page 118\)](#)
- ["no banner command" \(page 118\)](#)

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

- ["Banner tab" \(page 119\)](#)
- ["Custom Banner tab" \(page 120\)](#)

show banner command

The `show banner` command displays the banner.

The syntax for the `show banner` command is:

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

The `show banner` command is executed in the Privileged EXEC command mode.

["show banner parameters" \(page 118\)](#) describes the parameters for the `show banner` command.

show banner parameters

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

banner command

The **banner** command specifies the banner displayed at startup; either static or custom.

The syntax for the banner command is:

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

"[banner parameters](#)" (page 118) describes the parameters for this command.

banner parameters

Parameters and variables	Description
static custom	Sets 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	Specifies the characters in the line number.

This command is executed in the Privileged EXEC 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
```

The **no banner command** is executed in the Privileged EXEC command mode.

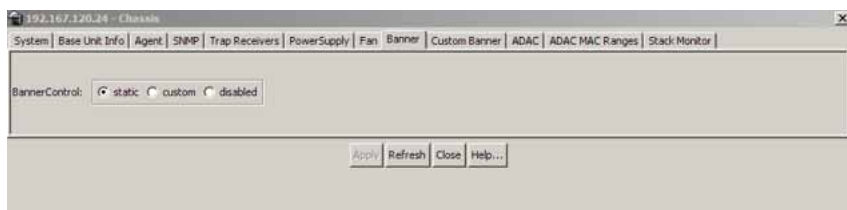
Banner tab

The Banner tab controls the CLI banner display.

To configure the Banner Control, follow this procedure:

Step Action

- 1 Open the **Edit Chassis** screen in the manner detailed at the beginning of this section.
- 2 Select the **Banner** tab. This tab is illustrated in the following figure.



—End—

The following table "[Banner tab items](#)" (page 119) describes the **Banner** tab items.

Banner tab items

Field	Description
BannerControl	<p>BannerControl specifies the banner to be displayed as soon as you connect to a Nortel Ethernet Routing Switch 5500 Series device. BannerControl has the following three options:</p> <ul style="list-style-type: none"> • The static option causes the predefined static banner to be used. • The custom option causes the previously set custom banner to be used when displaying a banner. • The disabled option prevents the display of any banners.

See also:

- "[System tab](#)" (page 237)
- "[Base Unit Info tab](#)" (page 241)
- "[Stack Info tab](#)" (page 243)

- "Agent tab" (page 246)
- "Power Supply tab " (page 247)
- "Fan tab " (page 249)
- "Custom Banner tab" (page 120)

Custom Banner tab

The Custom Banner tab customizes the CLI banner display.

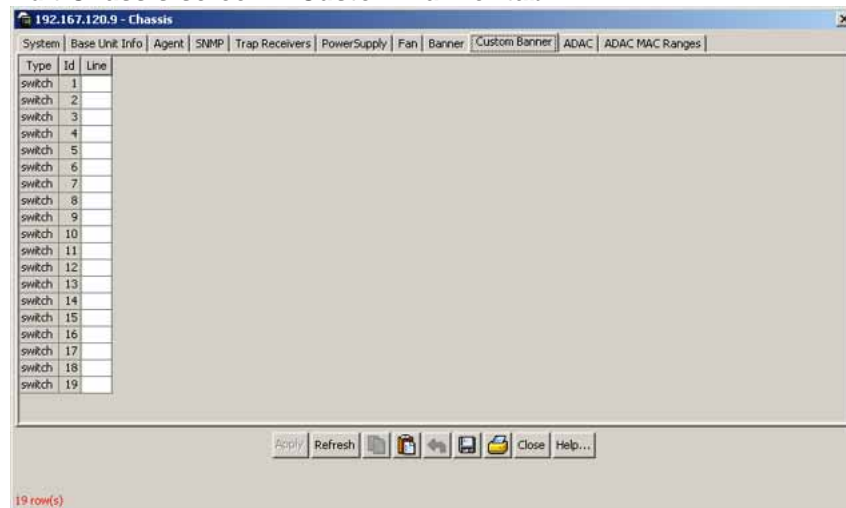
To customize the banner display, follow this procedure:

Step Action

- 1 Open the **Edit Chassis** screen in the manner detailed at the beginning of this section.
 - 2 Select the **Custom Banner** tab. This tab is illustrated in " [Edit Chassis screen -- Custom Banner tab](#)" (page 120).
-

—End—

Edit Chassis screen -- Custom Banner tab



The following table "[Custom Banner tab](#)" (page 121) describes the Custom Banner tab fields.

Custom Banner tab

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

Displaying complete GBIC information

Complete information can be obtained 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 does not show any 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 inclusion of 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. No special options are needed in these interfaces to display the additional information.

Shutdown command

This feature gives the switch administrator the ability to safely shut down the switch without fear of interrupting a process or corrupting the software image.

After the command is issued, the configuration is saved and blocking is performed, 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 resets the switch automatically.

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 2 minutes before resetting.

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 5500 Series

This chapter provides a general overview of the functionality and capabilities of the Nortel Ethernet Routing Switch 5500 Series. It contains information about the following topics:

- ["Hardware features" \(page 123\)](#)
- ["Auto Unit Replacement" \(page 132\)](#)
- ["Features of the Nortel Ethernet Routing Switch 5500 Series" \(page 142\)](#)
- ["Supported standards and RFCs" \(page 158\)](#)

Hardware features

This section provides information about the hardware features of the Nortel Ethernet Routing Switch 5500 Series.

Nortel Ethernet Routing Switch 5510

The Nortel Ethernet Routing Switch 5510 is a stackable Ethernet switch with 10/100/1000 Mb/s edge port connectivity.

The following are the two types of the Nortel Ethernet Routing Switch 5510 switches:

Nortel Ethernet Routing Switch 5510-24T

The Nortel Ethernet Routing Switch 5510-24T supports 10/100/1000Base-T, auto-sensing, and full-duplex RJ-45 ports.

The Nortel Ethernet Routing Switch 5510-24T also contains two mini GBIC slots. Nortel mini GBICs such as 1000Base-SX and 1000Base-LX optical transceivers can be inserted into these slots.

Nortel Ethernet Routing Switch 5510-48T

The Nortel Ethernet Routing Switch 5510-48T supports 10/100/1000Base-T, auto sensing full-duplex RJ-45 ports.

The Nortel Ethernet Routing Switch 5510-48T switch also contains two mini GBIC slots. Nortel mini GBICs such as 1000Base-SX and 1000Base-LX optical transceivers can be inserted into these slots.

Nortel Ethernet Routing Switch 5520

The Nortel Ethernet Routing Switch 5520 is an enterprise-level, Layer 4, diffserv-capable, stackable managed Gigabit switch.

The Nortel Ethernet Routing Switch 5520 supports the IEEE802.3AF standard. The switch supports Power over Ethernet (PoE).

PoE refers to the ability of a switch to power network devices over an Ethernet cable. Some of these devices include Voice over Internet Protocol (VoIP) phones, Wireless LAN Access Points, security cameras, access control points, and so on.

The following are the two types of the Nortel Ethernet Routing Switch 5520 switches:

Nortel Ethernet Routing Switch 5520-24T switch

The Nortel Ethernet Routing Switch 5520-24T switch contains 24 10/100/1000Base-T autosensing, full-duplex RJ-45 ports.

The Nortel Ethernet Routing Switch 5520-24T contains four mini GBIC slots. Insert Nortel mini GBICs such as 1000Base-SX and 1000Base-LX optical transceivers into these slots.

Nortel Ethernet Routing Switch 5520-48T switch

The Nortel Ethernet Routing Switch 5520-48T switch contains 48 10/100/1000Base-T autosensing, full-duplex RJ-45 ports.

The Nortel Ethernet Routing Switch 5520-48T switches contains four mini GBIC slots. Insert Nortel mini GBICs such as 1000Base-SX and 1000Base-LX optical transceivers into these slots.

Nortel Ethernet Routing Switch 5530-24TFD

The Nortel Ethernet Routing Switch 5530-24TFD is a 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains twelve shared SFP ports and two XFP ports.

User interface button

The user interface (UI) button in the Nortel Ethernet Routing Switch 5500 Series provides easy-to-use stacking configuration.

Note: The setting configured with the front-panel UI button overrides the settings on the rear-panel Base Unit switch.

The UI button can be used to:

- Set the unit as the base unit.
- Set the unit as a non-base unit.
- Set the unit to use the Base Unit Selector on the rear panel. This helps to determine whether the unit is a base or a non-base unit.
- Reset the stack.
- Reset the unit.
- Set the default IP address.
- Download a software image or configuration file from the USB port (5530-24TFD only).
- Upload a configuration file from the USB port (5530-24TFD only).

After your command is accepted by the Nortel Ethernet Routing Switch 5500 Series, the new configuration is stored in NVRAM.

The given options are discussed in the following sections.

Setting the unit as the base unit

To set the unit as the base unit with the UI button:

Step	Action
1	<p>Press the UI button and hold it for three seconds.</p> <p>The unit is now in configuration mode, and the color and status of the Status LED turns green blinking.</p>
2	<p>Press the UI button once.</p> <p>The Base LED turns on, and the Up and Down LEDs are steady green to indicate that the button press was recognized.</p>
3	<p>Press the UI button and hold it for three seconds to confirm the command.</p> <p>The color and status of the Status LED returns to steady green after the command is accepted.</p> <p>If the command is rejected, the Status LED turns amber blinking.</p> <p>Note: Changes in the base unit are reflected only after restarting the system.</p>

—End—

Setting the unit as the non-base unit

To set the unit as a non-base unit using the UI button:

Step	Action
1	<p>Press the UI button and hold it for three seconds.</p> <p>The unit is now in configuration mode, and the color and status of the Status LED turns green blinking.</p>
2	<p>Press the UI button twice.</p> <p>The Base LED is off, and the Up and Down LEDs are steady green.</p>
3	<p>Press the UI button and hold it for three seconds to confirm the command.</p> <p>The color and status of the Status LED returns to steady green after the command is accepted.</p> <p>If the command is rejected, the Status LED turns amber blinking.</p> <p>Note: Changes in the base unit are reflected only after restarting the system.</p>

—End—

Setting the rear-panel Unit Select switch as the Base Unit selector

To set the rear panel Unit Select switch as the Base Unit selector:

Step	Action
1	<p>Press the UI button and hold it for three seconds.</p> <p>The unit is now in configuration mode, and the color and status of the Status LED turns green, blinking.</p>
2	<p>Press the UI button four times.</p> <p>The Base LED blinks to indicate that the rear-panel switch is used to select the base unit after the next startup.</p>
3	<p>Press the UI button and hold it for three seconds to confirm the command.</p> <p>The color and status of the Status LED returns to steady green after the command is accepted.</p> <p>If the command is rejected, the Status LED turns amber blinking.</p>

Note: Changes in the base unit are reflected only after restarting the system.

—End—

Resetting the stack

To reset the stack using the UI button:

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

- | | |
|---|---|
| 1 | Press the UI button and hold it for three seconds.
The unit is now in configuration mode, and the color and status of the Status LED turns green blinking. |
| 2 | Press the UI button three times.
The color and status of the Base LED, Down LED, and Up LED blink amber. |
| 3 | Press the UI button and hold it for three seconds to confirm the command. |
-

—End—

Resetting the unit

To reset the unit at any time, with the UI button, do the following:

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

- | | |
|---|--|
| 1 | Press the UI button and hold it for eight seconds.
The color and status of the Pwr LED turns amber, slow blinking to indicate that the system will reset in less than three seconds. To stop the reset, release the UI button.
The color and status of the Pwr LED turns amber, with fast blinking to indicate that the system will reset in less than one second. To stop the reset, release the UI button. |
|---|--|
-

—End—

Downloading a software image using the USB Port (5530-24TFD Only)

The Nortel Ethernet Routing Switch 5530-24TFD includes a USB port on the front panel of the switch that can be used for a variety of tasks. This USB port can be used in conjunction with the UI button to load a new software image on to the switch.

To load a new software image by using the UI button and a USB Mass Storage Device, do the following:

Step	Action
1	Load the desired software image on to a USB Mass Storage Device. The software image file name must be 55xx.img . If the file name does not follow this format, the remainder of this process will fail.
2	Insert the USB Mass Storage Device into the front panel USB port located to the left of the console port connector on the 5530-24TFD.
3	Press the UI button six times.
4	If a file conforming to the naming conventions in step 1 is found, the software download process commences.
5	After the download process is complete, the switch resets.

Note: The switch downloads the software image regardless of version or the current stack state of the switch. This process provides no warnings and commences on any 5530-24TFD, whether it is a base unit, non-base unit, or stand-alone switch.

—End—

Downloading a configuration file using the USB Port (5530-24TFD Only)

The Nortel Ethernet Routing Switch 5530-24TFD includes a USB port on the front panel of the switch that can be used for a variety of tasks. This USB port can be used in conjunction with the UI button to load a new configuration file on to the switch.

To load a new configuration file by using the UI button and a USB Mass Storage Device, do the following:

Step	Action
1	Load the desired configuration file on to a USB Mass Storage Device. The configuration file name must be ascii_cfg_55xx . If the

file name does not follow this format, the remainder of this process will fail.

- 2 Insert the USB Mass Storage Device into the front panel USB port located to the left of the console port connector on the 5530-24TFD.
- 3 Press the UI button seven times.
- 4 If a file conforming to the naming conventions in step 1 is found, the configuration file download process commences.

Note: The switch downloads the configuration file regardless of version or the current stack state of the switch. This process provides no warnings and commences on any 5530-24TFD, whether it is a base unit, non-base unit, or stand-alone switch.

—End—

Uploading a configuration file to the USB port (5530-24TFD only)

The Nortel Ethernet Routing Switch 5530-24TFD includes a USB port on the front panel of the switch that can be used for a variety of tasks. This USB port can be used in conjunction with the UI button to copy the switch configuration file to a USB Mass Storage Device.

To copy the switch configuration file by using the UI button and a USB Mass Storage Device, do the following:

Step Action

- 1 Insert a USB Mass Storage Device into the USB port present on the front panel of the 5530-24TFD to the left of the console port connector (in a stack, connect the device to the USB port on the Base Unit).
- 2 Press the UI button eight times.
- 3 The switch configuration file is copied to the USB Mass Storage Device.

—End—

Abandoning a command

To abandon a command that was entered with the UI button, perform either one of the following:

- Wait for about 20 seconds after entering the one-press (set to base unit) or the two-press (reset to base). The command is ignored.

- Press the UI button five more times. This enables you to exit from the configuration mode. However, the settings on the switch are not changed.

Note: When resetting the unit using the UI, wait for 60 seconds after the last configuration change. The system takes up to 60 seconds to save the configuration changes to NVRAM.

The stack can be reset immediately after changing the configuration by using the UI button without losing any of the changed configuration.

Cooling fans

Always ensure that allowance is made when installing the switch to allow enough space on both sides for adequate air flow.

See *Nortel Ethernet Routing Switch 5500 Series Installation* (NN47200-300) for detailed information about installation topics.

Redundant power supply and uninterruptible power supply

The redundant power supply connector enables the connection of a backup power supply unit to the Nortel Ethernet Routing Switch 5500 Series. Nortel provides an optional Redundant Power Supply (RPS) for this purpose.

The Nortel Ethernet Routing Switch 5520 requires a different RPS from that of the Nortel Ethernet Routing Switch 5510. The Nortel Ethernet Routing Switch 5510 uses a Nortel Ethernet 10 RPS and the Nortel Ethernet Routing Switch 5520 uses Nortel Ethernet 15 RPS.

The Nortel Ethernet 10 power supply unit is a hot-swappable unit that provides uninterrupted operation in the event of power failure.

The Nortel Ethernet 10 power supply unit has a powerful, modular, redundant, and uninterruptible power supply (UPS) functionality in a single chassis. It provides scalable power redundancy and protection to your networking equipment.

The modules fit into the right-hand side of the rear of the chassis. The UPS and associated battery pack module fit into the front of the chassis.

The Nortel Ethernet RPSU 15 provides scalable power redundancy and protection to low-wattage networking equipment. The PSU modules slides into the front of the Nortel Ethernet 15 chassis.

One PSU module connected to a Nortel Ethernet Routing Switch 5520 can provide up to 15.4 W for each port on all 48 or 24 ports.

DC-DC Converter Module

The DC-DC Converter Module for the Nortel Ethernet Routing Switch 5510 operates in conjunction with the Nortel Ethernet Power Supply Unit 10 and 200 Watt AC/DC Power Supply Module.

The Nortel Ethernet Routing Switch 5520 uses Nortel Ethernet Redundant Power Supply Unit 15 and 600 Watt Power Supply Module.

The 100 Watt DC-DC Converter provides a plug-and-play redundant power supply unit for the Nortel Ethernet Routing Switch 5510, as well as other products available from Nortel.

Contact your Nortel sales representative to order the converter module (order number AL 9504007) for the Nortel Ethernet Routing Switch 5510.

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

Stacking capabilities

You can use the Nortel Ethernet Routing Switch 5500 Series in:

- A stand-alone switch configuration
- A stack configuration

The Nortel Ethernet Routing Switch 5500 Series have a built-in cascade port that enables the stacking of up to eight units.

A stack can consist of Nortel Ethernet Routing Switch 5510-24T, Nortel Ethernet Routing Switch 5510-48T, Nortel Ethernet Routing Switch 5520-24T, Nortel Ethernet Routing Switch 5520-48T and Nortel Ethernet Routing Switch 5530-24TFD units.

The cascade port provides an 80 Gb cascading mechanism for the stacks.

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

To set up a stack, do the following:

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 of 5510-24T and 5510-48T, either switch can act as the base unit.

—End—

Auto Unit Replacement

The Auto Unit Replacement (AUR) feature enables users 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 kept on during the procedure.

Note 1: In order for Auto Unit Replacement to function properly, the new unit and the existing units in the stack must all be running the same version of software (Release 4.2 software or later).

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.

Other information related 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. It is overwritten with the restored configuration from the stack.
- This feature can be disabled/enabled 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 mirror of a CFG image (in FLASH) 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 has been 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

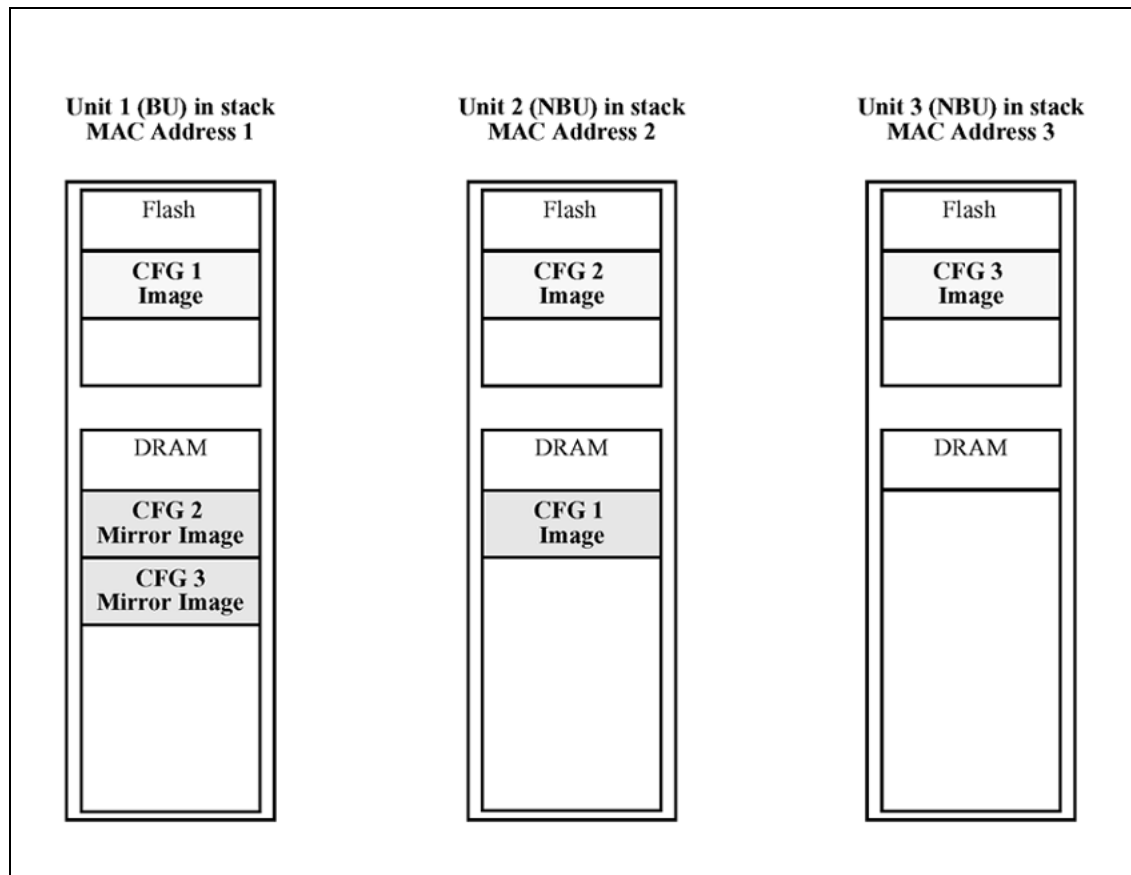
The CFG mirror image process is triggered by specific events.

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

"CFG mirror process in stack" (page 134) 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).

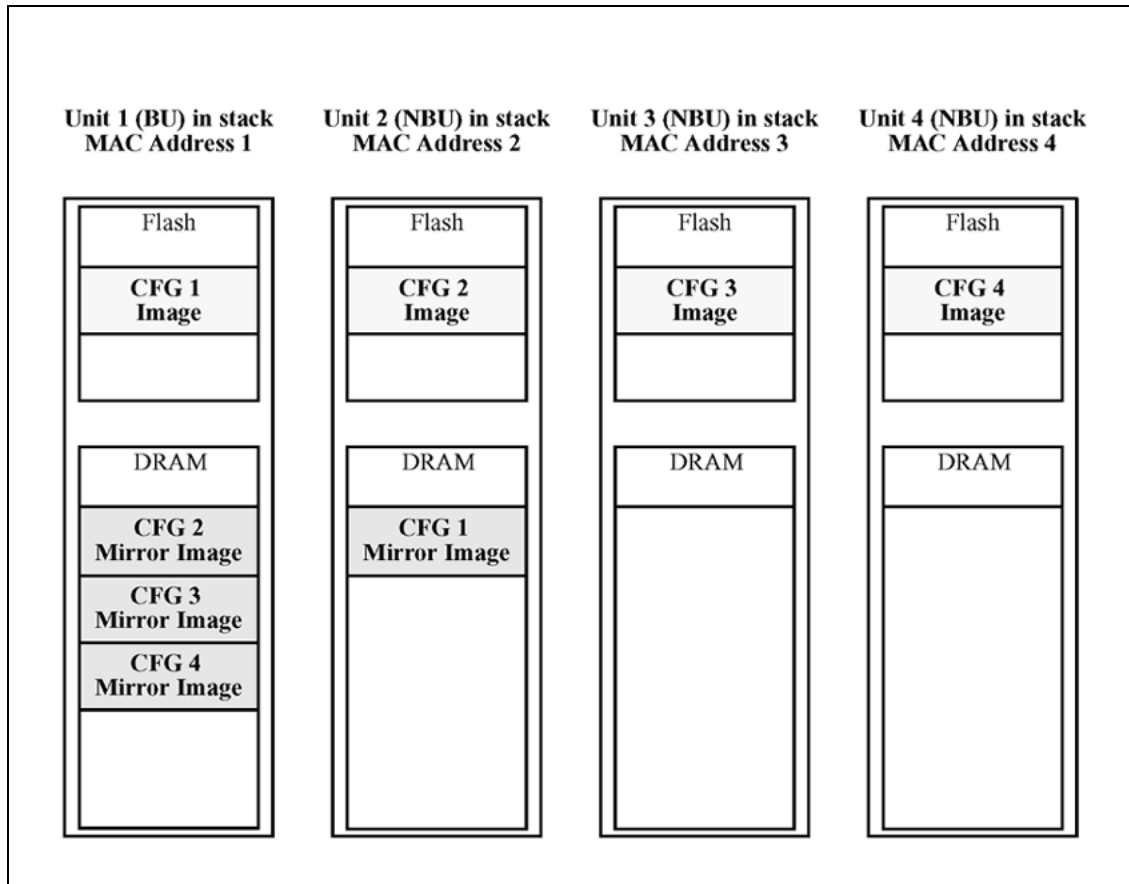
- Unit 1 (BU) contains mirror images for unit 2 (CFG 2) and unit 3 (CFG 3).
- Unit 2 (NBU), is the TEMP-BU. It contains a mirror image of unit 1 (CFG 1), in case the BU (unit 1) is removed from the stack.
- All three mirror images (CFG 1, CFG 2, and CFG 3) are active.
- Unit 2 is the Associated Unit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

CFG mirror process in stack



Adding a unit In a stack that does not have any INACTIVE CFG mirror images, adding 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 135), after adding 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

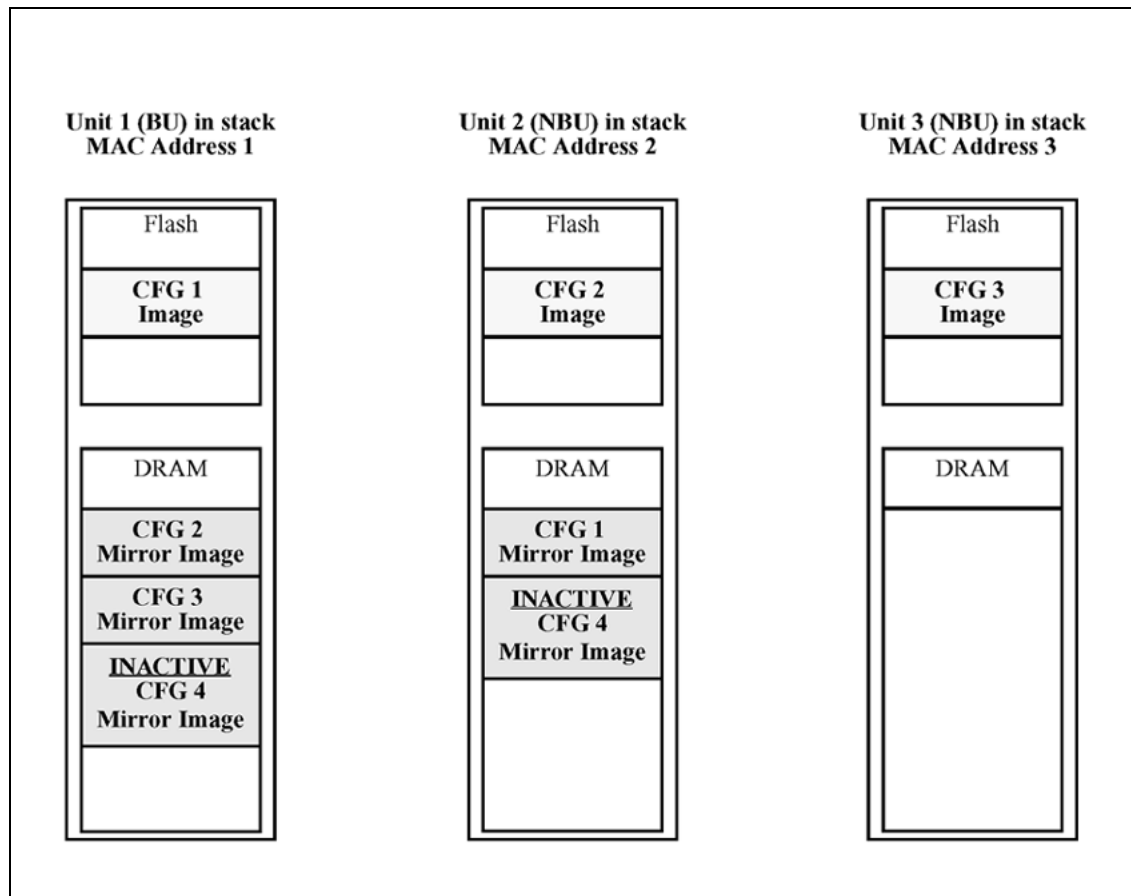


Removing an NBU When an NBU is removed from a stack, the related CFG mirror image in the stack becomes INACTIVE.

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 the removal of unit 4 from the stack shown in "CFG mirror images in the stack after adding unit 4" (page 135), the CFG 4 mirror image becomes INACTIVE (see "CFG mirror images after removing unit 4" (page 136)). Another copy of the INACTIVE CFG 4 mirror image is also created in unit 2.

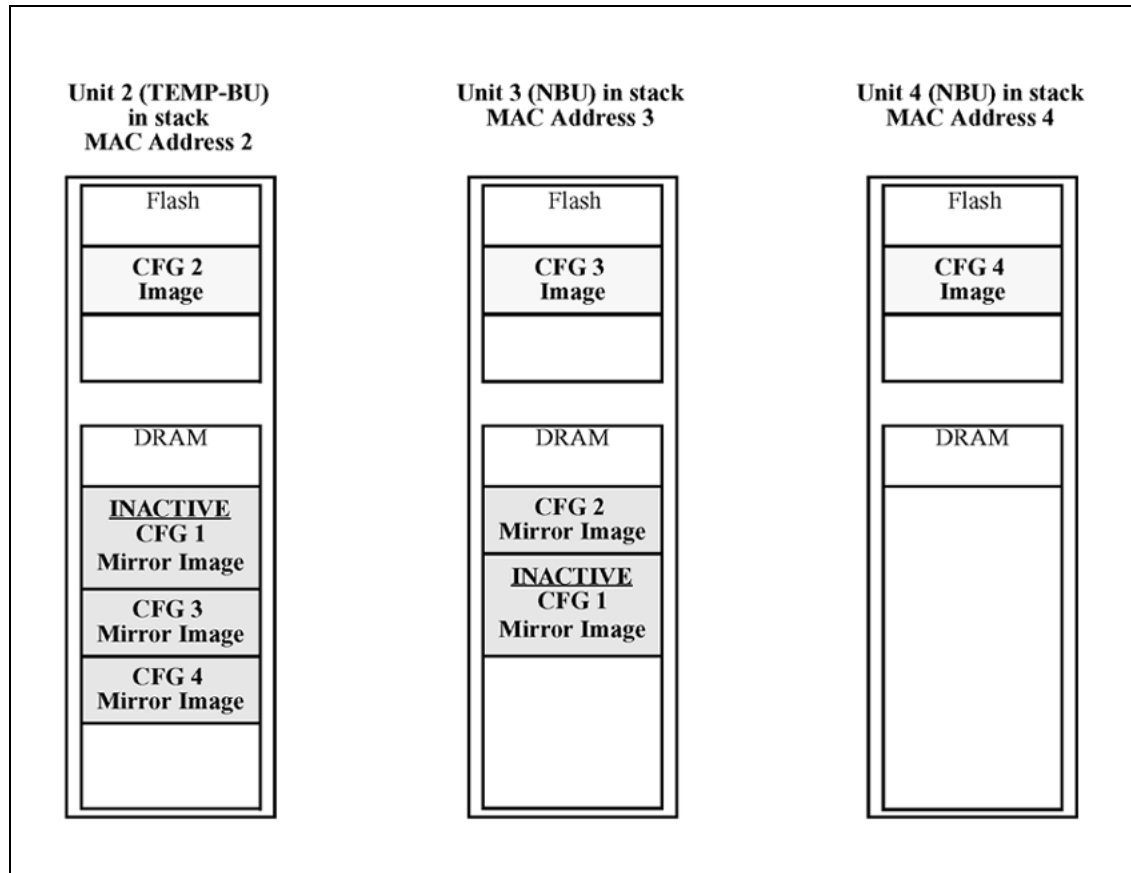
CFG mirror images after removing unit 4



Removing a BU When a BU is removed, 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 the removal of the BU from the stack shown in "CFG mirror images in the stack after adding unit 4" (page 135), the TEMP-BU (unit 2) has to mirror all the CFG images in the stack (see "CFG mirror images in the stack after removing the BU (unit 1)" (page 137)). 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 137):

- 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 stack's NBUs.
- The CFG 2 mirror image is created in unit 3. Unit 3 becomes the next TEMP-BU in case the current TEMP-BU is removed.

Restoring a CFG image

Restoring a CFG image is a process that 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 the following conditions are met.

- The AUR feature is enabled.

- There is at least one INACTIVE CFG mirror image 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.

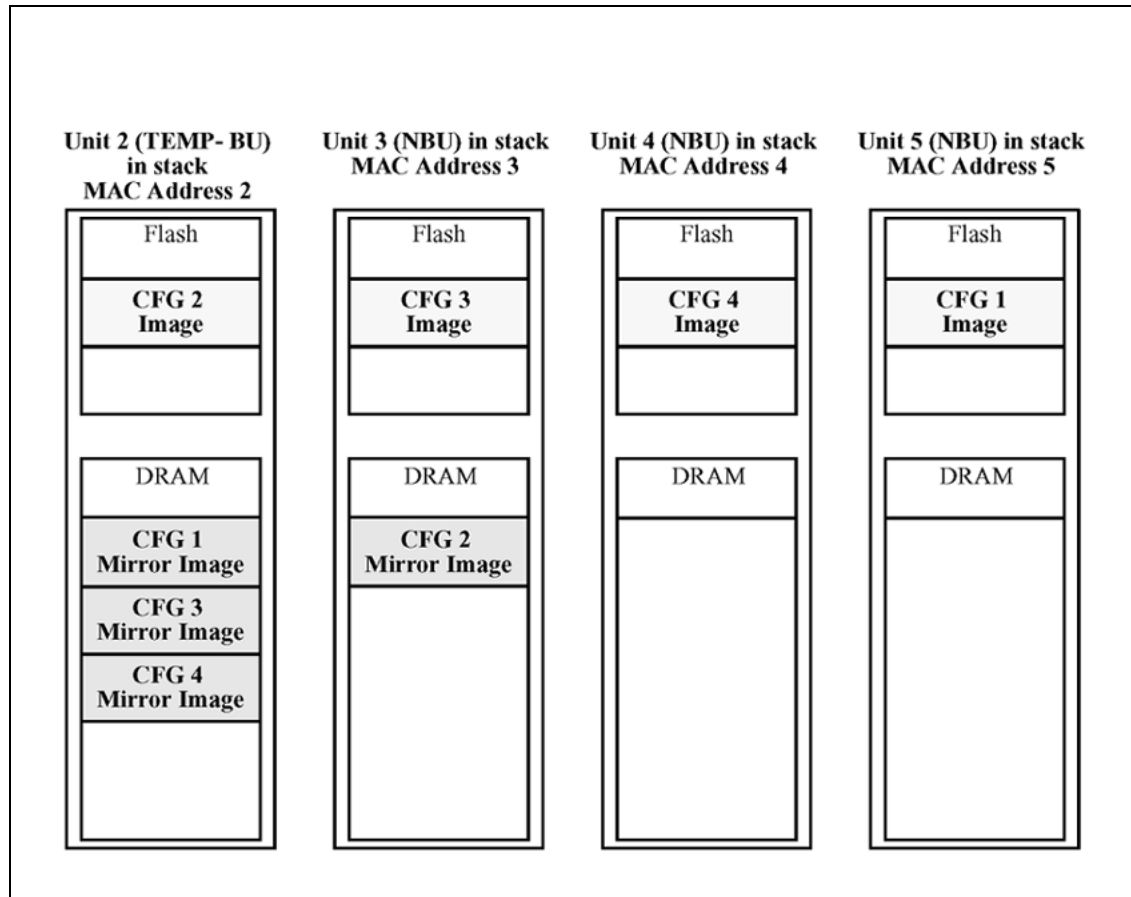
The image restore process consists of the following steps:

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

For example, if a unit 5 (MAC Address 5) is added to the stack shown in ["CFG mirror images in the stack after removing the BU \(unit 1\)"](#) (page 137), the following occurs (see ["CFG mirror images in the stack after adding unit 5"](#) (page 139)):

- The INACTIVE CFG 1 mirror image is copied to the CFG 5 image. Unit 5 now has the configuration of unit 1 that 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 CFG 1 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 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.

There are no parameters or variables 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
```

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

There are no parameters or variables 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
```

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

There are no parameters or variables 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
```

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

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

Configuring AUR using Device Manager

You also can enable or disable AUR using Device Manager by toggling the `AutoUnitReplacementEnabled` field in the **System** tab (see "[System tab](#)" (page 237)).

Agent Auto Unit Replacement (AAUR)

Software Release 4.2 and later supports an enhancement to the Auto Unit Replacement functionality known as Agent Auto Unit Replacement (AAUR). AAUR ensures 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:

Step	Action
1	When a stand-alone switch joins an AAUR-enabled stack, the switch software image is inspected.
2	If the switch software image is found to differ 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 reboot.

—End—

The CLI commands in the following sections are used to manage and configure AAUR. This functionality only can be managed currently through the CLI.

stack auto-unit-replacement-image enable command

The `stack auto-unit-replacement-image enable` command is used to enable Agent Auto Unit Replacement. Because AAUR is enabled by default, this command is only used if this functionality was previously disabled.

The syntax for this command is:

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

The `stack auto-unit-replacement-image enable` command is executed in the Global Configuration command mode.

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

The `no stack auto-unit-replacement-image enable` command is used to disable Agent Auto Unit Replacement. Because AAUR is enabled by default, this command must be executed if the AAUR functionality is not desired 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

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

The syntax of this command is:

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

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

show stack auto-unit-replacement-image command

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

The syntax of this command is:

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

The `show stack auto-unit-replacement-image` command is executed in the User EXEC command mode.

Features of the Nortel Ethernet Routing Switch 5500 Series

The Nortel Ethernet Routing Switch 5500 Series provides wire-speed switching that enables high-performance and low-cost connections to full-duplex and half-duplex 10/100/1000 Mb/s Ethernet Local Area Networks (LAN).

This section discusses the general features of the Nortel Ethernet Routing Switch 5500 Series.

- ["Flash memory storage" \(page 143\)](#)
- ["Policy-enabled networking" \(page 144\)](#)
- ["Power over Ethernet" \(page 144\)](#)
- ["Virtual Local Area Networks" \(page 144\)](#)
- ["Spanning Tree Protocol groups" \(page 145\)](#)
- ["Rapid Spanning Tree Protocol" \(page 146\)](#)
- ["Multiple Spanning Tree Protocol" \(page 146\)](#)
- ["Trunk groups" \(page 147\)](#)

- "Security" (page 147)
- "Port mirroring" (page 148)
- "Auto-MDI X" (page 148)
- "Auto-polarity" (page 149)
- "Autosensing and autonegotiation" (page 149)
- "ASCII configuration file" (page 153)
- "Displaying unit uptime" (page 155)
- "Port naming" (page 155)
- "Port error summary" (page 155)
- "IP address for each unit in a stack" (page 156)
- "BootP mode" (page 156)
- "Dynamic Host Configuration Protocol (DHCP)" (page 156)
- "Web quick start" (page 157)
- "Simple Network Time Protocol" (page 157)
- "Supported standards and RFCs" (page 158)

Flash memory storage

Switch software image storage

The Nortel Ethernet Routing Switch 5500 Series uses flash memory to store the switch software image.

Flash memory enables the updating the software image with a newer version without changing the switch hardware.

An in-band connection between the switch and the TFTP load host is required to download the software image.

Configuration parameter storage

All configuration parameters in the Nortel Ethernet Routing Switch 5500 Series are stored in flash memory.

These parameters are updated every 60 seconds if a change occurs, or whenever a reset command is executed.

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

Powering down the switch within 60 seconds can cause the changed configuration parameters to be lost.

Policy-enabled networking

The Nortel Ethernet Routing Switch 5500 Series enables the implementation of classes of services and assignment of priority levels to different types of traffic. Policies also can be configured to monitor the characteristics of traffic.

For example, in the Nortel Ethernet Routing Switch 5500 Series, it is possible to determine the sources, destinations, and protocols used by the traffic. It is also possible to perform a controlling action on the traffic when certain user-defined characteristics match.

The Nortel Ethernet Routing Switch 5500 Series supports Differentiated Services (DiffServ). DiffServ is a network architecture that enables service providers and enterprise network environments to offer varied levels of services for different types of data traffic.

DiffServ Quality of Service (QoS) enables you 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, DiffServ can be used to give preferential treatment to this data over other traffic.

Power over Ethernet

The Nortel Ethernet Routing Switch 5520 provides IEEE 802.3af compliant power or Power over Ethernet (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 such devices are IP Phones, Wireless LAN Access Points, security cameras, access control points and more.

The Nortel Ethernet Routing Switch 5520 automatically detects the network device requirements, and the switch dynamically supplies 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: Only the Nortel Ethernet Routing Switch 5520 supports Power over Ethernet (PoE).

A 4 pair Category 5 UTP cable must be used for PoE. A standard 2 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 5500 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 ingress the device containing an 802.1Q value. Untagged packets assume the PVID value assigned to the ingressing port as the 802.1Q value. The packets are forwarded only to those ports with VLAN membership lists containing the same 802.1Q value as the packet.

Automatic PVID automatically sets the PVID when you configure a port-based VLAN. When the port is added to the VLAN, the PVID value is the same value as the last port-based VLAN ID 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 assure that only the protocol-based VLAN ports are flooded with the specified protocol type packets. The maximum number of available protocols is 13 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 applies, the packet belongs to the VLAN identified by the PVID of the ingress port.

The Nortel Ethernet Routing Switch 5500 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 5500 Series or across a stack of switches.

Spanning Tree Protocol groups

The Nortel Ethernet Routing Switch 5500 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 5500 Series supports a maximum of eight STGs running simultaneously.

The Nortel Ethernet Routing Switch 5500 Series supports a maximum of 256 VLANs. Each STG can have 32 VLANs.

Rapid Spanning Tree Protocol

The standard Spanning Tree implementation in 5500 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. It also maintains a backward compatibility with the IEEE 802.1d. In certain configurations, the recovery time of RSTP can be reduced to less than 1 second. The backward compatibility can be maintained by configuring a port to be in STP-compatible mode. A port operating 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

The Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s) enables the user to 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.

RSTP and MSTP enable the 5500 Series switch to achieve the following:

- Reduce converging time from 30 seconds to less than 1 or 2 seconds when there is topology change in the network (that is, port going up or down).
- Eliminate unnecessary flushing of the MAC database and flooding of traffic to the network with a new Topology Change mechanism.
- Backward compatibility with other switches that are running legacy 802.1d STP or Nortel MSTG (STP group 1 only).
- Under MSTP mode, 8 instances of RSTP can be supported simultaneously. 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 5500 Series supports two types of trunk groups. They are:

- Link Aggregation Group (LAG): Trunk groups that are formed by Link Aggregation.
- Multilink Trunk (MLT): Trunk groups that are formed by Nortel Ethernet Routing Switch 5500 Series Multilink Trunking.

Link Aggregation

Link Aggregation (LA) provides the mechanism for creating and managing trunk groups. A trunk group can be controlled and configured automatically with the Link Aggregation Control Protocol (LACP).

The LACP, as defined by IEEE 802.3ad standard, enables 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

Multilink Trunking (MLT) enables grouping of multiple ports, two to eight together, at the time of linking to another switch or server. Doing so, it increases the aggregate throughput of the interconnection between two devices by 8 Gb in full-duplex mode.

The Nortel Ethernet Routing Switch 5500 Series can be configured with up to 32 MultiLink Trunks.

The trunk members can be configured within a single unit in the stack. They also can be distributed 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 5500 Series:

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

EAPOL-based security (IEEE 802.1X)	Enables the exchange of authentication information between any end station or server connected to the switch and authentication server, such as a RADIUS server.
TACACS+	Provides centralized validation of users attempting to gain access to the switch. Authentication, authorization, and accounting services are separate.
IP manager list	Limits access to management features of the switch based on the management station IP address.
SNMPv3	enables access to the various services by using password authentication (MD5), secure-hash algorithm (SHA), and encryption using the Data Encryption Standard (DES).
SSL	Provides a secure web management interface.
SSH	Replaces telnet and provides a secure access to the user console menu and CLI interface.
DHCP snooping	Filters untrusted DHCP messages and verifies the source of DHCP messages to prevent DHCP spoofing
Dynamic ARP inspection	Validates ARP packets in the network to protect against “man-in-the-middle” attacks.
Nortel Secure Network Access	Provides a protective framework to completely secure the network from endpoint vulnerability. The Nortel Secure Network Access (Nortel SNA) solution addresses endpoint security and enforces policy compliance. Nortel SNA provides a policy-based, clientless approach to corporate network access.

For more information about specific security features, refer to *Configuring and Managing Security for Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0(217463-B)*.

Port mirroring

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

This feature enables you to 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.

Auto-MDI/X detects, receive, and transmit twisted pairs automatically. When auto-MDI/X is active, any straight or crossover category 5 cable can be used to provide connection to a port. If autonegotiation is disabled, then auto-MDI/X is not active.

Auto-polarity

The term *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 5500 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 has been reversed due to a wiring error. If autonegotiation is disabled, auto-polarity is not active.

Autosensing and autonegotiation

The Nortel Ethernet Routing Switch 5500 Series are autosensing and autonegotiating devices:

- The term *autosense* refers to a port's ability to *sense* the speed of an attached device.
- The term *autonegotiation* refers to a standardized 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 is used when the attached device is not capable of autonegotiation or is using 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 5500 Series reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the Nortel Ethernet Routing Switch 5500 Series, the ports negotiate down from 1000 Mb/s speed and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

Custom Autonegotiation Advertisements

In the Nortel Ethernet Routing Switch 5500 Series, the Custom Autonegotiation Advertisements (CANA) feature enables you 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 that are supported by the switch and attempt to establish a link at the highest common speed and duplex setting. By using CANA, the

port can be configured to advertise only certain speed and duplex settings, thereby allowing links to be established only at these settings, regardless of the highest common supported operating mode.

CANA also enables control over the IEEE802.3x flow control settings advertised by the port, as part of the autonegotiation process. Flow control advertisements can be set to Symmetric, Asymmetric, or Disabled if neither is selected.

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

- If a network can support only 10 Mb/s connection, a port can be configured to advertise only 10 Mb/s capabilities. Devices using autonegotiation to connect to this port connect at 10 Mb/s, even if both devices are capable of higher speeds.
- If a port is configured to advertise only 100 Mb/s full-duplex capability, the link becomes active only if the link partner is also capable of autonegotiating 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, it can be useful to 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 line:

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

["auto-negotiation-advertisements command sample output"](#) (page 150) shows sample output for this command.

auto-negotiation-advertisements command sample output

```
5510-48T(config-if)#auto-negotiation-advertisements port 5 10-full
5510-48T(config-if)#
```

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

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

"show auto-negotiation-advertisements command sample output" (page 151) and "show auto-negotiation-advertisements command sample output" (page 151) show sample output for this command. Port 5 has been configured to only advertise an operational mode of 10 Mb/s full duplex.

show auto-negotiation-advertisements command sample output

```
5510-48T#show auto-negotiation-advertisements
Port Autonegotiation Advertised Capabilities
-----
 1  10Full 10Half 100Full 100Half 1000Full      Pause
 2  10Full 10Half 100Full 100Half 1000Full      Pause
 3  10Full 10Half 100Full 100Half 1000Full      Pause
 4  10Full 10Half 100Full 100Half 1000Full      Pause
 5  10Full
 6  10Full 10Half 100Full 100Half 1000Full      Pause
 7  10Full 10Half 100Full 100Half 1000Full      Pause
 8  10Full 10Half 100Full 100Half 1000Full      Pause
 9  10Full 10Half 100Full 100Half 1000Full      Pause
10  10Full 10Half 100Full 100Half 1000Full      Pause
11  10Full 10Half 100Full 100Half 1000Full      Pause
12  10Full 10Half 100Full 100Half 1000Full      Pause
13  10Full 10Half 100Full 100Half 1000Full      Pause
14  10Full 10Half 100Full 100Half 1000Full      Pause
15  10Full 10Half 100Full 100Half 1000Full      Pause
16  10Full 10Half 100Full 100Half 1000Full      Pause
17  10Full 10Half 100Full 100Half 1000Full      Pause
18  10Full 10Half 100Full 100Half 1000Full      Pause
19  10Full 10Half 100Full 100Half 1000Full      Pause
20  10Full 10Half 100Full 100Half 1000Full      Pause
----More (q=Quit, space/return=Continue)----
```

show auto-negotiation-advertisements command sample output

```
5510-48T#show auto-negotiation-advertisements port 5
Port Autonegotiation Advertised Capabilities
-----
 5  10Full
5510-48T#
```

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

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

"show auto-negotiation-capabilities command sample output" (page 152) and "show auto-negotiation-capabilities command sample output" (page 152) show sample output for this command.

show auto-negotiation-capabilities command sample output

```

5510-48T#show auto-negotiation-capabilities
Port Autonegotiation Capabilities
-----
 1  10Full 10Half 100Full 100Half 1000Full          Pause
 2  10Full 10Half 100Full 100Half 1000Full          Pause
 3  10Full 10Half 100Full 100Half 1000Full          Pause
 4  10Full 10Half 100Full 100Half 1000Full          Pause
 5  10Full 10Half 100Full 100Half 1000Full          Pause
 6  10Full 10Half 100Full 100Half 1000Full          Pause
 7  10Full 10Half 100Full 100Half 1000Full          Pause
 8  10Full 10Half 100Full 100Half 1000Full          Pause
 9  10Full 10Half 100Full 100Half 1000Full          Pause
10  10Full 10Half 100Full 100Half 1000Full          Pause
11  10Full 10Half 100Full 100Half 1000Full          Pause
12  10Full 10Half 100Full 100Half 1000Full          Pause
13  10Full 10Half 100Full 100Half 1000Full          Pause
14  10Full 10Half 100Full 100Half 1000Full          Pause
15  10Full 10Half 100Full 100Half 1000Full          Pause
16  10Full 10Half 100Full 100Half 1000Full          Pause
17  10Full 10Half 100Full 100Half 1000Full          Pause
18  10Full 10Half 100Full 100Half 1000Full          Pause
19  10Full 10Half 100Full 100Half 1000Full          Pause
20  10Full 10Half 100Full 100Half 1000Full          Pause
----More (q=Quit, space/return=Continue)----

```

show auto-negotiation-capabilities command sample output

```

5510-48T#show auto-negotiation-capabilities port 5
Port Autonegotiation Capabilities
-----
 5  10Full 10Half 100Full 100Half 1000Full          Pause
5510-48T#

```

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 line:

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

Silencing advertisements To set a port to not transmit any 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 line:

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

"default auto-negotiation-advertisements command sample output" (page 153) and "no auto-negotiation-advertisements command sample output" (page 153) show sample output from these commands.

default auto-negotiation-advertisements command sample output

```
5510-48T(config-if)#default auto-negotiation-advertisements port 5
5510-48T(config-if)#
```

no auto-negotiation-advertisements command sample output

```
5510-48T(config-if)#no auto-negotiation-advertisements port 5
5510-48T(config-if)#
```

ASCII configuration file

The Nortel Ethernet Routing Switch 5500 Series enables you to 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 console menus or CLI.

After the file is downloaded, the configuration file automatically configures the switch or stack according to the CLI commands given 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 KBs; larger configuration files must be split into multiple files.

Use a text editor to edit the ASCII configuration. The command format is the same as you use in the CLI.

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

When you initiate the downloading of the ASCII configuration file from the console interface, the console does not display any output. Therefore, it is important that you review the commands in the file to ensure accuracy and completeness.

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. This enables you to determine how long each unit has been connected to the stack. You can use the Command Line Interface (CLI) commands `system` 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 from a single console port.

Use the console interface (CI) menus or the CLI to configure the IP addresses for each unit within a stack.

BootP mode

The Nortel Ethernet Routing Switch 5500 Series supports the Bootstrap protocol (BootP).

BootP enables you to retrieve an ASCII configuration file name and configuration server address.

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

The Nortel Ethernet Routing Switch 5500 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 5500 Series BootP requests.

The BootP modes supported by the Nortel Ethernet Routing Switch 5500 Series are:

- BootP or Last Address mode
- BootP When Needed. This is the default mode.
- BootP Always
- BootP Disabled. Disabling BootP also disables DHCP.

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol is defined by the RFC 2131. DHCP allows individual TCP/IP hosts on an IP network to obtain their configuration information from a DHCP server (or servers) that have no exact information about the individual hosts until they request configuration parameters.

This reduces the work of system administrators, especially in larger IP networks, by eliminating the need to manually set every IP address. The most significant pieces of information distributed through DHCP are:

- the IP address
- the network mask

- the IP address of the gateway

In many networks, DHCP must coexist with VLANs, and the DHCP client can make its broadcasts only in the trusted VLANs. The DHCP client will run at startup just like the BootP client. The DHCP client restricts its discovery broadcasts to the management VLAN.

The DHCP modes supported by the Nortel Ethernet Routing Switch 5500 Series are:

- DHCP or Last Address mode
- DHCP When Needed.
- DHCP Always
- DHCP Disabled. Disable DHCP by setting BootP Disabled.

The host cannot act as a DHCP relay while the DHCP client is running.

Web quick start

The WEB Quick Start feature enables you 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.

The WEB Quick Start screen enables you 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 4)

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. NTP enables clocks to be synchronized to a few milliseconds, depending on the clock source and local clock hardware.

SNTP synchronizes to the Universal Coordinated Time (UTC) with an error of less than one 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.

SNTP accuracy is typically in the order of "significant fractions of a second." This accuracy is related to the latencies between the SNTP client device and the NTP server. In a low latency network, the SNTP accuracy can be reduced to the sub-100 millisecond range and, to further increase the accuracy, a simple latency measurement algorithm can be used. The intended accuracy for this implementation is one second, which is sufficient for logs and time displays on user interfaces.

The SNTP feature allows you to set an offset from GMT for the time zone of your location. You can also set a start date and end date and offset for Daylight Savings Time.

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

When SNTP is enabled (the default state is disabled), the system synchronizes with the configured NTP server at bootup (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. SNTP 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 five minutes between each retry.

Supported standards and RFCs

This section lists the standards and RFCs supported by the Nortel Ethernet Routing Switch 5500 Series.

Standards

The following IEEE Standards contain information germane to the Nortel Ethernet Routing Switch 5500 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)
- IEEE 802.1ab (Link Layer Discovery Protocol)

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 5520 is a Power Sourcing Equipment (PSE). It supports 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 Nortel Ethernet Routing Switch 5520 to power network devices over the Ethernet cable. Some such devices include IP Phones, Wireless LAN Access Points, security cameras, access control points, and so on.

The PoE features supported by the Nortel Ethernet Routing Switch 5520 switch 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
- for each port power management and monitoring
- AC and DC disconnection
- Load under voltage/current and over voltage/current detection
- At least 320 W power available for PSE ports from the internal power supply
- Supplies up to 6.6 W for each port on all 48 ports
- Supplies up to 16 W for each port on all 24 ports of the 5520-24T
- 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

PoE can be configured from the CLI, SNMP, and web interfaces. For details, refer to the following sections:

- "PoE overview" (page 162)
- "Port power priority" (page 163)
- "External power source" (page 164)
- "Stacking" (page 164)
- "Power pairs" (page 164)
- "Power availability" (page 165)
- "Diagnosing and correcting PoE problems" (page 169)
- "Power management" (page 171)
- "Configuring PoE using the CLI" (page 172)
- "Viewing PoE ports using the JDM" (page 175)
- "Configuring PoE using the JDM" (page 176)
- "Configuring PoE using the Web-based Management Interface" (page 176)

PoE overview

The Nortel Ethernet Routing Switch 5520 is ideal to use with Nortel Business Communication Manager system, IP phones, hubs, and wireless access points. You can use this switch in conjunction with all network devices.

By using the Nortel Ethernet Routing Switch 5520, you can plug any IEEE802.3af-compliant powered device into a front-panel port and receive power in that port. Data also can be passed simultaneously passed on that port. This capability is called Power over Ethernet (PoE).

The IEEE 802.3af draft standard regulates a maximum of 15.4 watts (W) of power for each port; that is, a power device cannot request more than 15.4 watts (W) of power. As different network devices require different levels of power, the overall available power budget of the Nortel Ethernet Routing Switch 5520 depends on your power configuration and the particular connected network devices. If you connect an IP device that requires more than 16 Watts of power, you see an error on that port notifying you of an overload.

The Nortel Ethernet Routing Switch 5520 automatically detects all IEEE 802.3af-draft-compliant powered devices attached to each front-panel port and immediately sends power to that appliance. The switch also automatically detects how much power each device requires and supplies

the required DC voltage at a set current based on the load conditions and current availability. The switch supports both PoE and standard LAN devices.

The power detection function of the Nortel Ethernet Routing Switch 5520 operates independently of the data link status. Power can be requested by a device that is already operating the link for data, or it can be requested by a device that is not yet operational. That is, the Nortel Ethernet Routing Switch 5520-48T-PWR switch provides power to a requesting device even if the data link for that port is disabled. The switch monitors the connection and automatically disconnects power from a port when the device is removed or changed, as well as when a short occurs.

The Nortel Ethernet Routing Switch 5520-48T-PWR switch also automatically detects those devices that do not require power connections from it, such as laptop computers or other switching devices, and does not send any power to those devices. You control the supply of power to specific ports by setting the maximum allowed power to each port in 1 watt increments, from 3 watts to 16 watts.

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 make connection 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's power budget, the power is returned 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 20 are configured as low priority
- Port 21 is configured as high priority
- Ports 1 to 20 are connected to powered devices

The devices connected to the ports consume the available Nortel Ethernet Routing Switch 5520 switch power.

The device connected to port 21 requests power from the Nortel Ethernet Routing Switch 5520. The switch provides the required power as port 21 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 20 and provides power to port 21. If another port drops power, the system automatically reinstates power to port 20.

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 5520 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 Nortel Ethernet Routing Switch 5520 up to 8 units high. These stacks also can be configured for redundancy.

Power pairs

The Nortel Ethernet Routing Switch 5520 supports wiring as mentioned in the IEEE 802.3af draft standard.

The Nortel Ethernet Routing Switch 5520 supports power to Signal pair only.

Note: The RJ-45 ports 45, 46, 47, and 48 in the Nortel Ethernet Routing Switch 5520-48T may still supply PoE power to the attached devices, even if the corresponding SFP ports are being used for data connectivity.

"[Signal power pair RJ-45 port connector pin assignments](#)" (page 164) shows the RJ-45 connector pin assignments for configuring 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 Nortel Ethernet Routing Switch 5520-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 Nortel Ethernet Routing Switch 5520. You can use a separately orderable power and control cable for this purpose and plug it the back of the switch.

You can allocate a maximum of 16 W power for each port to the PoE devices connected to the Nortel Ethernet Routing Switch 5520. You can allocate power by using the physical power sources.

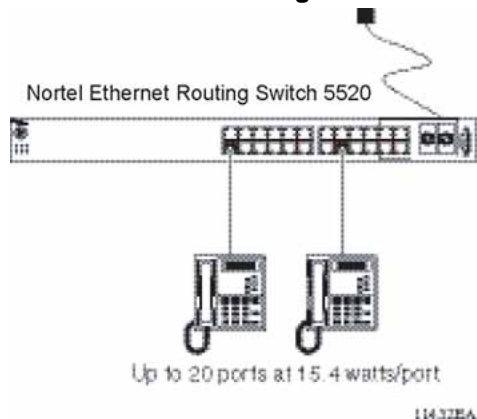
The power sources are physically attached to the switch. You can have just the internal power or you can attach an optional Nortel Ethernet Redundant Power Supply Unit 15. Ensure that you know the actual physical power sources for your Nortel Ethernet Routing Switch 5520.

Internal power source only option

Using the Nortel Ethernet Routing Switch 5520-PWR switch and its internal power source only option, you have a total of 320 watts of available power. You can power up to 48 ports at 6.6 W for each port with this configuration or 20 ports at the max power of 15.4 W for each port.

"Nortel Ethernet Routing Switch 5520 operating on internal power source only" (page 166) describes the switch operating on internal power source only.

Nortel Ethernet Routing Switch 5520 operating on internal power source only



"Power source and available power for powered devices" (page 166) describes the power source and available power by using the internal power source only option.

Power source and available power for powered devices

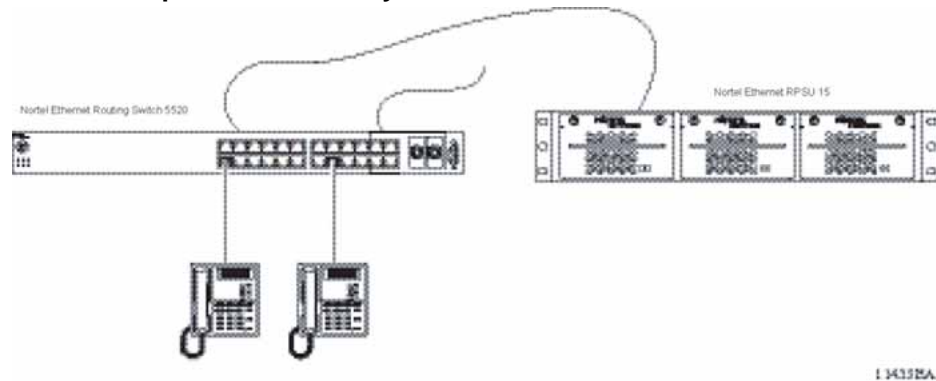
Power Source	Available Power for Powered Devices
AC Connection	320 watts

External power source only option

Using the Nortel Ethernet Routing Switch 5520-PWR switch and its external power source the only option (Nortel Ethernet Redundant Power Supply Unit 15) you have is a total of 320 watts of available power. You can power up to 48 ports at 6.6 W for each port with this configuration or 20 ports at the maximum power of 15.4 W for each port

"Nortel Ethernet Routing Switch 5520 operating on Nortel Ethernet RPSU 15 as an external power source" (page 167) describes the Nortel Ethernet Routing Switch 5520 operating only on the external power source.

Nortel Ethernet Routing Switch 5520 operating on Nortel Ethernet RPSU 15 as an external power source only



"Power source and available power for powered devices" (page 167) describes the power source and available power by using the external power source only option.

Power source and available power for powered devices

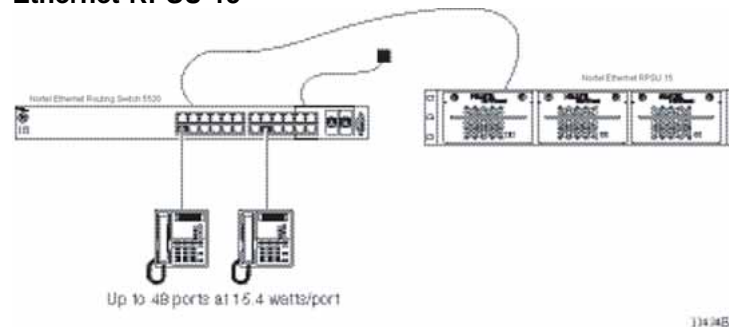
Power Source	Available Power for Powered Devices
Nortel Ethernet RPSU 15	320 watts

Power sharing option

"Power-sharing with the Nortel Ethernet Routing Switch 5520 and the Nortel Ethernet RPSU 15" (page 167) shows the use of the Nortel Ethernet Routing Switch 5520 with the Nortel Ethernet 15 RPSU as an external power source with the power sharing configuration.

In this case, both the internal power (AC) source is connected along with the Nortel Ethernet 10 PSU (DC) source. This power sharing configuration supplies 740W to the Nortel Ethernet Routing Switch 5520-PWR. This enables all 48 ports to supply the Max power of 15.4W for each port.

Power-sharing with the Nortel Ethernet Routing Switch 5520 and the Nortel Ethernet RPSU 15



"Power availability for power sharing with external power source" (page 168) shows the available PoE power when you configure a Nortel Ethernet Routing Switch 5520 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 watts
Nortel Ethernet RPSU 15	320 watts
Total Power (Power Sharing)	740 watts

With the addition of the Nortel Ethernet RPSU 15, you have a total of 740 watts of PoE non-redundant power, which enables up to 48 ports to be powered at 15.4 watts.

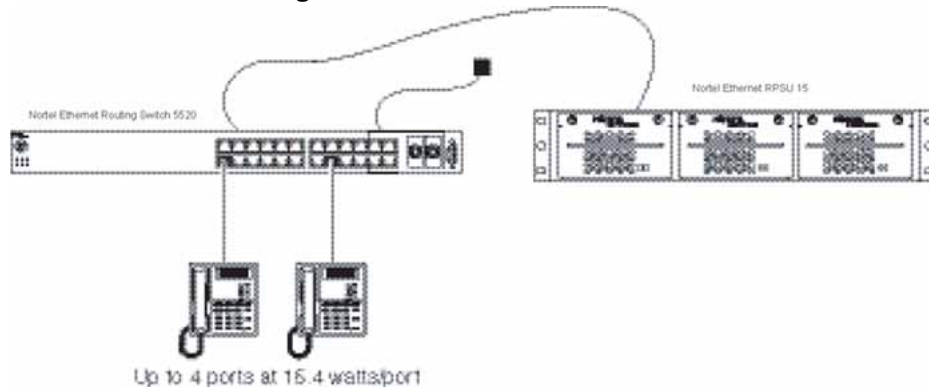
Power Supply Unit (PSU) option

An external power source (Nortel Ethernet RPSU 15) can provide redundant power to the Nortel Ethernet Routing Switch 5520. That is, the power fails over to the Nortel Ethernet RPSU 15 in case there is a problem with the switch's internal power.

"Nortel Ethernet Routing Switch 5520 and the Nortel Ethernet RPSU 15" (page 168) demonstrates the use of the Nortel Ethernet Routing Switch 5520-PWR switch with the Nortel Ethernet RPSU 15 as an external power source with RPSU configuration.

If the Nortel Ethernet Routing Switch 5520 is supplying 320 watts of power to Powered Devices 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 RPSU 15.

Nortel Ethernet Routing Switch 5520 and the Nortel Ethernet RPSU 15



"Power availability with the PSU option" (page 169) shows the available PoE power when you configure a Nortel Ethernet Routing Switch 5520 for RPSU along with an external power source.

By using the Nortel Ethernet RPSU 15, you have a total of 320W of PoE redundant power, which enables up to 48 ports to be powered at 6.6W.

Power availability with the PSU option

Power Source	Available Power for Powered Devices
AC	320 watts
Nortel Ethernet RPSU 15	320 watts
Total Power (RPSU)	320 watts

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 5520.

Messages

"Error messages displayed by PoE ports" (page 169) 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	Port delivers the requested power to the IP device.
Disabled	The port power state is disabled.
Invalid PD	The port is detecting a device that is not authorized to request for power.
Deny low priority	Power disabled from the port because of port setting and demands on power budget.
Overload	Power 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 has occurred.

Connecting the PSU

Perform the following steps in the order specified to connect the PSU to the Nortel Ethernet Routing Switch 5520:

Step	Action
1	Ensure that the DC ON/OFF switch on the back of the Nortel Ethernet Routing Switch 5520 is in the OFF position.
2	Plug the external power source into the DC connector receptacle on the back of the Nortel Ethernet Routing Switch 5520, by using the 2-pin power connector and 10-pin control connector.
3	Attach the ground lug on a cable to a grounding point.
4	Plug the power cord from the Nortel Ethernet RPSU 15 to the wall outlet.
5	Plug the power cord from Nortel Ethernet Routing Switch 5520 into the wall outlet.
6	Turn the DC ON/OFF breaker on the back of the switch to the ON position.

—End—

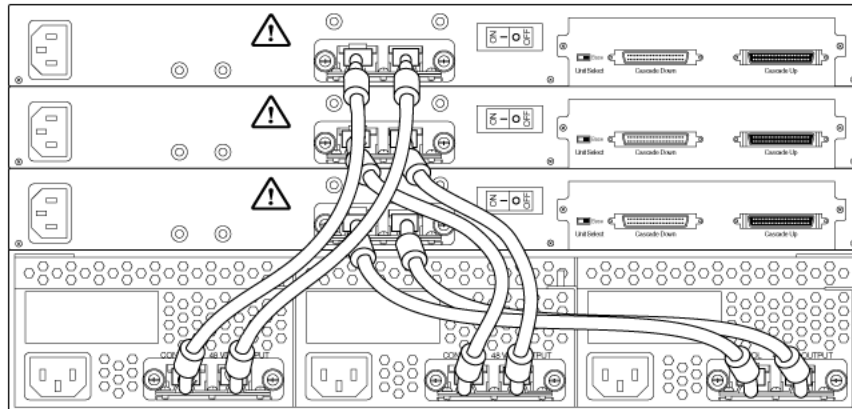
**CAUTION**

Ensure that the DC ON/OFF breaker is in the OFF position before you connect or disconnect the optional external power source.

["External power source connected to back of the Nortel Ethernet Routing Switch 5520"](#) (page 171) shows 3 Nortel Ethernet RPSU 15s connected to the back of a stack of 3 Nortel Ethernet Routing Switch 5520 switches.

Note: The grounding wire is connected with a screw, and a star washer is provided on the base of the Nortel Ethernet Routing Switch 5520.

External power source connected to back of the Nortel Ethernet Routing Switch 5520



553-AAA2984

Power management

The Nortel Ethernet Routing Switch 5520 uses several device management systems, such as the Web-based Management Interface, the Command Line Interface (CLI), and Device Manager (DM), as well as Optivity for network-level management services.

By using the CLI, Web, or DM, you can configure the level of power to specific ports, as well as 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 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 is returned to the dropped port.

For example, assume the following scenario:

- Ports 1 to 20 are configured as low priority
- Port 21 is configured as high priority
- Ports 1 to 20 are connected to powered devices
- Devices on ports are consuming all the available Nortel Ethernet Routing Switch 5520-PWR power
- A device is connected to port 21 and requests power

In this scenario, the Nortel Ethernet Routing Switch 5520 provides power to the device on port 21 because that port is configured as high priority. However, to maintain the power budget, the switch drops one of the ports configured as a lower priority. As all the other ports (1 to 20) are configured

with a low priority, the switch drops power to the highest port number. In this case, the switch drops power to port 20 and provides power to port 21. If another port drops power, the switch automatically reinstates power to port 20.

You configure the autodiscovery power process as either IEEE 802.3af compliant or IEEE 802.3af draft compliant and legacy:

- 802.3af -- detection method outlined in IEEE 802.3af draft standard
- legacy -- detection standard in use prior to 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 overload on any port, and the rest of the ports remain functioning.

Note: Ensure that the switch is set 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 details the commands necessary to configure PoE using the CLI:

- ["Set port power enable or disable" \(page 172\)](#)
- ["Set port power priority" \(page 173\)](#)
- ["Set power limit for channels" \(page 173\)](#)
- ["Set traps control" \(page 174\)](#)
- ["Show main power status" \(page 174\)](#)
- ["Set power usage threshold" \(page 174\)](#)
- ["Setting PoE detection method" \(page 175\)](#)
- ["Show port power status" \(page 175\)](#)
- ["Show port power measurement" \(page 175\)](#)

Set port power enable or disable

The `poe-shutdown` command is used to disable Power Over Ethernet to a port.

The syntax for the `poe-shutdown` command is:

```
poe poe-shutdown [port <portlist>]
```

The `no poe-shutdown` command is used to enable Power Over Ethernet to a port.

The syntax for the `no poe-shutdown` command is:

```
no poe poe-shutdown [port <portlist>]
```

In either command, substitute `<portlist>` with the ports on which PoE is enabled or disabled.

The `poe poe-shutdown` and `no poe poe-shutdown` commands are executed in the 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 173) 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.

The `poe-priority` command is executed in the 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 173) 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 Watts.

The `poe-limit` command is executed in the 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.

The `show poe-main-status` command is executed in the 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 174) 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

The `show poe-main-configure` command is executed in the 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}
```

The `poe-pd-detect-type 802dot3af_and_legacy` command is executed in the 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.

The `show poe-port-status` command is executed in the 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.

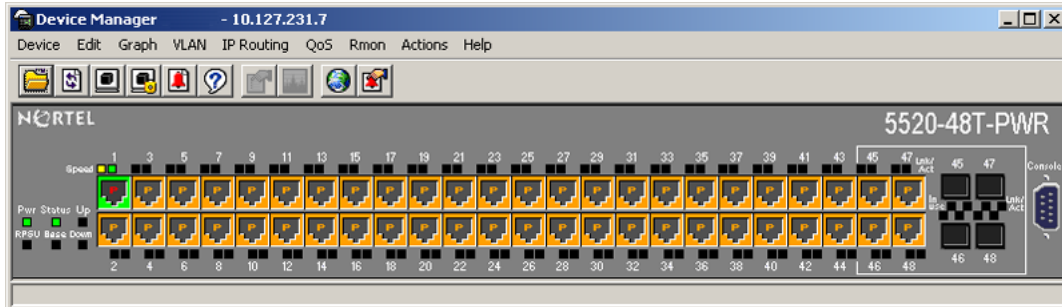
The `show poe-power-measurement` command is executed in the Global Configuration command mode.

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 5520. This additional information is provided 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 5520-48T-PWR" (page 176) displays an example of the Front Panel view of a Nortel Ethernet Routing Switch 5520-48T-PWR.

Nortel Ethernet Routing Switch 5520-48T-PWR



"Power Aspect color codes" (page 176) explains what the different colors displayed by the power aspect represent.

Power Aspect color codes

Color	Description
Green	Indicates that the port is currently delivering power.
Red	Indicates that the power and detection mechanism for the port is disabled.
Orange	Indicates that the power and detection mechanism for the port is enabled. The port is not currently delivering power.
White/Gray	Indicates that the power and detection mechanism for the port is unknown.

Note: The data and power aspect coloring schemes are independent of each other. The initial status for both data and power aspect for the port can be viewed. 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, refer to "Editing and viewing switch PoE configurations" (page 262).

Configuring PoE using the Web-based Management Interface

The following sections detail PoE configuration and management using the Web-based Management Interface:

- "Configuring power management on the switch" (page 177)

- "Configuring power management for the ports" (page 178)

Configuring power management on the switch

The **Global Power Management** screen enables the configuration and viewing of power settings for the switch.

To configure power management, complete these tasks:

Step	Action
1	Open the Global Power Management screen by selecting Configuration > Power Management > Global Power Management from the menu. This screen is illustrated in "Global Power Management page" (page 177).
2	Click Submit after entering the necessary settings.

—End—

Global Power Management page

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

"Global Power Management fields" (page 178) describes the items on the **Global Power Management** screen.

Global Power Management fields

Item	Description
Available DTE Power	Displays the power provided by the Nortel Ethernet Routing Switch 5520 switch to the devices. The range of power that is available from internal power supply is 320W--740W.
DTE Power Status	Displays the status of the PoE feature. The values that maybe displayed are: Normal or Error.
DTE Power Consumption	Displays the total power usage.
Power Pair	Displays the Power Pair (part of the RJ-45 pin connectors) that you chose to supply power.
Traps Control	Displays the status of the traps control. You can enable or disable this feature.
PD Detect Type	Displays the standard that you are using for power detection. The standard that you select can be any one of the following: <ul style="list-style-type: none"> • IEEE 802.3af • IEEE 802.3af and legacy.
Power Source Present	Displays the mode of power supply that the Nortel Ethernet Routing Switch 5520 currently uses. The mode of power supply can be any one of the following values: <ul style="list-style-type: none"> • AC only - signifies that the switch is using internal power supply. • DC only - signifies that the switch is using external power supply. • AC and DC - signifies that the switch is using both external and internal <p>This is a read-only field.</p>
AC Power Status	Displays the status of the AC power supply.
DC Power Status	Displays 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 these tasks:

Step	Action
1	Open the Port Property page by selecting Configuration > Power Management > Port Property from the menu. This screen is illustrated in "Port Property page" (page 179).
2	Click Submit after entering the necessary settings.

—End—

Port Property page

Options, skins, help and informat

Configuration > Power Management > Port Property

Port Power Setting

Unit **3**

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			16	Low			
Stack	Enabled			16	Low			

Unit **3**

Submit

"Port Property fields" (page 179) describes the items on the **Port Property** fields.

Port Property fields

Item	Description
Port	Denotes the port number.

Item	Description
Admin. Status	<p>Used to set the power status. The values that are available are:</p> <ul style="list-style-type: none"> • Enabled • Disabled <p>The default value is Enabled.</p>
Current Status	<p>Displays the current status of the port. The values that can be displayed are:</p> <ul style="list-style-type: none"> • Disable • Detecting • Detected • Delivering Power • Error • Invalid PD • Test • Deny Low Priority • Overload
Classification	<p>Displays the operational status of the port PD classification.</p>
Limit (Watt)	<p>This field is used to set the maximum power that the switch can supply to a port. The default value is 16 watts.</p>
Priority	<p>This field is used to set the priority of a port. The Priority of a port is used 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)	Displays the voltage supplied by the port.
Current (mA)	Displays the current supplied by the port.
Power (Watt)	Displays the Power supplied by the port.

Switch administration tasks

This chapter describes basic switch administration tasks that are not specific to any switch application. For complete information about administration tasks specific to a switch application, consult the appropriate book.

This chapter contains information about the following topics:

- "General switch administration using the CLI" (page 183)
- "General Switch Administration using the Web-based Management Interface" (page 214)
- "General Switch Administration using the JDM" (page 235)

General switch administration using the CLI

This section outlines the Command Line Interface commands used in general switch administration. It contains information about the following topics:

- "Multiple switch configurations" (page 184)
- "New Unit Quick Configuration" (page 185)
- "IP blocking" (page 186)
- "Assigning and clearing IP addresses" (page 187)
- "Assigning and clearing IP addresses for specific units" (page 190)
- "Displaying interfaces" (page 192)
- "Setting port speed" (page 192)
- "Testing cables with the Time Domain Reflectometer" (page 195)
- "Enabling Autotopology" (page 196)
- "Enabling rate-limiting" (page 200)
- "Using Simple Network Time Protocol" (page 202)
- "Real time clock configuration" (page 207)
- "Custom Autonegotiation Advertisements" (page 209)
- "Connecting to Another Switch" (page 210)

- ["Domain Name Server \(DNS\) Configuration" \(page 212\)](#)

Multiple switch configurations

In Software Release 4.2 and later, the Nortel Ethernet Routing Switch 5500 Series supports the storage of two switch configurations in flash memory. The switch can use either configuration and must be reset in order for the configuration change to take effect.

A regular reset of the switch synchronizes any configuration changes to the active configuration whereas a reset to defaults causes the active configuration to be set 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's active configuration and the stack's active configuration. If the two are not the same, the new stack unit resets and loads the stack's active configuration.

The following CLI commands are used to configure and use multiple switch configuration:

- ["show nvram block command" \(page 184\)](#)
- ["copy config nvram block command" \(page 184\)](#)
- ["copy nvram config block command" \(page 185\)](#)

show nvram block command

This command shows the configurations currently stored on the switch. The syntax for this command is:

```
show nvram block
```

This command is executed in the Global Configuration command mode.

copy config nvram block command

This command copies the current configuration to one of the flash memory spots. The syntax for this command is:

```
copy config nvram block <1-2> name <block_name>
```

["copy config nvram block parameters" \(page 184\)](#) 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>	The name to attach to this block. Names can be up to 40 characters in length with no spaces.

This command is executed in the 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 causes the switch to reset so that the new configuration can be loaded.

This command is executed in the Global Configuration command mode.

New Unit Quick Configuration

In Software Release 4.2 and later, the New Unit Quick Configuration feature enables the creation of a default configuration that can be applied to any new unit entering a stack configuration. This enables new units to be added to the stack without the need to reset the stack.

To configure and enable this feature using the CLI, refer to the following commands (all commands in this section are executed in the Global Configuration command mode):

- ["quickconfig enable" \(page 185\)](#)
- ["no quickconfig enable" \(page 185\)](#)
- ["default quickconfig" \(page 185\)](#)
- ["quickconfig start-recording" \(page 186\)](#)

quickconfig enable

This command enables the quick configuration feature on the switch. The syntax for this command is:

```
quickconfig enable
```

no quickconfig enable

This command disables the quick configuration feature on the switch. The syntax for this command is:

```
no quickconfig enable
```

default quickconfig

This command sets the quick configuration feature to the factory default value. The syntax for this command is:

```
default quickconfig
```

quickconfig start-recording

This command is used on the stack base unit to record the default configuration that is applied to new units in the stack. The syntax for this command is:

```
quickconfig (start-recording) [u3]
```

To end the recording process type a "." (dot) in the CLI.

IP blocking

IP blocking provides a safeguard against the use of duplication IP addresses in a stack at the Layer 3 level. When a unit leaves a stack or reboots the IP blocking feature ensures that duplicate IPs are not present.

To configure and manage IP blocking using the CLI, refer to the following CLI commands:

- ["show ip blocking-mode" \(page 186\)](#)
- ["ip blocking-mode command" \(page 186\)](#)
- ["clear ip-blocking" \(page 187\)](#)
- ["default ip blocking-mode" \(page 187\)](#)

show ip blocking-mode

This command is used to show the current IP blocking parameters. The syntax for this command is:

```
show ip blocking-mode
```

This command is executed in the User EXEC command mode.

ip blocking-mode command

This command is used to set the level of ip blocking to perform in the stack. The syntax for this command is:

```
ip blocking-mode {full | none}
```

["ip blocking-mode parameters" \(page 186\)](#) outlines the parameters for this command.

ip blocking-mode parameters

Parameter	Description
full	Select this parameter to set IP blocking-mode to full. This never enables a duplicate IP address in a stack.
none	Select this parameter to set IP blocking-mode to none. This enables duplicate IP addresses unconditionally.

This command is executed in the Interface Configuration command mode.

clear ip-blocking

This command is used clear the current IP blocking-mode state. The syntax for this command is:

```
clear ip-blocking
```

This command is executed in the Privileged EXEC command mode.

default ip blocking-mode

This command sets the IP blocking mode to factory defaults. The syntax for this command is:

```
default ip blocking-mode
```

This command is executed in the Global Configuration command mode.

Assigning and clearing IP addresses

Using the CLI, IP addresses and gateway addresses can be assigned, cleared, and viewed. For details, refer to the following:

- ["ip address command" \(page 187\)](#)
- ["no ip address command" \(page 188\)](#)
- ["ip default-gateway command" \(page 188\)](#)
- ["no ip default-gateway command" \(page 189\)](#)
- ["show ip command" \(page 189\)](#)

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] <A.B.C.D> [netmask  
<A.B.C.D>] [default-gateway <A.B.C.DX>]
```

The `ip address` command is executed in the 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" \(page 188\)](#) describes the parameters for the `ip address` command.

ip address parameters

Parameters	Description
stack switch	Sets the IP address and netmask of the stack or the switch.
A.B.C.D	Denotes the IP address in dotted-decimal notation; netmask is optional.
netmask	Signifies the IP subnet mask for the stack or switch.
Default Gateway A.B.C.D	Displays the IP address of the default gateway. Enter the IP address of the default IP gateway.

Note: When the IP address or subnet mask is changed, 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}
```

The `no ip address` command is executed in the Global Configuration command mode.

"[no ip address parameters](#)" (page 188) 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 the IP address or subnet mask is changed, connectivity to Telnet and the Web Interface can be lost. Any new Telnet connection can be disabled and is required to 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 <A.B.C.D>
```

The `ip default-gateway` command is executed in the Global Configuration command mode.

"[ip default-gateway parameters](#)" (page 189) describes the parameters for the `ip default-gateway` command.

ip default-gateway parameters

Parameters	Description
A.B.C.D	Enter the dotted-decimal IP address of the default IP gateway.

Note: When the IP gateway is changed, 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
```

The `no ip default-gateway` command is executed in the Global Configuration command mode.

Note: When the IP gateway is changed, connectivity to Telnet and the Web Interface can be lost.

show ip command

The `show ip` command displays the IP configurations, BootP/DHCP 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/DHCP.

The syntax for the `show ip` command is:

```
show ip [dhcp] [default-gateway] [address]
```

The `show ip` command is executed in the User EXEC command mode.

If you do not enter any parameters, this command displays all IP-related configuration information.

"[show ip parameters](#)" (page 190) describes the parameters and variables for the `show ip` command.

show ip parameters

Parameters and variables	Description
bootp	Displays BootP-related IP information. The possibilities for status returned are: <ul style="list-style-type: none"> • always • disabled • last IP • when needed
dhcp client lease	Displays DHCP client lease information. The command displays information about configured lease time and lease time granted by the DHCP server.
default-gateway	Displays the IP address of the default gateway.
address	Displays the current IP address.
address source	Displays the BootP or DHCP client information. The possibilities for status returned are: <ul style="list-style-type: none"> • DHCP always • DHCP when needed • DHCP or last address • Disabled • BootP always • BootP when needed • BootP or last 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, refer to the following:

- ["ip address unit command" \(page 190\)](#)
- ["no ip address unit command" \(page 191\)](#)
- ["default ip address unit command" \(page 191\)](#)

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]
```

The `ip address unit` command is executed in the Global Configuration command mode.

"[ip address unit parameters](#)" (page 191) 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 is changed, 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>
```

The `no ip address unit` command is executed in the Global Configuration command mode.

"[no ip address parameters](#)" (page 191) 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 the IP address or subnet mask is changed, connectivity to Telnet and the Internet can be lost.

default ip address unit command

The `default ip address unit` command sets the IP address for the specified unit in a stack to all zeros (0).

The syntax for the `default ip address unit` command is:

```
default ip address unit <1-8>
```

The `default ip address unit` command is executed in the Global Configuration command mode.

"[default ip address unit parameters](#)" (page 192) describes the parameters for this command.

default ip address unit parameters

Parameters and variables	Description
unit <1-8>	Zeroes out the IP address for the specified unit.

Note: When the IP gateway is changed, connectivity to Telnet and the Internet can be lost.

Displaying interfaces

The status of all interfaces on the switch or stack can be viewed, 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>]
```

The `show interfaces` command is executed in the User EXEC command mode.

"[show interfaces parameters](#)" (page 192) describes the parameters and variables for the `show interfaces` command.

show interfaces parameters

Parameters and variables	Description
names <portlist>	Displays the interface names; enter specific ports if you want to see only those.

Setting port speed

To set port speed and duplexing using the CLI, refer to the following:

- "[speed command](#)" (page 193)
- "[default speed command](#)" (page 193)
- "[duplex command](#)" (page 194)

- ["default duplex command" \(page 195\)](#)

speed command

The `speed` command sets the speed of the port.

The syntax for the `speed` command is:

```
speed [port <portlist>] {10 | 100 | 1000 | auto}
```

The `speed` command is executed in the Interface Configuration command mode.

["speed parameters" \(page 193\)](#) describes the parameters and variables for the `speed` command.

speed parameters

Parameters and variables	Description
port <portlist>	Specifies the port numbers for which to configure the speed. Enter the port numbers you want to configure. Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.
10 100 1000 auto	Sets 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/disabling autonegotiation for speed also enables/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 speed of the port to the factory default speed.

The syntax for the `default speed` command is:

```
default speed [port <portlist>]
```

The `default speed` command is executed in the Interface Configuration command mode.

"Default speed parameters" (page 194) describes the parameters for this command.

Default speed parameters

Parameters and variables	Description
port <portlist>	Specifies the port numbers to set the speed to factory default. Enter the port numbers you want to set. Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.

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}
```

The `duplex` command is executed in the Interface Configuration command mode.

"Duplex parameters" (page 194) describes the parameters for this command.

Duplex parameters

Parameters and variables	Description
port <portlist>	Specifies the port numbers for which to reset the duplex mode to factory default values. Enter the port number you want 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	Sets duplex to: <ul style="list-style-type: none"> • full--full-duplex mode • half--half-duplex mode • auto--autonegotiation

Note: Enabling/disabling autonegotiation for speed also enables/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>]
```

The `default duplex` command is executed in the Interface Configuration command mode.

"Default duplex parameters" (page 195) describes the parameters for this command.

Default duplex parameters

Parameters and variables	Description
port <portlist>	Specifies the port numbers to reset the duplex mode to factory default values. Enter the port numbers you want 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.

Testing cables with the Time Domain Reflectometer

With Release 5.0 software, the Nortel Ethernet Routing Switch 5500 Series is equipped with a Time Domain Reflectometer (TDR). The TDR provides a diagnostic capability to test connected cables for defects (such as short pin and pin open). You can obtain TDR test results from the CLI or the JDM.

The cable diagnostic tests only apply to Ethernet copper ports; fiber ports cannot be tested.

You can initiate a test on multiple ports at the same time.

When you test a cable with the TDR, if the cable has a 10/100 MB/s link, the link is broken during the test and restored only when the test is complete. Use of the TDR does not affect 1 GB/s links.

Note: The accuracy margin of cable length diagnosis is between three to five meters. Nortel suggests the shortest cable for length information be five meters long.

With the following CLI commands, you can initiate a TDR cable diagnostic test and obtain test reports.

- "tdr test command" (page 196)
- "show tdr command" (page 196)

tdr test command

The `tdr test` command initiates a TDR test on a port or ports.

The syntax for this command is:

```
tdr test <portlist>
```

where `<portlist>` specifies the ports to be tested.

The `tdr test` command is in the `privExec` command mode.

show tdr command

The `show tdr` command displays the results of a TDR test.

The syntax for this command is:

```
show tdr <portlist>
```

where `<portlist>` specifies the ports for which to display the test results.

The `show tdr` command is in the `privExec` command mode.

Enabling Autotopology

The Optivity Autotopology protocol can be configured using the CLI.

For more information about Autotopology, refer to <http://www.nortel.com/support>. (The product family for Optivity and Autotopology is Data and Internet.)

To enable autotopology using the CLI, refer to the following:

- "autotopology command" (page 196)
- "no autotopology command" (page 197)
- "default autotopology command" (page 197)
- "show autotopology settings command" (page 197)
- "show autotopology nmm-table command" (page 197)

autotopology command

The `autotopology` command enables the Autotopology protocol.

The syntax for the `autotopology` command is:

```
autotopology
```

The `autotopology` command is executed in the 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
```

The `no autotopology` command is executed in the 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
```

The `default autotopology` command is executed in the 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
```

The `show autotopology settings` command is executed in the 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
```

The `show autotopology nmm-table` command is executed in the 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 5500 Series, can control traffic on this port using the `flowcontrol` command.

To enable flow control using the CLI, refer to the following:

- ["flowcontrol command" \(page 198\)](#)
- ["no flowcontrol command" \(page 199\)](#)
- ["default flowcontrol command" \(page 199\)](#)

flowcontrol command

The `flowcontrol` command is used only on Gigabit Ethernet ports and controls the traffic rates during congestion.

The syntax for the `flowcontrol` command is:

```
flowcontrol [port <portlist>] {asymmetric | symmetric | auto
| disable}
```

The `flowcontrol` command is executed in the Interface Configuration mode.

["Flowcontrol parameters" \(page 198\)](#) describes the parameters for this command.

Flowcontrol parameters

Parameters and variables	Description
port <portlist>	Specifies 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 which have speed set to 1000/full.
asymmetric symmetric auto disable	Sets the mode for flow control: <ul style="list-style-type: none"> • asymmetric--PAUSE frames can only flow in one direction. • symmetric--PAUSE frames can flow in either direction.

Parameters and variables	Description
	<ul style="list-style-type: none"> • <code>auto</code>--sets the port to automatically determine the flow control mode (default). • <code>disable</code>--disables flow control on the port.

no flowcontrol command

The `no flowcontrol` command is used only on Gigabit Ethernet ports and disables flow control.

The syntax for the `no flowcontrol` command is:

```
no flowcontrol [port <portlist>]
```

The `no flowcontrol` command is executed in the Interface Configuration mode.

"[No flowcontrol parameters](#)" (page 199) describes the parameters for this command.

No flowcontrol parameters

Parameters and variables	Description
<code>port <portlist></code>	<p>Specifies the port numbers for which to disable flow control.</p> <p>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.</p>

default flowcontrol command

The `default flowcontrol` command is used only on Gigabit Ethernet ports and sets the flow control to `auto`, which automatically detects the flow control.

The syntax for the `default flowcontrol` command is:

```
default flowcontrol [port <portlist>]
```

The `default flowcontrol` command is executed in the Interface Configuration mode.

"[Default flowcontrol parameters](#)" (page 200) describes the parameters for the command.

Default flowcontrol parameters

Parameters and variables	Description
port <portlist>	Specifies the port numbers to default to auto 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, refer to the following:

- ["show rate-limit command" \(page 200\)](#)
- ["rate-limit command" \(page 200\)](#)
- ["no rate-limit command" \(page 201\)](#)
- ["default rate-limit command" \(page 201\)](#)

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
```

The `show rate-limit` command is executed in the 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>}
```

The `rate-limit` command is executed in the Interface Configuration command mode.

["Rate-limit parameters" \(page 201\)](#) describes the parameters for this command.

Rate-limit parameters

Parameters and values	Description
port <portlist>	Specifies the port numbers to configure for rate-limiting. Enter the port numbers you want to configure. Note: If you omit this parameter, the system uses the port number you specified in the interface command.
multicast <pct> broadcast <pct> both <pct>	Applies rate-limiting to the type of traffic. Enter an integer between 1 and 10 to set the rate-limiting percentage: <ul style="list-style-type: none"> • multicast--applies rate-limiting to multicast packets • broadcast--applies rate-limiting to broadcast packets • both--applies 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>]
```

The `no rate-limit` command is executed in the Interface Configuration command mode.

"[No rate-limit parameters](#)" (page 201) describes the parameters for this command.

No rate-limit parameters

Parameters	Description
port <portlist>	Specifies the port numbers to disable for rate-limiting. Enter the port numbers you want to disable. Note: If you omit this parameter, the system uses the port number you specified in the interface command.

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>]
```

The `default rate-limit` command is executed in the Interface Configuration command mode.

"Default rate-limit parameters" (page 202) describes the parameters for this command.

Default rate-limit parameters

Parameters	Description
port <portlist>	Specifies the port numbers on which to reset rate-limiting to factory default. Enter the port numbers on which 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 (UCT) 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 you have trouble using 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.

Using SNTP provides a real-time timestamp for the software, shown as Greenwich Mean Time (GMT).

If SNTP is enabled, 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 is not performed 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, refer to the following commands:

- "show SNTP command" (page 203)
- "show sys-info command" (page 203)
- "SNTP enable command" (page 203)
- "no SNTP enable command" (page 203)

- "SNTP server primary address command" (page 204)
- "SNTP server secondary address command" (page 204)
- "no SNTP server command" (page 205)
- "SNTP sync-now command" (page 205)
- "SNTP sync-interval command" (page 205)
- "Configuring local time zone" (page 272)
- "Configuring daylight savings time" (page 206)

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
```

The `show SNTP` command is executed in the 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
```

The `show sys-info` command is executed in the 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
```

The `SNTP enable` command is executed in the 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 snntp enable` command is:

```
no snntp enable
```

The `no snntp enable` command is executed in the Global Configuration command mode.

SNTP server primary address command

The `snntp server primary address` command specifies the IP addresses of the primary NTP server.

The syntax for the `snntp server primary address` command is:

```
snntp server primary address <A.B.C.D>
```

The `snntp server primary address` command can be executed in the Global Configuration command mode.

"[SNTP server primary address parameters](#)" (page 204) describes the parameters for this command.

SNTP server primary address parameters

Parameters	Description
<A.B.C.D>	Enter the IP address of the primary NTP server in dotted-decimal notation.

SNTP server secondary address command

The `snntp server secondary address` command specifies the IP addresses of the secondary NTP server.

The syntax for the `snntp server secondary address` command is:

```
snntp server secondary address <A.B.C.D>
```

The `snntp server secondary address` command is executed in the Global Configuration command mode.

"[SNTP server secondary address parameters](#)" (page 204) 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}
```

The `no sntp server` command is executed in the Global Configuration command mode.

"[no SNTP server parameters](#)" (page 205) describes the parameters for this command.

no SNTP server parameters

Parameters	Description
primary	Clear primary SNTP server address.
secondary	Clear 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
```

The `sntp sync-now` command is executed in the 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>
```

The `sntp sync-interval` command is executed in the Global Configuration command mode.

"[SNTP sync-interval parameters](#)" (page 206) describes the parameters for this command.

SNTP sync-interval parameters

Parameters	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.

Configuring the local time zone

Configure your switch for your local time zone.

Step Action

- 1 In the NNCLI, set the global configuration mode.
`configure`
- 2 Enable sntp server.
- 3 Set clock time zone using the clock command.
`clock time-zone zone hours [minutes]`

Parameters	Description
zone	Time zone acronym to be displayed when showing system time (up to 4 characters).
hours	Difference from UTC in hours. This can be any value between -12 and +12.
minutes	Optional: This is the number of minutes difference from UTC. Minutes can be any value between 0 and 59.

—End—

setting time zone example

```
clock time-zone PST -8
```

This command sets the time zone to UTP minus 8 hours and the time zone will be displayed as "PST."

Configuring daylight savings time

Configure local daylight savings time recurring change dates.

Step Action

- 1 In the NNCLI, set the global configuration mode.

```
configure
```

- 2 Enable sntp server.
- 3 Set the date to change to daylight savings time.

```
clock summer-time zone date day month year hh:mm day
month year hh:mm [offset]
```

Parameters and variables	Description
date	Indicates that daylight savings time should start and end on the specified days every year.
day	Date to start daylight savings time.
month	Month to start daylight savings time.
year	Year to start daylight savings time.
hh:mm	Hour and minute to start daylight savings time.
day	Date to end daylight savings time.
month	Month to end daylight savings time.
year	Year to end daylight savings time.
hh:mm	Hour and minute to end daylight savings time.
offset	Number of minutes to add during the summer time.
zone	The time zone acronym to be displayed when daylight savings time is in effect. If it is unspecified, it defaults to the time zone acronym set when the time zone was set.

—End—

set daylight savings time example

```
clock summer-time BST date 28 Mar 2007 2:00 30 Aug 2007
15:00 +60
```

This command sets the daylight savings time to begin at 02:00 on March 28, 2007 and end on August 30th, 2007 at 15:00. The change to daylight savings moves the clock forward by 60 minutes and "BST" will be displayed as the time zone acronym. These changes to and from daylight savings time will happen automatically.

Real time clock configuration

In addition to SNTP time configuration, a real-time clock (RTC) is available to provide the switch with time information. This RTC provides the switch information in the instance that SNTP time is not available.

Use the following commands to view and configure the RTC:

- "clock set command" (page 208)
- "Clock sync-rtc-with-SNTP enable command" (page 208)
- "no clock sync-rtc-with-SNTP enable" (page 208)
- "Default clock sync-rtc-with-SNTP enable" (page 209)
- "Clock source command" (page 209)
- "default clock source" (page 209)

clock set command

This command is used to set the RTC. The syntax of the clock set command is:

```
clock set {<LINE> | <hh:mm:ss>}
```

"clock set parameters" (page 208) outlines the parameters for this command.

clock set parameters

Parameter	Description
<LINE>	A string in the format of mmddyyyyhhmmss that defines the current local time.
<hh:mm:ss>	Numeric entry of the current local time in the manner specified.

This command is executed in the Privileged EXEC command mode.

Clock sync-rtc-with-SNTP enable command

This command enables the syncing of the RTC with the SNTP clock when the SNTP clock synchronizes.

The syntax for this command is:

```
clock sync-rtc-with-sntp enable
```

This command is executed in the Global Configuration command mode.

no clock sync-rtc-with-SNTP enable

This command disables the syncing of the RTC with the SNTP clock when the SNTP clock synchronizes.

The syntax for this command is:

```
no clock sync-rtc-with-sntp enable
```

This command is executed in the Global Configuration command mode.

Default clock sync-rtc-with-SNTP enable

This command sets the synchronizing of the RTC with the SNTP clock to factory defaults.

The syntax for this command is:

```
default clock sync-rtc-with-sntp enable
```

This command is executed in the Global Configuration command mode.

Clock source command

This command sets the default clock source for the switch.

The syntax for this command is:

```
clock source {sntp | rtc | sysUpTime}
```

Substitute {sntp | rtc | sysUpTime} with the clock source selection.

This command is executed in the Global Configuration command mode.

default clock source

This command sets the clock source to factory defaults. The syntax of this command is:

```
default clock source
```

This command is executed in the Global Configuration command mode.

Custom Autonegotiation Advertisements

Custom Autonegotiation Advertisement (CANA) customizes the capabilities that are advertised. It also controls the capabilities that are advertised by the Nortel Ethernet Routing Switch 5500 Series as part of the auto-negotiation process.

The following sections describe configuring CANA using the CLI:

- ["Configuring CANA" \(page 209\)](#)
- ["Viewing current autonegotiation advertisements" \(page 210\)](#)
- ["Viewing hardware capabilities" \(page 210\)](#)
- ["Setting default auto-negotiation-advertisements" \(page 210\)](#)
- ["no auto-negotiation-advertisements command" \(page 210\)](#)

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 line:

```
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 its 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 line:

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

The `default auto-negotiation-advertisements` command can be executed in the 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>]
```

The `no auto-negotiation-advertisements` command can be executed in the Interface Configuration mode.

Connecting to Another Switch

Using the Command Line Interface (CLI), it is possible to communicate with another switch while maintaining the current switch connection. This is accomplished with the familiar `ping` and `telnet` commands.

ping command

Use the `ping` command to determine if communication with another switch can be established.

The syntax for this command is:

```
ping <ip_address | dns_host_name> [continuous] [count <#
of packets>] [datasize <packet size>] [debug] [interval
<seconds>] [timeout <seconds>]
```

This command can be executed in the User EXEC command mode but is usable in any command mode.

"[ping command parameters and variables](#)" (page 211) shows the command parameters of the `ping` command.

ping command parameters and variables

Parameters and variables	Description
<ip_address dns_host_name>	The IP address or the DNS hostname of the unit to test.
continuous	Ping in continuous mode.
count <# of packets>	Number of packets to send.
datasize <packet size>	The packet size to send.
debug	Enable ping debug mode.
interval <seconds>	Interval before retransmission.
timeout <seconds>	Ping timeout in seconds.

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 hostname of the unit with which to communicate.

This command is executed in the User EXEC command mode.

Domain Name Server (DNS) Configuration

Domain name servers are used when the switch needs to resolve a domain name (such as "nortel.com") to an IP address. The following commands allow for the configuration of the switch domain name servers:

- "show ip dns command" (page 212)
- "ip domain-name command" (page 212)
- "no ip domain-name command" (page 212)
- "default ip domain-name command" (page 213)
- "ip name-server command" (page 213)
- "no ip name-server command" (page 213)

show ip dns command

The `show ip dns` command is used 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
```

This command is executed in the User EXEC command mode.

ip domain-name command

The `ip domain-name` command is used 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 to be used. A domain name is determined to be valid if it contains alphanumeric characters and contains at least one period (.).

This command is executed in the Global Configuration command mode.

no ip domain-name command

The `no ip domain-name` command is used to clear a previously configured default DNS domain name for the switch.

The syntax for this command is:

```
no ip domain-name
```

This command is executed in the Global Configuration command mode.

default ip domain-name command

The `default ip domain-name` command is used 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
```

This command is executed in the Global Configuration command mode.

ip name-server command

The `ip name-server` command is used 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 213) 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.

This command is executed in the Global Configuration command mode.

no ip name-server command

The `no ip name-server` command is used 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 214) 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.

This command is executed in the Global Configuration command mode.

General Switch Administration using the Web-based Management Interface

This section contains information about the following topics:

- "[Viewing stack information](#)" (page 214)
- "[Viewing summary switch information](#)" (page 216)
- "[Changing stack numbering](#)" (page 218)
- "[Identifying unit numbers](#)" (page 220)
- "[Configuring BootP, DHCP, IP, and gateway settings](#)" (page 220)
- "[Modifying system settings](#)" (page 230)
- "[Managing remote access by IP address](#)" (page 231)
- "[Configuring the Real-Time Clock](#)" (page 234)

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.

To view stack information:

Step Action

- 1 Open the **Stack Information** screen by selecting **Summary > Stack Information** from the menu. This screen is illustrated in "Stack information page" (page 215).
-

—End—

Stack information page

Summary > Stack Information

Stack Information	
System Description	Ethernet Routing Switch 5510-24T
Software Version	v5.0.0.
MAC Address	BA-D1-B1-40-20-01
IP Address	10.107.101.11
Manufacturing Date Code	06122003
Serial #	SNR1BB11026
Operational State	Normal

Stack Inventory							
Unit	Description	Pluggable Port	Pluggable Port	Pluggable Port	Pluggable Port	Software Version	Operational State
1	Ethernet Routing Switch 5510 - 24T 24 10/100/1000BaseTX plus 2 Overlapped GBIC slots	(23) None	(24) None			v5.0.0.	Normal
2	Ethernet Routing Switch 5510 - 48T 48 10/100/1000BaseTX plus 2 Overlapped GBIC slots	(47) None	(48) None			v5.0.0.	Normal

The following table "Stack Information screen fields" (page 215) 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.
	Manufacturing Date Code	The date of manufacture of the board in ASCII format: YYYYMMDD.

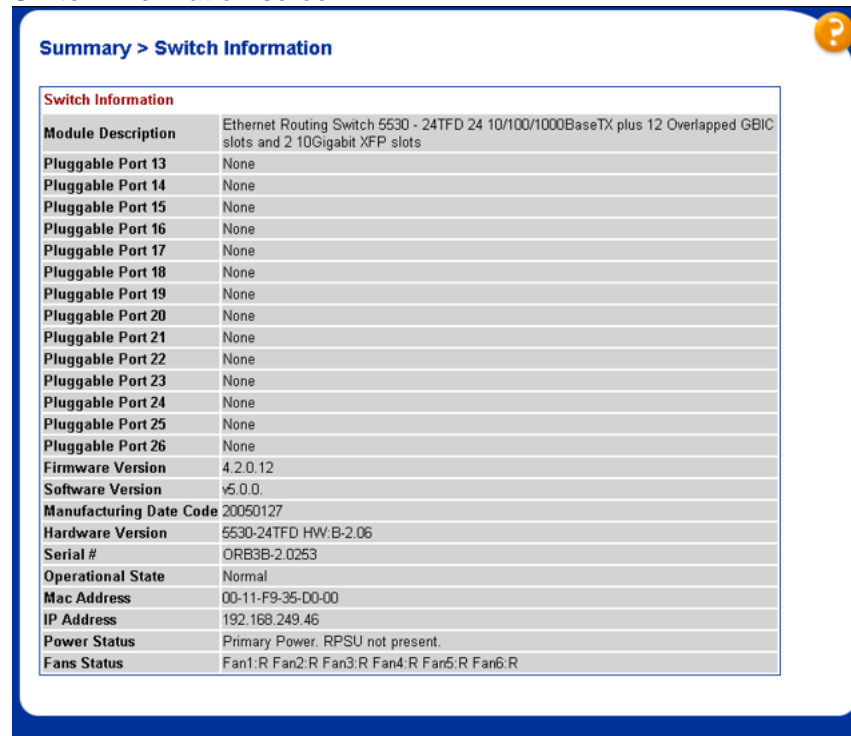
Section	Fields	Description
	Serial Number	The serial number of the base unit.
	Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.
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 218) .
	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

To view summary switch information:

Step	Action
1	Open the Switch Information screen by selecting Summary > Switch Information from the menu. This screen is illustrated in "Switch Information screen" (page 217) .

Switch Information screen



Switch Information	
Module Description	Ethernet Routing Switch 5530 - 24TFD 24 10/100/1000BaseTX plus 12 Overlapped GBIC slots and 2 10Gigabit XFP slots
Pluggable Port 13	None
Pluggable Port 14	None
Pluggable Port 15	None
Pluggable Port 16	None
Pluggable Port 17	None
Pluggable Port 18	None
Pluggable Port 19	None
Pluggable Port 20	None
Pluggable Port 21	None
Pluggable Port 22	None
Pluggable Port 23	None
Pluggable Port 24	None
Pluggable Port 25	None
Pluggable Port 26	None
Firmware Version	4.2.0.12
Software Version	v5.0.0.
Manufacturing Date Code	20050127
Hardware Version	5530-24TFD HW:B-2.06
Serial #	ORB3B-2.0253
Operational State	Normal
Mac Address	00-11-F9-35-D0-00
IP Address	192.168.249.46
Power Status	Primary Power. RPSU not present.
Fans Status	Fan1:R Fan2:R Fan3:R Fan4:R Fan5:R Fan6:R

The following table "Switch Information page fields" (page 217) describes the fields on the Switch Information screen.

Switch Information page fields

Item	Description
Unit	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 218).
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.
Mac Address	The MAC address of the device.

Item	Description
IP Address	The IP address of the device.
Power Status	The current power status of the device: Primary Power. RPSU not present Primary Power. RPSU present Redundant Power. Primary power failed Unavailable

- 2 In stacked configurations, click the number of the device to view in the upper left-hand corner of the screen.

—End—

Changing stack numbering

If the system is in a stack, existing stack numbering information can be viewed and renumbered.

Note: The unit number does not affect the base unit designation.

To view or renumber devices within the stack framework:

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

- 1 Open the **Stack Numbering** screen by selecting **Summary > Stack Numbering** from the menu. This screen is illustrated in "[Stack Numbering page](#)" (page 219).

Stack Numbering page

Summary > Stack Numbering

Stack Numbering Setting

Current Unit Number	MAC Address	New Unit Number
1	BA-D1-B1-40-20-00	1
2	BA-D6-B0-42-60-00	2

Submit

Target Replacement Setting

Target Unit to Replace

Submit

The following table "Stack Numbering screen fields" (page 219) 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 also can include unit numbers of units that are no longer participating in the stack (not currently 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. 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 you are replacing. You use this field when you are replacing a failed unit with a new switch.

- 2 Choose the new number to assign to the switch.
- 3 Click **Submit**.
- 4 A message prompts for confirmation of the request. Click **Yes**.

—End—

Identifying unit numbers

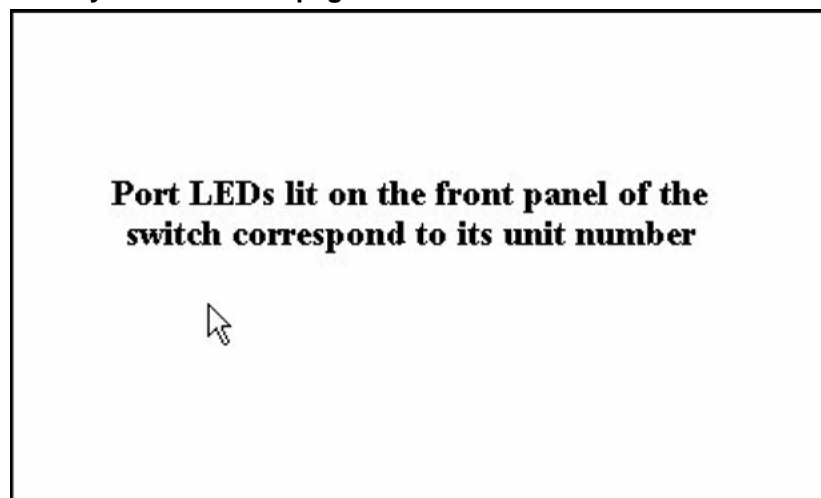
Identify the unit numbers of the switches participating in a stack configuration by viewing the LEDs on the front panel of each switch.

To identify unit numbers in your configuration:

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

- | | |
|---|---|
| 1 | Open the Identify Unit Numbers screen by selecting Summary > Identify Unit Numbers from the menu. This screen is illustrated in "Identify Unit Numbers page" (page 220). |
|---|---|

Identify Unit Numbers page



- | | |
|---|--|
| 2 | To continue viewing summary information or to start the configuration process, choose another option from the main menu. |
|---|--|

—End—

Configuring BootP, DHCP, IP, and gateway settings

BootP or DHCP mode settings can be configured and modified 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 **Submit** is clicked.

To configure BootP/DHCP, IP, and gateway settings follow this procedure:

Step Action

- 1 Open the **IP** screen by selecting **Configuration > IP** from the menu. This screen is illustrated in "IP page for a stand-alone Nortel Ethernet Routing Switch 5500 Series" (page 221) and "IP page for a stack" (page 221).

IP page for a stand-alone Nortel Ethernet Routing Switch 5500 Series

Configuration > IP

IP Setting

	Configurable	In Use	Last BootP
BootP Request Mode	BootP Disabled		
In-Band Stack IP Address	0.0.0.0	0.0.0.0	0.0.0.0
In-Band Switch IP Address	192.168.151.170	192.168.151.170	0.0.0.0
In-Band Subnet Mask	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	192.168.151.1	192.168.151.1	0.0.0.0

Submit

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	0.0.0.0	0.0.0.0	0.0.0.0
In-Band Switch IP Address	192.168.249.46	192.168.249.46	0.0.0.0
In-Band Subnet Mask	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	192.168.249.1	0.0.0.0	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 222) 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 any 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 remote management if no BootP server is set up for the switch, but it enables the switch to boot normally.
Boot Mode Setting (continued)		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. Note: This mode causes the same operation for DHCP.

Section	Item	Range	Description
		BootP or Last Address	<p>Choose this mode to inform the switch, at each start-up, to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its non-volatile memory.</p> <p>Note: Valid parameters obtained in using BootP always replace current information stored in the non-volatile memory.</p>
			<p>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 any of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.</p>
		DHCP When Needed	<p>Choose this mode to inform the switch to send a DHCP 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.</p>
		DHCP Always	<p>Choose this mode to inform the switch, each time the switch boots, to ignore any stored network parameters and send a DHCP request. If the DHCP request fails, the switch boots with the factory default IP configuration.</p>
		DHCP or Last Address	<p>Choose this mode to inform the switch, at each start-up, to obtain its IP configuration using DHCP. If the DHCP request fails, the switch uses the last IP address stored in its non-volatile memory.</p>

Section	Item	Range	Description
IP Setting	In-Band Stack IP Address	A.B.C.D	Type a new stack IP address in the appropriate format.
	In-Band Switch IP Address	A.B.C.D	Type a new switch IP address in the appropriate format. Note: When the IP address is entered 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.
	In-Band Subnet Mast	A.B.C.D	Type a new subnet mask in the appropriate format.
	In-Use		The column header for the read-only fields in this screen. The data displayed in this column represents data that is currently in use.
	Last BootP		The column header for the read-only fields in this screen. The read-only data displayed in this column represents data obtained from the last BootP or DHCP reply received.
Gateway Setting	Default Gateway	A.B.C.D	Type an IP address for the default gateway in the appropriate format.

Note: If an IP address is assigned to the device and the BootP process times out, the BootP mode remains the default mode of BootP when needed.

However, if the device does not have an assigned IP address 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 rebooting the device.

- 2 In the fields provided, enter the IP configuration information.
- 3 Click **Submit**.

—End—

Setting DHCP mode to always

Set the DHCP client to always using the Web-based command interface.

Step	Action
1	Click on the Configuration menu.
2	Click on IP . The Configuration > IP window appears.
3	From the BootP Request Mode list, choose DHCP Always .
4	Click Submit .

—End—

Note: When working with a stack, the DHCP setting chosen affects entire stack but server port must be in the management VLAN.

Detailed configuration example for DHCP

DHCP provides the following benefits:

- DHCP Client for Stack or Switch IP Address
- Ability to negotiate with the server
- Obtain an IP Address, a netmask, the IP address of the gateway, the lease time and up to three IP addresses of DNS servers.
- CLI control and ACG support
- JDM control
- Web control

Enabling the DHCP Client and starting the autoconfiguration process

The DHCP Client obtains an IP Address, a netmask, the IP address of the gateway, lease time, and the IP address of the DNS server.

To enable the use of DHCP Client for stack/switch, you have the following possibilities.

- **dhcp-always:** Use the DHCP client.
- **dhcp-last-address:** Use the last time DHCP server.
- **dhcp-when-needed:** Use DHCP client when needed.

```
55XX(config)#ip address source [dhcp-always|dhcp-when-needed|
dhcp-last-address]
```

After you select the desired DHCP mode, boot the switch/stack. DHCP Client will start after switch and stack ports enter the forwarding state. If no active DHCP server is found after a number of retries, the Boot mode will fail to 'Disabled' but will be restored at next reboot. The situation is different for 'DHCP or Last Address' mode; if no active DHCP server is found after several retries, the 'Last BootP/DHCP' configuration will pass 'In use' and switch or stack will be configured with last known settings successfully received from a DHCP Server.

To inspect the DHCP Client mode, use the following command

```
55XX(config)#show ip address source
Bootp/DHCP Mode: DHCP Always
```

The possible modes displayed are:

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

To inspect DHCP Client mode, IP configuration and DNS servers received from DHCP server, use the following commands

```
55XX(config)#show ip
Bootp/DHCP Mode: DHCP Always

          Configured      In Use      Last BootP/DHCP
-----
Stack IP Address: 0.0.0.0      10.100.92.4  10.100.92.4
Switch IP Address: 0.0.0.0      0.0.0.0     0.0.0.0
Subnet Mask:      0.0.0.0      255.255.255.0 255.255.255.0
Default Gateway: 0.0.0.0      10.100.92.1  10.100.92.1

55XX(config)#show ip dns
DNS Default Domain name: None

DNS Servers
-----
10.100.92.3
10.100.92.2
0.0.0.0
```

Among the options received from the DHCP server you have also the lease time. You can view the lease time with the following command

```
55XX(config)#show ip dhcp client lease
Configured Lease Time: 65535 seconds
Granted Lease Time: 65535 seconds
```

There are two timers, a configured lease time, and a lease time granted by DHCP server to the DHCP Client.

You can force the DHCP Client to renew its lease acquired from the DHCP Server. This refreshes the expiry time of the lease.

```
55XX(config)#renew dhcp
```

You can modify the lease time on the fly and renegotiate it with the DHCP server. Use this command in conjunction with the 'renew dhcp' command.

Step	Action
1	Modify the configured lease time <pre>55XX(config)#ip dhcp client lease 60</pre> <pre>55XX(config)#show ip dhcp client lease</pre> <pre>Configured Lease Time: 60 seconds</pre> <pre>Granted Lease Time: 65535 seconds</pre>
2	Use the <code>renew dhcp</code> command to renegotiate the lease time with the DHCP Server. <pre>55XX(config)#renew dhcp</pre> <pre>55XX(config)#show ip dhcp client lease</pre> <pre>Configured Lease Time: 60 seconds</pre> <pre>Granted Lease Time: 60 seconds</pre>

—End—

You can also return to the default configured lease time (`none`), and renegotiate this lease time again with DHCP Server.

```
55XX(config)#show ip dhcp client lease
```

```
Configured Lease Time: 3600 seconds
```

```
Granted Lease Time: 3600 seconds
```

```
55XX(config)#default ip dhcp client lease
```

```
55XX(config)#renew dhcp
```

```
55XX(config)#show ip dhcp client lease
```

```
Configured Lease Time: none
```

```
Granted Lease Time: 1800 seconds
```

To disable the use of DHCP Client and use manually configured IP settings, use the following commands.

configured-address: User-configured IP address

```
55XX(config)# ip address source configured-address
```

```
55XX(config)#show ip address source
```

Bootp/DHCP Mode: Disabled

```
55XX(config)#show ip
Bootp/DHCP Mode: Disabled

           Configured      In Use      Last BootP/DHCP
-----
Stack IP Address: 0.0.0.0          10.100.92.4
Switch IP Address: 0.0.0.0          0.0.0.0
Subnet Mask:      0.0.0.0          255.255.255.0
Default Gateway:  0.0.0.0          10.100.92.1
```

These commands disable the DHCP Client. This permits you to set the IP configuration manually.

DHCP Client - JDM configuration You can configure the DHCP Client from the JDM. Use **Edit > Chassis** and **BootMode**.

DHCP BootMode options

The screenshot shows the JDM configuration window for a Nortel Ethernet Routing Switch 5500 Series. The 'BootMode' section is expanded, showing several radio button options: 'other', 'local', 'net', 'netWhenNeeded', 'netOrLastAddress', 'dhcp', 'dhcpWhenNeeded', and 'dhcpOrLastAddress'. The 'netWhenNeeded' option is selected. Other configuration details visible include 'sysDescr: Ethernet Routing Switch 5520-24T-PWR HW:00', 'sysUpTime: 3 days, 23h:53m:43s', 'sysObjectID: 1.3.6.1.4.1.45.3.59.1', 'ManagementVlanId: 1', 'StackInsertionUnitNumber: 0', and 'AutoUnitReplacementEnabled' checked.

DHCP BootMode options

Option	Description
dhcp	Corresponds to DHCP Always mode.
dhcpWhenNeeded	Corresponds to DHCP When Needed mode.

Option	Description
dhcpOrLastAddress	Corresponds to DHCP or Last Address mode.
local	Correspond to the Locally configured address mode, where the DHCP client is Disabled.

To use DHCP Client for stack or switch, chose the desired DHCP option, click **Apply**, and boot the stack or switch. After you reboot, the DHCP Client starts and configures the stack or switch.

You can view the current DHCP mode in **Edit > Chassis, BootMode**.

To disable the DHCP Client and use locally configured IP settings, select **local** and click **Apply**.

DHCP Client - Web configuration You can configure the DHCP Client from the Web. Go to **Configuration > IP section , BootP Request Mode**.

BootP Request Mode options

The screenshot shows the 'Configuration > IP' page. On the left is a navigation tree with 'Access (RW)' expanded to 'Configuration' and 'IP' selected. The main content area is titled 'IP Setting' and contains a table with the following data:

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	192.167.120.24	192.167.120.24	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	0.0.0.0	0.0.0.0

Below the table is a 'Submit' button.

Choose one of the following DHCP Client or BootP options:

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

To use DHCP Client for stack or switch, chose the desired DHCP option, click **Submit**, and boot the stack or switch. After you reboot, the DHCP Client will start and configure the stack or switch.

To view the selected DHCP option and settings received from the DHCP server, click **Configuration > IP**.

To disable the DHCP Client and use locally configured settings, select **BootP Disabled**. BootP Disabled corresponds to the locally configured address mode.

Modifying system settings

The system name, system location, and network manager contact information can be configured or changed.

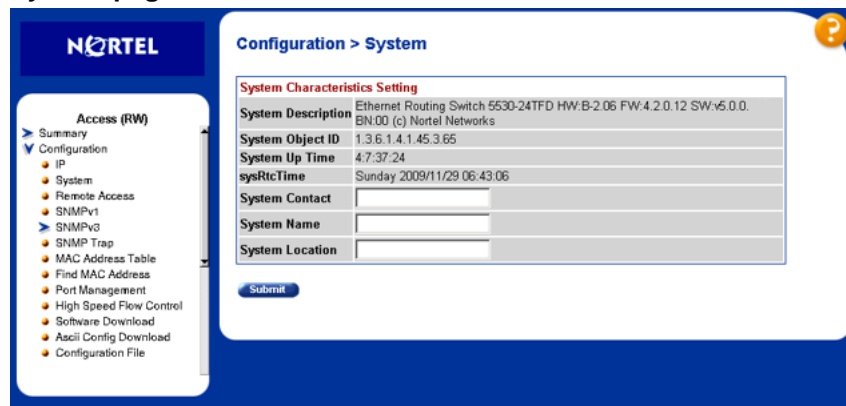
Note: The configurable parameters on the System screen are displayed in a read only-format on the Web-based Management Interface System Information home page.

To configure system settings:

Step Action

- 1 Open the **System** screen by selecting **Configuration > System** from the menu. This screen is illustrated in "[System page](#)" (page 230).

System page



The following table "[System page items](#)" (page 230) 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.

Item	Description
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, mcarlson@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, follow this procedure:

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

- 1 Open the **Remote Access** screen by selecting **Configuration > Remote Access** from the menu. This screen is illustrated in "[Remote Access page](#)" (page 232).

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 233) describes the fields on the **Remote Access** page.

Remote Access page fields

Section	Item	Range	Description
Remote Access Settings	Telnet/Access	Allowed Disallowed	Enables Telnet access.
	Telnet/Use List	Yes No	Restricts Telnet access to the specified 50 source IP addresses.
	SNMP/Access	Allowed Disallowed	Enables SNMP access.
	SNMP/Use List	Yes No	Restricts SNMP access to the specified 50 source IP addresses.
	Web Page/Access		Displays allowed Web Interface access.
	Web/Use List	Yes No	Restricts Web Interface access to the specified 50 source IP addresses.
Allowed Source IP and Subnet Mask	Allowed Source IP	A.B.C.D	Enter the source IP address you want to allow switch access.
	Allowed Source Mask	A.B.C.D	Enter the source IP mask you want to allow switch access.

- 2 Complete fields as described in the table.
- 3 Click **Submit**.

—End—

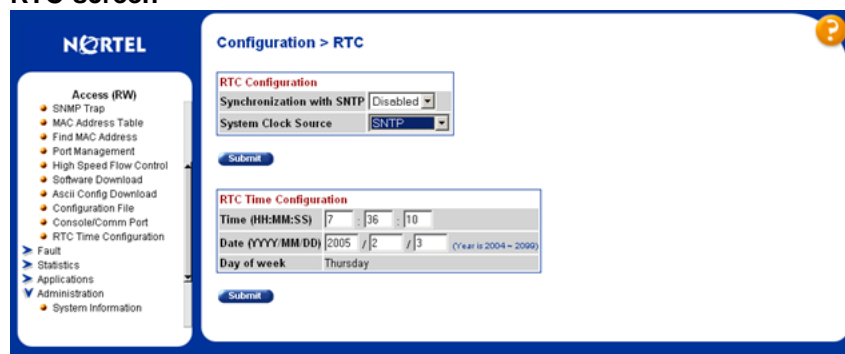
Configuring the Real-Time Clock

To configure the real-time clock, follow this procedure:

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

- | | |
|---|--|
| 1 | Open the Real Time Clock screen by selecting Configuration > RTC Time Configuration from the menu. This screen is illustrated in "RTC screen" (page 234). |
|---|--|

RTC screen



- | | |
|---|--|
| 2 | In the fields provided, configure the Real Time Clock. "Real Time Clock fields" (page 234) outlines the fields on this screen. |
|---|--|

Real Time Clock fields

Section	Field	Description
RTC Configuration	Synchronize with SNTP	Select whether or not the RTC synchronizes with SNTP.
	System Clock Source	Select the clock that the switch uses by default.
RTC Time Configuration	Time	Enter the current time in a 24-hour format.
	Date	Enter the current date.
	Day of the Week	Displays the day of the week based on entries in the Time and Date fields.

- | | |
|---|-----------------------|
| 3 | Click Submit . |
|---|-----------------------|

—End—

General Switch Administration using the JDM

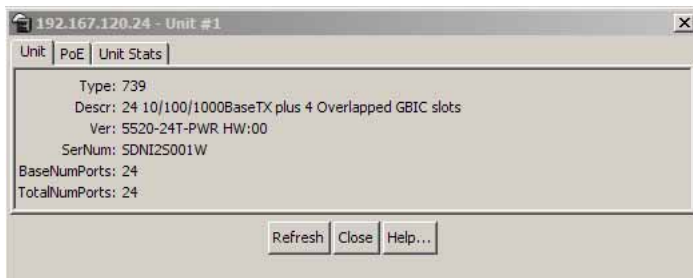
This section contains information about the following topics:

- "Viewing Unit information" (page 235)
- "Viewing SFP GBIC ports" (page 236)
- "Editing the chassis configuration" (page 236)
- "Editing and viewing switch ports" (page 250)
- "Editing and viewing switch PoE configurations" (page 262)
- "Editing Bridging Information" (page 265)
- "Configuring SNMP" (page 270)
- "Viewing topology information using Device Manager" (page 274)

Viewing Unit information

To view Unit information, follow this procedure:

Step	Action
1	Select the unit by clicking in the Device View area of the switch.
2	Open the Unit screen by selecting Edit > Unit from the menu. This screen is illustrated in the following figure.



The following table "Unit tab items" (page 235) describes the Unit screen fields.

Unit tab items

Field	Description
Type	Specifies the type number.
Descr	Specifies the type of switch.
Ver	Specifies the version number of the switch
SerNum	Specifies the serial number of the switch.
BaseNumPorts	Specifies the base number of ports.
TotalNumPorts	Specifies the total number of ports.

—End—

Viewing SFP GBIC ports

The details of an SFP GBIC port only if the port is active.

To view the SFP GBIC ports, follow this procedure:

Step	Action
1	Select the SFP GBIC ports from the Device View .
2	Open the Port screen by selecting Edit > Port from the menu.

—End—

Editing the chassis configuration

Chassis configuration can be edited from the Edit Chassis screen.

To open the Edit Chassis screen, complete these tasks:

Step	Action
1	Select the chassis in the Device View .
2	Open the Edit Chassis screen by selecting Edit > Chassis from the menu.

—End—

The following sections provide a description of the tabs in the **Edit Chassis** screen:

- ["System tab"](#) (page 237)
- ["Base Unit Info tab"](#) (page 241)
- ["Stack Info tab"](#) (page 243)
- ["Agent tab"](#) (page 246)
- ["Power Supply tab "](#) (page 247)
- ["Fan tab "](#) (page 249)

For information on the **Banner** tab or the **Custom Banner** tabs, refer to ["Banner tab"](#) (page 119) or ["Custom Banner tab"](#) (page 120).

For information on the **SNMP** and **Trap Receivers** tabs, refer to *Nortel Ethernet Routing Switch 5500 Series Security — Configuration* (NN47200-501). For information on the **ADAC** and **ADAC MAC Ranges**, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking* (NN47200-502). For information on the Stack Monitor, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration — System Monitoring* (NN47200-505).

System tab

Use the **System** tab to specify, among other things, tracking information for a device and device descriptions.

To open the **System** tab:

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


- | | |
|---|--|
| 1 | Open the Edit Chassis screen in the manner detailed at the beginning of this section. |
|---|--|

Edit Chassis screen - System tab

Note: The chassis keeps track of the elapsed time and calculates the time and date using the system clock of the Device Manager machine as a reference.

The following table 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	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.
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.
NextBootMgmtProtocol	The transport protocols to use after the next boot of the agent.
StackInsertionUnitNumber	The unit number to be assigned to the next unit that joins the stack. The value cannot be set 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 when determining the unit number of new units.

Field	Description
AutoUnitReplacement Enabled	Determines whether auto-unit-replacement is enabled or disabled.
CurrentMgmtProtocol	Read only: The current transport protocols that the agent supports.
BootMode	The source from which to load the initial protocol configuration information to boot the switch the next time. The options available are <ul style="list-style-type: none"> • local • net • netWhenNeeded • netOrLastAddress • dhcp • dhcpWhenNeeded • dhcpOrLastAddress
ImageLoadMode	Read only: The source from which to load the agent image at the next boot.
CurrentImageVersion	Read only: The version number of the agent image that is currently used on the switch.
LocalStorageImage Version	Read only: The version number of the agent image that is stored in flash memory on the switch.
NextBootDefaultGateway	Read only: The IP address of the default gateway for the agent to use after the next time the switch is booted.
CurrentDefaultGateway	Read only: The IP address of the default gateway that is currently in use.
NextBootLoadProtocol	Read only: The transport protocol to be used by the agent 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.

—End—

See also:

- ["Base Unit Info tab" \(page 241\)](#)
- ["Stack Info tab" \(page 243\)](#)
- ["Agent tab" \(page 246\)](#)
- ["Power Supply tab " \(page 247\)](#)
- ["Fan tab " \(page 249\)](#)
- ["Banner tab" \(page 119\)](#)
- ["Custom Banner tab" \(page 120\)](#)

Configuring to always use DHCP For more information about DHCP, see ["Configuring and enabling DHCP" \(page 115\)](#).

Set the switch to always use DHCP.

Step	Action
1	Select the chassis in the Device view.
2	Choose Chassis from the Edit menu. The Edit Chassis window appears.
3	In the BootMode section of the window, select the dhcp option button to set dhcp Always mode.
4	Click Apply to activate the new mode on the switch.

—End—

Configuring to use DHCP when needed Set the switch to use DHCP when needed.

For more information about DHCP, see ["Configuring and enabling DHCP" \(page 115\)](#).

Step	Action
1	Select the chassis in the Device view.
2	Choose Chassis from the Edit menu. The Edit Chassis window appears.
3	In the BootMode section of the window, select the dhcpWhenNeeded option button to set dhcp When Needed mode.
4	Click Apply to activate the new mode on the switch.

—End—

Configuring to use DHCP or last address Set the switch to use DHCP or last address.

For more information about DHCP, see ["Configuring and enabling DHCP" \(page 115\)](#).

Step	Action
1	Select the chassis in the Device view.
2	Choose Chassis from the Edit menu. The Edit Chassis window appears.
3	In the BootMode section of the window, select the dhcpOrLastAddress option button to set dhcp Or Last Address mode.
4	Click Apply to activate the new mode on the switch.

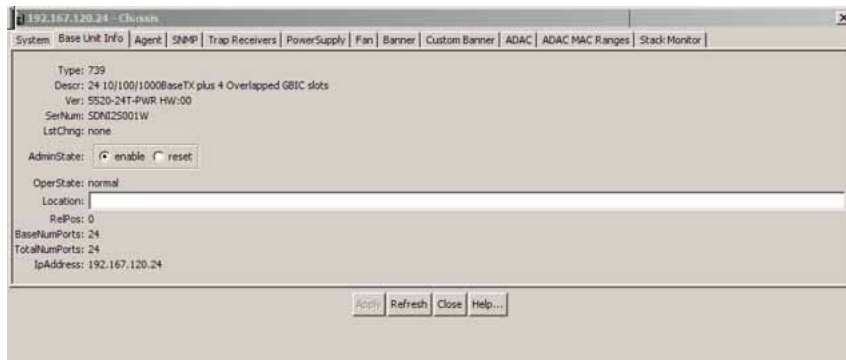
—End—

Base Unit Info tab

The **Base Unit Info** tab provides read-only information about the operating status of the hardware and whether or not the default factory settings are being used.

To open the **Base Unit Info** tab:

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. See the Base Unit Info tab in the following illustration.



The following table "Base Unit Info tab items" (page 242) 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 the current state was entered 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 only resets the base unit.
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 237)

- "Stack Info tab" (page 243)
- "Agent tab" (page 246)
- "Power Supply tab " (page 247)
- "Fan tab " (page 249)
- "Banner tab" (page 119)
- "Custom Banner tab" (page 120)

—End—

Stack Info tab

Like the **Base Unit Info** tab, the **Stack Info** tab provides read-only information about the operating status of the *stacked* switches and whether or not the default factory settings are being used.

To open the **Stack Info** tab:

Step Action

- 1 Open the Edit **Chassis** screen in the manner detailed at the beginning of this section.
- 2 Click the **Stack Info** tab. This tab is illustrated in "Edit Chassis screen -- Stack Info tab" (page 243).

Edit Chassis screen -- Stack Info tab

Index	Descr	Location	LstChng	AdminState	OperState	Ver	SerNum	BaseNumPorts	TotalNumPorts	IpAddress
1	24 10/100/1000BaseTx plus 2 Overlapped GBIC slots		0 day, 00h:00m:15s	enable	normal	5510-24T HW:ROB.5	SNR1BB11026	24	24	0.0.0.0
2	48 10/100/1000BaseTx plus 2 Overlapped GBIC slots		0 day, 00h:00m:15s	enable	normal	5510-48T HW:ROB.6	SNR0BB61062	48	48	0.0.0.0

The following table "Stack Info tab fields" (page 243) describes the **Stack Info** tab fields.

Stack Info tab fields

Field	Description
Descr	A description of the component or subcomponent. If not available, the value is a zero length string.

Field	Description
Location	<p>The geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected together 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 is applicable only to components that can be found 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 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	<p>The value of sysUpTime when it was detected that the component/sub-component was added to the chassis. If this action has not occurred since the cold/warm start of the agent, then the value is zero.</p>
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 some other 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

Field	Description
	<ul style="list-style-type: none"> test--starts self test of component, with the result to be normal, warning, nonFatalErr, or fatalErr in object s5ChasComOperState The allowable (and meaningful) values are determined by the component type.
OperState	<p>The current operational state of the component. The possible values are:</p> <ul style="list-style-type: none"> other--some other state notAvail--state not available removed--component removed disabled--operation disabled normal--normal operation resetInProg--reset in progress testing--doing a self test warning--operating at warning level nonFatalErr--operating at error level fatalErr--error stopped operation <p>The allowable (and meaningful) values are determined by the component type.</p>
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 237)

- "Base Unit Info tab" (page 241)
- "Agent tab" (page 246)
- "Power Supply tab " (page 247)
- "Fan tab " (page 249)
- "Banner tab" (page 119)
- "Custom Banner tab" (page 120)

—End—

Agent tab

The **Agent** tab provides read-only information about the addresses that the agent software uses to identify the switch.

To open the **Agent** tab:

Step Action

- 1 Open the **Edit Chassis** screen in the manner detailed at the beginning of this section.
- 2 Select the **Agent** tab. This tab is illustrated in "Edit Chassis dialog box -- Agent tab" (page 246).

Edit Chassis dialog box -- Agent tab

NextBootIpAddr	NextBootNetMask	LoadServerAddr	ImageFileName	ValidFlag	BootRouterAddr	MacAddr
192.168.249.46	255.255.255.0	192.168.249.10	flagship_500s.img	valid	0.0.0.0	00:11:f9:35:d0:00

The following table "Agent tab fields" (page 246) describes the Agent tab fields.

Agent tab fields

Field	Description
NextBootpAddr	The IP address of the BootP server to be used the next time the switch is booted.
NextBootNetMask	The subnet mask to be used 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.

Field	Description
ValidFlag	Indicates if the configuration and/or image files were downloaded from this interface and if the file names have not been changed.
BootRouterAddr	The IP address of the boot router for the configuration file and/or the image file.
MacAddr	The switch's MAC address.

See also

- ["System tab" \(page 237\)](#)
- ["Base Unit Info tab" \(page 241\)](#)
- ["Stack Info tab" \(page 243\)](#)
- ["Agent tab" \(page 246\)](#)
- ["Power Supply tab " \(page 247\)](#)
- ["Fan tab " \(page 249\)](#)
- ["Banner tab" \(page 119\)](#)
- ["Custom Banner tab" \(page 120\)](#)

—End—

Power Supply tab

The Power Supply tab provides read-only information about the operating status of the switch power supplies.

The power supply parameters are slightly different for the Nortel Ethernet Routing Switch 5520, as it supports Power over Ethernet (PoE).

To open the **PowerSupply** tab:

Step Action

- 1 Open the **Edit Chassis** screen in the manner detailed at the beginning of this section.
- 2 Select the **PowerSupply** tab. This tab is illustrated in "[Edit Chassis screen -- Power Supply tab](#)" (page 248).

Edit Chassis screen -- Power Supply tab

—End—

The following table "Power Supply tab fields" (page 248) describes the **Power Supply** tab fields.

Power Supply tab fields

Field	Description
OperStat	<p>The operational state of the power supply. Possible values include:</p> <ul style="list-style-type: none"> • other: Some other state. • notAvail: State not available. • removed: Component was removed. • disabled: Operation disabled. • normal: State is in normal operation. • resetInProg: There is a reset in progress. • testing: System is doing 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: A module needs to be configured. The allowable values are determined by the component type.

See also:

- "System tab" (page 237)
- "Base Unit Info tab" (page 241)
- "Stack Info tab" (page 243)
- "Agent tab" (page 246)
- "Fan tab " (page 249)
- "Banner tab" (page 119)

- "Custom Banner tab" (page 120)

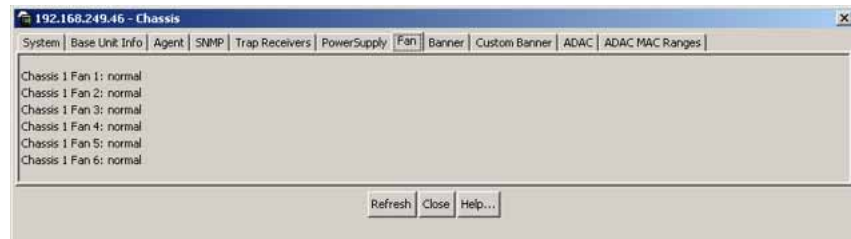
Fan tab

The Fan tab provides read-only information about the operating status of the switch fans.

To open the **Fan** tab:

Step	Action
1	Open the Edit Chassis screen in the manner detailed at the beginning of this section.
2	Select the Fan tab. This tab is illustrated in " Edit Chassis screen -- Fan tab" (page 249).

Edit Chassis screen -- Fan tab



—End—

The following table "Fan tab fields" (page 249) describes the Fan tab fields.

Fan tab fields

Field	Description
OperStat	<p>The operational state of the fan. Values include:</p> <ul style="list-style-type: none"> • other: Some other 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 doing 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 operation notConfig: Fan needs to be configured. The allowable values are determined by the component type.

See also:

- "System tab" (page 237)
- "Base Unit Info tab" (page 241)
- "Stack Info tab" (page 243)
- "Agent tab" (page 246)
- "Power Supply tab" (page 247)
- "Banner tab" (page 119)
- "Custom Banner tab" (page 120)

Editing and viewing switch ports

Port configuration tasks are performed 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** from the menu. Multiple ports can be edited by selecting ports from the **Device View** with the Control (CTRL) key depressed. Examples of the **Port** screen are illustrated in "Port screen with one port selected" (page 250) and "Port screen with multiple ports selected" (page 251).

Port screen with one port selected

As demonstrated in "Port screen with one port selected" (page 250) and "Port screen with multiple ports selected" (page 251), the presentation of the Port screen differs when one port is selected or multiple ports are selected. This difference is mainly in presentation although some options are not be available when multiple ports are selected. 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
3(1/3)	1/3	Nort...	eth...	eth...	1514	00:11:49:3...	up	down	0 day, 19...	enabled	true	Full	Full	mbps1000	1000	10Half, 1
5(1/5)	1/5	Nort...	eth...	eth...	1514	00:11:49:3...	up	down	0 day, 19...	enabled	true	Full	Full	mbps1000	1000	10Half, 1

The following sections provide a description of some of the tabs on the Port screen:

- "Interface tab" (page 251)
- "PoE tab" (page 256)
- "Configuring Rate Limiting" (page 257)
- "TDR tab" (page 258)

For information on the **VLAN**, **LACP**, **VLACP**, **ADAC**, and **STP BPDU-Filtering** tabs, refer to *Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking* (NN47200-502). For information on the **EAPOL**, **EAPOL Advance**, and **NSNA** tabs, refer to *Nortel Ethernet Routing Switch 5500 Series Security — Configuration* (NN47200-501).

Interface tab

The **Interface** tab shows the basic configuration and status of a port.

To view the **Interface** tab, follow this procedure:

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

- | | |
|---|---|
| 1 | Select the port to edit from the Device View . Select Edit > Port from the menu. The Port screen opens with the Interface tab displayed. This tab is illustrated in "Port screen -- Interface tab" (page 252). |
|---|---|

Port screen -- Interface tab

The screenshot shows the 'Interface' tab of the configuration interface for a Nortel Ethernet Routing Switch 5530-24TFD Module - Port 5. The window title is '192.168.249.46 - Port 1/5'. The interface is currently configured with the following settings:

- Index: 5
- Name: (empty)
- Descr: Nortel Ethernet Routing Switch 5530-24TFD Module - Port 5
- Type: ethernet-csmacd
- Mtu: 1514
- PhysAddress: 00-11-f9-35-d0-00
- AdminStatus: up down
- OperStatus: down
- LastChange: 0 day, 19h:00m:15s
- LinkTrap: enabled disabled
- AutoNegotiate:
- AdminDuplex: half full
- OperDuplex: full
- AdminSpeed: mbps10 mbps100 mbps1000 mbps10000
- OperSpeed: 1000 mbps
- AutoNegotiationCapability: 10Half, 10Full, 100Half, 100Full, 1000Full, PauseFrame
- AutoNegotiationAdvertisements:
 - 10Half 10Full 100Half
 - 100Full 1000Half 1000Full
 - PauseFrame AsymPauseFrame
- MLId: 0
- IsPortShared: portNotShared
- PortActiveComponent: fixedPort

Buttons at the bottom: Apply, Refresh, Close, Help...

To continue, go to:

- " Interface tab" (page 251)

Interface tab items

The following table "Interface tab fields" (page 252) describes the Interface tab fields.

Interface tab fields

Field	Description
Index	A unique value assigned to each interface. The value ranges between 1 and 64 standalone. On stack, the index value of the first port of the second unit is 65. The maximum value is 512.
Name	Use this field to 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.

Field	Description
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 a managed system is initialized, 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. It remains 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.</p>
LastChange	<p>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.</p>
LinkTrap	<p>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).</p>
AutoNegotiate	<p>Indicates whether this port is enabled for autonegotiation or not.</p>

Field	Description
AdminDuplex	Sets the administrative duplex mode of the port (half or full).
OperDuplex	Shows 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>Specifies 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> <p>bit 7 - Asymmetric PAUSE frame support advertisements</p> <p>If auto-negotiation is not supported by the port hardware, then all bits reflect a value of zero.</p>

Field	Description
AutoNegotiation Advertisements	<p>Specifies 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 only used 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>
MltId	The multilink trunk to which the port is assigned (if any).
IsPortShared	Displays if the selected port is a shared port or not.
PortActive Component	Displays the active component of shared ports.

2 Click **Apply** after making any changes.

See also

- ["PoE tab" \(page 256\)](#)
- ["Configuring Rate Limiting" \(page 257\)](#)
- ["TDR tab" \(page 258\)](#)

—End—

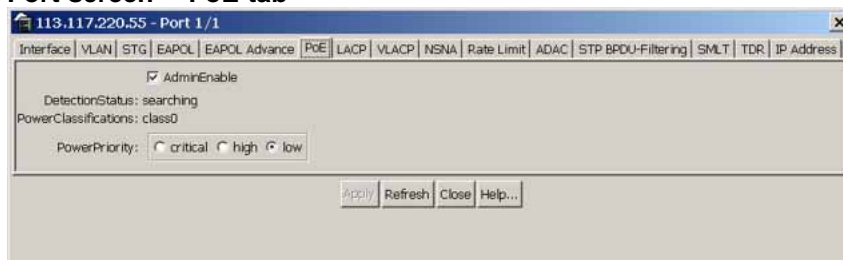
PoE tab

The **PoE** tab enables the configuration of the PoE power settings for a port in the Nortel Ethernet Routing Switch 5520. This tab is not displayed for units other than the 5520.

To view the **PoE** tab, follow this procedure:

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

- | | |
|---|--|
| 1 | Select the port to edit from the Device View . Select Edit > Port from the menu. The Port screen appears. Select the PoE tab. This tab is illustrated in "Port screen -- PoE tab" (page 256). |
|---|--|

Port screen -- PoE tab

"PoE tab fields" (page 256) describes the **PoE** tab fields.

PoE tab fields

Field	Description
AdminEnable	Enables or disables PoE on this port.
Detection Status	Displays the operational status of the power-device detecting mode on the specified port: <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 detected--detecting function detects a valid powered device but the port is not supplying power deliveringPower--detection found a valid powered device and the port is delivering power fault--power-specific fault detected on port

Field	Description
	<ul style="list-style-type: none"> invalidPD--detecting function found an invalid powered device denyLowPriority--port disabled by management system to supply power to higher-priority ports test--detecting device in test mode <p>Note: Nortel recommends against using the test operational status.</p>
PowerClassifications	Displays the operational status of the port PD classification.
PowerPriority	<p>Sets the power priority for the specified port to:</p> <ul style="list-style-type: none"> critical high low

Note: The **PoE** tab is for setting Power over Ethernet (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 251)
- "Configuring Rate Limiting" (page 257)
- "TDR tab" (page 258)

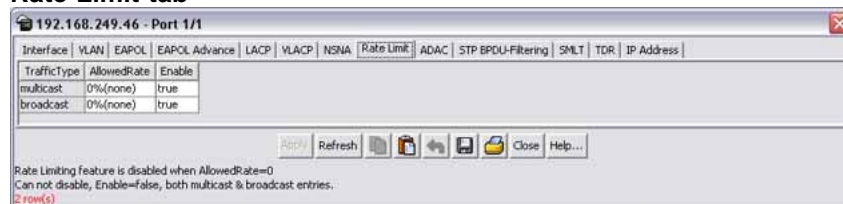
Configuring Rate Limiting

You can use the **Rate Limit** tab to configure the Rate Limiting for a single port.

To view the Rate Limit tab:

Step Action

- 1 Select the port to test from the **Device View**.
- 2 Select **Edit > Port** from the menu. 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	Specifies the two types of traffic that can be set with rate limiting: broadcast and multicast.
AllowedRate	Sets the rate limiting percentage. The available range is from 0% (none) to 10%.
Enable	Enables and disables rate limiting on the port for the specified traffic type. Options are true (enabled) or false (disabled).

—End—

See also

- [" Interface tab" \(page 251\)](#)
- ["PoE tab" \(page 256\)](#)
- ["TDR tab" \(page 258\)](#)

TDR tab

With Release 5.0 software, the 5500 Series switch is equipped with a Time Domain Reflectometer (TDR). The TDR provides a diagnostic capability to test connected cables for defects (such as short pin and pin open). Use the TDR tab to initiate cable diagnostic tests on attached cables.

The cable diagnostic tests only apply to Ethernet copper ports; fiber ports cannot be tested. You can initiate a test on multiple ports at the same time.

When you test a cable with the TDR, if the cable has a 10/100 MB/s link, the link is broken during the test and restored only when the test is complete. Use of the TDR does not affect 1 GB/s links.

Note: The accuracy margin of cable length diagnosis is between three to five meters. Nortel suggests the shortest cable for length information be five meters long.

To initiate a TDR test:

- | Step | Action |
|------|--|
| 1 | Select the port to test from the Device View . |
| 2 | Select Edit > Port from the menu. The Port screen appears. |
| 3 | Select the TDR tab.
The TDR tab appears. |

TDR tab



- Select the **StartTest** option. (If multiple ports are selected, select **true** from the **StartTest** field for each port that you want to test.)
- Click **Apply**.

"TDR tab fields" (page 259) describes the TDR tab fields.

TDR tab fields

Field	Description
StartTest	Enables the TDR test.
TestDone	Indicates whether a TDR test is complete.

Field	Description
CableStatus	<p>Status of the cable as a whole. The status of a cable is, in a sense, a summation of the status of its pairs. If all the pairs are normal, the cable is normal. If the cable consists of zero or more normal pairs and one or more open pairs, the cable is considered open. If the cable consists of shorted pairs and normal pairs, it is considered shorted. Any combination of open and shorted pairs is considered simply failed.</p> <ul style="list-style-type: none"> • cableFail • cableNormal • cableOpen • cableShorted • cableNotApplicable • cableUntested
Pair1Status	<p>The status of a single pair in the cable:</p> <ul style="list-style-type: none"> • pairFail • pairNormal • pairOpen • pairShorted • pairNotApplicable • pairNotTested • pairForce <p>Note: If a 10MB or 100MB link is established without autonegotiation, Pair 2 will return Forced mode. The pair length is meaningless in this case.</p>
Pair1Length	Pair Length, in meters, measured by Time Domain Reflectometry.
Pair2Status	The status of a single pair in the cable.
Pair2Length	Pair Length, in meters, measured by Time Domain Reflectometry.
Pair3Status	The status of a single pair in the cable.
Pair3Length	Pair Length, in meters, measured by Time Domain Reflectometry.
Pair4Status	The status of a single pair in the cable.

Field	Description
Pair4Length	Pair Length, in meters, measured by Time Domain Reflectometry.
CableLength	Length of cable in meters based on average electrical length of 4 pairs. Measurement can be done when traffic is live or not.
Pair1Polarity	The polarity of a single pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair1Swap	The pair swap in the cable: <ul style="list-style-type: none"> • normal • swapped • invalid • error This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair1Skew	Pair skew is measured in nanoseconds. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.
Pair2Polarity	The polarity of a single pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair2Swap	The pair swap in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair2Skew	Pair skew is measured in nanoseconds. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.
Pair3Polarity	The polarity of a single pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.

Field	Description
Pair3Swap	The pair swap in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair3Skew	Pair skew is measured in nanoseconds. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.
Pair4Polarity	The polarity of a single pair in the cable.
Pair4Swap	The pair swap in the cable.
Pair4Skew	Differential cable pair length in meters. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.

—End—

See also

- [" Interface tab" \(page 251\)](#)
- ["PoE tab" \(page 256\)](#)
- ["Configuring Rate Limiting" \(page 257\)](#)

Editing and viewing switch PoE configurations

The Power over Ethernet (PoE) parameters that apply to the whole switch can be configured and viewed using the Unit screen.

The PowerSupply tab on the Edit Chassis screen displays the status of the internal Nortel Ethernet Routing Switch 5500 Series power supply.

Note: View and edit the PoE parameters for each Nortel Ethernet Routing Switch 5520 one by one. If more than one unit is selected, the PoE power parameters, such as the PoE tab, are not displayed.

Edit the PoE parameters from the Edit Unit screen on Nortel Ethernet Routing Switch 5520 units.

To open the Edit Unit screen:

Step Action

- 1 Select the unit.
 - 2 Open the **Edit Unit** screen by selecting **Edit > Unit** from the menu.
-

—End—

Unit tab for a single unit

To open the Unit tab for a single unit, follow this 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.



The following table "Unit tab items" (page 263) describes the Unit tab items.

Unit tab items

Item	Description
Type	The switch type.
Descr	A description of the switch hardware including number of ports and transmission speed.
Ver	Displays the switch hardware version.
SerNum	Displays the serial number of this device.
BaseNumPorts	Displays the number of base ports on the switch.
TotalNumPorts	Displays the total number of ports on the switch, including MDA ports.

See also

- "PoE tab for a single unit" (page 264)

—End—

PoE tab for a single unit

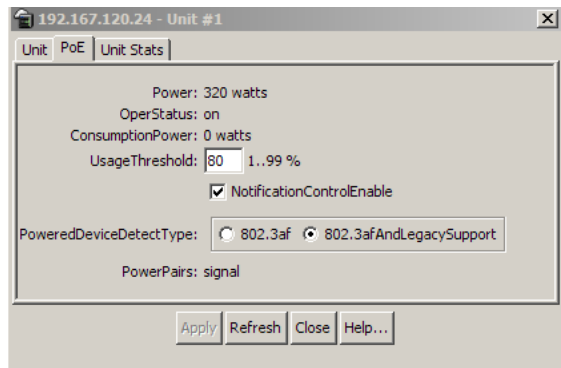
To set the power usage threshold, the power pairs to use, and the power detection method to use, select a *single* Nortel Ethernet Routing Switch 5520 unit.

Note: These parameters only can be viewed and set by selecting a *single* unit. If more than one unit is selected, the **PoE** tab is not displayed.

To open the **PoE** tab for a *single* unit:

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

- 1 Select the relevant Nortel Ethernet Routing Switch 5520 unit.
- 2 Open the **Unit** screen by selecting **Edit > Unit** from the menu.
- 3 Select the **PoE** tab. See the **PoE** tab in the following illustration.



The following table "PoE tab items for a single unit" (page 264) describes the PoE tab items for a single unit.

PoE tab items for a single unit

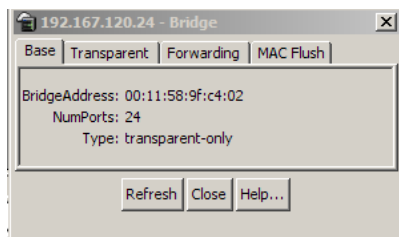
Item	Description
Power	Displays the total power available to the Nortel Ethernet Routing Switch 5520.

Item	Description
OperStatus	Displays the power state of the Nortel Ethernet Routing Switch 5520.: <ul style="list-style-type: none"> • on • off • faulty
Consumption Power	Displays the power being used by the Nortel Ethernet Routing Switch 5520.
Usage Threshold	Enables you to set a percentage of the total power usage of the Nortel Ethernet Routing Switch 5520 switch based on which the system sends a trap. <p>Note: You must have the traps enabled (see NotificationControlEnable) to receive a power usage trap.</p>
Notification Control Enable	Enables you to enable or disable sending traps if the switch's power usage exceed the percentage set in the UsageThreshold field.
PowerDevice DetectType	Enables you to 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
PowerPairs	Displays the RJ-45 pin pairs that the switch uses to send power to the ports on the switch.

—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** from the menu. See the **Bridge** screen in the following illustration.



For details, refer to the following topics:

- ["Base tab" \(page 266\)](#)
- ["Transparent tab" \(page 267\)](#)
- ["Forwarding tab" \(page 268\)](#)

For more information on the Mac Flush tab, see *Nortel Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and Link Aggregation (NN47200-502)*.

Base tab

The **Base** tab displays basic Bridge information including the MAC address, type, and number of ports participating in the Bridge.

The MAC address used by the bridge must be referred to in a unique fashion; moreover, it must be the smallest MAC address (numerically) of all ports that belong to the bridge. However, it is only required to be unique when integrated with *dot1dStpPriority*. A unique *BridgeIdentifier* is formed that is used in the Spanning Tree Protocol.

To view the **Base** tab, follow this procedure:

Step Action

- 1 Open the **Bridge** screen by selecting **Edit > Bridge** from the menu. The **Bridge** screen appears with the **Base** tab selected.
["Bridge screen -- Base tab fields" \(page 266\)](#) describes the fields on this tab.

Bridge screen -- Base tab fields

Field	Description
BridgeAddress	MAC address of the bridge when it is referred to in a unique fashion. This address must be the smallest MAC address of all ports that belong to the bridge. However, it is has to be unique. When concatenated with <i>dot1dStpPriority</i> , a unique bridge ID is formed that is then used in the Spanning Tree Protocol.

Field	Description
NumPorts	Number of ports controlled by the bridging entity.
Type	Indicates 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" \(page 267\)](#)
- ["Forwarding tab" \(page 268\)](#)

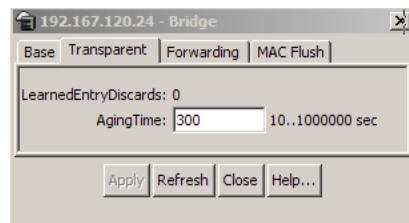
Transparent tab

The **Transparent** tab is used to view information about learned forwarding entries.

To view the **Transparent** tab, follow this procedure:

Step Action

- 1 Open the **Bridge** screen by selecting **Edit > Bridge** from the menu. The **Bridge** screen appears. Select the **Transparent** tab. See the **Transparent** tab in the following screen.



"Bridge screen -- Transparent tab fields" (page 268) describes the fields on this tab.

Bridge screen -- Transparent tab fields

Field	Description
LearnedEntryDiscards	Number of Forwarding Database entries learned that have been discarded due to a lack of space in the Forwarding Database. If this counter is increasing, 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 been occurring but is not persistent.
AgingTime	Timeout period in seconds for aging out dynamically learned forwarding information. Note: The 802.1D-1990 specification recommends a default of 300 seconds.

- 2 Click **Apply** if the **AgingTime** field is modified.

—End—

See also:

- "Base tab" (page 266)
- "Forwarding tab" (page 268)

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, follow this procedure:

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

- 1 Open the **Bridge** screen by selecting **Edit > Bridge** from the menu. The **Bridge** screen appears. Select the **Forwarding** tab. See the **Forwarding** tab in the following illustration.

Status	Address	Port	VlanIds
learned	00:08:02:de:0e:ab	1/24	1
learned	00:0c:f8:42:70:78	1/24	1
mgmt	00:11:58:9f:c4:00	0	
learned	00:50:52:f5:20:01	1/24	1
learned	00:60:fd:cb:b8:c1	1/24	1

5 row(s)

To continue, go to:

- ["Forwarding tab fields" \(page 269\)](#)

—End—

See also:

- ["Base tab" \(page 266\)](#)
- ["Transparent tab" \(page 267\)](#)

Forwarding tab fields

The following table describes the Forwarding tab fields.

Forwarding tab fields

Field	Description
Status	<p>The values of this fields 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. • 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 some other MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is being used to determine if a frames addressed to the value of dot1dTpFdbAddress are being forwarded.
Address	A unicast MAC address for which the bridge has forwarding or filtering information.

Field	Description
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 have the forwarding/filtering information for this address (located 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(3).</p>
VlanIds	VLANIDs of which this port is a member.

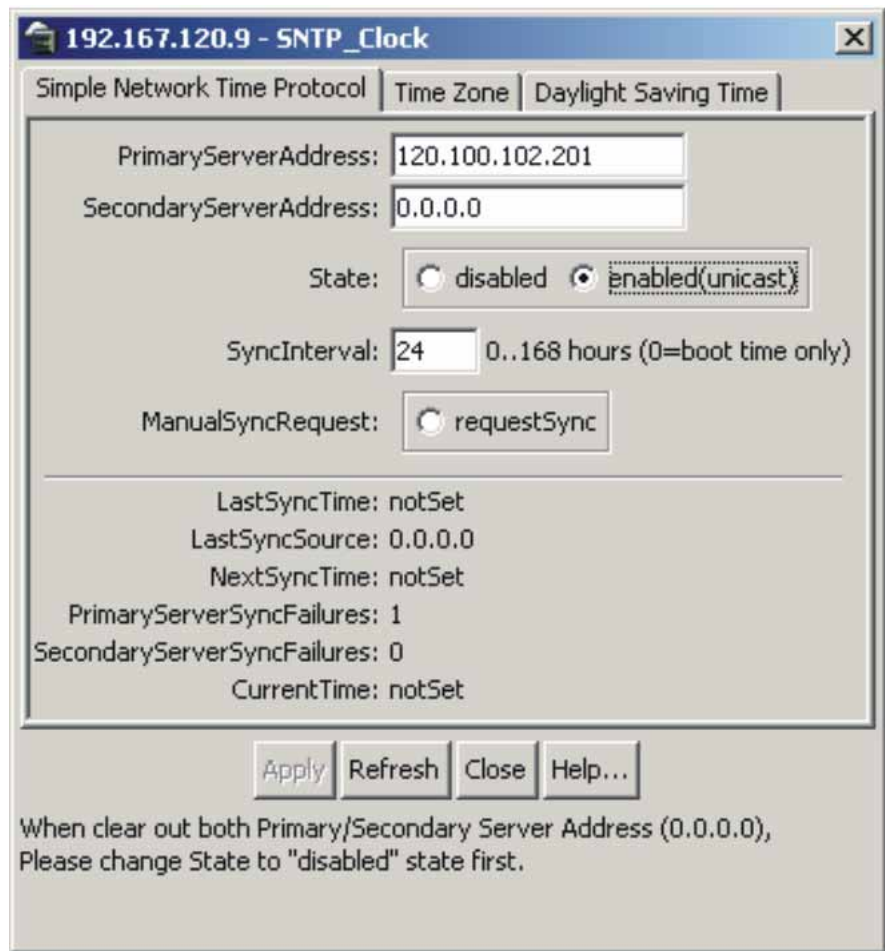
Configuring SNTP

The **SNTP/Clock** screen contains the parameters for configuring Simple Network Time Protocol (SNTP).

To open the **SNTP/Clock** screen:

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

- | | |
|---|--|
| 1 | From the Edit menu, choose SNTP/Clock . The SNTP_clock dialog box appears with the Simple Network Time Protocol tab. |
|---|--|



192.167.120.9 - SNTP_Clock

Simple Network Time Protocol | Time Zone | Daylight Saving Time

PrimaryServerAddress: 120.100.102.201

SecondaryServerAddress: 0.0.0.0

State: disabled enabled(unicast)

SyncInterval: 24 0..168 hours (0=boot time only)

ManualSyncRequest: requestSync

LastSyncTime: notSet
 LastSyncSource: 0.0.0.0
 NextSyncTime: notSet
 PrimaryServerSyncFailures: 1
 SecondaryServerSyncFailures: 0
 CurrentTime: notSet

Apply Refresh Close Help...

When clear out both Primary/Secondary Server Address (0.0.0.0),
 Please change State to "disabled" state first.

- 2 Edit the fields as indicated by the table.

The following table describes the **Simple Network Time Protocol** fields.

Field	Description
PrimaryServer Address	The IP address of the primary SNTP server.
SecondaryServer Address	The IP address of the secondary SNTP server.

Field	Description
State	Controls whether the device uses the Simple Network Time Protocol to synchronize the device clock to the Coordinated Universal Time. 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	Controls the frequency, in hours, with which the device attempts to synchronize with the NTP servers.
ManualSynchRequest	Specifies that the device must immediately attempt to synchronize with the NTP servers.
LastSynchTime	Specifies the UTC when the device last synchronized with an NTP server.
LastSynchSource	Specifies the IP source address of the NTP server with which this device last synchronized.
NextSynchTime	Specifies the UTC at which the next synchronization is scheduled.
PrimaryServerSynchFailures	Specifies the number of times the switch failed to synchronize with the primary server address. However, synchronization with the secondary server address can still occur.
SecondaryServerSynchFailures	Specifies the number of times the switch failed to synchronize with the secondary server address.
CurrentTime	Specifies the UTC for the switch.

- 3 Click **Refresh**.

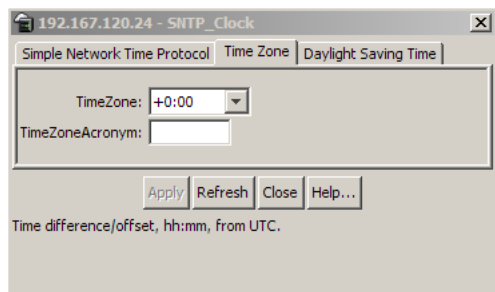
—End—

Configuring local time zone

Set the local time zone on the ERS 5500.

Step Action

- 1 From the **Edit** menu, choose **SNTP/Clock**. The SNTP_Clock dialog box appears.
- 2 Click the **Time Zone** tab. The **Time Zone** tab appears.



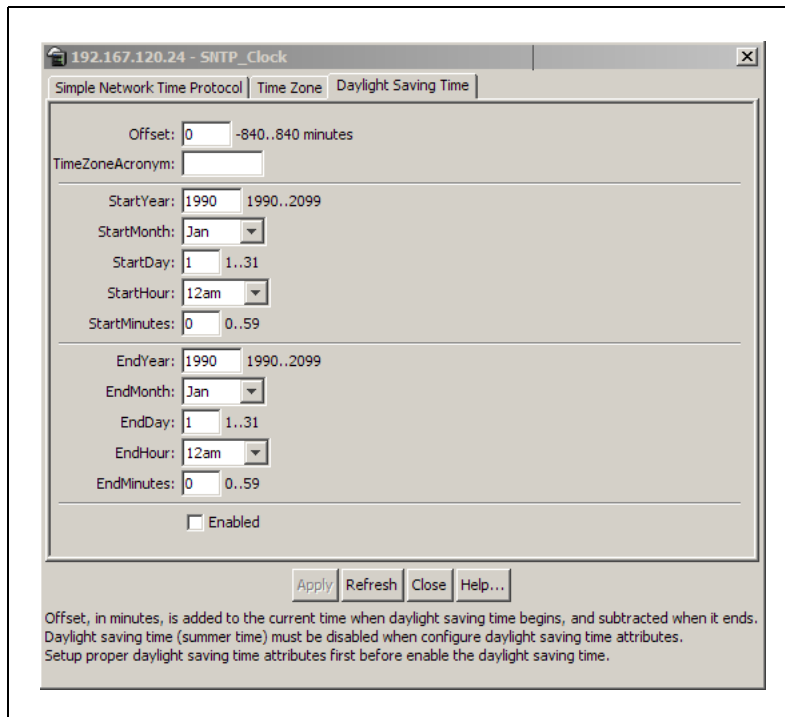
- 3 Type the time zone offset in the **TimeZone** box.
- 4 Type a time zone acronym in the **TimeZoneAcronym** box.
- 5 Click **Apply**.

—End—

Configuring daylight savings time

Set daylight saving start and end time on the ERS 5500.

Step	Action
1	From the Edit menu, choose SNTP/Clock . The SNTP_Clock dialog box appears.
2	Click the Daylight Saving Time tab. The Daylight Saving Time tab appears.



- 3 Type the number of minutes to shift the clock in the **Offset** box.
- 4 Type the time zone acronym for the change in the **TimeZoneAcronym** box.
- 5 Select the **StartYear**, **StartMonth**, **StartDate**, **StartHour** and type the **StartMinutes** (if applicable) to define when to switch the clock to daylight saving time.
- 6 Select the **EndYear**, **EndMonth**, **EndDate**, **EndHour** and type the **EndMinutes** (if applicable) to define when to switch the clock back to normal time.
If you want to keep the same daylight saving time changeover dates, you can set the **EndYear** to a year in the future.
- 7 Click **Enabled** to enable daylight savings time.
- 8 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 275)

- ["Topology Table tab" \(page 275\)](#)

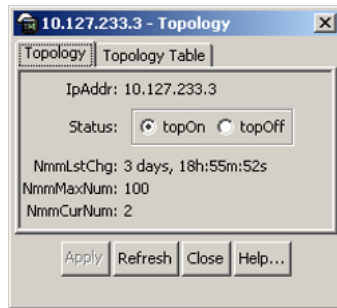
Topology tab

To view topology information:

From the Device Manager menu bar, 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" \(page 275\)](#)

Topology Table tab

To view more topology information:

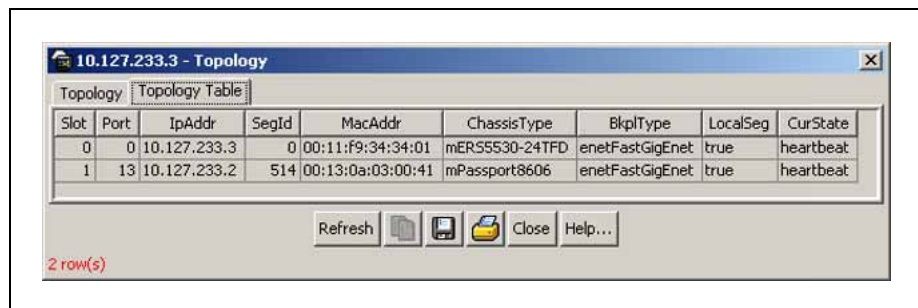
Step	Action
------	--------

- | | |
|---|--|
| 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.



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 has recently changed. heartbeat: Topology information is unchanged. new: The sending agent is in a new state.

—End—

See also:

- ["Topology tab" \(page 275\)](#)

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 279)
- ["Configuring LLDP using the CLI"](#) (page 284)
- ["Configuring LLDP using Device Manager"](#) (page 304)

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.

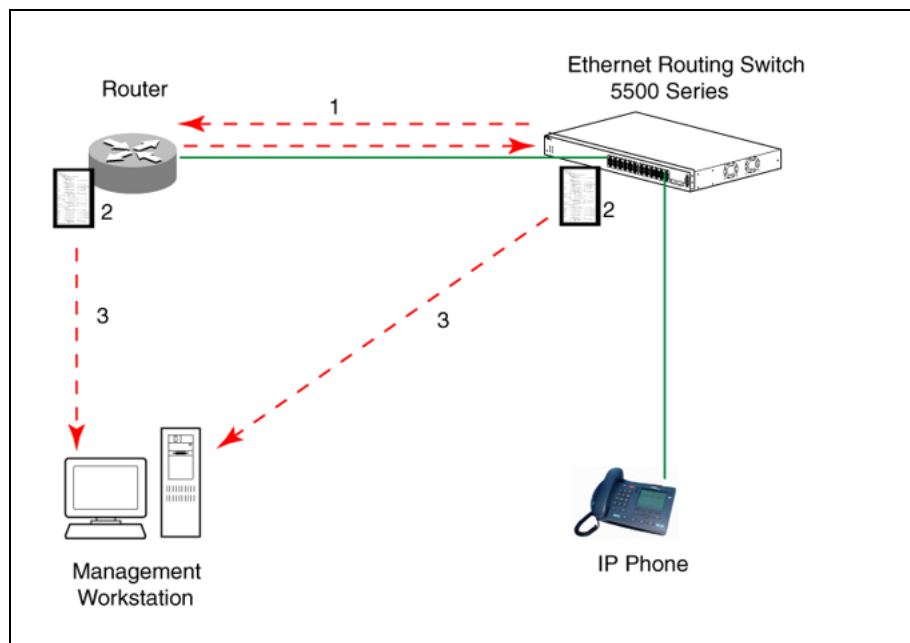
Each LLDP station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN (802.3 Ethernet with 5500 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"](#) (page 280) 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, refer to the following:

- ["Management TLVs" \(page 281\)](#)
- ["IEEE 802.1 organizationally-specific TLVs" \(page 282\)](#)
- ["IEEE 802.3 organizationally-specific TLVs" \(page 282\)](#)
- ["Organizationally-specific TLVs for MED devices" \(page 282\)](#)

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 5500 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.

Organizationally-specific TLVs for MED devices

The optional organizationally-specific TLVs for use by Media Endpoint Devices (MED) and MED network connectivity devices are:

- **Capabilities TLV** enables a network element to advertise the LLDP-MED TLVs it is capable of supporting.
- **Network Policy Discovery TLV** is a fixed length TLV that enables both network connectivity devices and endpoints to advertise VLAN type, VLAN identifier (VID), and Layer 2 and Layer 3 priorities associated with a specific set of applications on a port. In addition, an LLDP-MED endpoint advertises this TLV for supported application types to enable the discovery of specific policy information and the diagnosis of network policy configuration mismatch issues.

- **Location Identification TLV** allows network connectivity devices to advertise the appropriate location identifier information for an endpoint to use in the context of location-based applications. The Location Identification Discovery extension enables the advertisement of location identifier information to Communication Endpoint Devices (Class III), based on the configuration of the Network Connectivity Device to which it is connected. This is expected to be related to wiremap or similar network topology data, such that the configuration of the Network Connectivity Device can uniquely identify the physical location of the connected MED Endpoint, and hence the correct location identifier information for it to use.
- **Extended Power-via-MDI TLV** enables advanced power management between an LLDP-MED endpoint and network connectivity devices. The Extended Power-via-MDI TLV enables the advertisement of fine grained power requirement details, endpoint power priority, and power status for both endpoint and network connectivity devices.
- **Inventory TLVs** are important in managed VoIP networks. Administrative tasks in these networks are made easier by access to inventory information about VoIP entities. The LLDP Inventory TLVs consist of the following:
 - **LLDP-MED Hardware Revision TLV** allows the device to advertise its hardware revision.
 - **LLDP-MED Firmware Revision TLV** allows the device to advertise its firmware revision.
 - **LLDP-MED Software Revision TLV** allows the device to advertise its software revision.
 - **LLDP-MED Serial Number TLV** allows the device to advertise its serial number.
 - **LLDP-MED Manufacturer Name TLV** allows the device to advertise the name of its manufacturer.
 - **LLDP-MED Model Name TLV** allows the device to advertise its model name
 - **LLDP-MED Asset ID TLV** allows the device to advertise its asset ID

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 279). This section covers the following commands:

- "[lldp command](#)" (page 285)
- "[lldp port command](#)" (page 285)
- "[lldp tx-tlv command](#)" (page 286)
- "[lldp tx-tlv dot1 command](#)" (page 286)
- "[lldp tx-tlv dot3 command](#)" (page 287)
- "[lldp tx-tlv med command](#)" (page 287)
- "[lldp location-identification coordinate-base command](#)" (page 288)
- "[lldp location-identification civic-address command](#)" (page 289)
- "[show lldp command](#)" (page 295)
- "[default lldp command](#)" (page 290)
- "[default lldp port command](#)" (page 291)
- "[default lldp tx-tlv command](#)" (page 292)
- "[default lldp tx-tlv dot1 command](#)" (page 292)
- "[default lldp tx-tlv dot3 command](#)" (page 293)
- "[default lldp tx-tlv med command](#)" (page 293)
- "[no lldp port command](#)" (page 294)
- "[no lldp tx-tlv command](#)" (page 294)
- "[no lldp tx-tlv dot1 command](#)" (page 294)
- "[no lldp tx-tlv dot3 command](#)" (page 295)
- "[no lldp tx-tlv med command](#)" (page 295)

- ["show lldp port command"](#) (page 297)
- ["LLDP configuration example"](#) (page 298)

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>] [med-fast-start <1-10>]
```

The `lldp` command is in the config command mode.

["lldp command parameters and variables"](#) (page 285) describes the parameters and variables for the `lldp` command.

lldp command parameters and variables

Parameters and variables	Description
tx-interval <5-32768>	sets the interval between successive transmission cycles
tx-hold-multiplier <2-10>	sets the multiplier for the tx-interval used to compute the Time To Live value for the TTL TLV
reinit-delay <1-10>	sets the delay for the reinitialization attempt if the adminStatus is disabled
tx-delay <1-8192>	sets the minimum delay between successive LLDP frame transmissions
notification-interval <5-3600>	sets the interval between successive transmissions of LLDP notifications
med-fast-start <1-10>	sets the MED Fast Start repeat count value

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}]
```

The `lldp port` command is in the config-if command mode.

["lldp port command parameters and variables"](#) (page 286) describes the parameters and variables for the `lldp port` command.

lldp port command parameters and variables

Parameters and variables	Description
port <portlist>	specifies the ports affected by the command
config notification	enables notification when new neighbor information is stored or when existing information is removed
status {rxOnly txAndRx txOnly}	sets the LLDPDU transmit and receive status on the ports 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]
```

The `lldp tx-tlv` command is in the config-if command mode.

"[lldp tx-tlv command parameters and variables](#)" (page 286) describes the parameters and variables for the `lldp tx-tlv` command.

lldp tx-tlv command parameters and variables

Parameters and variables	Description
port <portlist>	specifies the ports affected by the command
port-desc	port description TLV
sys-name	system name TLV
sys-desc	system description TLV
sys-cap	system capabilities TLV
local-mgmt-addr	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 config-if command mode.

"[lldp tx-tlv dot1 command parameters and variables](#)" (page 287) 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>	specifies the ports affected by the command
port-vlan-id	Port VLAN ID TLV
vlan-name	VLAN Name TLV
port-protocol-vlan-id	Port and Protocol VLAN ID TLV
protocol-identity [EAP] [LLDP] [STP]	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]
```

The `lldp tx-tlv dot3` command is in the config-if command mode.

"[lldp tx-tlv dot3 command parameters and variables](#)" (page 287) 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>	specifies the ports affected by the command
mac-phy-config-status	MAC/Phy Configuration/Status TLV
mdi-power-support	Power Via MDI TLV
link-aggregation	Link Aggregation TLV
maximum-frame-size	Maximum Frame Size TLV

lldp tx-tlv med command

The `lldp tx-tlv med` command sets the optional organizationally-specific TLVs for use by MED devices to be included in the transmitted LLDPDUs. The syntax for the `lldp tx-tlv med` command is:

```
lldp tx-tlv [port <portlist>] med [med-capabilities]
[extendedPSE] [inventory] [location] [network-policy]
```

The `lldp tx-tlv med` command is in the config-if command mode.

"[lldp tx-tlv med command parameters and variables](#)" (page 288) describes the parameters and variables for the `lldp tx-tlv med` command.

lldp tx-tlv med command parameters and variables

Parameters and variables	Description
port <portlist>	specifies the ports affected by the command
med-capabilities	MED Capabilities TLV (MED TLVs are transmitted only if MED Capabilities TLVs are transmitted)
extendedPSE	Extended PSE TLV
inventory	Inventory TLVs
location	Location Identification TLV
network-policy	Network Policy TLV

lldp location-identification coordinate-base command

The `lldp location-identification coordinate-base` command sets the coordinate-base parameters for LLDP location identification information. The syntax for the `lldp location-identification coordinate-base` command is:

```
lldp location-identification coordinate-base [latitude]
[longitude] [altitude] [datum]
```

The `lldp location-identification coordinate-base` command is in the config-if command mode.

"[lldp location-identification coordinate-base command parameters](#)" (page 288) describes the parameters and variables for the `lldp location-identification coordinate-base` command.

lldp location-identification coordinate-base command parameters

Field	Description
altitude [+ -] [0-4194303.fraction] [meters floors]	Altitude, in meters or floors.

Field	Description
datum [NAD83/MLLW NAD83/NAVD88 WGS84]	Reference datum The valid options are: <ul style="list-style-type: none"> • NAD83/MLLW: North American Datum 1983, Mean Lower Low Water • NAD83/NAVD88: North American Datum 1983, North American Vertical Datum of 1988 • WGS84: World Geodesic System 1984, Prime Meridian Name: Greenwich
latitude [0-90.00] [NORTH SOUTH]	Latitude in degrees, and relative to the equator.
longitude [0-180.00] [EAST WEST]	Longitude in degrees, and relative to the prime meridian.

lldp location-identification civic-address command

The `lldp location-identification civic-address` command sets the LLDP civic address parameters. The syntax for the `lldp location-identification civic-address` command is:

```
lldp location-identification civic-address country-code
[additional-code] [additional-information] [apartment]
[block] [building] [city] [city-district ] [county]
[floor] [house-number] [house-number-suffix] [landmark]
[leading-street-direction] [name] [p.o.box] [place-type]
[postal-community-name] [postal/zip-code] [room-number]
[state] [street] [street-suffix] [trailing-street-suffix]
```

The `location-identification civic-address` command is in the `config-if` command mode.

"[lldp location-identification civic-address parameters](#)" (page 289) describes the parameters and variables for the `lldp location-identification civic-address` command.

lldp location-identification civic-address parameters

Field	Description
additional-code	Additional code
additional-information	Additional location information
apartment	Unit (apartment, suite)
block	Neighborhood, block
building	Building (structure)
city	City, township, shi (JP)

Field	Description
city-district	City division, city district, ward
country-code	Country code value (2 capital letters)
county	County, parish, gun (JP), district (IN)
floor	Floor
house-number	House number
house-number-suffix	House number suffix
landmark	Landmark or vanity address
leading-street-direction	Leading street direction
name	Residence and office occupant
p.o.box	Post office box
place-type	Office
postal-community-name	Postal community name
postal/zip-code	Postal/Zip code
room-number	Room number
state	National subdivisions (state, canton, region)
street	Street
street-suffix	Street suffix
trailing-street-suffix	Trailing street suffix

lldp location-identification ecs-elin command

The `lldp location-identification ecs-elin` command sets the LLDP emergency call service - emergency location identification number (ECS-ELIN). The syntax for the `lldp location-identification ecs-elin` command is:

```
lldp location-identification ecs-elin <ecs-elin>
```

where `<ecs-elin>` specifies a 10 to 25 digit numerical string.

The `lldp location-identification ecs-elin` command is in the config-if command mode.

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]
[med-fast-start]
```

If no parameters are specified, the `default lldp` sets all parameters to their default parameters.

The `default lldp` command is in the config command mode.

"[default lldp command parameters and variables](#)" (page 291) describes the parameters and variables for the `default lldp` command.

default lldp command parameters and variables

Parameters and variables	Description
tx-interval	sets the retransmit interval to the default value (30)
tx-hold-multiplier	sets the transmission multiplier to the default value (4)
reinit-delay	sets the reinitialize delay to the default value (2)
tx-delay	sets the transmission delay to the default value (2)
notification-interval	sets the notification interval to the default value (5)
med-fast-start	sets the MED Fast Start repeat count value to the default value (4)

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]
```

The `default lldp port` command is in the config-if command mode.

"[default lldp port command parameters and variables](#)" (page 291) describes the parameters and variables for the `default lldp port` command.

default lldp port command parameters and variables

Parameters and variables	Description
port <portlist>	specifies the ports affected by the command
config notification	sets the config notification to its default value (disabled)
status	sets 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]
```

The `default lldp tx-tlv` command is in the config-if command mode.

"[default lldp tx-tlv command parameters and variables](#)" (page 292) 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>	specifies the ports affected by the command
port-desc	Port description TLV (default value is false: not included)
sys-name	System name TLV (default value is false: not included)
sys-desc	System description TLV (default value is false: not included)
sys-cap	System capabilities TLV (default value is false: not included)
local-mgmt-addr	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] ]
```

The `default lldp tx-tlv dot1` command is in the config-if command mode.

"[default lldp tx-tlv dot1 command parameters and variables](#)" (page 293) 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>	specifies the ports affected by the command
port-vlan-id	Port VLAN ID TLV (default value is false: not included)
vlan-name	VLAN Name TLV (default value is none)
port-protocol-vlan-id	Port and Protocol VLAN ID TLV (default value is none)
protocol-identity [EAP] [LLDP] [STP]	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]
```

The `default lldp tx-tlv dot3` command is in the config-if command mode.

"[default lldp tx-tlv dot3 command parameters and variables](#)" (page 293) 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>	specifies the ports affected by the command
mac-phy-config-status	MAC/Phy Configuration/Status TLV (default value is false: not included)
mdi-power-support	Power Via MDI TLV (default value is false: not included)
link-aggregation	Link Aggregation TLV (default value is false: not included)
maximum-frame-size	Maximum Frame Size TLV (default value is false: not included)

default lldp tx-tlv med command

The `default lldp tx-tlv med` command sets the optional organizationally-specific TLVs for MED devices to their default values. The syntax for the `default lldp tx-tlv med` command is:

```
default lldp tx-tlv [port <portlist>] med [med-capabilities]
[extendedPSE] [inventory] [location] [network-policy]
```

The `default lldp tx-tlv med` command is in the config-if command mode.

"[default lldp tx-tlv med command parameters and variables](#)" (page 294) describes the parameters and variables for the `default lldp tx-tlv med` command.

default lldp tx-tlv med command parameters and variables

Parameters and variables	Description
port <portlist>	specifies the ports affected by the command
med-capabilities	MED Capabilities TLV (default value is false: not included)
extendedPSE	Extended PSE TLV (default value is false: not included)
inventory	Inventory TLVs (default value is false: not included)
location	Location Identification TLV (default value is false: not included)
network-policy	Network Policy 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]
```

The `no lldp port` command is in the config-if 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]
```

The `no lldp tx-tlv` command is in the config-if 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] ]
```

The `no lldp tx-tlv dot1` command is in the config-if 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]
```

The `no lldp tx-tlv dot3` command is in the config-if command mode.

no lldp tx-tlv med command

The `no lldp tx-tlv med` command specifies the optional Management TLVs not to include in the transmitted LLDPDUs. The syntax for the `no lldp tx-tlv med` command is:

```
no lldp tx-tlv [port <portlist>] med [med-capabilities]
[extendedPSE] [inventory] [location] [network-policy]
```

The `no lldp tx-tlv med` command is in the config-if 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 | med | detail}]
[mgmt-sys-data]
[rx-stats] [tx-stats] [stats] [pdu-tlv-size]
[tx-tlv {dot1 | dot3 | med }]
[neighbor { dot1 [vlan-names | protocol-id] } | [dot3]
| { med [capabilities] [network-policy] [location]
[extended-power] [inventory] } | [detail] ]
[neighbor-mgmt-addr]
```

The `show lldp` command is in the 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 med detail}	<p>Displays 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 med: displays the MED 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	Displays the local management system data.
rx-stats	Displays the LLDP receive statistics for the local system.
tx-stats	Displays the LLDP transmit statistics for the local system.
stats	Displays the LLDP table statistics for the remote system.
pdu-tlv-size	Displays the different TLV sizes and the number of TLVs in an LLDPDU.
tx-tlv {dot1 dot3 med }	<p>Displays 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 med: displays status for MED 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] { med [capabilities] [network-policy] [location] [extended-power] [inventory] } [detail]	<p>Displays 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 med: displays MED TLVs: <ul style="list-style-type: none"> — capabilities: Capabilities TLV

Parameters and variables	Description
	<ul style="list-style-type: none"> — network-policy: Network Policy Discovery TLV — location: Location Identification TLV — extended-power: Extended Power-via-MDI TLV — inventory: Inventory TLVs • detail: displays all TLVs
[neighbor-mgmt-addr]	Displays 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 | med}]
[neighbor {dot1 [vlan-names | protocol-id] } | [dot3] |
{med [capabilities] [network-policy] [location]
[extended-power] [inventory]} | [detail] ]}
[neighbor-mgmt-addr]
```

The `show lldp port` command is in the exec command mode.

show lldp port command parameters

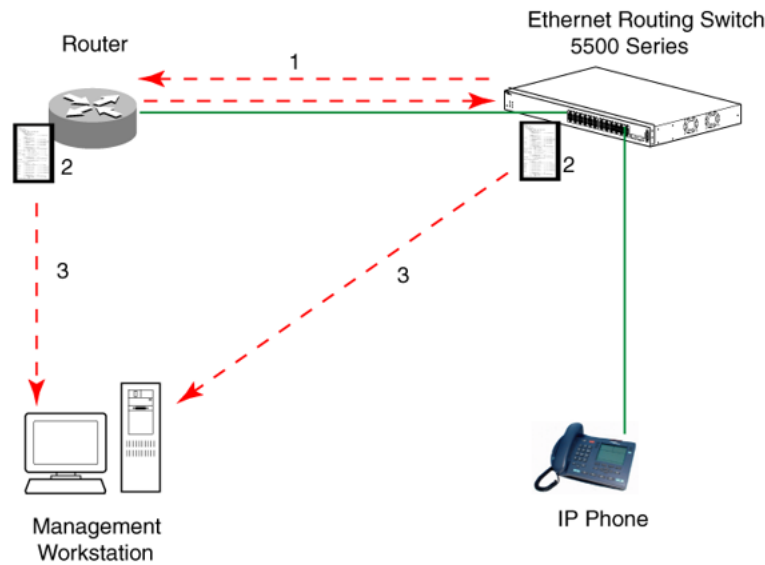
Parameters and variables	Description
rx-stats	Displays the LLDP receive statistics for the local port.
tx-stats	Displays the LLDP transmit statistics for the local port.
pdu-tlv-size	Displays the different TLV sizes and the number of TLVs in an LLDPDU.
tx-tlv {dot1 dot3 med }	<p>Displays which TLVs are 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 • med: displays status for MED TLVs <p>To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.</p>

Parameters and variables	Description
<pre>neighbor { dot1 [vlan-names protocol-id] } [dot3] { med [capabilities] [network-policy] [location] [extended-power] [inventory] } [detail]</pre>	<p>Displays 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 • med: displays MED TLVs: <ul style="list-style-type: none"> — capabilities: Capabilities TLV — network-policy: Network Policy Discovery TLV — location: Location Identification TLV — extended-power: Extended Power-via-MDI TLV — inventory: Inventory TLVs • detail: displays all TLVs.
[neighbor-mgmt-addr]	Displays 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 (LLDPDU are sent at 30 seconds). With the default settings, only the mandatory TLVs are sent, but the switch can receive any LLDP Core, DOT1, DOT3 or MED TLV from its peers.

["LLDP configuration example" \(page 299\)](#)

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. Notice 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 Configure the location information for the LLDP-MED Location Identification TLV.
There are three coordinate sets available for location advertisement.
- 16 Enable the LLDP-MED Capabilities TLV for transmission. (indicates the supported LLDP-MED TLVs and the LLDP-MED device type of the LLDP sending device)
MED TLVs are transmitted only if MED-Capabilities TLV is transmitted
- 17 Enable the Network Policy TLV for transmission. (advertises the available MED applications available on the LLDP sending device and the policies required to use the applications)
- 18 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)
- 19 Enable the Extended Power-via-MDI TLV for transmission. (provides detailed informations regarding the PoE parameters of the LLDP sending device)
- 20 Enable the Inventory – Hardware Revision TLV for transmission. (indicates the hardware revision of the LLDP sending device)

- 21 Enable the Inventory – Firmware Revision TLV for transmission. (indicates the firmware revision of the LLDP sending device)
- 22 Enable the Inventory – Software Revision TLV for transmission. (indicates the software revision of the LLDP sending device)
- 23 Enable the Inventory – Serial Number TLV for transmission. (indicates the serial number of the LLDP sending device)
- 24 Enable the Inventory – Manufacturer Name TLV for transmission. (indicates the manufacturer name of the LLDP sending device)
- 25 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 299)

Modifying the default LLDP Tx interval Enter configuration commands, one for each line. End with CNTL/Z.

```
5520-24T-PWR>enable
5520-24T-PWR#configure terminal
5520-24T-PWR(config)#lldp tx-interval 60
```

Checking the new LLDP global settings

```
5520-24T-PWR(config)#show lldp
```

```
-----
TxInterval:60
TxHoldMultiplier:4
RxInitDelay:2
TxDelay:2
NotificationInterval:5
MedFastStartRepeatCount:4
```

Enabling all LLDP Core TLVs for transmission on the router and IP Phone ports

```
5520-24T-PWR(config)#interface fastEthernet 1,13
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 port-desc
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 sys-name
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 sys-desc
```

```
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 sys-cap
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 local-mgmt-addr
```

Checking the LLDP settings of the router and IP Phone ports

```
5520-24T-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

```
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 dot1
port-vlan-id
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 dot1
port-protocol-vlan-id
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 dot1 vlan-name
5520-24T-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

```
5520-24T-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

```
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 dot3
mac-phy-config-status
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 dot3
mdi-power-support
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 dot3
link-aggregation
```

```
5520-24T-PWR(config-if)#lldp tx-tlv port 1,13 dot3
maximum-frame-size
```

Checking the LLDP settings of the router and IP Phone ports

```
5520-24T-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
-----
```

Enabling all LLDP MED TLVs for transmission on the router and IP Phone ports The first three commands are required to configure the location identification for the LLDP-MED Location Identification TLV.

```
5530-24TFD(config-if)#lldp location-identification
civic-address country-code US city Boston
5530-24TFD(config-if)#lldp location-identification
coordinate-base altitude 3 floors
5530-24TFD(config-if)#lldp location-identification ecs-elin
1234567890
5530-24TFD(config-if)#lldp tx-tlv med port 1,13 med-
capabilities
5530-24TFD(config-if)#lldp tx-tlv med port 1,13 network-
policy
5530-24TFD(config-if)#lldp tx-tlv med port 1,13 location
5530-24TFD(config-if)#lldp tx-tlv med port 1,13 extendedPSE
5530-24TFD(config-if)#lldp tx-tlv med port 1,13 inventory
```

Checking the new LLDP settings of the router and IP Phone ports

```
5530-24TFD(config-if)#show lldp tx-tlv med
```

```
-----
lldp port med tlvs
-----
```

```
-----
Port   Med      Network   Location   Extended
Inventory Capabilities Policy      PSE
-----
```

```
1      true     true     true     true     true
13     true     true     true     true     true
-----
```

Configuring LLDP using Device Manager

The following sections contain instructions for configuring and viewing LLDP information using Device Manager:

- "Viewing and configuring LLDP global and transmit properties" (page 304)
- "LLDP_Port_dot1 dialog box" (page 331)
- "LLDP_Port_dot_3 dialog box" (page 342)
- "LLDP_Port_med dialog box" (page 354)

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 304)
- "Port tab" (page 308)
- "TX Stats tab" (page 311)
- "Graphing LLDP transmit statistics" (page 312)
- "RX Stats tab" (page 313)
- "Graphing LLDP receive statistics" (page 315)
- "Local System tab" (page 316)
- "Local Port tab" (page 320)
- "Local Management tab" (page 322)
- "Neighbor tab" (page 323)
- "Neighbor Mgmt Address tab" (page 326)
- "Unknown TLV tab" (page 327)
- "Organizational Defined Info tab" (page 329)

Globals tab

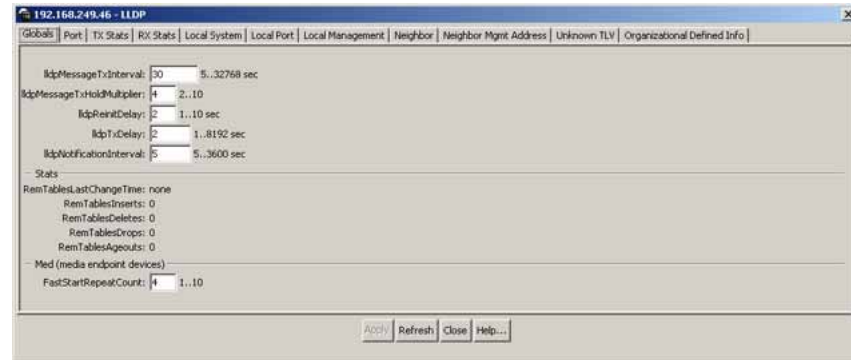
With the **Globals** tab, you can configure LLDP transmit properties and view remote table statistics.

Use the following procedure to open the Globals tab:

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 305)). |
|---|---|

LLDP Globals tab



"LLDP Globals tab fields" (page 305) 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 in

Field	Description
	IldpStatsRemTablesDeletes, because the deletion is only a partial deletion. If the failure is the result of a lack of resources, the IldpStatsRemTablesDrops counter is incremented once.
RemTablesDeletes	The number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in IldpRemoteSystemsData and IldpExtensions 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.
RemTablesDrops	The number of times the complete set of information advertised by a particular MSAP can not be entered into tables contained in IldpRemoteSystemsData and IldpExtensions objects because of insufficient resources.
RemTablesAgeouts	The number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in IldpRemoteSystemsData and IldpExtensions 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.
FastStartRepeatCount	The number of times the fast start LLDPDU is sent during the activation of the fast start mechanism defined by LLDP-MED.

—End—

See also:

- "Port tab" (page 308)

- "TX Stats tab" (page 311)
- "Graphing LLDP transmit statistics" (page 312)
- "RX Stats tab" (page 313)
- "Graphing LLDP receive statistics" (page 315)
- "Local System tab" (page 316)
- "Local Port tab" (page 320)
- "Local Management tab" (page 322)
- "Neighbor tab" (page 323)
- "Neighbor Mgmt Address tab" (page 326)
- "Unknown TLV tab" (page 327)
- "Organizational Defined Info tab" (page 329)

Port tab

With the Port tab, you can set the optional TLVs to include in the LLPDUs transmitted by each port.

Use the following procedure to open the Port tab:

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

PortNum	AdminStatus	NotificationEnable	TLVstxEnable	MvntxEnable(dot1)	TLVstxEnable(dot3)	CapSupported(med)	TLVstxEnable(med)	NotifyEnable(med)
1/1	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/2	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/3	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/4	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/5	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/6	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/7	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/8	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/9	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/10	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/11	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/12	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/13	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/14	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/15	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/16	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/17	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/18	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/19	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/20	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/21	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/22	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/23	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/24	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/25	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false
1/26	txAndRx	false	false			capabilities, networkPolicy, location, inventory		false

"Port tab fields" (page 309) 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, for each port, 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>
VLANTxEnable(dot1)	<p>Specifies whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is included in the transmitted LLDPDUs.</p>

Field	Description
TLVsTxEnable(dot3)	<p>Sets the optional IEEE 802.3 organizationally defined TLVs to be included in the transmitted LLDPDUs:</p> <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.
CapSupported(med)	Identifies which MED system capabilities are supported on the local system.
TLVsTxEnable(med)	<p>Sets the optional organizationally defined TLVs for MED devices to include in the transmitted LLDPDUs:</p> <ul style="list-style-type: none"> • capabilities: Capabilities TLVs • networkPolicy: Network Policy TLVs • location: Emergency Communications System Location TLVs • extendedPSE: Extended PoE TLVs with PSE capabilities • inventory: Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Model Name, and Asset ID TLVs.
NotifyEnable(med)	A value of true enables sending the topology change traps on this port. A value of false disables sending the topology change traps on this port.

—End—

See also:

- ["Globals tab" \(page 304\)](#)
- ["TX Stats tab" \(page 311\)](#)
- ["Graphing LLDP transmit statistics" \(page 312\)](#)
- ["RX Stats tab" \(page 313\)](#)
- ["Graphing LLDP receive statistics" \(page 315\)](#)

- "Local System tab" (page 316)
- "Local Port tab" (page 320)
- "Local Management tab" (page 322)
- "Neighbor tab" (page 323)
- "Neighbor Mgmt Address tab" (page 326)
- "Unknown TLV tab" (page 327)
- "Organizational Defined Info tab" (page 329)

TX Stats tab

With the TX Stats tab, you can view LLDP transmit statistics by port.

Use the following procedure to open the TX Stats tab:

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 311)).

TX Stats tab



"TX Stats tab fields" (page 311) 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 304)
- "Port tab" (page 308)

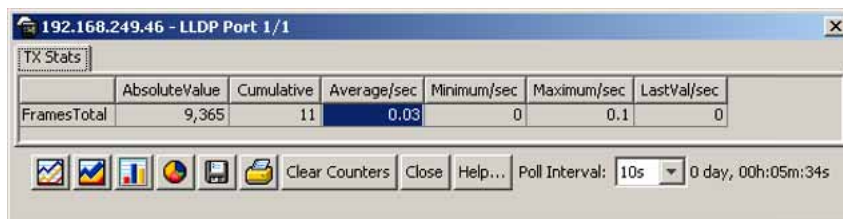
- "Graphing LLDP transmit statistics" (page 312)
- "RX Stats tab" (page 313)
- "Graphing LLDP receive statistics" (page 315)
- "Local System tab" (page 316)
- "Local Port tab" (page 320)
- "Local Management tab" (page 322)
- "Neighbor tab" (page 323)
- "Neighbor Mgmt Address tab" (page 326)
- "Unknown TLV tab" (page 327)
- "Organizational Defined Info tab" (page 329)

Graphing LLDP transmit statistics

Use the following procedure to graph LLDP transmit statistics:

Step Action

- 1 From the **TX Stats** tab "TX Stats tab" (page 311)), select the port for which you want to display statistics.
- 2 Click **Graph**.
The TX Stats - Graph dialog box appears.



- 3 Highlight a data column to graph.
- 4 Click one of the graph buttons.

—End—

See also:

- "Globals tab" (page 304)
- "Port tab" (page 308)
- "TX Stats tab" (page 311)

- "RX Stats tab" (page 313)
- "Graphing LLDP receive statistics" (page 315)
- "Local System tab" (page 316)
- "Local Port tab" (page 320)
- "Local Management tab" (page 322)
- "Neighbor tab" (page 323)
- "Neighbor Mgmt Address tab" (page 326)
- "Unknown TLV tab" (page 327)
- "Organizational Defined Info tab" (page 329)

RX Stats tab

With the RX Stats tab, you can view LLDP receive statistics by port.

Use the following procedure to open the RX Stats tab:

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 RX Stats tab. The RX Stats tab appears ("RX Stats tab" (page 313)).

RX Stats tab

PortNum	FramesDiscardedTotal	FramesErrors	FramesTotal	TLVsDiscardedTotal	TLVsRecognizedTotal	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

"RX Stats tab fields" (page 313) describes the RX Stats tab fields.

RX Stats tab fields

Field	Description
PortNum	Port number.

Field	Description
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.
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 IldpRemoteSystemsData and IldpExtensions objects because the information timeliness interval has expired." This counter is similar to IldpStatsRemTablesAgeouts, except that it is on a for each-port basis. This enables NMS to poll tables associated with the IldpRemoteSystemsData 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 rxOnly, txOnly or txAndRx, the counter associated with the same port is reset to 0. The agent also flushes all remote system information

Field	Description
	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" \(page 304\)](#)
- ["Port tab" \(page 308\)](#)
- ["TX Stats tab" \(page 311\)](#)
- ["Graphing LLDP transmit statistics" \(page 312\)](#)
- ["Graphing LLDP receive statistics" \(page 315\)](#)
- ["Local System tab" \(page 316\)](#)
- ["Local Port tab" \(page 320\)](#)
- ["Local Management tab" \(page 322\)](#)
- ["Neighbor tab" \(page 323\)](#)
- ["Neighbor Mgmt Address tab" \(page 326\)](#)
- ["Unknown TLV tab" \(page 327\)](#)
- ["Organizational Defined Info tab" \(page 329\)](#)

Graphing LLDP receive statistics

Use the following procedure to graph LLDP receive statistics:

Step	Action
1	From the RX Stats tab " RX Stats tab" (page 313) , select the port for which you want to display statistics.
2	Click Graph . The RX Stats - Graph dialog box appears.

	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

- 3 Highlight a data column to graph.
- 4 Click one of the graph buttons.

—End—

See also:

- "Globals tab" (page 304)
- "Port tab" (page 308)
- "TX Stats tab" (page 311)
- "Graphing LLDP transmit statistics" (page 312)
- "RX Stats tab" (page 313)
- "Local System tab" (page 316)
- "Local Port tab" (page 320)
- "Local Management tab" (page 322)
- "Neighbor tab" (page 323)
- "Neighbor Mgmt Address tab" (page 326)
- "Unknown TLV tab" (page 327)
- "Organizational Defined Info tab" (page 329)

Local System tab

With the Local System tab, you can view LLDP properties for the local system.

Use the following procedure to open the Local System tab:

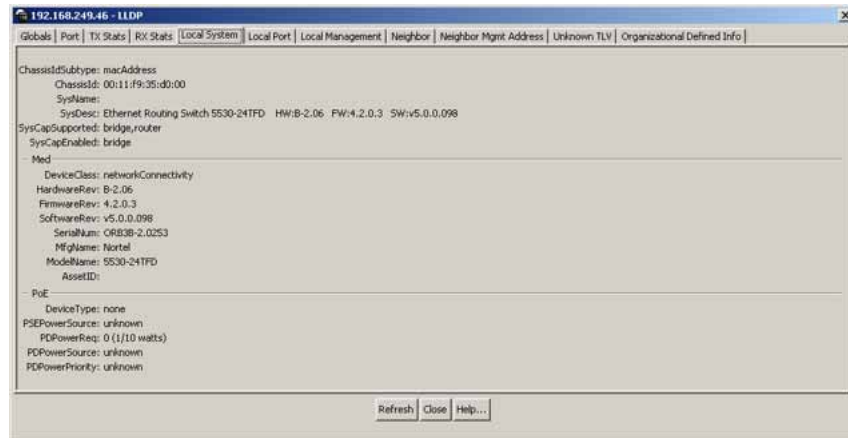
Step Action

- 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 317)).

Local System tab



"Local System tab fields" (page 317) 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	chassis ID
SysName	local system name
SysDesc	local system description
SysCapSupported	identifies the system capabilities supported on the local system
SysCapEnabled	identifies the system capabilities that are enabled on the local system
DeviceClass	local MED device class

Field	Description
HardwareRev	the vendor-specific hardware revision string as advertised by the local device
FirmwareRev	the vendor-specific firmware revision string as advertised by the local device
SoftwareRev	the vendor-specific software revision string as advertised by the local device
SerialNum	the vendor-specific serial number as advertised by the local device
MfgName	the vendor-specific manufacturer name as advertised by the local device
ModelName	the vendor-specific model name as advertised by the local device
AssetID	the vendor-specific asset tracking identifier as advertised by the local device
DeviceType	<p>defines the type of Power-via-MDI (Power over Ethernet) advertised by the local device:</p> <ul style="list-style-type: none"> • pseDevice: indicates that the device is advertised as a Power Sourcing Entity (PSE). • pdDevice: indicates that the device is advertised as a Powered Device (PD) • none: indicates that the device does not support PoE
PSEPowerSource	<p>defines the type of PSE Power Source advertised by the local device:</p> <ul style="list-style-type: none"> • primary: indicates that the device advertises its power source as primary • backup: indicates that the device advertises its power source as backup
PDPowerReq	specifies the value of the power required (in units of 0.1 watts) by a Powered Device (PD)

Field	Description
PDPowerSource	<p>defines the type of power source advertised as in use by the local device:</p> <ul style="list-style-type: none"> • fromPSE: indicates that the device advertises its power source as received from a PSE • local: indicates that the device advertises its power source as local • localAndPSE: indicates that the device advertises its power source as using both local and PSE power
PDPowerPriority	<p>defines the priority advertised as required by this PD:</p> <ul style="list-style-type: none"> • critical: indicates that the device advertises its power priority as critical, see RFC 3621 • high: indicates that the device advertises its power priority as high, see RFC 3621 • low: indicates that the device advertises its power priority as low, see RFC 3621

—End—

See also:

- ["Globals tab" \(page 304\)](#)
- ["Port tab" \(page 308\)](#)
- ["TX Stats tab" \(page 311\)](#)
- ["Graphing LLDP transmit statistics" \(page 312\)](#)
- ["RX Stats tab" \(page 313\)](#)
- ["Graphing LLDP receive statistics" \(page 315\)](#)
- ["Local Port tab" \(page 320\)](#)
- ["Local Management tab" \(page 322\)](#)
- ["Neighbor tab" \(page 323\)](#)
- ["Neighbor Mgmt Address tab" \(page 326\)](#)
- ["Unknown TLV tab" \(page 327\)](#)

- "Organizational Defined Info tab" (page 329)

Local Port tab

With the Local Port tab, you can view LLDP port properties for the local system.

Use the following procedure to open the Local Port tab:

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 320)). |

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 320) 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" \(page 304\)](#)
- ["Port tab" \(page 308\)](#)
- ["TX Stats tab" \(page 311\)](#)
- ["Graphing LLDP transmit statistics" \(page 312\)](#)
- ["RX Stats tab" \(page 313\)](#)
- ["Graphing LLDP receive statistics" \(page 315\)](#)
- ["Local System tab" \(page 316\)](#)
- ["Local Management tab" \(page 322\)](#)
- ["Neighbor tab" \(page 323\)](#)
- ["Neighbor Mgmt Address tab" \(page 326\)](#)
- ["Unknown TLV tab" \(page 327\)](#)
- ["Organizational Defined Info tab" \(page 329\)](#)

Local Management tab

With the Local Management tab, you can view LLDP management properties for the local system.

Use the following procedure to open the Local Management tab:

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 **Local Management** tab.
The Local Management tab appears ("[Local Management tab](#)" ([page 322](#))).

Local Management tab



"[Local Management tab fields](#)" ([page 322](#)) 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" \(page 304\)](#)
- ["Port tab" \(page 308\)](#)
- ["TX Stats tab" \(page 311\)](#)
- ["Graphing LLDP transmit statistics" \(page 312\)](#)
- ["RX Stats tab" \(page 313\)](#)
- ["Graphing LLDP receive statistics" \(page 315\)](#)
- ["Local System tab" \(page 316\)](#)
- ["Local Port tab" \(page 320\)](#)
- ["Neighbor tab" \(page 323\)](#)
- ["Neighbor Mgmt Address tab" \(page 326\)](#)
- ["Unknown TLV tab" \(page 327\)](#)
- ["Organizational Defined Info tab" \(page 329\)](#)

Neighbor tab

With the Neighbor tab, you can view LLDP properties for the remote system.

Use the following procedure to open the Neighbor tab:

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 324)).

Neighbor tab



"[Neighbor tab fields](#)" (page 324) 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" \(page 304\)](#)
- ["Port tab" \(page 308\)](#)
- ["TX Stats tab" \(page 311\)](#)
- ["Graphing LLDP transmit statistics" \(page 312\)](#)
- ["RX Stats tab" \(page 313\)](#)
- ["Graphing LLDP receive statistics" \(page 315\)](#)
- ["Local System tab" \(page 316\)](#)
- ["Local Port tab" \(page 320\)](#)
- ["Local Management tab" \(page 322\)](#)
- ["Neighbor Mgmt Address tab" \(page 326\)](#)
- ["Unknown TLV tab" \(page 327\)](#)
- ["Organizational Defined Info tab" \(page 329\)](#)

Neighbor Mgmt Address tab

With the Neighbor Mgmt Address tab, you can view LLDP management properties for the remote system.

Use the following procedure to open the Neighbor Mgmt Address tab:

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 326)).

Neighbor Mgmt Address tab



"[Neighbor Mgmt Address tab fields](#)" (page 326) describes the Neighbor Mgmt Address tab fields.

Neighbor Mgmt Address tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
AddrSubtype	The type of encoding used in the associated Addr object.
Addr	The management address associated with the remote system.

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 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" \(page 304\)](#)
- ["Port tab" \(page 308\)](#)
- ["TX Stats tab" \(page 311\)](#)
- ["Graphing LLDP transmit statistics" \(page 312\)](#)
- ["RX Stats tab" \(page 313\)](#)
- ["Graphing LLDP receive statistics" \(page 315\)](#)
- ["Local System tab" \(page 316\)](#)
- ["Local Port tab" \(page 320\)](#)
- ["Local Management tab" \(page 322\)](#)
- ["Neighbor tab" \(page 323\)](#)
- ["Unknown TLV tab" \(page 327\)](#)
- ["Organizational Defined Info tab" \(page 329\)](#)

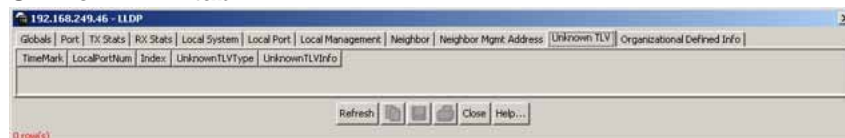
Unknown TLV tab

With the Unknown TLV tab, you can view details about unknown TLVs received on the local system.

Use the following procedure to open the Unknown TLV tab:

- | 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 Unkown TLV tab appears (" Unknown TLV tab " (page 328)). |

Unknown TLV tab



"[Unknown TLV tab fields](#)" (page 328) describes the Unkown TLV tab fields.

Unknown TLV tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
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 304)
- "[Port tab](#)" (page 308)
- "[TX Stats tab](#)" (page 311)
- "[Graphing LLDP transmit statistics](#)" (page 312)

- "RX Stats tab" (page 313)
- "Graphing LLDP receive statistics" (page 315)
- "Local System tab" (page 316)
- "Local Port tab" (page 320)
- "Local Management tab" (page 322)
- "Neighbor tab" (page 323)
- "Neighbor Mgmt Address tab" (page 326)
- "Organizational Defined Info tab" (page 329)

Organizational Defined Info tab

With the Organizational Defined Info tab, you can view Organizationally-specific properties for the remote system.

Use the following procedure to open the Organizational Defined Info tab:

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 329)).

Organizational Defined Info tab



"[Organizational Defined Info tab fields](#)" (page 329) describes the Organizational Defined Info tab fields.

Organizational Defined Info 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.
OrgDefInfoOUI	The Organizationally Unique Identifier (OUI), 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 IldpRemOrgDefInfoSubtype 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 IldpRemOrgDefInfoIndex 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 304)

- "Port tab" (page 308)
- "TX Stats tab" (page 311)
- "Graphing LLDP transmit statistics" (page 312)
- "RX Stats tab" (page 313)
- "Graphing LLDP receive statistics" (page 315)
- "Local System tab" (page 316)
- "Local Port tab" (page 320)
- "Local Management tab" (page 322)
- "Neighbor tab" (page 323)
- "Neighbor Mgmt Address tab" (page 326)
- "Unknown TLV tab" (page 327)

LLDP_Port_dot1 dialog box

You can use the **LLDP_Port_dot1** dialog box to configure and view IEEE 802.1 LLDP information. For details, refer to the following tabs:

- "Local VLAN Id tab" (page 331)
- "Local Protocol VLAN tab" (page 332)
- "Local VLAN Name tab" (page 334)
- "Local Protocol tab" (page 335)
- "Neighbor VLAN Id tab" (page 337)
- "Neighbor Protocol VLAN tab" (page 338)
- "Neighbor VLAN Name tab" (page 340)
- "Neighbor Protocol tab" (page 341)

Local VLAN Id tab

With the Local VLAN Id tab, you can view LLDP VLAN ID properties for the local system.

Use the following procedure to open the Local VLAN Id tab:

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 332)). |
|---|--|

Local VLAN Id tab

PortNum	VlanId
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 332) describes the Local VLAN Id tab fields.

Local VLAN Id tab fields

Field	Description
PortNum	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 332)
- "Local VLAN Name tab" (page 334)
- "Local Protocol tab" (page 335)
- "Neighbor VLAN Id tab" (page 337)
- "Neighbor Protocol VLAN tab" (page 338)
- "Neighbor VLAN Name tab" (page 340)
- "Neighbor Protocol tab" (page 341)

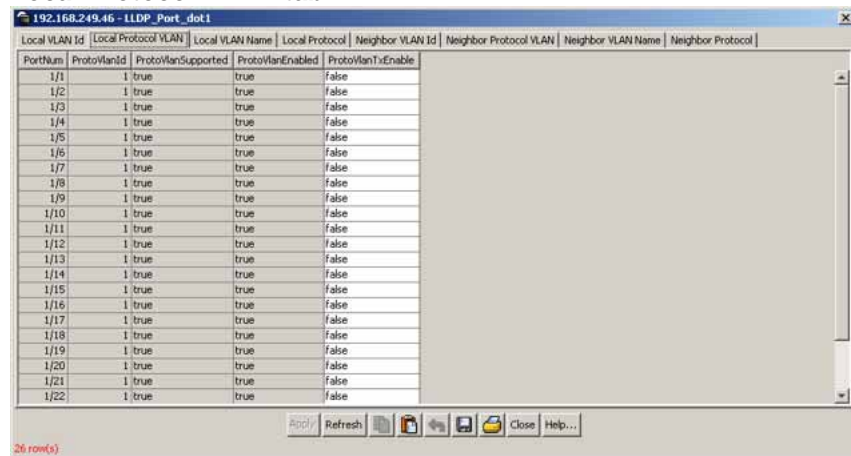
Local Protocol VLAN tab

With the Local Protocol VLAN tab, you can view LLDP Protocol VLAN properties for the local system.

Use the following procedure to open the Local Protocol VLAN tab:

- | 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 VLAN tab.
The Local Protocol VLAN tab appears (" Local Protocol VLAN tab " (page 333)). |

Local Protocol VLAN tab



"[Local Protocol VLAN tab fields](#)" (page 333) describes the Local Protocol VLAN tab fields.

Local Protocol VLAN tab fields

Field	Description
PortNum	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	Indicates whether the local port supports port and protocol VLANs.
ProtoVlanEnabled	Indicates whether the port and protocol VLANs are enabled on the local port.
ProtoVlanTxEnable	Indicates whether the corresponding local port and protocol VLAN information are transmitted from the port.

—End—

See also:

- "Local VLAN Id tab" (page 331)
- "Local VLAN Name tab" (page 334)
- "Local Protocol tab" (page 335)
- "Neighbor VLAN Id tab" (page 337)
- "Neighbor Protocol VLAN tab" (page 338)
- "Neighbor VLAN Name tab" (page 340)
- "Neighbor Protocol tab" (page 341)

Local VLAN Name tab

With the Local VLAN Name tab, you can view LLDP VLAN Name properties for the local system.

Use the following procedure to open the Local VLAN Name tab:

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 334)).

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

26 row(s)

"Local VLAN Name tab fields" (page 335) describes the Local VLAN Name tab fields.

Local VLAN Name tab fields

Field	Description
PortNum	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 331)
- "Local Protocol VLAN tab" (page 332)
- "Local Protocol tab" (page 335)
- "Neighbor VLAN Id tab" (page 337)
- "Neighbor Protocol VLAN tab" (page 338)
- "Neighbor VLAN Name tab" (page 340)
- "Neighbor Protocol tab" (page 341)

Local Protocol tab

With the **Local Protocol** tab, you can view LLDP protocol properties for the local system.

Use the following procedure to open the Local Protocol tab:

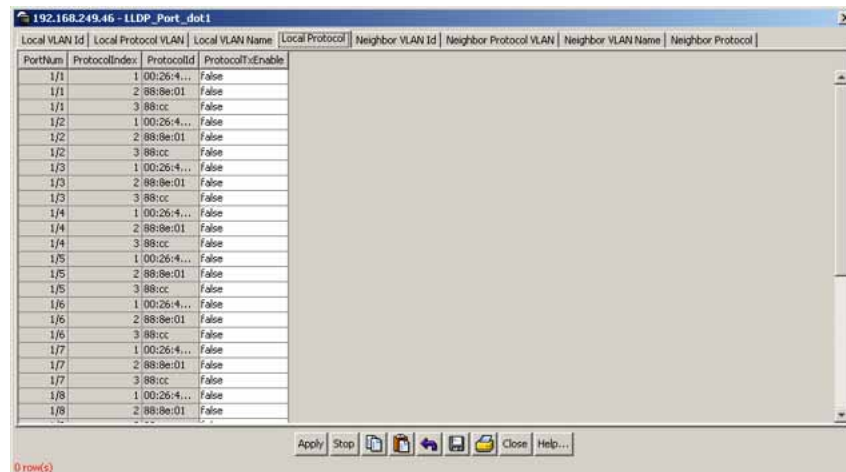
Step	Action
------	--------

- | | |
|---|--|
| 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 336)).

Local Protocol tab



"Local Protocol tab fields" (page 336) describes the Local Protocol tab fields.

Local Protocol tab fields

Field	Description
PortNum	Port number.
ProtocolIndex	An arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocolId	The octet string value used to identify the protocols associated with the given port of the local system.
ProtocolTxEnable	Indicates whether the corresponding Local System Protocol Identity instance is transmitted on the port.

—End—

See also:

- "Local VLAN Id tab" (page 331)
- "Local Protocol VLAN tab" (page 332)

- "Local VLAN Name tab" (page 334)
- "Neighbor VLAN Id tab" (page 337)
- "Neighbor Protocol VLAN tab" (page 338)
- "Neighbor VLAN Name tab" (page 340)
- "Neighbor Protocol tab" (page 341)

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 337)).

Neighbor VLAN Id tab



"[Neighbor VLAN Id tab fields](#)" (page 337) 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" \(page 331\)](#)
- ["Local Protocol VLAN tab" \(page 332\)](#)
- ["Local VLAN Name tab" \(page 334\)](#)
- ["Local Protocol tab" \(page 335\)](#)
- ["Neighbor Protocol VLAN tab" \(page 338\)](#)
- ["Neighbor VLAN Name tab" \(page 340\)](#)
- ["Neighbor Protocol tab" \(page 341\)](#)

Neighbor Protocol VLAN tab

With the Neighbor Protocol VLAN tab, you can view LLDP Protocol VLAN properties for the remote system.

Use the following procedure to open the Neighbor Protocol VLAN tab:

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" \(page 339\)](#)").

Neighbor Protocol VLAN tab

"Neighbor Protocol VLAN tab fields" (page 339) describes the Neighbor Protocol VLAN tab fields.

Neighbor Protocol VLAN tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
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	Indicates whether the remote port supports port and protocol VLANs.
ProtoVlanEnabled	Indicates whether the port and protocol VLANs are enabled on the remote port.

—End—

See also:

- "Local VLAN Id tab" (page 331)
- "Local Protocol VLAN tab" (page 332)
- "Local VLAN Name tab" (page 334)
- "Local Protocol tab" (page 335)
- "Neighbor VLAN Id tab" (page 337)
- "Neighbor VLAN Name tab" (page 340)
- "Neighbor Protocol tab" (page 341)

Neighbor VLAN Name tab

With the Neighbor VLAN Name tab, you can view LLDP VLAN Name properties for the remote system.

Use the following procedure to open the Neighbor VLAN Name tab:

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 340)).

Neighbor VLAN Name tab



"[Neighbor VLAN Name tab fields](#)" (page 340) describes the **Neighbor VLAN Name** tab fields.

Neighbor VLAN Name tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
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 331)
- "Local Protocol VLAN tab" (page 332)
- "Local VLAN Name tab" (page 334)
- "Local Protocol tab" (page 335)
- "Neighbor VLAN Id tab" (page 337)
- "Neighbor Protocol VLAN tab" (page 338)
- "Neighbor Protocol tab" (page 341)

Neighbor Protocol tab

With the Neighbor Protocol tab, you can view LLDP Protocol properties for the remote system.

Use the following procedure to open the Neighbor Protocol tab:

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 341)).

Neighbor Protocol tab

"[Neighbor Protocol tab fields](#)" (page 341) describes the Neighbor Protocol tab fields.

Neighbor Protocol 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.
ProtocolIndex	This object represents an arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocolId	Identifies the protocols associated with the remote port.

—End—

See also:

- "Local VLAN Id tab" (page 331)
- "Local Protocol VLAN tab" (page 332)
- "Local VLAN Name tab" (page 334)
- "Local Protocol tab" (page 335)
- "Neighbor VLAN Id tab" (page 337)
- "Neighbor Protocol VLAN tab" (page 338)
- "Neighbor VLAN Name tab" (page 340)

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 details, refer to the following tabs:

- "Local Port Auto-negotiation tab" (page 343)
- "Local PoE tab" (page 344)
- "Local Link Aggregate tab" (page 346)
- "Local Max Frame tab" (page 347)
- "Neighbor Port Auto-negotiation tab" (page 348)
- "Neighbor PoE tab" (page 350)
- "Neighbor Link Aggregate tab" (page 352)
- "Neighbor Max Frame tab" (page 353)

Local Port Auto-negotiation tab

With the Local Port Auto-negotiation tab, you can view LLDP auto-negotiation properties for the local system.

Use the following procedure to open the Local Port Auto-negotiation tab:

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

- 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 343)).

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 343) describes the Local Port Auto-negotiation tab fields.

Local Port Auto-negotiation tab fields

Field	Description
PortNum	Port number.
AutoNegSupported	Indicates whether the local port supports Auto-negotiation.
AutoNegEnabled	Indicates whether Auto-negotiation is enabled on the local port.
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 344)
- "Local Link Aggregate tab" (page 346)
- "Local Max Frame tab" (page 347)
- "Neighbor Port Auto-negotiation tab" (page 348)
- "Neighbor PoE tab" (page 350)
- "Neighbor Link Aggregate tab" (page 352)
- "Neighbor Max Frame tab" (page 353)

Local PoE tab

With the Local PoE tab, you can view LLDP PoE properties for the local system.

Use the following procedure to open the Local PoE tab:

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	spare	class0
1/2	pClassPSE	false	false	false	spare	class0
1/3	pClassPSE	false	false	false	spare	class0
1/4	pClassPSE	false	false	false	spare	class0
1/5	pClassPSE	false	false	false	spare	class0
1/6	pClassPSE	false	false	false	spare	class0
1/7	pClassPSE	false	false	false	spare	class0
1/8	pClassPSE	false	false	false	spare	class0
1/9	pClassPSE	false	false	false	spare	class0
1/10	pClassPSE	false	false	false	spare	class0
1/11	pClassPSE	false	false	false	spare	class0
1/12	pClassPSE	false	false	false	spare	class0
1/13	pClassPSE	false	false	false	spare	class0
1/14	pClassPSE	false	false	false	spare	class0
1/15	pClassPSE	false	false	false	spare	class0
1/16	pClassPSE	false	false	false	spare	class0
1/17	pClassPSE	false	false	false	spare	class0
1/18	pClassPSE	false	false	false	spare	class0
1/19	pClassPSE	false	false	false	spare	class0
1/20	pClassPSE	false	false	false	spare	class0
1/21	pClassPSE	false	false	false	spare	class0
1/22	pClassPSE	false	false	false	spare	class0
1/23	pClassPSE	false	false	false	spare	class0
1/24	pClassPSE	false	false	false	spare	class0
1/25	pClassPSE	false	false	false	spare	class0

"Local PoE tab fields" (page 345) describes the Local PoE tab fields.

Local PoE tab fields

Field	Description
PortNum	Port number.
PowerPortClass	Identifies the port Class of the local port.
PowerMDISupported	Indicates whether MDI power is supported on the local port.
PowerMDIEnabled	Indicates 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 • class2 • class3 • class4

—End—

See also:

- "Local Port Auto-negotiation tab" (page 343)
- "Local Link Aggregate tab" (page 346)
- "Local Max Frame tab" (page 347)
- "Neighbor Port Auto-negotiation tab" (page 348)

- "Neighbor PoE tab" (page 350)
- "Neighbor Link Aggregate tab" (page 352)
- "Neighbor Max Frame tab" (page 353)

Local Link Aggregate tab

With the Local Link Aggregate tab, you can view LLDP link aggregation properties for the local system.

Use the following procedure to open the Local Link Aggregate tab:

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 346)).

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 346) describes the Local Link Aggregate tab fields.

Local Link Aggregate tab fields

Field	Description
PortNum	Port number.

Field	Description
LinkAggStatus	Specifies 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" \(page 343\)](#)
- ["Local PoE tab" \(page 344\)](#)
- ["Local Max Frame tab" \(page 347\)](#)
- ["Neighbor Port Auto-negotiation tab" \(page 348\)](#)
- ["Neighbor PoE tab" \(page 350\)](#)
- ["Neighbor Link Aggregate tab" \(page 352\)](#)
- ["Neighbor Max Frame tab" \(page 353\)](#)

Local Max Frame tab

With the Local Max Frame tab, you can view LLDP maximum frame size properties for the local system.

Use the following procedure to open the Local Max Frame tab:

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" \(page 348\)](#)").

Local Max Frame tab

PortNum	MaxFrameSize
1/1	9216
1/2	9216
1/3	9216
1/4	9216
1/5	9216
1/6	9216
1/7	9216
1/8	9216
1/9	9216
1/10	9216
1/11	9216
1/12	9216
1/13	9216
1/14	9216
1/15	9216
1/16	9216
1/17	9216
1/18	9216
1/19	9216
1/20	9216
1/21	9216

"Local Max Frame tab fields" (page 348) describes the Local Max Frame tab fields.

Local Max Frame tab fields

Field	Description
PortNum	port number
MaxFrameSize	maximum frame size for the port

—End—

See also:

- "Local Port Auto-negotiation tab" (page 343)
- "Local PoE tab" (page 344)
- "Local Link Aggregate tab" (page 346)
- "Neighbor Port Auto-negotiation tab" (page 348)
- "Neighbor PoE tab" (page 350)
- "Neighbor Link Aggregate tab" (page 352)
- "Neighbor Max Frame tab" (page 353)

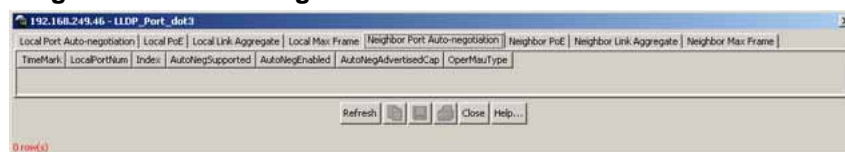
Neighbor Port Auto-negotiation tab

With the Neighbor Port Auto-Negotiation tab, you can view LLDP auto-negotiation properties for the remote system.

Use the following procedure to open the Neighbor Port Auto-Negotiation tab:

- | 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 349)). |

Neighbor Port Auto-negotiation tab



"[Neighbor Port Auto-negotiation tab fields](#)" (page 349) describes the Neighbor Port Auto-negotiation tab fields.

Neighbor Port Auto-negotiation tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
AutoNegSupported	The truth value used to indicate whether the given port (associated with a remote system) supports Auto-negotiation.
AutoNegEnabled	Indicates 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 343)
- "Local PoE tab" (page 344)
- "Local Link Aggregate tab" (page 346)
- "Local Max Frame tab" (page 347)
- "Neighbor PoE tab" (page 350)
- "Neighbor Link Aggregate tab" (page 352)
- "Neighbor Max Frame tab" (page 353)

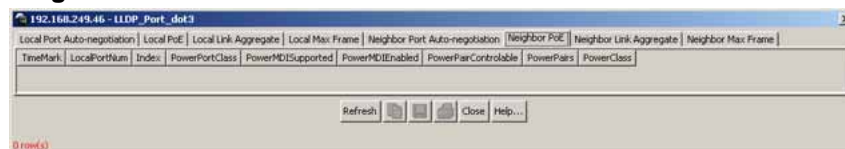
Neighbor PoE tab

With the Neighbor PoE tab, you can view LLDP PoE properties for the remote system.

Use the following procedure to open the Neighbor PoE tab:

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 350)).

Neighbor PoE tab

"Neighbor PoE tab fields" (page 350) describes the Neighbor PoE tab fields.

Neighbor PoE 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.
PowerPortClass	Identifies the port Class of the remote port.
PowerMDISupported	Indicates whether MDI power is supported on the remote port.
PowerMDIEnabled	Indicates 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.
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 343)
- "Local PoE tab" (page 344)
- "Local Link Aggregate tab" (page 346)

- "Local Max Frame tab" (page 347)
- "Neighbor Port Auto-negotiation tab" (page 348)
- "Neighbor Link Aggregate tab" (page 352)
- "Neighbor Max Frame tab" (page 353)

Neighbor Link Aggregate tab

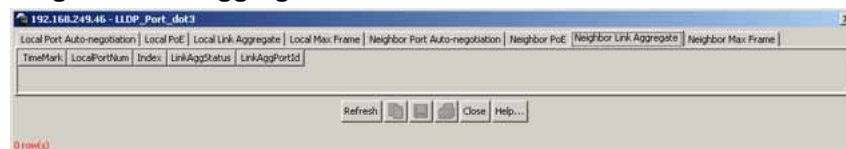
With the Neighbor Link Aggregate tab, you can view LLDP link aggregation properties for the remote system.

Use the following procedure to open the Neighbor Link Aggregate tab:

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 352)). |

Neighbor Link Aggregate tab fields



"[Neighbor Link Aggregate tab fields](#)" (page 352) describes the Neighbor Link Aggregate tab fields.

Neighbor Link Aggregate tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.

Field	Description
LinkAggStatus	Specifies 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" \(page 343\)](#)
- ["Local PoE tab" \(page 344\)](#)
- ["Local Link Aggregate tab" \(page 346\)](#)
- ["Local Max Frame tab" \(page 347\)](#)
- ["Neighbor Port Auto-negotiation tab" \(page 348\)](#)
- ["Neighbor PoE tab" \(page 350\)](#)
- ["Neighbor Link Aggregate tab" \(page 352\)](#)
- ["Neighbor Max Frame tab" \(page 353\)](#)

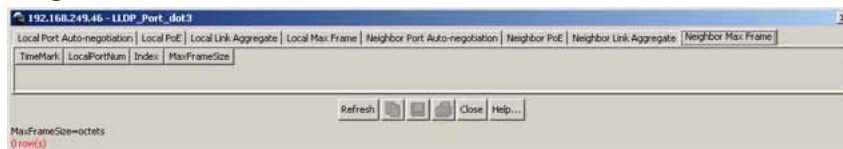
Neighbor Max Frame tab

With the Neighbor Max Frame tab, you can view LLDP maximum frame size properties for the remote system.

Use the following procedure to open the Neighbor Max Frame tab:

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" \(page 354\)](#)").

Neighbor Max Frame tab

"Neighbor Max Frame tab fields" (page 354) describes the Neighbor Max Frame tab fields.

Neighbor Max Frame tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
MaxFrameSize	Maximum Frame Size for the remote port.

—End—

See also:

- "Local Port Auto-negotiation tab" (page 343)
- "Local PoE tab" (page 344)
- "Local Link Aggregate tab" (page 346)
- "Local Max Frame tab" (page 347)
- "Neighbor Port Auto-negotiation tab" (page 348)
- "Neighbor PoE tab" (page 350)
- "Neighbor Link Aggregate tab" (page 352)

LLDP_Port_med dialog box

You can use the LLDP_Port_med dialog box to configure and view MED LLDP information. For details, refer to the following tabs:

- "Local Policy tab" (page 355)
- "Local Location tab" (page 357)

- "Local PoE PSE tab" (page 363)
- "Neighbor Capabilities tab" (page 365)
- "Neighbor Policy tab" (page 366)
- "Neighbor Location tab" (page 368)
- "Neighbor PoE tab" (page 372)
- "Neighbor PoE PSE tab" (page 373)
- "Neighbor PoE PD tab" (page 375)
- "Neighbor Inventory tab" (page 377)

Local Policy tab

With the Local Policy tab, you can view LLDP policy properties for the local system.

Use the following procedure to open the Local Policy tab:

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

- | | |
|---|--|
| 1 | From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port med. |
|---|--|

The LLDP_Port_med dialog box appears with the Local Policy tab displayed ("Local Policy tab" (page 355)).

Local Policy tab

PortNum	PolicyVarID	PolicyPriority	PolicyDiscp	PolicyUnknown	PolicyTagged
1/1	0	0	0	true	0
1/2	0	0	0	true	0
1/3	0	0	0	true	0
1/4	0	0	0	true	0
1/5	0	0	0	true	0
1/6	0	0	0	true	0
1/7	0	0	0	true	0
1/8	0	0	0	true	0
1/9	0	0	0	true	0
1/10	0	0	0	true	0
1/11	0	0	0	true	0
1/12	0	0	0	true	0
1/13	0	0	0	true	0
1/14	0	0	0	true	0
1/15	0	0	0	true	0
1/16	0	0	0	true	0
1/17	0	0	0	true	0
1/18	0	0	0	true	0
1/19	0	0	0	true	0

"Local Policy tab fields" (page 355) describes the Local Policy tab fields.

Local Policy tab fields

Field	Description
PortNum	Port number.

Field	Description
PolicyVlanID	An extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1p priority level is significant and the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the local port.
PolicyDscp	This object contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the given port on the local system.
PolicyUnknown	A value of true indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID, the Layer 2 priority, and the DSCP value fields are ignored. A value of false indicates that this network policy is defined.
PolicyTagged	A value of true indicates that the application is using a tagged VLAN. A value of false indicates that for the specific application, the device is using an untagged VLAN or does not support a port based VLAN operation. In this case, both the VLAN ID and the Layer 2 priority fields are ignored, and only the DSCP value has relevance.

—End—

See also:

- ["Local Location tab" \(page 357\)](#)
- ["Local PoE PSE tab" \(page 363\)](#)
- ["Neighbor Capabilities tab" \(page 365\)](#)
- ["Neighbor Policy tab" \(page 366\)](#)
- ["Neighbor Location tab" \(page 368\)](#)
- ["Neighbor PoE tab" \(page 372\)](#)

- "Neighbor PoE PSE tab" (page 373)
- "Neighbor PoE PD tab" (page 375)
- "Neighbor Inventory tab" (page 377)

Local Location tab

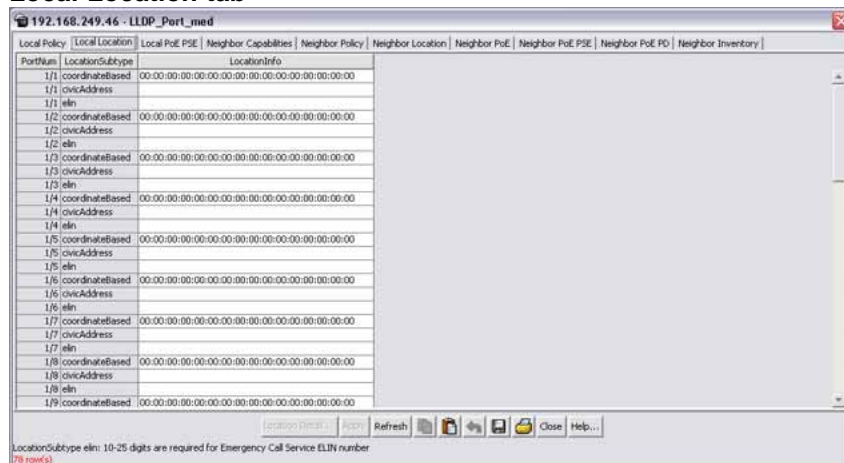
With the Local Location tab, you can view LLDP location properties for the local system.

To view the Local Location tab:

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

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port med**.
The LLDP_Port_med dialog box appears with the Local Policy tab displayed.
- 2 Click the **Local Location** tab.
The Local Location tab appears.

Local Location tab



"Local Location tab fields" (page 357) describes the Local Location tab fields.

Local Location tab fields

Field	Description
PortNum	Port number.

Field	Description
LocationSubtype	The location subtype advertised by the remote device: <ul style="list-style-type: none"> • unknown • coordinateBased • civicAddress • elin
LocationInfo	The location information. The parsing of this information is dependent on the value LocationSubtype.

—End—

See also:

- ["Local Policy tab" \(page 355\)](#)
- ["Local PoE PSE tab" \(page 363\)](#)
- ["Neighbor Capabilities tab" \(page 365\)](#)
- ["Neighbor Policy tab" \(page 366\)](#)
- ["Neighbor Location tab" \(page 368\)](#)
- ["Neighbor PoE tab" \(page 372\)](#)
- ["Neighbor PoE PSE tab" \(page 373\)](#)
- ["Neighbor PoE PD tab" \(page 375\)](#)
- ["Neighbor Inventory tab" \(page 377\)](#)

Viewing coordinate-based location details

You can select and view or configure details for coordinate-based locations listed on the Local Location tab.

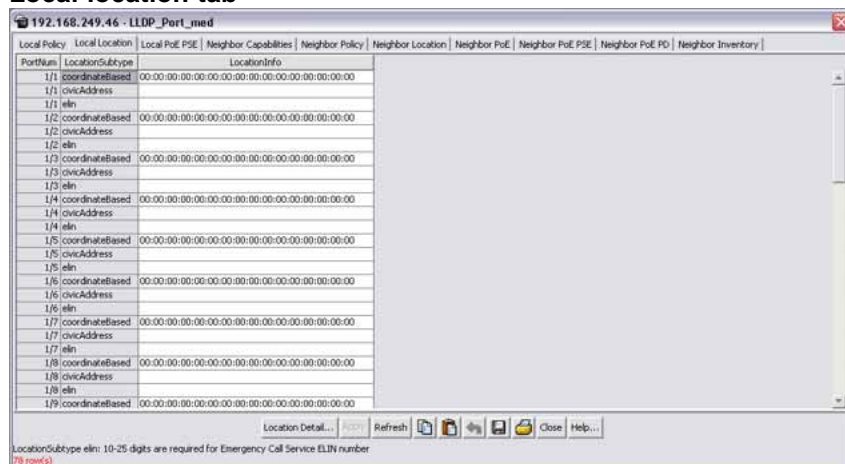
To view or configure details for coordinate-based locations:

Step Action

- 1 From the **Local Location** tab, select a location with the **LocationSubtype** listed as **coordinateBased**.

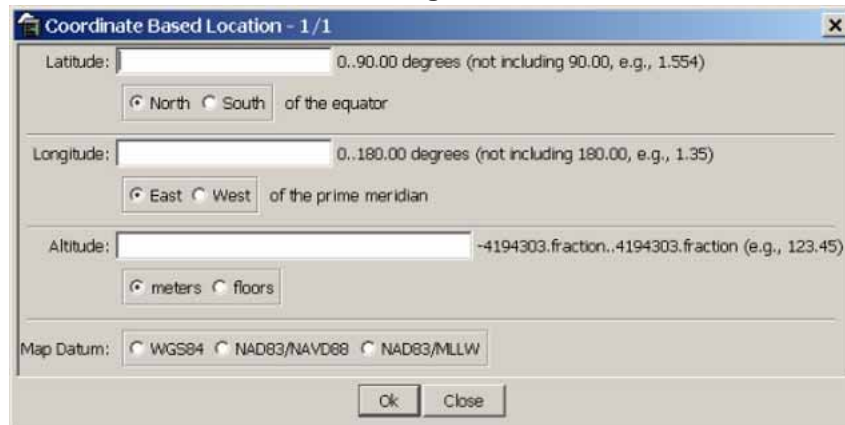
The Location Detail button is activated.

Local location tab



- 2 Click the **Location Details** button.
The Coordinate Based Location dialog box opens.

Coordinate Based Location dialog box



The following table describes the Coordinate Based Location dialog box fields.

Coordinate Based Location dialog box fields

Field	Description
Latitude	Specifies the latitude in degrees, and its relation to the equator (North or South).
Longitude	Specifies the longitude in degrees, and its relation to the prime meridian (East or West).

Field	Description
Altitude	Specifies the altitude, and the units of measurement used (meters or floors).
Map Datum	Specifies the reference datum. The format can be one of the following: <ul style="list-style-type: none"> WGS84: World Geodesic System 1984, Prime Meridian Name: Greenwich NAD83/NAVD88 North American Datum 1983/ North American Vertical Datum of 1988 NAD83/MLLW: North American Datum 1983/ Mean Lower Low Water

3 Enter details and click **OK**.

4 Click **Close**.

—End—

Viewing civic address location details

You can select and view or configure details for civic address locations listed on the Local Location tab.

To view and configure details for civic address locations:

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

1 From the **Local Location** tab, select a location with the **LocationSubtype** listed as **civicAddress**

The Location Detail button is activated.

Local location tab

Local Policy	Local Location	Local Port PSE	Neighbor Capabilities	Neighbor Policy	Neighbor Location	Neighbor Port	Neighbor Port PSE	Neighbor Port PD	Neighbor Inventory
PortNum	LocationSubtype	LocationInfo							
1/1	coordinateBased	00:00:00:00:00:00:00:00:00:00:00:00:00:00							
1/1	civicAddress								
1/1	eln								
1/2	coordinateBased	00:00:00:00:00:00:00:00:00:00:00:00:00:00							
1/2	civicAddress								
1/2	eln								
1/3	coordinateBased	00:00:00:00:00:00:00:00:00:00:00:00:00:00							
1/3	civicAddress								
1/3	eln								
1/4	coordinateBased	00:00:00:00:00:00:00:00:00:00:00:00:00:00							
1/4	civicAddress								
1/4	eln								
1/5	coordinateBased	00:00:00:00:00:00:00:00:00:00:00:00:00:00							
1/5	civicAddress								
1/5	eln								
1/6	coordinateBased	00:00:00:00:00:00:00:00:00:00:00:00:00:00							
1/6	civicAddress								
1/6	eln								
1/7	coordinateBased	00:00:00:00:00:00:00:00:00:00:00:00:00:00							
1/7	civicAddress								
1/7	eln								
1/8	coordinateBased	00:00:00:00:00:00:00:00:00:00:00:00:00:00							
1/8	civicAddress								
1/8	eln								
1/9	coordinateBased	00:00:00:00:00:00:00:00:00:00:00:00:00:00							

LocationSubtype eln: 10-25 digits are required for Emergency Call Service ELN number
78 row(s)

- 2 Click the **Location Detail** button.
The Civic Address Location dialog box opens.

Civic Address Location dialog box

The following table describes the Civic Address Location dialog box.

Civic Address Location dialog box fields

Field	Description
Country Code	Country code (2 upper case letters)
State	National subdivisions (state, canton, region)
County	County, parish, gun (JP), district (IN)
City	City, township, shi (JP)
City District	City division, city district, ward

Field	Description
Block (Neighborhood, block)	Neighborhood, block
Street	Street
Leading street direction	Leading street direction
Trailing street suffix	Trailing street suffix
Street suffix	Street suffix
House number	House number
House number suffix	House number suffix
Landmark or vanity address	Landmark or vanity address
Additional Location info	Additional location information
Name (Residence and office occupant)	Residence and office occupant
Postal/Zip code	Postal/Zip code
Building (structure)	Building (structure)
Apartment (suite)	Unit number (apartment, suite)
Floor	Floor
Room number	Room number
Place type	Office
Postal community name	Postal community name
Post office box P.O.Box	Post office box
Additional Code	Additional code

3 Enter details and click **OK**.

4 Click **Close**.

—End—

Local PoE PSE tab

With the Local PoE PSE tab, you can view LLDP PoE PSE properties for the local system.

Use the following procedure to open the Local PoE PSE tab:

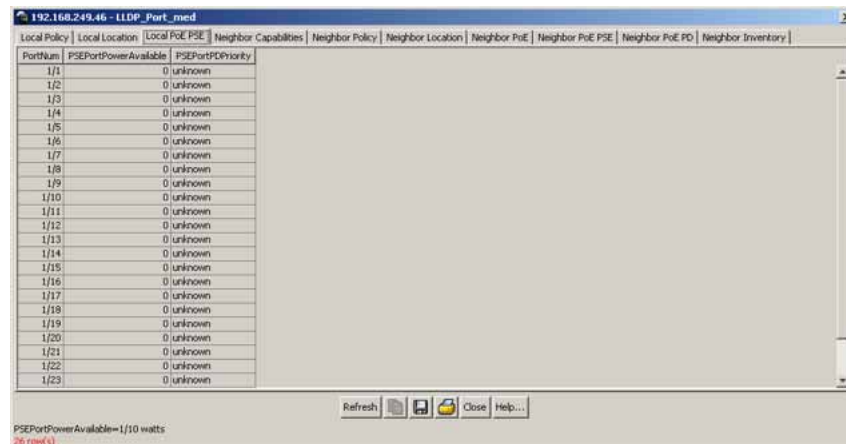
Step	Action
------	--------

1	From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port med .
---	---

The LLDP_Port_med dialog box appears with the Local Policy tab displayed.

- 2 Click the **Local PoE PSE** tab.
The Local PoE PSE tab appears ("[Local PoE PSE tab](#)" (page 364)).

Local PoE PSE tab



"[Local PoE PSE tab fields](#)" (page 364) describes the Local PoE PSE tab fields.

Local PoE PSE tab fields

Field	Description
PortNum	Port number.
PSEPortPowerAvailable	This object contains the value of the power available (in units of 0.1 watts) from the PSE through this port.
PSEPortPDPriority	Indicates the PD power priority that is advertised on this PSE port: <ul style="list-style-type: none"> • unknown: priority is not configured or known by the PD • critical: the device advertises its power priority as critical, see RFC 3621 • high: the device advertises its power priority as high, see RFC 3621 • low: the device advertises its power priority as low, see RFC 3621

—End—

See also:

- "Local Policy tab" (page 355)
- "Local Location tab" (page 357)
- "Neighbor Capabilities tab" (page 365)
- "Neighbor Policy tab" (page 366)
- "Neighbor Location tab" (page 368)
- "Neighbor PoE tab" (page 372)
- "Neighbor PoE PSE tab" (page 373)
- "Neighbor PoE PD tab" (page 375)
- "Neighbor Inventory tab" (page 377)

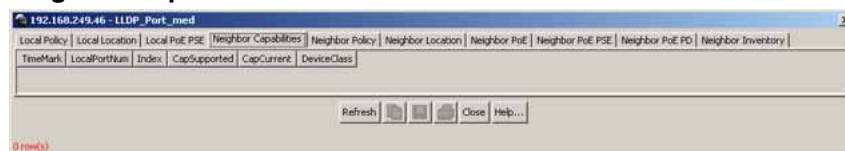
Neighbor Capabilities tab

With the Neighbor Capabilities tab, you can view LLDP capabilities properties for the remote system.

Use the following procedure to open the Neighbor Capabilities tab:

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port med**.
The LLDP_Port_med dialog box appears with the Local Policy tab displayed.
- 2 Click the **Neighbor Capabilities tab**.
The Neighbor Capabilities tab appears ("[Neighbor Capabilities tab](#)" (page 365)).

Neighbor Capabilities tab

"[Neighbor Capabilities tab fields](#)" (page 365) describes the Neighbor Capabilities tab fields.

Neighbor Capabilities 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.
CapSupported	Identifies the MED system capabilities supported on the remote system.
CapCurrent	Identifies the MED system capabilities that are enabled on the remote system.
DeviceClass	Remote MED device class.

—End—

See also:

- ["Local Policy tab" \(page 355\)](#)
- ["Local Location tab" \(page 357\)](#)
- ["Local PoE PSE tab" \(page 363\)](#)
- ["Neighbor Policy tab" \(page 366\)](#)
- ["Neighbor Location tab" \(page 368\)](#)
- ["Neighbor PoE tab" \(page 372\)](#)
- ["Neighbor PoE PSE tab" \(page 373\)](#)
- ["Neighbor PoE PD tab" \(page 375\)](#)
- ["Neighbor Inventory tab" \(page 377\)](#)

Neighbor Policy tab

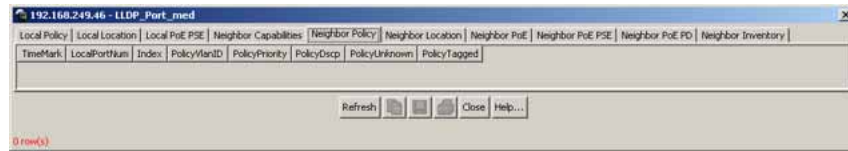
With the Neighbor Policy tab, you can view LLDP policy properties for the remote system.

Use the following procedure to open the Neighbor Policy tab:

Step	Action
1	From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port med . The LLDP_Port_med dialog box appears with the Local Policy tab displayed.
2	Click the Neighbor Policy tab .

The Neighbor Policy tab appears ("[Neighbor Policy tab](#)" (page 367)).

Neighbor Policy tab



"[Neighbor Policy tab fields](#)" (page 367) describes the Neighbor Policy tab fields.

Neighbor Policy tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
PolicyVlanID	An extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1p priority level is significant and that the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the remote system connected to the port.
PolicyDscp	This object contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the remote system connected to the port.

Field	Description
PolicyUnknown	A value of true indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID, the Layer 2 priority, and the DSCP value fields are ignored. A value of false indicates that this network policy is defined.
PolicyTagged	A value of true indicates that the application is using a tagged VLAN. A value of false indicates that for the specific application, the device is using an untagged VLAN or does not support a port based VLAN operation. In this case, both the VLAN ID and the Layer 2 priority fields are ignored, and only the DSCP value has relevance.

—End—

See also:

- ["Local Policy tab" \(page 355\)](#)
- ["Local Location tab" \(page 357\)](#)
- ["Local PoE PSE tab" \(page 363\)](#)
- ["Neighbor Capabilities tab" \(page 365\)](#)
- ["Neighbor Location tab" \(page 368\)](#)
- ["Neighbor PoE tab" \(page 372\)](#)
- ["Neighbor PoE PSE tab" \(page 373\)](#)
- ["Neighbor PoE PD tab" \(page 375\)](#)
- ["Neighbor Inventory tab" \(page 377\)](#)

Neighbor Location tab

With the Neighbor Location tab, you can view LLDP location properties for the remote system.

Use the following procedure to open the Neighbor Location tab:

Step	Action
1	From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port med . The LLDP_Port_med dialog box appears with the Local Policy tab displayed.

- 2 Click the **Neighbor Location** tab.
The Neighbor Location tab appears ("[Neighbor Location tab](#)" (page 369)).

Neighbor Location tab



"[Neighbor Location tab fields](#)" (page 369) describes the Neighbor Location tab fields.

Neighbor Location tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
LocationSubtype	The location subtype advertised by the remote device: <ul style="list-style-type: none"> unknown coordinateBased civicAddress elin
LocationInfo	The location information advertised by the remote device. The parsing of this information is dependent on the location subtype.

—End—

See also:

- "[Local Policy tab](#)" (page 355)
- "[Local Location tab](#)" (page 357)

- "Local PoE PSE tab" (page 363)
- "Neighbor Capabilities tab" (page 365)
- "Neighbor Policy tab" (page 366)
- "Neighbor PoE tab" (page 372)
- "Neighbor PoE PSE tab" (page 373)
- "Neighbor PoE PD tab" (page 375)
- "Neighbor Inventory tab" (page 377)

Viewing coordinate-based location details

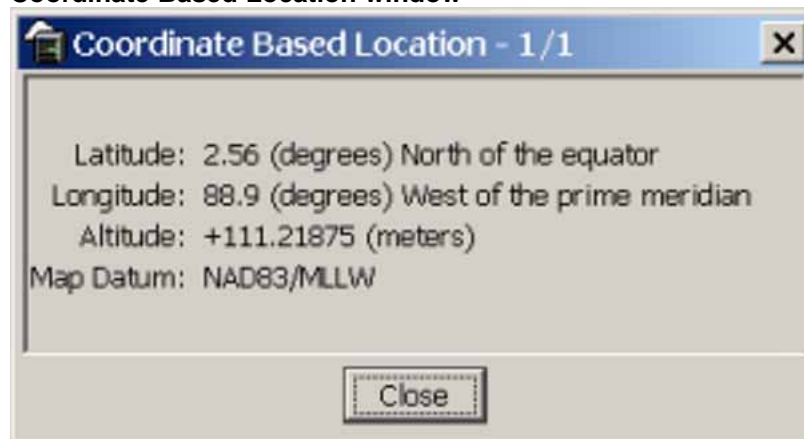
From the Neighbor Location tab, you can select coordinate-based locations and view details for the remote system.

To view coordinate-based location details:

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

- 1 From the **Neighbor Location** tab, select a location with the **LocationSubtype** listed as **coordinateBased**
The Location Details button is activated.
- 2 Click the **Location Details** button.
The Coordinate Based Location window displays the selected location details.

Coordinate Based Location window



- 3 Click **Close**.

—End—

Viewing civic address location details

From the Neighbor Location tab, you can select civic address locations and view details for the remote system.

To view civic address location details:

Step	Action
1	From the Neighbor Location tab, select a location with the LocationSubtype listed as civicAddress The Location Details button is activated.
2	Click the Location Details button. The Civic Address Location window displays the selected location details.

Civic Address Location window



- 3 Click **Close**.

—End—

Neighbor PoE tab

With the Neighbor PoE tab, you can view LLDP PoE properties for the remote system.

Use the following procedure to open the Neighbor PoE tab:

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port med**.
The LLDP_Port_med dialog box appears with the Local Policy tab displayed.
- 2 Click the **Neighbor PoE** tab.
The Neighbor PoE tab appears ("[Neighbor PoE tab](#)" (page 372)).

Neighbor PoE tab



"[Neighbor PoE tab fields](#)" (page 372) describes the Neighbor PoE tab fields.

Neighbor PoE tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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

Field	Description
	monotonically increasing index values to new entries, starting with one, after each reboot.
PoeDeviceType	<p>Defines the type of Power-via-MDI (Power over Ethernet) advertised by the remote device:</p> <ul style="list-style-type: none"> • pseDevice: indicates that the device is advertised as a Power Sourcing Entity (PSE). • pdDevice: indicates that the device is advertised as a Powered Device (PD). • none: indicates that the device does not support PoE.

—End—

See also:

- "Local Policy tab" (page 355)
- "Local Location tab" (page 357)
- "Local PoE PSE tab" (page 363)
- "Neighbor Capabilities tab" (page 365)
- "Neighbor Policy tab" (page 366)
- "Neighbor Location tab" (page 368)
- "Neighbor PoE PSE tab" (page 373)
- "Neighbor PoE PD tab" (page 375)
- "Neighbor Inventory tab" (page 377)

Neighbor PoE PSE tab

With the Neighbor PoE PSE tab, you can view LLDP PoE PSE properties for the remote system.

Use the following procedure to open the Neighbor PoE PSE tab:

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port med.**

The LLDP_Port_med dialog box appears with the Local Policy tab displayed.

- 2 Click the **Neighbor PoE PSE tab**.
The Neighbor PoE PSE tab appears ("[Neighbor PoE PSE tab](#)" (page 374)).

Neighbor PoE PSE tab



"[Neighbor PoE PSE tab fields](#)" (page 374) describes the Neighbor PoE PSE tab fields.

Neighbor PoE PSE tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
PSEPowerAvailable	Specifies the power available (in units of 0.1 watts) from the PSE connected remotely to this port.
PSEPowerSource	Defines the type of PSE Power Source advertised by the remote device. <ul style="list-style-type: none"> • primary: indicates that the device advertises its power source as primary. • backup: indicates that the device advertises its power source as backup.
PSEPowerPriority	Specifies the priority advertised by the PSE connected remotely to the port: <ul style="list-style-type: none"> • critical: indicates that the device advertises its power priority as critical, see RFC 3621. • high: indicates that the device advertises its power priority as high, see RFC 3621.

Field	Description
	<ul style="list-style-type: none"> low: indicates that the device advertises its power priority as low, see RFC 3621.

—End—

See also:

- "Local Policy tab" (page 355)
- "Local Location tab" (page 357)
- "Local PoE PSE tab" (page 363)
- "Neighbor Capabilities tab" (page 365)
- "Neighbor Policy tab" (page 366)
- "Neighbor Location tab" (page 368)
- "Neighbor PoE tab" (page 372)
- "Neighbor PoE PD tab" (page 375)
- "Neighbor Inventory tab" (page 377)

Neighbor PoE PD tab

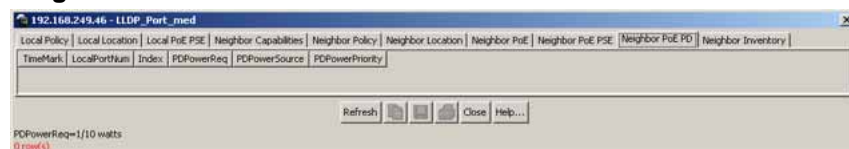
With the Neighbor PoE PD tab, you can view LLDP PoE PD properties for the remote system.

Use the following procedure to open the Neighbor PoE PD tab:

Step Action

- 1 From the **Device Manager** menu bar, choose **Edit > Diagnostics > 802.1ab > Port med**.
The LLDP_Port_med dialog box appears with the Local Policy tab displayed.
- 2 Click the **Neighbor PoE PD tab**.
The Neighbor PoE PD tab appears ("Neighbor PoE PD tab" (page 375)).

Neighbor PoE PD tab



"Neighbor PoE PD tab fields" (page 376) describes the Neighbor PoE PD tab fields.

Neighbor PoE PD tab fields

Field	Description
TimeMark	The TimeFilter for this entry.
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.
PDPowerReq	Specifies the value of the power required (in units of 0.1 watts) by a Powered Device (PD) connected remotely to the port.
PDPowerSource	Defines the type of Power Source advertised as being used by the remote device: <ul style="list-style-type: none"> • fromPSE: indicates that the device advertises its power source as received from a PSE. • local: indicates that the device advertises its power source as local. • localAndPSE: indicates that the device advertises its power source as using both local and PSE power.
PDPowerPriority	Defines the priority advertised as being required by the PD connected remotely to the port: <ul style="list-style-type: none"> • critical: indicates that the device advertises its power priority as critical, see RFC 3621. • high: indicates that the device advertises its power priority as high, see RFC 3621. • low: indicates that the device advertises its power priority as low, see RFC 3621.

—End—

See also:

- "Local Policy tab" (page 355)
- "Local Location tab" (page 357)
- "Local PoE PSE tab" (page 363)
- "Neighbor Capabilities tab" (page 365)
- "Neighbor Policy tab" (page 366)
- "Neighbor Location tab" (page 368)
- "Neighbor PoE tab" (page 372)
- "Neighbor PoE PSE tab" (page 373)
- "Neighbor Inventory tab" (page 377)

Neighbor Inventory tab

With the Neighbor Inventory tab, you can view LLDP Inventory properties for the remote system.

Use the following procedure to open the Neighbor Inventory tab:

Step	Action
1	From the Device Manager menu bar, choose Edit > Diagnostics > 802.1ab > Port med . The LLDP_Port_med dialog box appears with the Local Policy tab displayed.
2	Click the Neighbor Inventory tab. The Neighbor Inventory tab appears (" Neighbor Inventory tab " (page 377)).

Neighbor Inventory tab

"[Neighbor Inventory tab fields](#)" (page 377) describes the Neighbor Inventory tab fields.

Neighbor Inventory 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.
HardwareRev	The vendor-specific hardware revision string as advertised by the remote device.
FirmwareRev	The vendor-specific firmware revision string as advertised by the remote device.
SoftwareRev	The vendor-specific software revision string as advertised by the remote device.
SerialNum	The vendor-specific serial number as advertised by the remote device.
MfgName	The vendor-specific manufacturer name as advertised by the remote device.
ModelName	The vendor-specific model name as advertised by the remote device.
AssetID	The vendor-specific asset tracking identifier as advertised by the remote device.

—End—

See also:

- ["Local Policy tab" \(page 355\)](#)
- ["Local Location tab" \(page 357\)](#)
- ["Local PoE PSE tab" \(page 363\)](#)
- ["Neighbor Capabilities tab" \(page 365\)](#)
- ["Neighbor Policy tab" \(page 366\)](#)
- ["Neighbor Location tab" \(page 368\)](#)
- ["Neighbor PoE tab" \(page 372\)](#)
- ["Neighbor PoE PSE tab" \(page 373\)](#)
- ["Neighbor PoE PD tab" \(page 375\)](#)

Index

Symbols/Numerics

802.1ab 279

A

AAUR 141
 AbsoluteValue statistics 49
 access 110, 231
 Actions menu 43
 address field 190
 address source field 190
 AdminDuplex field 254
 AdminEnable field 256
 AdminSpeed field 254
 AdminState field 242, 245
 AdminStatus field 253
 Agent Auto Unit Replacement 141
 Agent tab 246
 Alarm Manager button 43
 allocating bandwidth 42
 Allowed Source IP field 233
 Allowed Source Mask field 233
 Area Chart button 54
 area graph example 50
 ASCII configuration file 153
 AUR 132
 configuring with Device Manager 140
 configuring with the CLI 139
 AuthenticationTraps field 238
 Auto Unit Replacement 132
 auto-MDI X 148
 AutoNegotiate field 253
 autonegotiation 192
 description 149

AutoNegotiationCapability field 254
 autopolarity 149
 AutoPvid field 238
 autosense description 149
 Autotopology
 configuring with CLI 196
 autotopology command 196
 available power 264
 Average statistics 49

B

banner command 118
 Banner tab 119
 Bar Chart button 54
 Base tab 266
 base unit 124
 setting 125, 126, 126
 Base Unit switch 69
 BaseNumPorts field 242, 245, 263
 blinking LEDs 45
 boot command 113
 BootMode field 239
 BootP 189
 configuring 220
 modes 114
 request modes 222
 Bootp 156
 BootP Always field 222
 BootP Disabled field 222
 bootp field 190
 BootP or Last Address field 223
 BootP Request Mode field 222
 BootP When Needed field 222
 BootRouterAddr tab 247

- Bridge parameter
 - Base tab
 - BridgeAddress field 266
 - NumPorts field 267
 - Type 267
 - Forwarding tab
 - Address field 269
 - Port field 270
 - Status field 269
- broadcast traffic 200
- buttons
 - dialog boxes 48
 - toolbar 43
- C**
- CANA 149
 - configuring with CLI 209
- chassis
 - configuration, editing 236
- class of service 42
- CLI
 - accessing 15
 - command modes 17
- color-coded ports 45
- commands
 - UI button 129
- config file 154
- configuration
 - PoE, by port 256
 - PoE, switch parameters 262
- configuration file
 - automatically downloading 107
- configuration file with USB port 128
- configuration files
 - in Device Manager 97
 - in the CLI 95
 - in Web-based management 102
- configuring and enabling
 - DHCP 115
- connecting external power source 169
- console password
 - setting with Web-based management 82
- ConsumptionPower field 265
- conversation steering 148
- Copy button 48
- Cumulative statistics 49
- CurrentDefaultGateway field 239
- CurrentImageVersion field 239
- CurrentMgmtProtocol field 239
- Custom Autonegotiation Advertisements 149
- Custom Banner tab 120
- D**
- data, exporting 52
- daylight saving time
 - configure 273
- DC power source
 - connection 169
- DC-DC converter module 130
- default autotopology command 197
- default duplex command 195
- default flowcontrol command 199
- Default Gateway field 224
- default ip address unit command 191
- default ipbootp server command 115
- default management interface
 - setting 109
- default rate-limit command 201
- default speed command 193
- default telnet-access command 112
- default-gateway field 190
- deliveringPower message 257
- denyLowPriority message 257
- Descr field 242, 243, 252, 263
- Description field 216
- detected message 257
- Detection field 257
- Device Manager 20
- Device menu 42
- device view, summary 44
- DHCP 156, 240
 - configuring 115
 - enabling 115
- DHCP Always field 223
- dhcp client lease field 190
- DHCP or Last Address field 223
- DHCP When Needed field 223
- dhcpOrLastAddress 241
- dhcpWhenNeeded 240
- Differentiated Services 42
- Disable command 47

disabled port, color 45
disabling power on ports 256
DNS
 configuring with CLI 212
duplex command 194
duplex mode 192
Dynamic Host Configuration Protocol
 (DHCP) 156

E

Edit command 47
Edit menu 42
Edit Selected button 43
Enable command 47
enabling power on ports 256
errors 155
Export Data button 48, 52
external power source
 connecting 169

F

factory default configuration 69
Fan tab 249
fans 130
feature license file
 configuring with CLI 67
 configuring with Device Manager 68
feature licensing 66
Firmware Version field 217
flash memory for software image
 upgrades 143
flow control 198
flowcontrol command 198
Forwarding tab 268, 268

G

gateway 187
gateway addresses, configuring 220
GBIC information
 displaying 121
GBIC ports 236
Gigabit Ethernet 198
Globe button 43
graph
 creating 52

 modifying 53
Graph command 47
Graph menu 42
Graph Selected button 43, 53
graph types 49

H

hardware description 216, 217
hardware features 123
hardware information
 displaying 121
Hardware Version field 217
Help button 43
Help menu 43
Help, Device Manager 55
Home Page menu 55
Horizontal button 54

I

Identify Unit Numbers page 220
IEEE 802.1ab 279
IEEE 802.3u standard 149
ImageLoadMode field 239
In-Band Stack IP Address field 224
In-Band Subnet Mask field 224
In-Band Switch IP Address field 224
In-Use field 224
Index field 252
Insert button 48
Interface tab 251
interfaces
 displaying 192
IP address 187, 187, 188, 190, 191, 220
 for each unit 156, 190, 220
ip address command 187
IP Address field 215, 218
ip address unit command 190
IP blocking
 configuring with CLI 186
ip bootp server command 114
ip default-gateway command 188
IP gateway address 220
IP manager list 231
IP page 220
IP Routing menu 42
IpAddress field 242, 245

IsPortShared field 255

J

Java Device Manager 20

JDM 20

L

LACP 147

Last BootP field 224

LastChange field 253

LastLoadProtocol field 239

LastValue statistics 49

LEDs 220

legend, port color 43, 46

Line Chart button 54

Link Aggregation 147

Link Layer Discovery Protocol (802.1ab) 279

link, lacking, color 45

LinkTrap field 253

LLDP 279

 Configuring with CLI 284

 configuring with Device Manager 304

local time zone

 configure 272

LocalStorageImageVersion field 239

Location field 242, 244

Log Scale button 54

loopback testing port, color 46

LstChng field 242, 244

M

MAC address 217

MAC Address field 215, 219

Mac Address field 217

MacAddr field 247

ManagementVlanId field 238

Manufacturing Date Code field 215, 217

Maximum statistics 49

MDAs 198

menu bar, Device Manager 42

menus. See individual menu names 42

MIBs 159

Minimum statistics 49

MtId field 255

Module Description field 217

MSTP 146

Mtu field 252

multicast traffic 200

MultiLink Trunking

 description 147

multiple objects, selecting 44

multiple spanning tree groups 145

Multiple Spanning Tree Protocol 146

N

Name field 252

netmask 187, 190

network administrator

 contact information 230, 231

new table entry, creating 48

New Unit Number field 219

NextBootDefaultGateway field 239

NextBootLoadProtocol field 239

NextBootMgmtProtocol field 238

NextBootNetMask field 246, 246

NextBootpAddr field 246

no autotopology command 197

no banner command 118

no flowcontrol command 199

no ip address command 188

no ip address unit command 191

no ip bootp server command 115

no ip default-gateway 189

no rate-limit command 201

no telnet-access command 111

no web-server command 113

NotificationControlEnable field 265

numbering

 stacks 218

 unit 217, 219, 220

NVRAM 184

O

object types 44

objects

 editing 48

 selecting 44

online Help 43, 55

Open Device button 43

operating port, color 45

Operational State field 216, 217

OperDuplex field 254

OperSpeed field 254, 255
 OperState field 242, 245, 248, 250
 OperStatus field 253, 265

P

passwords
 setting with CLI 75
 Paste button 48
 PhysAddress field 252
 ping command 211
 Pluggable port 216
 PoE 144, 161
 available power 264
 configuration, editing 263
 configuring with CLI 172
 configuring with Device Manager 175
 configuring with Web-based
 management 176
 disabling 256
 enabling 256
 error codes 169
 error messages 257
 port priority 257
 port settings 256
 power being used 265
 priority 257
 status codes 169
 traps 265, 265
 PoE tab 256
 PoE tab for a single unit 264
 policy-enabled networking 144
 DiffServ 144
 polling interval 52
 port color legend 46
 Port dialog box 250
 port errors 155
 port mirroring
 conversation steering 148
 Nortel StackProbe 148
 port shortcut menu 47
 port, naming 155
 port, power detection 257
 PortActiveComponent field 255
 ports 192
 color-coded 45
 disabled 45

 graphing 251
 selecting 44
 Power 256
 power being used 265
 power detection for each port 257
 Power field 264
 Power over Ethernet 144, 161
 power priority 257
 power status 216
 Power Status field 218
 Power Supply tab 248
 Power tab for a single unit 264
 power usage traps 265
 PowerDetectionMethod fieldtroubleshooting
 power detection method 265
 PowerPairs field 265
 PowerPriority field 257
 Print button 48
 publications
 related 159

Q

QoS 144
 QoS menu 42
 Quality of Service 42
 quick configuration 185

R

RADIUS authentication
 configuring with CLI 77
 Rapid Spanning Tree Protocol 145, 146
 Rate Limit tab 257
 rate-limit command 200
 rate-limiting 200
 Real Time Clock
 configuring with CLI 207
 Real-time clock
 configuring with Web-based
 management 234
 rear-panel base unit switch 69
 Reboot field 238
 redundant power 130
 Refresh Device Status button 43
 RelPos field 242
 requirements
 remote access 110

- Reset Changes button 48
- resetting stack 127
- resetting the unit 124, 130
- resetting unit 127
- RFCs 159
- RPSU 130
- RSTP 146

- S**
- sample ASCII config file 154
- searching message 257
- security 110
- serial number 263
- Serial Number field 216, 217
- SerNum field 242, 245, 263
- Serviceability menu 42
- setting TFTP parameters with the CLI 94
- shortcut menus
 - port 47
 - switch unit 46
- show banner command 117
- show interfaces command 192
- show ip command 189
- show rate-limit command 200
- shutdown command 121
- Simple Network Time Protocol 202
- Simple Network Time Protocol (SNTP) 157
- Simple Network Time Protocol tab 270
- single object, selecting 44
- SNMP 159
- SNMP Access field 233
- SNMP traps 55
- SNMP Use List field 233
- SNTP 157, 202
 - configuring with CLI 202
 - configuring with Device Manager 270
 - setting daylight saving time 273
 - setting time zone 272
- SNTP tab 270
- software
 - image upgrades 143
 - updating 85
 - updating with Device Manager 88
 - updating with the CLI 86
 - updating with Web-based management 91
 - software download with USB port 128
 - Software Version field 215, 217
 - software versions 214
 - spanning tree groups 145
 - speed 192
 - speed command 193
 - Stack Info tab 243
 - Stack Information page 214
 - stack information, viewing 214
 - Stack Numbering page 218
 - Stack Numbering Setting table 219
 - stack numbering, configuring 218
 - Stacked button 54
 - stacking 69, 124, 131, 214, 218
 - replacing units 219
 - resetting 130
 - standards 158, 158
 - standby port, color 45
 - static|custom field 118
 - statistics
 - for a single object 51
 - for multiple objects 52
 - graphing 49
 - single port 52
 - types 49
 - statistics dialog box, multiple objects 52
 - statistics dialog boxes 42
 - Stop button 48
 - STP 145
 - subnet mask 187, 190
 - summary options
 - changing stack numbering 218
 - identifying unit numbers 220
 - viewing
 - stack information 214
 - switch information 216
 - Switch administration using CLI 183
 - switch configuration 184
 - switch information
 - viewing 216
 - Switch Information page 216
 - switch stack, selecting 45
 - switch unit shortcut menu 46
 - switch, selecting 44
 - sysContact field 238
 - sysDescr field 238
 - sysLocation field 238

- sysName field 238
 - sysObjectID 238
 - System Contact field 231
 - System Description field 215, 230
 - System Location field 231
 - system location, naming 230
 - System Name field 231
 - system name, configuring 230
 - System Object ID field 230
 - System page 230
 - system settings
 - modifying 230
 - system contact 231
 - system location 231
 - system name 231
 - System tab 237
 - System Up Time field 231
 - sysUpTime field 238
- T**
- tabular port statistics 155
 - Target Replacement Setting field 219
 - Target Unit to Replace field 219
 - TDR
 - configuring with CLI 195
 - TDR tab 258
 - Telnet 110, 110
 - Telnet Access field 233
 - Telnet button 43, 54
 - telnet command 211
 - Telnet password
 - setting with Web-based management 81
 - Telnet session 43, 54
 - Telnet Use List field 233
 - telnet-access command 110
 - terminal setup 109
 - tested port, color 45
 - testing cables 195
 - TLVs
 - IEEE 802.1 organizationally-specific 282
 - IEEE 802.3 organizationally-specific 282
 - Management 281
 - Organizationally-specific for MED devices 282
 - toolbar, Device Manager 43
 - topology information
 - viewing with Device Manager 274
 - Topology tab 275
 - Topology Table tab 275
 - TotalNumPorts 242, 245
 - TotalNumPorts field 263
 - traffic
 - Gigabit Ethernet 198
 - rate-limiting 200
 - Transparent tab 267
 - trap log 55
 - Trap Log button 43
 - traps 265
 - power 265
 - troubleshooting
 - access 110, 188, 191, 231
 - config file 153
 - configuration loss 130
 - DC power source 169
 - external power source 169
 - locations of Help files 55
 - PoE 257, 264
 - PoE tab 262
 - power pairs 265
 - receiving traps 55
 - spanning tree groups 145
 - stacking 69
 - VLANs 145
 - trunks 147
 - Type field 242, 252, 263
 - types of objects 44
- U**
- UI button 124
 - commands 129
 - Unit field 216, 217
 - unit number 217, 219
 - identifying 220
 - numbering units 216
 - Unit Select switch 69
 - Unit tab 236
 - unit uptime 155
 - UNIX, receiving traps 55
 - unmanageable port, color 46
 - updating software 85
 - UsageThreshold field 265

user access limitations
 setting with CLI 75
 setting with Web-based Management 79
User Interface button 124

V

ValidFlag tab 247
value, changed 48
Ver field 242, 245, 263
VLAN menu 42
VlanIds 270
VLANs
 number of 145

port-based 145
protocol-based 145

W

Web Page Access field 233
Web password
 setting with Web-based management 79
Web quick start 157
Web session 43
Web Use List field 233
Web-based Management Interface 56
web-server command 112

Nortel Ethernet Routing Switch 5500 Series

Configuration — System

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

Publication: NN47200-500
Document status: Standard
Document version: 03.01
Document date: 27 August 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.

