



Nortel Ethernet Routing Switch 5000 Series

Configuration — System

Document status: Standard
Document version: 04.02
Document date: 12 December 2008

Copyright © 2005-2008, Nortel Networks
All Rights Reserved.

Sourced in Canada and the United States of America

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel Networks Inc. software license agreement

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

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

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

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

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE

SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General 1. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

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

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

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

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

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

Contents

New in this release	9
Features	9
Dual Agent support	9
IPv6	9
Other changes	10
Document changes	10
<hr/>	
Introduction	11
NNCLI command modes	11
<hr/>	
System configuration fundamentals	15
Feature licensing	15
Trial license	15
User access limitations	15
Customizing NNCLI banner	16
TFTP server	16
Configuration downloads to a switch	16
Updating switch software	16
LED activity during software download	17
Unit quick configuration feature	17
ASCII configuration file	17
Multiple switch configuration management	18
Stacking fundamentals	18
Stacking capabilities	18
Stack monitor	19
Auto Unit Replacement (AUR)	20
Agent Auto Unit Replacement (AAUR)	21
IP blocking	22
Boot agent image	22
Next Boot image and system Boot-up in Dual Agent	23
Combination image	25
Supported BootP modes	26
BootP mode	26
IPv6 management	26
The IPv6 header	27

IPv6 addresses	28
Interface ID	28
Address formats	28
IPv6 extension headers	29
Comparison of IPv4 and IPv6	30
ICMPv6	31
Neighbor discovery	31
ND messages	32
Neighbor discovery cache	34
Router discovery	35
Path MTU discovery	36
Dynamic Host Configuration Protocol	36
Simple Network Time Protocol	36
Initial configuration using the Web quick start window	37
Auto-MDI X	38
Auto-polarity	38
Autosensing and autonegotiation	38
Custom Autonegotiation Advertisements	39
Power over Ethernet fundamentals	43
PoE overview	44
Power source	45
Stacking	45
Power pairs	46
Diagnosing and correcting PoE problems	46
Messages	46
Connecting the PSU	46
Power management	48
LLDP fundamentals	51
Link Layer Discover Protocol (IEEE 802.1ab) Overview	51
LLDP operational modes	52
Connectivity and management information	52
Procedures for system configuration	57
System configuration with NNCLI	57
General switch administration with NNCLI	57
Changing switch software in NNCLI	91
Configuration files in NNCLI	93
Automatically downloading a configuration file with NNCLI	95
Terminal setup	96
Setting the default management interface	97
Setting Telnet access	97
Setting boot parameters	100
Defaulting to BootP-when-needed	101
Shutdown command	102

NNCLI Help	103
Clearing the default TFTP server with NNCLI	103
Configuring a default TFTP server with NNCLI	103
Configuring daylight savings time with NNCLI	104
Configuring default clock source with NNCLI	105
Configuring Dual Agent with NNCLI	105
Configuring IPv6 with NNCLI	107
Configuring LLDP with NNCLI	122
Configuring local time zone with NNCLI	142
Configuring PoE detection method with NNCLI	143
Customizing NNCLI banner with NNCLI	146
Displaying the default TFTP server with NNCLI	147
Displaying complete GBIC information	147
Displaying hardware information	147
Configuring AUR with NNCLI	148
Agent Auto Unit Replacement (AAUR)	149
Enabling feature license files	150
Setting the server for Web-based management with NNCLI	151
Setting user access limitations	152
System configuration with Device Manager	155
Changing switch software in Device Manager	156
Configuration files in Device Manager	158
Automatically downloading a configuration file with Device Manager	163
General Switch Administration with Device Manager	163
Configuring LLDP with Device Manager	188
Configuring Auto Unit Replacement	237
Configuring local time zone	237
Configuring daylight savings time	238
Viewing topology information with Device Manager	239
Configuring IPv6 with Device Manager	240
Configuring PoE with Device Manager	254
Copying the license file	256
Customizing NNCLI banner	257
Viewing PoE ports with Device Manager	259
System configuration with Web-based management	260
Configuration files in Web-based management	260
General Switch Administration with Web-based management	263
Changing switch software in Web-based management	278
Configuring PoE with Web-based management	279
Configuring IPv6 with Web-based management	284
Managing remote access by IP address with Web-based management	285
Modifying system settings with Web-based management	285
Setting user access limitations with Web-based management	285

Configuration reference	291
Factory default configuration	291
Index	297

New in this release

The following sections detail what's new in Nortel Ethernet Routing Switch 5000 Series software release 6.0:

- ["Features" \(page 9\)](#)
- ["Other changes" \(page 10\)](#)

Features

See the following sections for feature changes:

- ["Dual Agent support" \(page 9\)](#)
- ["IPv6" \(page 9\)](#)

Dual Agent support

This feature provides support for two agents and configurations for either an Ethernet Routing Switch 5500 or 5600 series pure stack or for a mixed stack that contains both Ethernet Routing Switch 5500 and 5600 series switches. Dual Agent functionality is not supported on Ethernet Routing Switch 5510.

You can choose to have either Agent image boot the switch or stack when specified. In addition, you can specify when one agent image will become the primary (immediate, next reboot, or scheduled reboot).

For more information, see

- ["Boot agent image" \(page 22\)](#)

IPv6

In Release 6.0, the Ethernet Routing Switch 5000 Series supports IPv6. This feature provides dual stack support for both IPv4 and IPv6 addresses.

For more information, see

- ["IPv6 management" \(page 26\)](#)

Other changes

For information about changes that are not feature-related, see the following sections:

- ["Document changes" \(page 10\)](#)

Document changes

This document is modified to align with Nortel Customer Documentation Standards. For more information about these standards, see *Nortel Ethernet Routing Switch 5000 Series Documentation Roadmap*, NN47200-101.

Introduction

This document provides the information and procedures required to configure the software for the Ethernet Routing Switch 5000 Series.

Unless otherwise indicated, this information applies to:

- Nortel Ethernet Routing Switch 5510-24T
- Nortel Ethernet Routing Switch 5510-48T
- Nortel Ethernet Routing Switch 5520-24T-PWR
- Nortel Ethernet Routing Switch 5520-48T-PWR
- Nortel Ethernet Routing Switch 5530-24TFD
- Nortel Ethernet Routing Switch 5698-TFD
- Nortel Ethernet Routing Switch 5698-TFD-PWR
- Nortel Ethernet Routing Switch 5650-TD
- Nortel Ethernet Routing Switch 5650-TD-PWR
- Nortel Ethernet Routing Switch 5632-FD

The term "Ethernet Routing Switch 5000 Series" is used in this document to describe the features common to the switches mentioned above.

A switch is referred to by its specific name while describing a feature exclusive to the switch.

The Ethernet Routing Switch 5000 Series switches operate in the Stand-alone Mode and Stacking Mode in this product release. A switch can be in Stand-alone Mode or in Stacking Mode, not both.

NNCLI command modes

NNCLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration

- Interface Configuration
- Router Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter NNCLI in User EXEC mode and use the **enable** command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC 5530-24TFD>	No entrance command, default mode	exit or logout
Privileged EXEC 5530-24TFD#	enable	exit or logout
Global Configuration 5530-24TFD(config)#	configure	mode, enter: end or exit To exit NNCLI completely, enter: logout
Interface Configuration 5530-24TFD(config-if)# interface vlan	From Global Configuration mode: To configure a port, enter: interface fastethernet <port number> To configure a VLAN, enter: interface fastethernet <vlan number>	To return to Global Configuration mode, enter: Exit To return to Privileged EXEC mode, enter: end To exit NNCLI completely, enter: logout
Router Configuration 5530-24TFD(config-if)#	From Global Configuration mode: To configure OSPF, enter: router ospf	To return to Global Configuration mode, enter: Exit

Command mode and sample prompt	Entrance commands	Exit commands
	To configure RIP, enter: router rip To configure VRRP, enter: router vrrp	To return to Privileged EXEC mode, enter: end To exit NNCLI completely, enter: logout

See *Nortel Ethernet Routing Switch 5000 Series Fundamentals* (NN47200-104) for more information about NNCLI command modes.

Navigation

- ["System configuration fundamentals" \(page 15\)](#)
- ["Power over Ethernet fundamentals" \(page 43\)](#)
- ["LLDP fundamentals" \(page 51\)](#)
- ["Procedures for system configuration" \(page 57\)](#)
- ["Configuration reference" \(page 291\)](#)

System configuration fundamentals

The following sections contain system configuration fundamentals for the Nortel Ethernet Routing Switch 5000 Series.

Feature licensing

With Release 6.0 software, you must have an Advanced License or a Trial license to enable certain features. These software licenses support the following five features:

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

For more information about licenses, see *Nortel Ethernet Switch 5000 Fundamentals* (NN47200-104).

Trial license

Release 6.0 offers a Trial 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.

For more information about licenses, see *Nortel Ethernet Switch 5000 Fundamentals* (NN47200-104).

User access limitations

NNCLI 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 NNCLI before you begin these tasks.

Customizing NNCLI banner

The banner presented when a user logs in to the switch through NNCLI 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 NNCLI banner with NNCLI, refer to the following procedures:

- ["show banner command" \(page 146\)](#)
- ["banner command" \(page 146\)](#)
- ["no banner command" \(page 147\)](#)

To customize NNCLI banner with Device Manager, refer to the following procedures:

- ["Banner tab" \(page 257\)](#)
- ["Custom Banner tab" \(page 258\)](#)

TFTP server

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:

- ["Configuring a default TFTP server with NNCLI" \(page 103\)](#)
- ["Displaying the default TFTP server with NNCLI" \(page 147\)](#)
- ["Clearing the default TFTP server with NNCLI" \(page 103\)](#)

Configuration downloads to a switch

The following sections provide information about configuration downloads.

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 Web-based management or NNCLI.

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 you change the switch software on a Nortel Ethernet Routing Switch 5530-24TFD or 5600 series with software stored on 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 you use the NNCLI, ensure that NNCLI is in **Privileged EXEC** mode.
- If you use Web-based management, ensure that you have **read-write** access.

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

- ["Changing switch software in NNCLI" \(page 91\)](#)
- ["Changing switch software in Device Manager" \(page 156\)](#)
- ["Changing switch software in Web-based management" \(page 278\)](#)
- ["LED activity during software download" \(page 17\)](#)

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.

Unit quick configuration feature

You can use the quick configuration commands to automatically integrate a new unit into a stack. See ["New Unit Quick Configuration" \(page 61\)](#) for more information and the commands.

ASCII configuration file

With the Nortel Ethernet Routing Switch 5500 Series you can download a user-editable ASCII configuration file from a TFTP server.

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

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

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

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

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

See "[Retrieving an ASCII configuration file](#)" (page 159) for more information and the NNCLI commands.

Multiple switch configuration management

The Nortel Ethernet Routing Switch 5000 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.

- "[show nvram block command](#)" (page 60)
- "[copy config nvram block command](#)" (page 60)
- "[copy nvram config block command](#)" (page 60)

Stacking fundamentals

Stacking capabilities

You can use the Nortel Ethernet Routing Switch 5000 Series switches in either of the following configurations:

- stand-alone
- stack

The Nortel Ethernet Routing Switch 5000 Series switches have a built-in cascade port to stack up to eight units.

A stack can consist of any combination of Nortel Ethernet Routing Switch 5000 Series switches.

ATTENTION

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

To set up a stack, perform the following procedure.

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

ATTENTION

In a hybrid stack of Nortel Ethernet Routing Switch 5000 Series, you must set an Nortel Ethernet Routing Switch 5600 Series switch type as the base unit.

—End—

Stack monitor

Release 6.0 provides two modes of operation for Nortel Ethernet Routing Switch 5000 Series stacks.

- Pure
- Hybrid

You can create a pure stack with up to eight Ethernet Routing Switch 5500 Series switches or eight Nortel Ethernet Routing Switch 5600 Series switches. .

You can create a hybrid or mixed stack of up to eight switches that is a combination of Ethernet Routing Switch 5500 Series switches and Ethernet Routing Switch 5600 Series switches.

ATTENTION

In a hybrid stack of Nortel Ethernet Routing Switch 5000 Series, you must set an Nortel Ethernet Routing Switch 5600 Series switch type as the base unit.

Stack manager is responsible for the following functions that form and maintain a stack.

- Base unit selection.
- Unit discovery.
- Unit number assignment.
- Database exchange.
- Join stack handling.
- Programming the hardware for the stack to function as a system.

Stack manager also handles link events from the Hello module when a unit is added or removed from the stack. Based on the event, the stack manager again runs through the state machine to discover the newly added unit or change the stack configuration. Stack manager supports following stack configurations:

- Ring topology: All the units are connected as a ring.
- Upstream: All the non-base units are upstream to the base unit.
- Downstream: All the non-base units are downstream to the base unit.
- Up Down: Non base units are both upstream and downstream of the base unit.

Stack manager supports a maximum of eight switches in a pure or hybrid stack. Although the design does not restrict the number of ports in a stack, Nortel recommends that the number does not exceed 400 ports.

To create a hybrid stack, you must first set the mode parameter on the Ethernet Routing Switch 5600 Series switches to mixed mode. Ethernet Routing Switch 5500 Series switches do not have a mode parameter.

See [<insert link>](#) for more information about the stack manager and the procedure and NNCLI commands to set the stack manager.

Auto Unit Replacement (AUR)

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

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

ATTENTION

For Auto Unit Replacement to function properly, the new unit and the existing units in the stack must all run the same version of software. AUR 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 AUR does not load the configuration of the failed unit if it is replaced.

You can disable AUR with NNCLI. The switch retains the AUR state after a reset.

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—

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

See "[Agent Auto Unit Replacement \(AAUR\)](#)" (page 149) for more information about AAUR and the NNCLI commands.

IP blocking

Along with IP Routing, you can use Blocking Mode in two modes: full and none. The following paragraphs show how blocking mode acts for a stack.

You have a stack with IP Routing enabled and some Layer 3 VLANs. Assign VLANs ports from all the units. Set IP blocking-mode to Full on the base unit. Remove all the units from stack. All of the units will run in Layer 2 mode. No Layer 3 settings will be available on these units.

You have a stack with IP Routing enabled, and some Layer 3 VLANs. Assign VLANs ports from all the units. Set the IP blocking-mode to None on the base unit. Remove all of the units from stack. The Layer 3 settings made on the stack will be available on these units. By default IP blocking-mode is None.

Boot agent image

The Dual Agent feature provides support for two agents for Ethernet Routing Switch 5500 or 5600 series in stand-alone, pure stack or for a mixed (hybrid) stack configuration. Dual Agent functionality is not supported on Ethernet Routing Switch 5510.

The Dual Agent feature provides two agent images, the Agent Primary image and the Agent Secondary image. The Agent Primary image represents the agent image used for the next boot. User is able to select either image for the next boot.

An Ethernet Routing Switch 56xx unit has two combo images in the flash. In another word, an Ethernet Routing Switch 5600 unit has two Ethernet Routing Switch 56xx agent images and two Ethernet Routing Switch 55XX agent images in the flash. An Ethernet Routing Switch 55XX unit has two Ethernet Routing Switch 55XX images in the flash.

In a mixed stack with both Ethernet Routing Switch 5500 units and Ethernet Routing Switch 5600 units, an Ethernet Routing Switch 5600 must be the base unit. For a mixed stack to use the Dual Agent feature, the following conditions must be met:

- All Ethernet Routing Switch 5600 units must have the same agent software version.
- All Ethernet Routing Switch 5500 units must have the same agent software version.
- All unit agent software must have the same Interop Software Version Number (ISVN).

Special Case: If an Ethernet Routing Switch 5510 is the base unit, Dual Agent is disabled in the stack.

The Dual Agent Boot flag determines which agent image is the boot image. The diagnostics and agent software must use the same value for the Dual Agent Boot flag.

If the Dual Agent Boot flag is not set, the unit will boot from Agent 1 (default).

Next Boot image and system Boot-up in Dual Agent

The Next Boot image in Dual Agent is an agent image that is stored in the flash memory to be used for the next boot. In Dual Agent, there are two agent images in the flash memory, but only one image is assigned as the Next Boot image at a time.

When an agent image is downloaded to the switch, the unit resets and boots up with the newly downloaded image regardless of the value of the Next Boot image indicator. If an agent image is downloaded to the switch without a reset of the unit, the newly downloaded image becomes the Next Boot image.

You can change the Next Boot image at any time. The Next Boot image indicator (a value to indicate which agent image in the flash memory is used in the next boot) is stored in the NVRAM. This value, combined with other factors in the stack discovery process, determines which Dual Agent image the switch uses.

System boot-up for stand-alone

A stand-alone unit boots up with the Next Boot image from the NVRAM.

System boot-up for stack

The following lists the boot-up sequence:

- All the units in the stack start up with the Next Boot image.
- The stack does the following operations in the stack discovery phase:
 - The Next Boot image in the BU is used as the reference image.
 - If the Next Boot image in the NBU matches with the BU Next Boot image, the NBU continue to boot with the current Next Boot image.
 - If both images in the NBU do not match with the BU Next Boot image, the unit continues to boot with the current Next Boot image.
 - If the Next Boot image in the NBU does not match with the BU Next Boot image, but the other image in the NBU is matched, the matched image is selected as the Next Boot image then the unit is reset.

Dual Agent and Ethernet Routing Switch 5510

Dual Agent supports an Ethernet Routing Switch 5510 NBU with AAUR.

The following example shows how Dual Agent uses AAUR in a stack that contains Ethernet Routing Switch 5510 NBUs if you toggle the Next Boot image:

- All units in the stack reset with the new Next Boot image except for the Ethernet Routing Switch 5510 NBUs that will reset with only the agent image because they do not have the second image.
- All the units join stack except for the Ethernet Routing Switch 5510 units that now become stand-alone units because the agent image is now different from the one from in the stack.
- The Ethernet Routing Switch 5510 stand-alone units get the new image from the stack through AAUR and join the stack.

The following graphic shows what happens when you toggle the Next Boot image:

Figure 1
show boot image

```
5650TD (config)#show boot image
```

UNIT	PRIMARY	SECONDARY	ACTIVE
1	6.0.0.141	6.0.0.140	6.0.0.141
2	6.0.0.141	6.0.0.140	6.0.0.141
3	6.0.0.141	6.0.0.140	6.0.0.141

```
5650TD (config)#toggle-next-boot-image
5650TD (config)#show boot image
```

UNIT	PRIMARY	SECONDARY	ACTIVE
1	6.0.0.140	6.0.0.141	6.0.0.141
2	6.0.0.140	6.0.0.141	6.0.0.141
3	6.0.0.140	6.0.0.141	6.0.0.141

```
5650TD (config)#boot
```

After the restart, the device starts up with version 6.0.0.140. This becomes the active image

Figure 2
show boot image after restart

```
5650TD (config)#show boot image
```

UNIT	PRIMARY	SECONDARY	ACTIVE
1	6.0.0.140	6.0.0.141	6.0.0.140
2	6.0.0.140	6.0.0.141	6.0.0.140
3	6.0.0.140	6.0.0.141	6.0.0.140

Combination image

The Combination (Combo) Agent Image contains the header of the image and two agent images, a 56xx agent image and a 55XX agent image.

Download combination image

Any 55xx software release before release 6.0 does not support the Combo image.

A stand-alone unit or a stack that uses the Ethernet Routing Switch 5000 Series Software Release 6.0 can download a combo image. Release 6.0 is available in two different formats: a file in Combo format version 6.0 and a file in 55xx image format version 6.0.

The 55xx image format in this release is necessary because not all of the current 55xx releases support the Combo image.

Ethernet Routing Switch 5600 stand-alone

The unit downloads the combo image through the TFTP or USB port then stores the image in a flash device.

Ethernet Routing Switch 5000 Series mixed stack

The base unit receives the combo image through the TFTP or USB port then transfers the image to the non-base units. The Ethernet Routing Switch 5600 unit non-base units receive the combo image and the Ethernet Routing Switch 5500 non-base units receive the 5500 series image that is extracted from the combo image.

All of the units in the stack store the received image in flash devices.

Ethernet Routing Switch 5500 stand-alone

The unit extracts the 5500 series image from the combo image through the TFTP or USB port then stores the image in a flash device.

Ethernet Routing Switch 5000 Series mixed stack

The base unit extracts the 5500 series image through the TFTP or USB port then transfers the image to the non-base units.

All of the units in the stack store the received image in flash devices.

Combo Diagnostic Image

The Combo Diagnostic Image contains the header of the image and two Diagnostic images: a 56xx diagnostic image and a 55xx diagnostic image.

Any 55xx software release before release 6.0 does not support the Combo Diagnostic image.

A stand-alone unit or a stack that uses the Ethernet Routing Switch 5000 Series software release 6.0 can download a combo diagnostic image.

This diagnostic release for the new software release 6.0 is available in two different formats: a file in Combo format and a file in 55xx format. The 55xx image format in this release is necessary because all the current 55xx releases do not support the Combo diagnostic image.

The considerations for downloading a Combo Agent Image also apply to downloading a Combo Diagnostic Image.

Supported BootP modes

BootP mode

The Nortel Ethernet Routing Switch 5000 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 5000 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 5000 Series BootP requests.

The BootP modes supported by the Nortel Ethernet Routing Switch 5000 Series are:

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

IPv6 management

This module provides information about the IPv6 management feature of the Nortel Ethernet Routing Switch 5000 Series switch platforms.

Navigation

- ["The IPv6 header" \(page 27\)](#)
- ["IPv6 addresses" \(page 28\)](#)
- [Figure 3 "IPv6 address format" \(page 28\)](#)

- "Interface ID" (page 28)
- "Address formats" (page 28)
- "IPv6 extension headers" (page 29)
- "Comparison of IPv4 and IPv6" (page 30)
- "ICMPv6" (page 31)
- "Neighbor discovery" (page 31)
- "ND messages" (page 32)
- "Neighbor discovery cache" (page 34)
- "Router discovery" (page 35)
- "Path MTU discovery" (page 36)

IPv6 Management allows the user to configure an IPv6 address on the management VLAN. This enables IPv6 connectivity. The management VLAN can have both an IPv4 and an IPv6 address configured simultaneously (Ethernet Routing Switch 5000 Series switches function as a dual stack network node).

There is no IPv6 routing support in the current phase and therefore only one IPv6 interface is associated to the management VLAN. You can perform IPv6 interface configuration with NNCLI, SNMP (Device Manager) or Web-based management. Web-based management is limited to enabling and configuring address and prefix. For more control over IPv6, use NNCLI or Device Manager.

IPv6 Management adds support for new standard MIBs (IP-MIB — RFC 4293, TCP-MIB — RFC 4022, UDP-MIB — RFC 4113) as well as the enterprise MIB rclpv6.

The IPv6 header

The IPv6 header contains the following fields:

- a 4-bit Internet Protocol version number, with a value of 6
- an 8-bit traffic class field, similar to Type of Service in IPv4
- a 20-bit flow label that identifies traffic flow for additional Quality of Service (QoS)
- a 16-bit unsigned integer, the length of the IPv6 payload
- an 8-bit next header selector that identifies the next header
- an 8-bit hop limit unsigned integer that decrements by 1 each time a node forwards the packet (nodes discard packets with hop limit values of 0)

- a 128-bit source address
- a 128-bit destination address

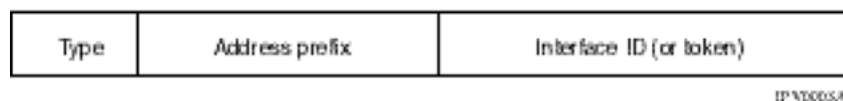
IPv6 addresses

IPv6 addresses are 128 bits in length. The address identifies a single interface or multiple interfaces. IPv4 addresses, in comparison, are 32 bits in length. The increased number of possible addresses in IPv6 solves the inevitable IP address exhaustion inherent to IPv4.

The IPv6 address contains two parts: an address prefix and an IPv6 interface ID. The first 3 bits indicate the type of address that follows.

The following graphic shows the IPv6 address format.

Figure 3
IPv6 address format



An example of a unicast IPv6 address is 1080:0:0:0:8:8000:200C:417A

Interface ID

The interface ID is a unique number that identifies an IPv6 node (a host or a router). For stateless autoconfiguration, the ID is 64 bits in length.

In IPv6 stateless autoconfiguration, the interface ID is derived by a formula that uses the link layer 48-bit MAC address. (In most cases, the interface ID is a 64-bit interface ID that contains the 48-bit MAC address.) The IPv6 interface ID is as unique as the MAC address.

If you manually configure interface IDs or MAC addresses (or both), no relationship between the MAC address and the interface ID is necessary. A manually configured interface ID can be longer or shorter than 64 bits.

Address formats

The format for representing an IPv6 address is

n:n:n:n:n:n:n

n is the hexadecimal representation of 16 bits in the address. An example is as follows:

FF01:0:0:0:0:0:43

Each nonzero field must contain at least one numeral. Within a hexadecimal field, however, leading zeros are not required.

Certain classes of IPv6 addresses commonly include multiple contiguous fields containing hexadecimal 0. The following sample address includes five contiguous fields containing zeroes with a double colon (::):

```
FF01::43
```

You can use a double colon to compress the leading zero fields in a hexadecimal address. A double colon can appear once in an address.

An IPv4-compatible address combines hexadecimal and decimal values as follows:

```
x:x:x:x:x:d.d.d.d
```

x:x:x:x:x is a hexadecimal representation of the six high-order 16-bit pieces of the address, and d.d.d.d is a decimal representation of the four 8-bit pieces of the address. For example:

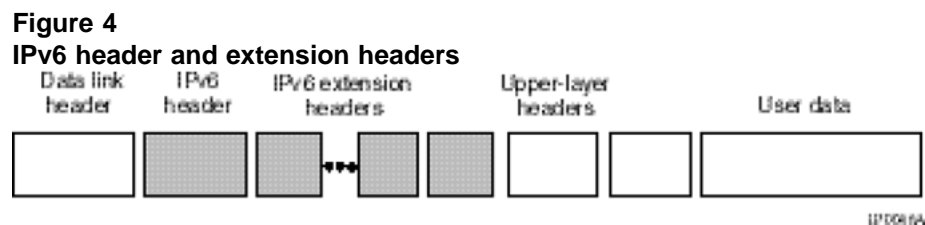
```
0:0:0:0:0:0:13.1.68.3
```

or

```
::13.1.68.3
```

IPv6 extension headers

IPv6 extension headers describe processing options. Each extension header contains a separate category of options. A packet can include zero or more extension headers. The following graphic shows the IPv6 header and extension headers:



IPv6 examines the destination address in the main header of each packet it receives; this examination determines whether the router is the packet destination or an intermediate node in the packet data path. If the router is the destination of the packet, IPv6 examines the header extensions that contain options for destination processing. If the router is an intermediate node, IPv6 examines the header extensions that contain forwarding options.

By examining only the extension headers that apply to the operations it performs, IPv6 reduces the amount of time and processing resources required to process a packet.

IPv6 defines the following extension headers:

- The hop-by-hop extension header contains optional information that all intermediate IPv6 routers examine between the source and the destination.
- The end-to-end extension header contains optional information for the destination node.
- The source routing extension header contains a list of one or more intermediate nodes that define a path for the packet to follow through the network, to its destination. The packet source creates this list. This function is similar to the IPv4 source routing options.
- The fragmentation extension header uses an IPv6 source to send packets larger than the size specified for the path maximum transmission unit (MTU).
- The authentication extension header and the security encapsulation extension header, used singly or jointly, provide security services for IPv6 datagrams.

Comparison of IPv4 and IPv6

The following table compares key differences between IPv4 and IPv6.

Table 1
IPv4 and IPv6 differences

Feature	IPv4	IPv6
¹ Ethernet Routing Switch 5000 Series does not support IPsec. ² Ethernet Routing Switch 5000 Series does not perform Router discovery or advertise as a router. ³ Ethernet Routing Switch 5000 Series does not implement any form of automatic configuration of IPv6 address in release 6.0.		
Address length	32 bits	128 bits
IPsec support ¹	Optional	Required
QoS support	Limited	Improved
Fragmentation	Hosts and routers	Hosts only
Minimum MTU (packet size)	576 bytes	1280 bytes
Checksum in header	Yes	No
Options in header	Yes	No
Link-layer address resolution	ARP (broadcast)	Multicast Neighbor Discovery Messages

Feature	IPv4	IPv6
Multicast membership	IGMP	Multicast Listener Discovery (MLD)
Router discovery ²	Optional	Required
Uses broadcasts	Yes	No
Configuration ³	Manual, DHCP	Automatic, DHCP

ICMPv6

Internet Control Message Protocol (ICMP) version 6 maintains and improves upon features from ICMP for IPv4. ICMPv6 reports the delivery of forwarding errors, such as destination unreachable, packet too big, time exceeded, and parameter problem. ICMPv6 also delivers information messages such as echo request and echo reply.

ATTENTION

ICMPv6 plays an important role in IPv6 features such as neighbor discovery, Multicast Listener Discovery, and path MTU discovery.

Neighbor discovery

IPv6 nodes (routers and hosts) on the same link use neighbor discovery (ND) to discover link layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided for IPv4 with the Address Resolution Protocol (ARP) and router discovery. Neighbor discovery replaces ARP in IPv6.

Hosts use ND to discover the routers in the network that you can use as the default routers, and to determine the link layer address of their neighbors attached on their local links. Routers also use ND to discover their neighbors and their link layer information. Neighbor discovery also updates the neighbor database with valid entries, invalid entries, and entries migrated to different locations.

Neighbor discovery protocol provides you with the following:

- Address and prefix discovery: hosts determine the set of addresses that are on-link for the given link. Nodes determine which addresses or prefixes are locally reachable or remote with address and prefix discovery.
- Router discovery: hosts discover neighboring routers with router discovery. Hosts establish neighbors as default packet-forwarding routers.
- Parameter discovery: host and routers discover link parameters such as the link MTU or the hop limit value placed in outgoing packets.

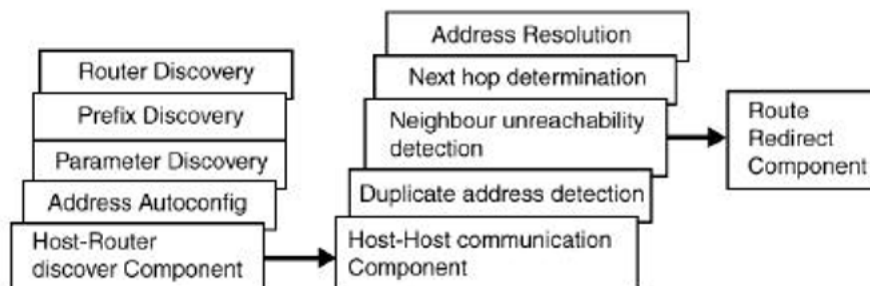
- Address autoconfiguration: nodes configure an address for an interface with address autoconfiguration.
- Duplicate address detection: hosts and nodes determine if an address is assigned to another router or a host.
- Address resolution: hosts determine link layer addresses (MAC for Ethernet) of the local neighbors (attached on the local network), provided the IP address is known.
- Next-hop determination: hosts determine how to forward local or remote traffic with next-hop determination. The next hop can be a local or remote router.
- Neighbor unreachability detection: hosts determine if the neighbor is unreachable, and address resolution must be performed again to update the database. For neighbors you use as routers, hosts attempt to forward traffic through alternate default routers.
- Redirect: routers inform the host of more efficient routes with redirect messages.

Neighbor discovery uses three components:

- host-router discovery
- host-host communication component
- redirect

The following graphic shows the neighbor discovery components:

Figure 5
Neighbor discovery components



ND messages

The following table shows new ICMPv6 message types.

Table 2
IPv6 and IPv4 neighbor comparison

IPv4 neighbor function	IPv6 neighbor function	Description
ARP Request message	Neighbor solicitation message	A node sends this message to determine the link-layer address of a neighbor or to verify that a neighbor is still reachable through a cached link-layer address. You can also use neighbor solicitations for duplicate address detection.
ARP Reply message	Neighbor advertisement	A node sends this message either in response to a received neighbor solicitation message or to communicate a link layer address change.
ARP cache	Neighbor cache	The neighbor cache contains information about neighbor types on the network.
Gratuitous ARP	Duplicate address detection	A host or node sends a request with its own IP address to determine if another router or host uses the same address. The source receives a reply from the duplicate device. Both hosts and routers use this function.
Router solicitation message (optional)	Router solicitation (required)	The host sends this message upon detecting a change in a network interface operational state. The message requests that routers generate router advertisement immediately rather than at the scheduled time.
Router advertisement message (optional)	Router advertisement (required)	Routers send this message to advertise their presence together with various links and Internet parameters either periodically or in response to a router solicitation message. Router advertisements contain prefixes that you use for on-link

IPv4 neighbor function	IPv6 neighbor function	Description
		determination or address configuration, and a suggested hop limit value.
Redirect message	Redirect message	Routers send this message to inform hosts of a better first hop for a destination.

Neighbor discovery cache

The neighbor discovery cache lists information about neighbors in your network.

The neighbor discovery cache can contain the following types of neighbors:

- static: a configured neighbor
- local: a device on the local system
- dynamic: a discovered neighbor

The following table describes neighbor cache states.

Table 3
Neighbor cache states

State	Description
Incomplete	A node sends a neighbor solicitation message to a multicast device. The multicast device sends no neighbor advertisement message in response.
Reachable	You receive positive confirmation within the last reachable time period.
Stale	A node receives no positive confirmation from the neighbor in the last reachable time period.
Delay	A time period longer than the reachable time period passes since the node received the last positive confirmation, and a packet was sent within the last DELAY_FIRST_PROBE_TIME period. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME period

State	Description
	of entering the DELAY state, neighbor solicitation is sent and the state is changed to PROBE.
Probe	Reachability confirmation is sought from the device every retransmit timer period.

The following events involve Layer 2 and Layer 3 interaction when processing and affect the neighbor cache:

- flushing the Virtual Local Area Network (VLAN) media access control (MAC)
- removing a VLAN
- performing an action on all VLANs
- removing a port from a VLAN
- removing a port from a spanning tree group (STG)
- removing a multi-link trunk group from a VLAN
- removing a Multi-Link Trunking port from a VLAN
- removing a Multi-Link Trunking port from an STG
- performing an action that disables a VLAN, such as removing all ports from a VLAN
- disabling a tagged port that is a member of multiple routable VLANs

Router discovery

IPv6 nodes discover routers on the local link with router discovery. The IPv6 router discovery process uses the following messages:

- Router advertisement
- Router solicitation

Router advertisement

Configured interfaces on an IPv6 router send out router-advertisement messages. Router-advertisements are also sent in response to router-solicitation messages from IPv6 nodes on the link.

Router solicitation

An IPv6 host without a configured unicast address sends router solicitation messages.

Path MTU discovery

IPv6 routers do not fragment packets. The source node sends a packet equal in size to the maximum transmission unit (MTU) of the link layer. The packet travels through the network to the destination. If the packet encounters a link with a smaller MTU, the router sends the source node an ICMP error message containing the MTU size of the next link.

The source IPv6 node then resends a packet equal to the size of the MTU included in the ICMP message.

The default MTU value for a regular interface is 1500.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) 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 5000 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.

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.

Initial configuration using the Web quick start window

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)

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 5000 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 5000 Series are autosensing and autonegotiating devices:

- The term *autosense* refers to ability of a port 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 5000 Series reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the Nortel Ethernet Routing Switch 5000 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 5000 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 with NNCLI

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 40) 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 40) and "show auto-negotiation-advertisements command sample output" (page 41) 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 41) and "show auto-negotiation-capabilities command sample output" (page 42) 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 42) and ["no auto-negotiation-advertisements command sample output"](#) (page 42) 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)#
```

Power over Ethernet fundamentals

The information in this section provides an overview of Power over Ethernet (PoE). See the *Nortel Ethernet Routing Switch 5000 Series Installation* (NN47200-300) for detailed information about the installation of power supplies and details about PoE.

PoE in Nortel Ethernet Routing Switch 5000 Series switches uses the IEEE 802.3af standard.

PoE is the ability 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 following 5000 Series switches provide PoE:

- Ethernet Routing Switch 5520-24T-PWR
- Ethernet Routing Switch 5520-48T-PWR
- Ethernet Routing Switch 5650-TD-PWR
- Ethernet Routing Switch 5698-TFD-PWR

The 5000 Series switches support the following PoE features:

- DTE power.
- Powered device (PD) discovery and classification.
- Capacitive detection to support legacy PD devices, including the Nortel and Cisco Legacy IP Phones.
- Port power management and monitoring for each port.
- AC and DC disconnection.
- Detection of load over or under voltage or current.
- PoE status LED for each port.
- Port prioritizing to guarantee DTE power available on high-priority ports
- Port pruning to prevent system failure

You can configure PoE with NNCLI, Device Manager, and Web-based management. See the following sections for details:

- ["PoE overview" \(page 44\)](#)
- ["Power source" \(page 45\)](#)
- ["Stacking" \(page 45\)](#)
- ["Power pairs" \(page 46\)](#)
- ["Diagnosing and correcting PoE problems" \(page 46\)](#)
- ["Power management" \(page 48\)](#)
- ["Configuring PoE with NNCLI" \(page 143\)](#)
- ["Viewing PoE ports with Device Manager" \(page 259\)](#)

PoE overview

The 5000 Series switches are ideal to use with Nortel Business Communication Manager system, IP phones, hubs, and wireless access points. You can use these switches in conjunction with all network devices.

By using the 5000 Series switches, you can plug any IEEE 802.3af-compliant powered device into a front-panel port of a PoE-capable switch and receive power. Data can be passed simultaneously on that port.

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 5000 Series switches depends on your power configuration and the particular connected network devices. If you connect an IP device that requires more than 16 W of power, you see an error on that port notifying you of an overload.

The 5000 Series switches automatically detect 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 5000 Series switches operate 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 5000 Series switches provide 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 5000 Series switches automatically detect 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 W increments, from 3 W to 16 W.

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

Power source

The Nortel Ethernet Redundant Power Supply 15 is available as an optional external power source for the Ethernet Routing Switch 5520. 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:

- 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.

The 5650-TD-PWR and 5698-TFD-PWR switches use modular power supply units. The PoE capability at each 5600 Series switch port depends on the power supply modules that you install. See *Nortel Ethernet Routing Switch 5000 Series Installation* (NN47200-300) for information about the power supplies and PoE.

The PoE capability of each 5650-TD-PWR or 5698-TFD-PWR switch port depends on the power supply modules that you install. See the *Nortel Ethernet Routing Switch 5000 Series Installation* (NN47200-300) for information about the PoE capability at each port as a function of the power supply modules.

Stacking

You can stack the 5000 Series switches up to 8 units high. These stacks also can be configured for redundancy.

Power pairs

The 5000 Series switches support wiring as mentioned in the IEEE 802.3AF draft standard.

The 5000 Series switches supports power to Signal pair only.

See the *Nortel Ethernet Routing Switch 5000 Series Installation* (NN47200-300) for connector pinout tables and wiring specifics.

Diagnosing and correcting PoE problems

This section discusses some common problems that you can encounter while using the PoE features of the 5000 Series switches.

See the *Nortel Ethernet Routing Switch 5000 Series Troubleshooting* (NN47200-700) for detailed troubleshooting information.

Messages

"[Error messages displayed by PoE ports](#)" (page 46) 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—

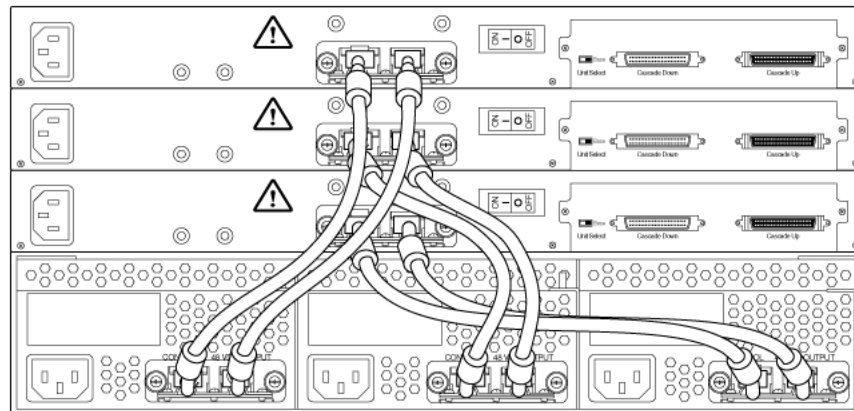
**CAUTION**

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 48) 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 5000 Series switch uses several device management systems, such as Web-based management, the Command Line Interface (NNCLI), and Device Manager, as well as Optivity for network-level management services.

With NNCLI, Web, or Device Manager, 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 5000 Series switch power
- A device is connected to port 21 and requests power

In this scenario, the 5000 Series switch 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.

LLDP fundamentals

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.

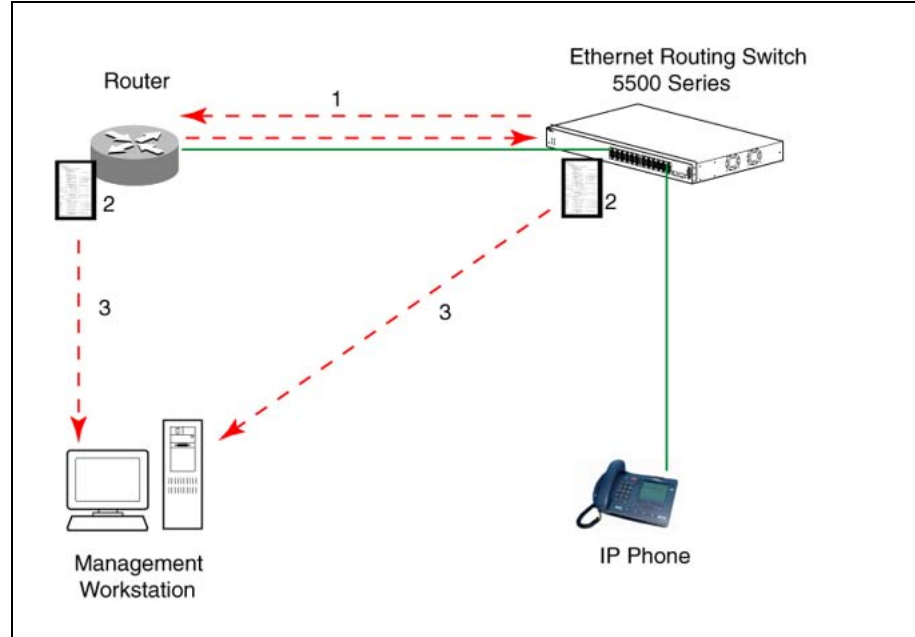
Each LLDP station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN (802.3 Ethernet with 5000 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 52) 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 and port IDs and system descriptions (if enabled) 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 NNCLI 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" \(page 53\)](#)
- ["IEEE 802.1 organizationally-specific TLVs" \(page 54\)](#)
- ["IEEE 802.3 organizationally-specific TLVs" \(page 54\)](#)
- ["Organizationally-specific TLVs for MED devices" \(page 54\)](#)

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 5000 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 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** provide switch information. 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

You can also use the `show sys-info` command to display information about the Inventory TLVs.

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.

Time to live interval The Time to live interval represents the tx-interval multiplied by the tx-hold-multiplier.

Med fast start Med fast start provides a burst of LLDPDU when the system initializes an LLDP MED transmission .

Procedures for system configuration

The following sections provide system configuration procedures.

Navigation

- ["System configuration with NNCLI" \(page 57\)](#)
- ["System configuration with Device Manager" \(page 155\)](#)
- ["System configuration with Web-based management" \(page 260\)](#)

System configuration with NNCLI

The following sections allow you to configure the system with NNCLI.

General switch administration with NNCLI

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

- ["Stack manager" \(page 58\)](#)
- ["Multiple switch configurations" \(page 60\)](#)
- ["New Unit Quick Configuration" \(page 61\)](#)
- ["IP blocking" \(page 62\)](#)
- ["Assigning and clearing IP addresses" \(page 63\)](#)
- ["Assigning and clearing IP addresses for specific units" \(page 67\)](#)
- ["Displaying interfaces" \(page 69\)](#)
- ["Setting port speed" \(page 69\)](#)
- ["Testing cables with the Time Domain Reflectometer" \(page 72\)](#)
- ["Enabling Autotopology" \(page 73\)](#)
- ["Enabling rate-limiting" \(page 77\)](#)
- ["Using Simple Network Time Protocol" \(page 79\)](#)
- ["Real time clock configuration" \(page 85\)](#)

- "Custom Autonegotiation Advertisements" (page 86)
- "Connecting to Another Switch" (page 88)
- "Domain Name Server (DNS) Configuration" (page 89)

Stack manager

Use the following procedures to integrate switches in a stack with the stack manager:

- "Configuring a pure stack with stack manager" (page 58)
- "Configuring a hybrid stack with stack manager" (page 58)

Configuring a pure stack with stack manager Use the following procedure to configure a pure stack with stack manager:

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

- | | |
|---|---|
| 1 | Upgrade the existing stack with release 6.0 software. |
|---|---|

—End—

Configuring a hybrid stack with stack manager Use the following procedure to configure a hybrid stack with stack manager:

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

- | | |
|---|--|
| 1 | Upgrade the existing stack with release 6.0 software. |
| 2 | Cable in one Ethernet Routing Switch 5600 Series switch into this stack.

<i>Once the new Ethernet Routing Switch 5600 Series switch joins the stack, it will have learned the entire configuration from the base unit and programmed its NVRAM. This switch can now be configured as base unit.</i> |
| 3 | To configure the Ethernet Routing Switch 5600 Series switch as the base unit, turn the power off to the whole stack and set the base unit switch on the Ethernet Routing Switch 5500 Series switch to Off and set the base unit switch on the Ethernet Routing Switch 5600 Series switch to On. |
| 4 | Turn the power on to the stack. The Ethernet Routing Switch 5600 Series switch is now the base unit in the stack.

<i>You can now add more than one Ethernet Routing Switch 5600 Series switch to the stack. You can add more Ethernet Routing</i> |

Switch 5600 Series switches to the stack up to the maximum of eight units.

—End—

show stack oper-mode An Ethernet Routing Switch 5000 Series stack is in one of two modes: Pure or Mixed.

This command is in the Global Configuration command mode.

The following procedure shows the stack operation mode with the **show stack oper-mode** command:

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

1	Enter show stack oper-mode
---	-----------------------------------

—End—

stack oper-mode {Pure|Mixed} You can configure the operating mode on all the Ethernet Routing Switch 5600 Series switches in the stack. Ethernet Routing Switch 5500 Series switches do not have a configurable operating mode as the software operates in only one mode.

This command is in the Global Configuration command mode.

This command is available only on the Ethernet Routing Switch 5600 Series switches in the stack or on an Ethernet Routing Switch 5600 Series stand-alone switch.

The following procedure configures the stack as Pure or Mixed with the **stack oper-mode {Pure|Mixed}** command:

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

1	Enter stack oper-mode {Pure Mixed} .
---	---

—End—

Job aid The following table defines the variables for the **stack oper-mode {Pure|Mixed}** command:

Table 4
stack oper-mode variable definitions

Variable	Definition
Pure	Sets stack manager for an Ethernet Routing Switch 5600 Series stack or stand-alone.
Mixed	Sets stack manager for a mixed Ethernet Routing Switch 5600 Series and Ethernet Routing Switch 5600 Series stack. Note: You must use an Ethernet Routing Switch 5600 Series switch as the base unit in a hybrid or mixed stack.

Multiple switch configurations

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

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 60) 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, use the New Unit Quick Configuration feature to create a default configuration that can be applied to any new unit entering a stack configuration.

You do not need to manually configure a new unit that is added to the existing stack.

However, if required, you can set the default values for VLAN Ids, port speed, duplex mode, PVID, tagging, and spanning tree groups on the new unit without the need to reset the stack during the process.

Note: All commands in this section are executed in the Global Configuration command mode except the `quickconfig start-recording` command which is executed in Privileged EXEC mode.

To configure and enable this feature with NNCLI, refer to the following commands:

- "quickconfig enable" (page 61)
- "no quickconfig enable" (page 61)
- "default quickconfig" (page 61)
- "quickconfig start-recording" (page 61)

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 The following 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 record a VLAN configuration or port configuration enter the following commands one on each line in NNCLI:

```
enable
config term
vlan port $/13-40 tag untagPvidonly
vlan create 10 name vlan_10 type port
vlan create 20 name vlan_20 type port
vlan members add 10 $/13-40
vlan members add 20 $/13-40
vlan ports $/13-40 pvid 10
interface fast $/13-34
speed 100
end
.
```



CAUTION

The first two commands must be `enable` and `config term`, otherwise the `config` commands that follow will not be applied.

Use `$` as a wild card for the slot. When you add a new unit to the stack the unit number is not known so the wild card character can match any slot number. To end the recording process enter a dot on a separate line in NNCLI.

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.

Use the following NNCLI commands to configure and manage IP blocking with NNCLI:

- "show ip-blocking" (page 62)
- "show ip blocking-mode" (page 63)
- "ip blocking-mode command" (page 63)
- "clear ip-blocking" (page 63)
- "default ip blocking-mode" (page 63)

show ip-blocking Use this command to show the current IP blocking state. The syntax for this command is

```
show ip-blocking
```

Execute this command in the User EXEC command mode.

show ip blocking-mode Use this command to show the current IP blocking parameters. The syntax for this command is

```
show ip blocking-mode
```

Execute this command in the User EXEC command mode.

ip blocking-mode command Use this command to set the level of ip blocking to perform in the stack. The syntax for this command is

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

The following table describes 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.

Execute this command in the Interface Configuration command mode.

clear ip-blocking Use this command to clear the current IP blocking-mode state. The syntax for this command is

```
clear ip-blocking
```

Execute this command in the Privileged EXEC command mode.

default ip blocking-mode Use this command to set the IP blocking mode to factory defaults. The syntax for this command is

```
default ip blocking-mode
```

Execute this command in the Global Configuration command mode.

Assigning and clearing IP addresses

You can assign, clear, and view IP addresses and gateway addresses with NNCLI. Use the following commands to perform various operations on IP and gateway addresses:

- ["ip address command" \(page 64\)](#)
- ["ip address source command" \(page 64\)](#)

- "no ip address command" (page 65)
- "ip default-gateway command" (page 66)
- "no ip default-gateway command" (page 66)
- "show ip command" (page 66)

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 64) 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.

ip address source command If you want to automatically obtain an IP address, subnet mask and default gateway on the switch or stack, you can use the `ip address` command with the `source` parameter. When you use DHCP, the switch or stack can also obtain up to three DNS server IP addresses.

The syntax for the `ip address source` command is


```
ip address source {bootp-always | bootp-last-address |
bootp-when-needed | configured-address | dhcp-always |
dhcp-last-address | dhcp-when-needed}
```

Execute the `ip address source` command in the Global Configuration command mode.

The following table describes the variables for the `ip address source` command:

Table 5
ip address source command variables

Variable	Description
bootp-always	Always use the bootp server.
bootp-last-address	Use the last bootp server.
bootp-when-needed	Use bootp server when needed.
dhcp-always	Always use the DHCP server.
dhcp-last-address	Use the last DHCP server.
dhcp-when-needed	Use DHCP client when needed.

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 65) 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 66) 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 67) 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 NNCLI to assign and clear IP addresses for a specific unit in a stack. For details, refer to the following:

- "ip address unit command" (page 67)
- "no ip address unit command" (page 68)
- "default ip address unit command" (page 68)

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 68) 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 68) 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 69) 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 Multi-Link 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 69) 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 with NNCLI, refer to the following:

- "[speed command](#)" (page 70)
- "[default speed command](#)" (page 70)
- "[duplex command](#)" (page 71)
- "[default duplex command](#)" (page 72)

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 70) 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 71) 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 71) 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 72) 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

The Nortel Ethernet Routing Switch 5000 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 NNCLI or Device Manager.

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. If the cable has a 10/100 MB/s link, the test results may be incomplete as the test does not test all of the pins in the connector. Use of the TDR does not affect 1 GB/s links.

See the *Nortel Ethernet Routing Switch Troubleshooting Guide* (NN47200-700) for more information on troubleshooting cables and for connector pin tables.

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 NNCLI commands, you can initiate a TDR cable diagnostic test and obtain test reports.

- "tdr test command" (page 73)
- "show tdr command" (page 73)

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 with NNCLI.

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 with NNCLI, refer to the following:

- "autotopology command" (page 73)
- "no autotopology command" (page 74)
- "default autotopology command" (page 74)
- "show autotopology settings command" (page 74)
- "show autotopology nmm-table command" (page 74)

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 5000 Series, can control traffic on this port using the `flowcontrol` command.

To enable flow control with NNCLI, refer to the following:

- ["flowcontrol command" \(page 75\)](#)
- ["no flowcontrol command" \(page 76\)](#)
- ["default flowcontrol command" \(page 76\)](#)

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" \(page 75\)](#) 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. • auto--sets the port to automatically determine the flow control mode (default). • disable--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 76) describes the parameters for this command.

No flowcontrol parameters

Parameters and variables	Description
port <portlist>	Specifies the port numbers for which to disable flow control. Note: If you omit this parameter, the system uses the ports you specified in the <code>interface</code> command, but only those ports that have speed set to 1000/full.

default flowcontrol command 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 76) 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 with NNCLI. For details, refer to the following:

- ["show rate-limit command" \(page 77\)](#)
- ["rate-limit command" \(page 77\)](#)
- ["no rate-limit command" \(page 78\)](#)
- ["default rate-limit command" \(page 78\)](#)

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" \(page 77\)](#) 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.

Parameters and values	Description
	Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.
multicast <pct> broadcast <pct> both <pct>	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 For 10 Gb/s links, the default value for limiting both broadcast and multicast is 10 percent.

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 78) 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. <p>Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.</p>

default rate-limit command The `default rate-limit` command restores the rate-limiting value for the specified port to the default setting.

The syntax for the `default rate-limit` command is:

```
default rate-limit [port <portlist>]
```

The `default rate-limit` command is executed in the Interface Configuration command mode.

"Default rate-limit parameters" (page 79) describes the parameters for this command.

Default rate-limit parameters

Parameters	Description
port <portlist>	<p>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.</p> <p>Note: If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.</p>

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 80)
- "show sys-info command" (page 80)
- "SNTP enable command" (page 80)
- "no SNTP enable command" (page 80)
- "SNTP server primary address command" (page 81)

- "SNTP server secondary address command" (page 81)
- "no SNTP server command" (page 81)
- "SNTP sync-now command" (page 82)
- "SNTP sync-interval command" (page 82)
- "Configuring local time zone" (page 237)
- "Configuring daylight savings time" (page 83)

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 SNTP enable` command is:


```
no sntp enable
```

The `no SNTP enable` command is executed in the Global Configuration command mode.

SNTP server primary address command The `SNTP server primary address` command specifies the IP addresses of the primary NTP server.

The syntax for the `SNTP server primary address` command is:

```
sntp server primary address [<ipv6_address> | <A.B.C.D>]
```

The `SNTP server primary address` command can be executed in the Global Configuration command mode.

"[SNTP server primary address parameters](#)" (page 81) 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 `SNTP server secondary address` command specifies the IP addresses of the secondary NTP server.

The syntax for the `SNTP server secondary address` command is:

```
sntp server secondary address [<ipv6_address> | <A.B.C.D>]
```

The `SNTP server secondary address` command is executed in the Global Configuration command mode.

"[SNTP server secondary address parameters](#)" (page 81) describes the parameters for this command.

SNTP server secondary address parameters

Parameters	Description
ipv6_address	Enter the IPv6 address of the secondary NTP server.
<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 82) 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 83) 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 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 NNCLI, set the global configuration mode. <code>configure</code>
2	Enable sntp server.
3	Set the date to change to daylight savings time. <code>clock summer-time zone date day month year hh:mm day month year hh:mm [offset]</code>

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 85)
- "Clock sync-rtc-with-SNTP enable command" (page 85)
- "no clock sync-rtc-with-SNTP enable" (page 86)
- "Default clock sync-rtc-with-SNTP enable" (page 86)
- "Clock source command" (page 86)
- "default clock source" (page 86)

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 85) 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 5000 Series as part of the auto-negotiation process.

The following sections describe configuring CANA with NNCLI:

- ["Configuring CANA" \(page 87\)](#)
- ["Viewing current autonegotiation advertisements" \(page 87\)](#)
- ["Viewing hardware capabilities" \(page 87\)](#)
- ["Setting default auto-negotiation-advertisements" \(page 87\)](#)

- "no auto-negotiation-advertisements command" (page 87)

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 <ipv6_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 88) shows the command parameters of the `ping` command.

ping command parameters and variables

Parameters and variables	Description
<ipv6_address dns_host_name>	The IPv6 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 NNCLI session. Communication can be established to only one external switch at a time using the `telnet` command.

The syntax for this command is:

```
telnet <ipv6_address | dns_host_name>
```

Substitute <ipv6_address | dns_host_name> with either the IPv6 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 89)
- "ip domain-name command" (page 89)
- "no ip domain-name command" (page 89)
- "default ip domain-name command" (page 90)
- "ip name-server command" (page 90)
- "no ip name-server command" (page 90)

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 [<ipv6_address> | <ip_address_1>
ip name-server [<ipv6_address> | <ip_address_2>]
ip name-server [<ipv6_address> | <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 90) outlines the parameters for this command.

ip name-server parameters

Parameter	Description
ipv6_address	The IPv6 address of the domain name server used by the switch.
<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 91) 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.

Changing switch software in NNCLI

To change the software version running on the switch with NNCLI, follow this procedure:

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

1	Access NNCLI through the Telnet protocol or a Console connection.
---	---

2	From the command prompt, use the download command with the following parameters to change the software version:
---	---

```
download [address <ipv6_address> | <a.b.c.d>] {primary
| secondary} {image <image name> |
image-if-newer <image name> | diag <image name> |
poe_module_image <image name>} [no-reset] [usb]
```

"[download parameters](#)" (page 92) explains the parameters for the `download` command.

download parameters

Parameter	Description
address <ipv6_address > <a.b.c.d>	This parameter is the IPv6 or 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.
primary secondary	This parameter determines if the image is the primary or secondary image.
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.
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 5000 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 or 5600 series switches, 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 93).

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 17).

Configuration files in NNCLI

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

For details, refer to the following:

- "Displaying the current configuration" (page 93)
- "Storing the current configuration" (page 93)
- "Restoring a system configuration" (page 94)
- "Saving the current configuration" (page 95)

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 5000 Series, the configuration file can be saved to a TFTP server. The

Nortel Ethernet Routing Switch 5530-24TFD or 5600 Series switches also provide 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 94) 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 the 5530-24TFD and 5600 series switches 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

NNCLI 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 94) 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 or 5600 Series switches, 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 95) 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.

Automatically downloading a configuration file with NNCLI

This feature is enabled through NNCLI 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 96) 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>
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.

Terminal setup

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

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 97) 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

You can set the default management interface with NNCLI 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

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

Note: Multiple users can access NNCLI 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 98)
- "no telnet-access command" (page 99)
- "default telnet-access command" (page 100)

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> <51-100>
<A.B.C.D> <WORD> [mask <A.B.C.D>]
```

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

The following table describes the parameters for the `telnet-access` command.

telnet-access parameters

Parameters	Description
enable disable	Enables or disables Telnet connection.
login-timeout <1-10>	Specify in minutes the time to wait for Telnet and Console login before the connection closes. 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.

Parameters	Description
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>] [source-ip <51-100> <WORD>]	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. Specify the source IPv6 address and prefix from which to allow connections.

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.

Using the following syntax for the `no telnet-access` command for an IPv4 address and mask pair:

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

Using the following syntax for the `no telnet-access` command for an IPv6 address and mask pair:

```
no telnet-access [source-ip [<51-100>]]
```

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

"[no telnet-access parameters](#)" (page 100) describes the parameters and variables for the `no telnet-access` command.

no telnet-access parameters

Parameters and variables	Description
source-ip [<1-50>] source-ip [<51-100>]	<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, the second to fiftieth indexes are set to 255.255.255.255/255.255.255.255, the fiftyfirst index is set to ::/0, and the fiftysecond to hundredth indexes are set to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128.</p> <p>When you specify a source-ip address, the specified pair is set to 255.255.255.255/255.255.255.255 for indexes between 1 and 50 and the specified pair is set to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 for indexes between 51 and 100.</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 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 101) 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 last reset count and reason for last reset; these two parameters do not default to factory defaults. Stack operational mode is retained only when resetting to partial-default.

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 NNCLI commands needed to configure BootP parameters:

- ["ip bootp server command" \(page 101\)](#)
- ["no ip bootp server command" \(page 102\)](#)
- ["default ip bootp server command" \(page 102\)](#)

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 102) 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.

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.

NNCLI Help

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

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

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

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

These commands are available in any command mode.

Clearing the default TFTP server with NNCLI

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.

Configuring a default TFTP server with NNCLI

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 [<ipv6_address> | <A.B.C.D>
```

To complete the command, replace either the `ipv6_address` or `<A.B.C.D>` with the IPv6 or IP address of the default TFTP server. This command must be executed in the Privileged EXEC command mode.

Configuring daylight savings time with NNCLI

Use the following procedure to configure the daylight savings time adjustment with NNCLI:

Step	Action
1	In NNCLI, set the Global Configuration command mode. <code>configure</code>
2	Enable sntp server.
3	Set the date to change to daylight savings time. <code>clock summer-time zone date day month year hh:mm day month year hh:mm [offset]</code>
—End—	

Job aid

The following table defines the variables for the `clock summer-time` command:

clock summer-time command variables

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.

Variables	Description
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.

set daylight savings time example

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.

```
clock summer-time BST date 28 Mar 2007 2:00 30 Aug 2007
15:00 +60
```

Configuring default clock source with NNCLI

This command sets the default clock source for the switch.

The syntax for this command is

```
clock source {rtp | sntp | sysUpTime}
```

Substitute {rtp | sntp | sysUpTime} with the clock source selection.

Run this command in Global Configuration command mode.

Configuring Dual Agent with NNCLI

Use the following procedures to configure the Dual Agent feature with NNCLI:

- ["Enhanced download command" \(page 105\)](#)
- ["Set the next boot Image" \(page 106\)](#)
- ["Show agent images" \(page 107\)](#)

Enhanced download command

You can update either active image or non-active image. Once the image download is done, the unit resets and restarts with the new image regardless of the value of the Next Boot image indicator. In case of image download without reset, the new image in the flash will be the Next Boot image.

To specify the download target image, use the following procedure:

download command

Step	Action
1	Enter <code>download [address <ipv6_address> <a.b.c.d>] {primary secondary} {image <image name> image-if-newer <image name> diag <image name> poe_module_image <image name>} [no-reset] [usb]</code>
—End—	

Job aid The following table defines the variables for the `download` command:

Table 6
download command variable definitions

Variable	Definition
ipv6_address	IPv6 IP address
a.b.c.d	IP address in dot notation.
primary secondary	Choose which image to download.
image <image name>	Download the specified image.
image-if-newer <image name>	Only download the image if the version is newer than the installed version.
diag <image name>	Download the specified diagnostic image.
poe_module_image <image name>	Download the specified PoE module image.
no-reset	Do not reset the switch.
usb	Download the image from the USB drive.

Note: Dual Agent supports the Ethernet Routing Switch 5510 NBUs through AAUR.

Set the next boot image

You can use NNCLI commands to change the next boot image of the device. Use the following procedures to change the next boot image:

- `toggle-next-boot-image`
- `boot secondary`

toggle-next-boot-image Use the following procedure to toggle the next boot image:

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

1	Enter <code>toggle-next-boot-image</code> .
---	---

You must restart the switch or stack after this command to use the next boot image as the new primary image.

—End—

boot secondary Use the following procedure to use the secondary boot image:

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

1	Enter <code>boot secondary</code> .
---	-------------------------------------

The switch or stack will restart automatically with the new image.

—End—

Show agent images

You can use NNCLI commands to list the following information about the agent images stored in flash memory:

- Primary image version
- Secondary mage name
- Active image version

To show the agent image information for agent images stored in the flash memory, use the following procedure:

show boot image command

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

1	Enter <code>show boot image</code> .
---	--------------------------------------

—End—

Configuring IPv6 with NNCLI

Use the following procedures to configure IPv6:

- ["Enabling IPv6 interface on the management VLAN" \(page 108\)](#)

- "Configuring IPv6 interface on the management VLAN" (page 109)
- "Displaying the IPv6 interface information" (page 109)
- "Displaying IPv6 interface addresses" (page 110)
- "Configuring an IPv6 address for a switch or stack" (page 111)
- "Displaying the IPv6 address for a switch or stack" (page 112)
- "Configuring IPv6 management interface" (page 113)
- "Disabling IPv6 globally" (page 114)
- "Displaying the global IPv6 configuration" (page 115)
- "Configuring an IPv6 default gateway for the switch or stack" (page 116)
- "Displaying the IPv6 default gateway" (page 116)
- "Configuring the IPv6 neighbor cache" (page 117)
- "Displaying the IPv6 neighbor information" (page 117)
- "Displaying IPv6 interface ICMP statistics" (page 118)
- "Displaying IPv6 interface statistics" (page 119)
- "Displaying IPv6 TCP statistics" (page 120)
- "Displaying IPv6 TCP connections" (page 121)
- "Displaying IPv6 TCP listeners" (page 121)
- "Displaying IPv6 UDP statistics and endpoints" (page 121)

You can only execute NNCLI commands for IPv6 interface configuration on the base unit of a stack. Use the Global Configuration mode to execute IPv6 commands.

Enabling IPv6 interface on the management VLAN

Use the following procedure to enable an IPv6 interface on the management VLAN:

Enabling IPv6 interface on the management VLAN

Step	Action
1	At the <code>config</code> prompt, enter <code>interface vlan 1</code> .
2	Enter <code>ipv6 interface enable</code> .
3	Enter <code>exit</code> to return to the main menu.

—End—

Use the following procedure to enable or disable ipv6 admin status and set icmp error interval:

ipv6 enable

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

- | | |
|---|---|
| 1 | Enter <code>ipv6 enable</code> |
| 2 | Enter <code>exit</code> to return to the main menu. |
-

—End—

Job aid The following table lists the variables and definitions for `ipv6 enable`:

Table 7
IPv6 variables and definitions

Variable	Definition
enable	Default admin status: enabled

Configuring IPv6 interface on the management VLAN

Use the following procedures to assign an IPv6 address to a VLAN:

config vlan

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

- | | |
|---|---|
| 1 | Go to the <code>config</code> prompt in NNCLI. |
| 2 | Enter <code>interface vlan 1</code> . |
| 3 | Enter <code>ipv6 interface enable</code> . |
| 4 | Enter <code>exit</code> to return to the main menu. |
-

—End—

Displaying the IPv6 interface information

Use the following procedure to display the IPv6 interface information:

show ipv6 interface

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

- | | |
|---|--|
| 1 | Enter <code>show ipv6 interface</code> . |
|---|--|
-

—End—

Job aid The following graphic shows the results of the `show ipv6 interface` command.

```
(config)#show ipv6 interface
-----
                                Interface Information
-----
IFINDX VLAN-ID MTU  PHYSICAL      ADMIN  OPER  RCHBLE  RETRAN  TYPE
                ADDRESS      STATE  STATE TIME   TIME
-----
10001  1          1522  0:11:f9:34:88:0  enabled up    30000  1000  ETHER

-----
                                Address Information
-----
INTF  IPV6                                TYPE  ORIGIN  STATUS
INDEX ADDRESS
-----
10001  3000:0:0:0:0:0:99                    UNICAST MANUAL  PREFERRED
10001  fe80:0:0:0:211:f9ff:fe34:8800        UNICAST OTHER  UNKNOWN

1 out of 1 Total Num of Interface Entries displayed.
2 out of 2 Total Num of Address Entries displayed.
```

Displaying IPv6 interface addresses

View IPv6 interface addresses to learn the addresses.

Prerequisites

Log on to the User EXEC mode in NNCLI.

Step Action

- 1 Use the following command to display IPv6 interface addresses:
`show ipv6 address interface [<WORD 0-45>]`
-

—End—

Job aid Use the data in the following table to help you use the `show ipv6 address interface` command.

Table 8
show ipv6 address interface variable definitions

Variable	Definition
[<word 0–45>]	Specifies the IPv6 address length assigned to the management interface.

The following table shows the field descriptions for this command.

Table 9
show ipv6 address interface command field descriptions

Field	Description
IPv6 ADDRESS	Specifies the IPv6 destination address.
TYPE	Specifies Unicast, the only supported type.
ORIGIN	Specifies a read-only value indicating the origin of the address. The origin of the address is other, manual, DHCP, linklayer, or random.
STATUS	Indicates the status of the IPv6 address. The values of the status are as follows: <ul style="list-style-type: none"> • PREFERRED • DEPRECATED • INVALID • INACCESSIBLE • UNKNOWN • TENTATIVE • DUPLICATE

Configuring an IPv6 address for a switch or stack

Step	Action
1	<pre>Enter ipv6 address { [<ipv6_address/prefix_length>] [stack <ipv6_address/prefix_length>] [switch <ipv6_address/prefix_length>] [unit <1-8> < ipv6_address/prefix_length>]</pre>
—End—	

Job aid**Table 10**
IPv6 variables and definitions

Variable	Definition
ipv6_address/prefix_length	
stack	IPv6 address and prefix length of stack.
switch	IPv6 address/prefix length of switch.
unit	IPv6 address/prefix length of unit number: 1 to 8

Displaying the IPv6 address for a switch or stack

Use the following procedure to display the IPv6 address for a switch or stack:

show ipv6 address**Step Action**

1 Enter `show ipv6 address`

—End—

show ipv6 address interface**Step Action**

1 Enter `show ipv6 address interface <ipv6_address>` to display all ipv6 interface addresses.

—End—

Job aid The following graphic shows the results of the `show ipv6 address interface` command.

Figure 6
show ipv6 address interface

```
(config)#show ipv6 address interface
-----
                                Address Information
-----
IPV6                               VID/BID/_TYPE  ORIGIN  STATUS
ADDRESS                            TID
-----
3000:0:0:0:0:0:0:99                V-1      UNICAST MANUAL  PREFERRED
fe80:0:0:0:211:f9ff:fe34:8800      V-1      UNICAST OTHER   UNKNOWN

2 out of 2 Total Num of Address Entries displayed.
```

Configuring IPv6 management interface

Use the following procedure to configure the IPv6 interface and create the VLAN IPv6 interface and set the parameters

Step	Action
1	Enter interface vlan <mgmt_vlan_id>.
2	Enter ipv6 interface [address <ipv6_address/prefix_length>].

—End—

Job aid The following table describes the variables for the `ipv6 interface` command:

Table 11
ipv6 interface command

Variable	Definition
address <ipv6_address/prefix_length>	Address or prefix length.
name <1-255>	Name: integer from 1 to 255
link-local <WORD 0-19>	Interface identifier,
mtu <1280-9600>	Default status: MTU 1280

Variable	Definition
reachable-time <0-3600000>	Time in milliseconds neighbor is considered reachable after a reachable confirmation message. Default: 30000
retransmit-timer <0-3600000>	Time in milliseconds between retransmissions of neighbor solicitation messages to a neighbor. Default: 1000

Disabling IPv6 globally

Use the following procedure to disable IPv6 globally:

Step Action

- 1 Enter `no ipv6 interface [address <ipv6_address>] [all] [enable]` to disable IPv6.

Note: If you do not specify a parameter, you can use the `no ipv6 interface` to delete an IPv6 interface.

—End—

Job aid The following table describes the variables for the `no ipv6 interface` command:

Table 12
no ipv6 interface command variables

Variable	Definition
address	Delete an IPv6 address.
all	Disable interface administrative status or delete an IPv6 address.
enable	Disable interface administrative status.

Returning IPv6 to default settings

Use the following procedure to return an IPv6 interface or address to the default settings:

Step Action

- 1 Enter `default ipv6 interface [all | enable | link-local | mtu | reachable-time | retransmit-timer]`.

—End—

Job aid The following table describes the variables for the `default ipv6 interface` command:

Table 13
default ipv6 interface command variables

Variable	Definition
all	Disable interface administrative status or delete an IPv6 address.
enable	Disable interface administrative status.
link-local	Default identifier.
mtu	Default MTU.
reachable-time	Default reachable time.
retransmit-timer	Default retransmit timer.

Configuring IPv6 global properties

Use the following procedure to configure the IPv6 global properties:

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

- | | |
|---|--|
| 1 | Enter <code>ipv6 [enable icmp <error-interval unreachable-msg>]</code> . |
|---|--|

—End—

Job aid The following table describes the variables for the `ipv6` command:

Table 14
ipv6 command variables

Variable	Description
enable	Enable the IPv6 global administrative status.
icmp	Set the IPv6 ICMP parameters. <ul style="list-style-type: none"> error-interval: Set the IPv6 ICMP error interval. unreach-msg: Enable the IPv6 ICMP unreachable-msg

Displaying the global IPv6 configuration

Use the following procedure to display the global IPv6 configuration:

Step	Action
1	Enter <code>show ipv6 global</code> to display the global IPv6 configuration.

—End—

Job aid The following table describes the `show ipv6 global` command results:

Table 15
show ipv6 global command results

Field	Default setting
forwarding	disabled
default-hop-cnt	30
number-of-interfaces	1
admin-status	enabled
icmp-error-interval	1000
icmp-redirect-msg	disabled
icmp-unreach-msg	disabled
multicast-admin-status	disabled

Configuring an IPv6 default gateway for the switch or stack

Step	Action
1	Enter <code>ipv6 default-gateway <ipv6_gateway address></code> to configure a default gateway.
2	Enter <code>no ipv6 default-gateway</code> to disable a default gateway.

—End—

Displaying the IPv6 default gateway

Use the following procedure to display the IPv6 address for the default gateway:

Step	Action
1	Enter <code>show ipv6 default-gateway</code> .

—End—

Configuring the IPv6 neighbor cache

Use the following procedure to add or remove a static neighbor cache entry:

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

- | | |
|---|--|
| 1 | Enter <code>ipv6 neighbor <ipv6_address> [port <port/slot>] [mac <H.H.H>]</code> to add a static neighbor cache entry. |
| 2 | Enter <code>no ipv6 neighbor <ipv6_address> [port <port/slot>] [mac <H.H.H>]</code> to remove a static neighbor cache entry. |
-

—End—

Displaying the IPv6 neighbor information

Use the following command to display IPv6 neighbor information:

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

- | | |
|---|---|
| 1 | Enter <code>show ipv6 neighbor [<ipv6_address>] [type {other dynamic static local}]</code> to display the address and status of the neighbor cache. |
|---|---|
-

—End—

Job aid The following graphic shows the output of the `show ipv6 neighbor` command.

```
(config)#show ipv6 neighbor
=====
Neighbor Information
=====
NET ADDRESS/          PHYS TYPE  STATE      LAST
PHYSICAL ADDRESS      INTF       UPD
=====
3000:0:0:0:0:0:0:0/   V-1  LOCAL  REACHABLE  0
00:11:f9:34:88:00
3000:0:0:0:0:0:0:1/   1/5  STATIC REACHABLE  387452
00:01:02:03:04:05
3000:0:0:0:0:0:0:99/  V-1  LOCAL  REACHABLE  385251
00:11:f9:34:88:00
fe80:0:0:0:211:f9ff:fe34:8800/  V-1  LOCAL  REACHABLE  385193
00:11:f9:34:88:00
```

Displaying IPv6 interface ICMP statistics

Use the following procedure to display IPv6 interface ICMP statistics:

Step Action

- 1 Enter `show ipv6 interface icmpstatistics [<1-4094>]`.
-

—End—

Job aid The following graphic shows a sample of the results from the `show ipv6 interface icmpstatistics` command.

Figure 7
show ipv6 interface icmpstatistics

```
(config)#show ipv6 interface icmpstatistics
-----
                                Icmp Stats
-----
Icmp stats for IfIndex = 10001

IcmpInMsgs: 1
IcmpInErrors: 1
IcmpInDestUnreachs : 1
IcmpInAdminProhibs : 0
IcmpInTimeExcds : 0
IcmpInParmProblems : 0
IcmpInPktTooBigs : 0
IcmpInEchos : 0
IcmpInEchoReplies : 0
<truncated>
```

Displaying IPv6 interface statistics

Use the following procedure to display IPv6 TCP statistics:

Step Action

- 1 Enter `show ipv6 interface statistics [1-4094]`.
-

—End—

Job aid The following graphic shows a sample of the results from the `show ipv6 interface statistics` command.

Figure 8
show ipv6 interface statistics

```
(config)#show ipv6 interface statistics
-----
                          Interface Stats
-----
If stats for IfIndex = 10001

InReceives: 0
InHdrErrors: 0
InTooBigErrors : 0
InNoRoutes : 0
InAddrErrors : 0
InUnknownProts : 0
InTruncatedPkts : 0
InDiscards : 0
InDelivers : 20
<truncated>
```

Displaying IPv6 TCP statistics

Use the following procedure to display IPv6 TCP statistics:

show ipv6 tcp

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

1	Enter <code>show ipv6 tcp</code> to display the TCP statistics for IPv6.
---	--

—End—

Job aid The following graphic shows a sample result from the `show ipv6 tcp` command.

Figure 9
show ipv6 tcp

```
(config)#show ipv6 tcp

show ipv6 tcp global statistics:
-----
ActiveOpens:      0
PassiveOpens:    0
AttemptFails:    0
EstabResets:     0
CurrEstab:       1
InSegs:          24
OutSegs:         20
RetransSegs:     2
InErrs:          0
OutRsts:         0
HCInSegs:        24
HCOutSegs:       20
```

Displaying IPv6 TCP connections

Use the following procedure to display IPv6 TCP connections:

Step Action

- 1 Enter `show ipv6 tcp connections` [`<WORD 0-128>`] [`<portList>`] [`<WORD 0-128>`].

—End—

Displaying IPv6 TCP listeners

Use the following procedure to display IPv6 TCP listeners:

Step Action

- 1 Enter `show ipv6 tcp listener`.

—End—

Displaying IPv6 UDP statistics and endpoints

Use the following procedure to display IPv6 UDP statistics and endpoints:

Step Action

- 1 Enter `show ipv6 udp` to show UDP statistics.

2 Enter `show ipv6 udp endpoints` to show UDP endpoints.

—End—

Configuring LLDP with NNCLI

You can enable and configure LLDP with NNCLI. For more information about LLDP, see "[Link Layer Discover Protocol \(IEEE 802.1ab\) Overview](#)" (page 51). This section covers the following commands:

- "[lldp command](#)" (page 122)
- "[lldp port command](#)" (page 123)
- "[lldp tx-tlv command](#)" (page 124)
- "[lldp tx-tlv dot1 command](#)" (page 124)
- "[lldp tx-tlv dot3 command](#)" (page 125)
- "[lldp tx-tlv med command](#)" (page 125)
- "[lldp location-identification coordinate-base command](#)" (page 126)
- "[lldp location-identification civic-address command](#)" (page 127)
- "[show lldp command](#)" (page 133)
- "[default lldp command](#)" (page 128)
- "[default lldp port command](#)" (page 129)
- "[default lldp tx-tlv command](#)" (page 129)
- "[default lldp tx-tlv dot1 command](#)" (page 130)
- "[default lldp tx-tlv dot3 command](#)" (page 131)
- "[default lldp tx-tlv med command](#)" (page 131)
- "[no lldp port command](#)" (page 132)
- "[no lldp tx-tlv command](#)" (page 132)
- "[no lldp tx-tlv dot1 command](#)" (page 132)
- "[no lldp tx-tlv dot3 command](#)" (page 133)
- "[no lldp tx-tlv med command](#)" (page 133)
- "[show lldp port command](#)" (page 135)
- "[LLDP configuration example](#)" (page 136)

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 123) 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 123) 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

Parameters and variables	Description
config notification	enables notification when new neighbor information is stored or when existing information is removed
status {rxOnly txAndRx txOnly}	sets the LLDP transmit and receive status on the ports rxonly: enables LLDP receive only. txAndRx: enables LLDP transmit and receive. txOnly: enables LLDP 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>] [local-mgmt-addr] [port-desc]
[sys-cap] [sys-desc] [sys-name]
```

The `lldp tx-tlv` command is in the config-if command mode.

"[lldp tx-tlv command variables](#)" (page 124) describes the parameters and variables for the `lldp tx-tlv` command.

lldp tx-tlv command variables

Variables	Description
local-mgmt-addr	Specifies the local management address TLV.
port <portlist>	Specifies the ports affected by the command.
port-desc	Specifies the port description TLV.
sys-cap	Specifies the system capabilities TLV.
sys-desc	Specifies the system description TLV.
sys-name	Specifies the system name 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-protocol-vlan-id
<vlanlist>] [port-vlan-id] {protocol-identity [EAP] [LLDP]
[STP]} [vlan-name <vlanlist>]
```

The `lldp tx-tlv dot1` command is in the config-if command mode.

"[lldp tx-tlv dot1 command parameters and variables](#)" (page 125) 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 [link-aggregation] [mac-phy-config-status] [maximum-frame-size] [mdi-power-support]
```

The `lldp tx-tlv dot3` command is in the config-if command mode.

"[lldp tx-tlv dot3 command parameters and variables](#)" (page 125) 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 [extendedPSE] [inventory] [location] [med-capabilities] [network-policy]
```

The `lldp tx-tlv med` command is in the config-if command mode.

"[lldp tx-tlv med command parameters and variables](#)" (page 126) 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 [altitude]
[datum] [latitude] [longitude]
```

The `lldp location-identification coordinate-base` command is in the config-if command mode.

"[lldp location-identification coordinate-base command parameters](#)" (page 126) 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.
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

Field	Description
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 127) 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)
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

Field	Description
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 129) 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 129) 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 130) 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 130) 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 131) 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 132) 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}	Displays the organizationally-specific TLV properties on the local switch: <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

Parameters and variables	Description
	<ul style="list-style-type: none"> 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 network-policy: Network Policy Discovery TLV location: Location Identification TLV extended-power: Extended Power-via-MDI TLV inventory: Inventory TLVs

Parameters and variables	Description
	<ul style="list-style-type: none"> 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] 1}
[neighbor-mgmt-addr]
```

The `show lldp port` command is in the exec command mode.

show lldp port command parameters

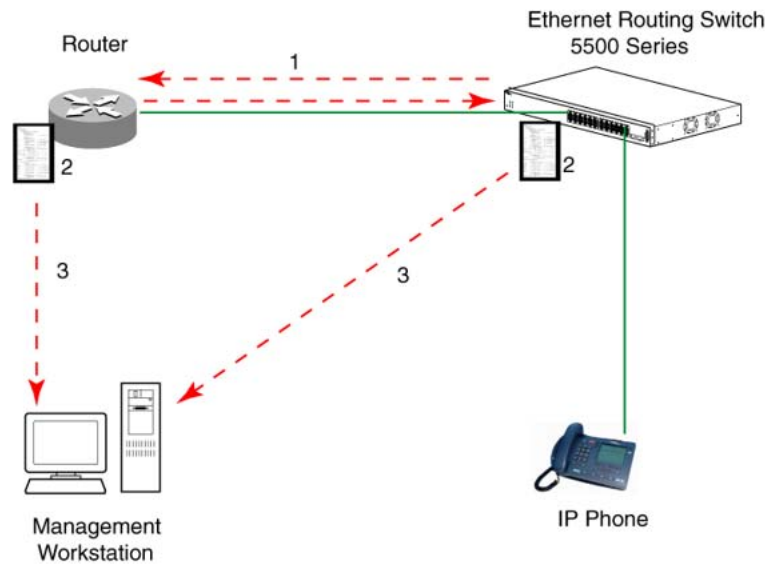
Parameters and variables	Description
rx-stats	Displays the LLDP receive statistics for the local port.
tx-stats	Displays the LLDP transmit statistics for the local port.
pdu-tlv-size	Displays the different TLV sizes and the number of TLVs in an LLDPDU.
tx-tlv {dot1 dot3 med }	<p>Displays which TLVs are 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.
<pre>[neighbor-mgmt-addr]</pre>	<p>Displays the port neighbor LLDP management address.</p>

LLDP configuration example By default, LLDP is enabled for Tx and Rx on all switch ports. The default value for the LLDP Tx interval is 30 seconds (LLDPDUs are sent at 30 seconds). With the default settings, only the mandatory TLVs are sent, but the switch can receive any LLDP Core, DOT1, DOT3 or MED TLV from its peers.

shows an example of LLDP configuration. For this example, the router is connected to the ERS 5000 Series port 1 and the IP Phone uses port 13.

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: The switch only transmits LLDP MED information if the neighbor is a MED-capable unit.

Detailed configuration commands The following section describes the detailed NNCLI commands required to carry out the configuration depicted in "[LLDP configuration example](#)" (page 137).

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
-----
```

Port	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-capabi
lities
5530-24TFD(config-if)#lldp tx-tlv med port 1,13 network-pol
icy
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 local time zone with NNCLI

SNTP uses Coordinated Universal Time (UTC) for all time synchronizations so it is not affected by different time zones. To have the switch report the time in your local time zone, you need to use the clock commands to set the local time zone.

You must enable SNTP before you set the time zone. If SNTP is not enabled, this command has no effect. If you enable SNTP and do not specify a time zone, UTC is shown by default.

Use the following procedure to configure your switch for your local time zone with NNCLI:

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

1	In NNCLI, set the Global Configuration command mode.
---	--

```
configure
```

2	Enable sntp server.
---	---------------------

3	Set clock time zone using the clock command.
---	--

```
clock time-zone zone hours [minutes]
```

—End—

Job aid

The following table defines the variables for the `clock time-zone` command:

clock time-zone command

Variables	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.

Configuring PoE detection method with NNCLI

Configuring PoE with NNCLI

The following section details the commands necessary to configure PoE with NNCLI:

- ["Set port power enable or disable" \(page 143\)](#)
- ["Set port power priority" \(page 143\)](#)
- ["Set power limit for channels" \(page 144\)](#)
- ["Set traps control" \(page 144\)](#)
- ["Show main power status" \(page 144\)](#)
- ["Set power usage threshold" \(page 145\)](#)
- ["Setting PoE detection method" \(page 145\)](#)
- ["Show port power status" \(page 145\)](#)
- ["Show port power measurement" \(page 145\)](#)

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" \(page 144\)](#) 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 144) 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 145) 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.

Customizing NNCLI banner with NNCLI 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 146) 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 147) 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.

Displaying the default TFTP server with NNCLI

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

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 NNCLI, 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 Web-based management and Device Manager. No special options are needed in these interfaces to display the additional information.

Configuring AUR with NNCLI

This section describes NNCLI 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.

Agent Auto Unit Replacement (AAUR)

Use the following commands to configure and use AAUR.

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.

Enabling feature license files

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" \(page 150\)](#)
- ["show license command" \(page 151\)](#)
- ["clear license command" \(page 151\)](#)

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 151) 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.

Setting the server for Web-based management with NNCLI

You can use NNCLI to enable or disable a web server for use with Web-based management. For details, refer to the following:

- "[web-server command](#)" (page 151)
- "[no web-server command](#)" (page 152)

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 152) 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 user access limitations

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 NNCLI through the Telnet protocol or a Console connection.
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> <p>"cli password parameters" (page 152) explains the parameters for the <code>cli password</code> command.</p>

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 NNCLI through the Telnet protocol or a Console connection.
- 2** From the command prompt, use the `cli password` command to enable or disable the desired password.

```
cli password {telnet | serial} {none | local | radius
| tacacs}
```

"cli password parameters" (page 153) 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 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 152), 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 NNCLI, the RADIUS server settings must be specified to complete the process. Ensure that **Global Configuration** mode is entered in NNCLI before beginning this task.

To enable RADIUS authentication through NNCLI, follow these steps:

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

- | | |
|---|---|
| 1 | Access NNCLI through the Telnet protocol or a Console connection. |
| 2 | From the command prompt, use the <code>radius-server</code> command to configure the server settings. |

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

"radius-server parameters" (page 154) explains the parameters for the `radius-server` command.

radius-server parameters

Parameter	Description
host <address>	This parameter is the IPv6 or 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 IPv6 or IP address of the backup server.
port <num>	This parameter is the UDP port number the RADIUS server uses to listen for requests.

Parameter	Description
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 NNCLI 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—

System configuration with Device Manager

This section contains the procedures to configure the system with Device Manager.

Changing switch software in Device Manager

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

Step	Action
1	From Device Manager menu select Edit, File System . The File System screen appears.
2	Select the Config/Image/Diag file tab.
3	In the fields provided, specify the information necessary to perform the download process.
4	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.

Job aid

The following table defines the variables in the File System window:

File System window

Variable	Description
TftpServerIpAddressType	The type of TFTP server on which the new software images are stored for download.
TftpServerIpAddress	The IP address of the TFTP server on which the new software images are stored for download.
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. .
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. .

Variable	Description
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.
Image	Specify if the image to download is the primary or secondary image.
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. • 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 or 5600 Series.

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

Configuration files in Device Manager

Device Manager provides tools for the storage and retrieval of configuration files.

For details, refer to the following topics:

- ["Storing the current ASCII configuration" \(page 158\)](#)
- ["Retrieving an ASCII configuration file" \(page 159\)](#)
- ["Storing a binary configuration file" \(page 160\)](#)
- ["Retrieving a binary configuration file" \(page 161\)](#)
- ["Viewing boot image information" \(page 162\)](#)

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 Device Manager FileSystem screen by selecting Edit, File System from Device Manager menu.
2	Select the Ascii Config Files tab.
3	Type the IP address of the desired TFTP server in the TftpServerInetAddress box.
4	Type the name of the configuration file in the AsciiConfigFilename box.
5	To save the configuration file to a USB storage device, select 9 if the device is a standalone or 1-8 if the device is a stack.
6	Select Upload Now in AsciiConfigManualUpload field to transfer the file to a TFTP server or UploadToUsb to transfer the file to a USB mass storage device.
7	Click Apply .
8	Check the AsciiConfigManualUpload field for the file transfer status. If the status of the file upload is <i>InProgress</i> , wait for up to two minutes and then click Refresh to see the new status. The file upload is complete when the status displays either <i>Passed</i> or <i>Failed</i> .

—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 Device Manager FileSystem screen by selecting Edit, File System from Device Manager menu.
2	Select the Ascii Config File tab.
3	If you retrieve the configuration file from a TFTP server, type the IP address of the desired TFTP server in the TftpServerInetAddress box.
4	If you retrieve the configuration file from a USB storage device, select 9 if the device is a stand-alone or 1-8 if the device is a stack.

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

—End—

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 Device Manager menu. |
| 2 | Select the Config/Image/Diag file tab. |
| 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 TftpServerInetAddress 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 Device Manager menu.
2	Select the Config/Image/Diag file tab.
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 TftpServerInetAddress 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 Device Manager 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.
Note: The shared graphic was removed in accordance with the NTDA for cloning of documents. The graphic that was removed was Edit_FileSystem_Save_Config.png
- 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.

Viewing boot image information

You can use the following procedure to see the version of the primary and secondary boot images on your system:

Step Action

- 1 Click **Edit, File System, Boot Image**.
- 2 Click **Refresh** to renew the information.

—End—

Table 16
Boot image variables

Variable	Definition
Chassis <1 to 8> Primary Image version	Displays the version number of the primary boot image.

Variable	Definition
Chassis <1 to 8> Secondary Image version	Displays the version number of the secondary boot image. This line is blank if the switch does not have a secondary image in memory.
Chassis <1 to 8> Running Image version	Displays the version number of the boot image currently running.

Automatically downloading a configuration file with Device Manager

This feature is enabled through Device Manager 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 Device Manager menu.
2	Select the AsciiConfigFile tab.
3	Type the IP address of the desired TFTP server in the TftpServerIpAddress 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—

General Switch Administration with Device Manager

This section contains information about the following topics:

- ["Viewing Unit information" \(page 164\)](#)

- "Viewing SFP GBIC ports" (page 164)
- "Editing the chassis configuration" (page 165)
- "Editing and viewing switch ports" (page 174)
- "Editing and viewing switch PoE configurations" (page 254)
- "Editing Bridging Information" (page 183)
- "Configuring SNTP" (page 186)
- "Viewing topology information with Device Manager" (page 239)

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. The following table "Unit tab items" (page 164) 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 165)
- "Base Unit Info tab" (page 168)
- "Stack Info tab" (page 169)
- "Power Supply tab " (page 172)
- "Fan tab " (page 173)

For information on the **Banner** tab or the **Custom Banner** tabs, refer to "Banner tab" (page 257) or "Custom Banner tab" (page 258).

For information on the **SNMP** and **Trap Receivers** tabs, refer to *Nortel Ethernet Routing Switch 5000 Series Security — Configuration* (NN47200-501). For information on the **ADAC** and **ADAC MAC Ranges**, refer to *Nortel Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and Multi-Link Trunking* (NN47200-502). For information on the Stack Monitor, refer to *Nortel Ethernet Routing Switch 5000 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. |
|---|--|

Note: The chassis keeps track of the elapsed time and calculates the time and date using the system clock of 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 to 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> <ul style="list-style-type: none"> bootPrimary: Use the primary boot image. bootSecondary: Use the secondary boot image.

Field	Description
AutoPvid	Click enabled or disabled. When you select enabled, Port VLAN ID (PVID) is automatically assigned.
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.
JumboFramesEnabled	Click to enable or disable jumbo frames.
NextBootMgmtProtocol	The transport protocols to use after the next boot of the agent.
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"> • bootpDisabled • bootpAlways • bootpWhenNeeded • bootpOrLastAddress • dhcp • dhcpWhenNeeded • dhcpOrLastAddress
CurrentImageVersion	Read only: The version number of the agent image that is currently used 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.

Field	Description
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	Read only: The transport protocol last used to load the image and configuration information about 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.

The following table 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.

Field	Description
OperState	The operational state of the switch.
Location	Type the physical location of the switch.
RelPos	The relative position of the switch.
BaseNumPorts	The number of base ports of the switch.
TotalNumPorts	The number of ports of the switch.
IpAddress	The base unit IP address.
RunningSoftwareVer	The software version.

—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.

The following table 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.
Location	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 . Notes: 1. This field is applicable only to components that can be found in either the Board or Unit groups. If the information is

Field	Description
	<p>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 • 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.

Field	Description
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.
RunningSoftwareVer	The software version.

—End—

Configuring Stack Mode Use the following procedure to configure the stack mode.

Procedure steps

Step	Action
1	Select Edit > Chassis from the menu. The Chassis dialog box appears.
2	Click the Stack Mode tab.
3	The current stack mode is displayed in the CurrentOperationalMode field.
4	Select the stack mode that will be used after the next boot from the NextBootOperationalMode field.
5	Click Apply .

—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.

—End—

The following table describes the **Power Supply** tab fields.

Power Supply tab fields

Field	Description
Description	Indicates the chassis number, power supply number, and the type of power supply.
OperStat	The operational state of the power supply. Possible values include: <ul style="list-style-type: none"> • other: Some other state. • notAvail: State not available.

Field	Description
	<ul style="list-style-type: none"> • removed: Component was removed. • disabled: Operation disabled. • normal: State is in normal operation. • resetInProgress: 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.

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.

—End—

The following table 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. • resetInProgress: A reset of the fan is in progress.

Field	Description
	<ul style="list-style-type: none"> testing: Fan is doing a self test. warning: Fan is operating at a warning level. nonFatalErr: Fan is operating at error level. fatalErr: An error stopped the fan operation notConfig: Fan needs to be configured. The allowable values are determined by the component type.

Editing and viewing switch ports

Port configuration tasks are performed in Device Manager 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.

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.

The following sections describe some of the tabs on the Port screen:

- "Interface tab" (page 174)
- "PoE tab" (page 178)
- "Configuring Rate Limiting" (page 179)
- "TDR tab" (page 180)

For information on the **VLAN, LACP, VLACP, ADAC, and STP BPDU-Filtering** tabs, refer to *Nortel Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and Multi-Link Trunking* (NN47200-502). For information on the **EAPOL, EAPOL Advance, and NSNA** tabs, refer to *Nortel Ethernet Routing Switch 5000 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	<p>Select the port to edit from the Device View. Select Edit, Port from the menu. The Port screen opens with the Interface tab displayed.</p> <p>To continue, go to:</p> <ul style="list-style-type: none"> • "Interface tab" (page 174)

Interface tab items

The following table 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.
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</p>

Field	Description
	state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
LinkTrap	Indicates whether linkUp/linkDown traps are generated for this interface. By default, this object has the value enabled for interfaces that do not operate on top of any other interface (as defined in the ifStackTable).
AutoNegotiate	Indicates whether this port is enabled for autonegotiation or not.
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>

Field	Description
	<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>
AutoNegotiation Advertisements	<p>Specifies the port speed and duplex abilities to be advertised during link negotiation.</p> <ul style="list-style-type: none"> • 10Half: 10 half duplex advertised • 10Full: 10 full duplex advertised • 100Half: 100 half duplex advertised • 100Full: 100 full duplex advertised • 1000Half: 1000 half duplex advertised • 1000Full: 1000 full duplex advertised • PauseFrame: PAUSE frame support advertised. • AsymPauseFrame: Asymmetric PAUSE frame support advertised. <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>
WanMode	<p>Set the area network type for a 10 GE port.</p> <ul style="list-style-type: none"> • none • wan • lan
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.

—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. |
|---|--|

describes the **PoE** tab fields.

PoE tab fields

Field	Description
AdminEnable	Enables or disables PoE on this port.
Detection Status	<p>Displays the operational status of the power-device detecting mode on the specified port:</p> <ul style="list-style-type: none"> • disabled: detecting function disabled • searching: detecting function is enabled and the system is searching for a valid powered device on this port • 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 • 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>

Field	Description
PowerClassifications	Displays the operational status of the port PD classification.
PowerPriority	Sets the power priority for the specified port to: <ul style="list-style-type: none"> critical high low
PowerLimit	Enter an integer from 3 to 16 W to set the power limit for the port.
Power Measurement	Read only: <ul style="list-style-type: none"> Voltage: in 1/10 v. Current: in 1/1000 A. Power: in 1/1000 W.

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—

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.

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.

Field	Description
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—

TDR tab The 5000 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.
4	Select the StartTest option. (If multiple ports are selected, select true from the StartTest field for each port that you want to test.)
5	Click Apply . "TDR tab fields" (page 180) describes the TDR tab fields.

TDR tab fields

Field	Description
StartTest	Enables the TDR test.

Field	Description
TestDone	Indicates whether a TDR test is complete.
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 1 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.

Field	Description
Pair4Status	The status of a single pair in the cable.
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.

Field	Description
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.
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—

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.

For details, refer to the following topics:

- ["Base tab" \(page 183\)](#)
- ["Transparent tab" \(page 184\)](#)
- ["Forwarding tab" \(page 185\)](#)

For more information on the Mac Flush tab, see *Nortel Ethernet Routing Switch 5000 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	<p>Open the Bridge screen by selecting Edit, Bridge from the menu. The Bridge screen appears with the Base tab selected.</p> <p>"Bridge screen -- Base tab fields" (page 184) describes the fields on this tab.</p>

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.
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—

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	<p>Open the Bridge screen by selecting Edit, Bridge from the menu. The Bridge screen appears. Select the Transparent tab.</p>

"Bridge screen -- Transparent tab fields" (page 185) 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—

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.

To continue, go to:

- ["Forwarding tab fields" \(page 186\)](#)

—End—

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.
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>
Id	The VLAN ID.

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. |
| 2 | Edit the fields as indicated by the table. |

The following table describes the **Simple Network Time Protocol** fields.

Field	Description
PrimaryServerInetAddressType	The IP address type (IPv4 or IPv6) of the primary SNTP server.
PrimaryServerInetAddress	The IP address of the primary SNTP server.
SecondaryServerInetAddressType	The IP address type (IPv4 or IPv6) of the secondary SNTP server.
SecondaryServerInetAddress	The IP address of the secondary SNTP server.
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.
LastSyncSourceInetAddressType	Specifies the IP source address type (IPv4 or IPv6) of the NTP server with which this device last synchronized.
LastSyncSourceInetAddress	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.

Field	Description
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 LLDP with Device Manager

The following sections contain instructions for configuring and viewing LLDP information with Device Manager:

- ["Viewing and configuring LLDP global and transmit properties" \(page 188\)](#)
- ["LLDP_Port_dot1 dialog box" \(page 207\)](#)
- ["LLDP_Port_dot_3 dialog box" \(page 214\)](#)
- ["LLDP_Port_med dialog box" \(page 222\)](#)

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" \(page 189\)](#)
- ["Port tab" \(page 191\)](#)
- ["TX Stats tab" \(page 194\)](#)
- ["Graphing LLDP transmit statistics" \(page 194\)](#)
- ["RX Stats tab" \(page 195\)](#)
- ["Graphing LLDP receive statistics" \(page 197\)](#)
- ["Local System tab" \(page 197\)](#)
- ["Local Port tab" \(page 199\)](#)
- ["Local Management tab" \(page 200\)](#)
- ["Neighbor tab" \(page 201\)](#)
- ["Neighbor Mgmt Address tab" \(page 203\)](#)

- "Unknown TLV tab" (page 204)
- "Organizational Defined Info tab" (page 205)

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 | <p>From Device Manager menu bar, choose Edit, Diagnostics, 802.1ab, LLDP.</p> <p>The LLDP dialog box appears with the Globals tab displayed.</p> <p>"LLDP Globals tab fields" (page 189) describes the Globals tab fields.</p> |
|---|---|

LLDP Globals tab fields

Field	Description
IldpMessageTxInterval	The interval (in seconds) at which LLDP frames are transmitted on behalf of this LLDP agent.
IldpMessageTxHoldMultiplier	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: $TTL = \min(65535, (IldpMessageTxInterval * IldpMessageTxHoldMultiplier))$ For example, if the value of IldpMessageTxInterval is 30, and the value of IldpMessageTxHoldMultiplier is 4, the value 120 is encoded in the TTL field in the LLDP header.
IldpReinitDelay	The IldpReinitDelay indicates the delay (in seconds) from when the LLDP Port AdminStatus of a particular port is disabled until reinitialization begins.
IldpTxDelay	The IldpTxDelay 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 IldpTxDelay is set by the following formula: $1 \leq IldpTxDelay \leq (0.25 * IldpMessageTxInterval)$

Field	Description
lldpNotificationInterval	This object controls the transmission of LLDP notifications. The agent must not generate more than one lldpRemTablesChange 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 lldpRemoteSystemsData 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 lldpStatsRemTableLastChangeTime to detect any missed lldpRemTablesChange 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 lldpRemoteSystemsData objects, and all LLDP extension objects associated with remote systems. An NMS can use this object to reduce polling of the lldpRemoteSystemsData objects.
RemTablesInserts	The number of times the complete set of information advertised by a particular MSAP is inserted into tables contained in lldpRemoteSystemsData and lldpExtensions 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 lldpStatsRemTablesInserts 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—

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 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. "Port tab fields" (page 192) describes the Port tab fields.

Port tab fields

Field	Description
PortNum	Port number.
AdminStatus	The administratively desired status of the local LLDP agent: <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	Controls, for each port, whether notifications from the agent are enabled. <ul style="list-style-type: none"> • true: indicates that notifications are enabled • false: indicates that notifications are disabled.

Field	Description
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)	Specifies whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is included in the transmitted LLDPDUs.
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

Field	Description
	<ul style="list-style-type: none"> 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—

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

- From Device Manager menu bar, choose **Edit, Diagnostics, 802.1ab, LLDP**.
The LLDP dialog box appears with the Globals tab displayed.
- Click the **TX Stats** tab.
"TX Stats tab fields" (page 194) 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—

Graphing LLDP transmit statistics Use the following procedure to graph LLDP transmit statistics:

Step	Action
1	From the TX Stats tab, 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—

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 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 fields" (page 195) describes the RX Stats tab fields.

RX Stats tab fields

Field	Description
PortNum	Port number.
FramesDiscardedTotal	The number of LLDP frames received on the port and discarded for any reason. This counter provides an indication that LLDP header formatting problems exist with the local LLDP agent in the sending system, or that LLDPDU validation problems exist with the local LLDP agent in the receiving system.
FramesErrors	The number of invalid LLDP frames received on the port, while the LLDP agent is enabled.

Field	Description
FramesTotal	The number of valid LLDP frames received on the port, while the LLDP agent is enabled.
TLVsDiscardedTotal	The number of LLDP TLVs discarded for any reason.
TLVsUnrecognizedTotal	The number of LLDP TLVs received on a given port that are not recognized by this LLDP agent on the indicated port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001 - 111 1110) in Table 9.1 of IEEE 802.1AB-2004. An unrecognized TLV can be a basic management TLV from a later LLDP version.
AgeoutsTotal	This counter represents the number of age-outs that occurred on a given port. An <i>age-out</i> is "the number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in <code>IldpRemoteSystemsData</code> and <code>IldpExtensions</code> objects because the information timeliness interval has expired." This counter is similar to <code>IldpStatsRemTablesAgeouts</code> , except that it is on a for each-port basis. This enables NMS to poll tables associated with the <code>IldpRemoteSystemsData</code> objects and all LLDP extension objects associated with remote systems on the indicated port only. This counter is set to zero during agent initialization. When the admin status for a port changes from disabled to <code>rxOnly</code> , <code>txOnly</code> or <code>txAndRx</code> , the counter associated with the same port is reset to 0. The agent also flushes all remote system information associated with the same port. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial aging is not allowed, and thus, does not change the value of this counter.

—End—

Graphing LLDP receive statistics Use the following procedure to graph LLDP receive statistics:

Step	Action
1	From the RX Stats tab, select the port for which you want to display statistics.
2	Click Graph . The RX Stats - Graph dialog box appears.
3	Highlight a data column to graph.
4	Click one of the graph buttons.

—End—

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 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 fields" (page 197) 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

Field	Description
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
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

Field	Description
PDPowerReq	specifies the value of the power required (in units of 0.1 watts) by a Powered Device (PD)
PDPowerSource	defines the type of power source advertised as in use by the local 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 required by this PD: <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—

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 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 fields" (page 200) describes the **Local Port** tab fields.

Local Port tab fields

Field	Description
PortNum	Port number.
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—

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
1	From Device Manager menu bar, choose Edit, Diagnostics, 802.1ab, LLDP . The LLDP dialog box appears with the Globals tab displayed.
2	Click the Local Management tab. The Local Management tab appears. "Local Management tab fields" (page 201) 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.
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 LLDPDUs.

—End—

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 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 fields" (page 202) 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.
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.

Field	Description
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—

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 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 fields" (page 203) 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.

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.
AddrSubtype	The type of encoding used in the associated Addr object.
Addr	The management address associated with the remote system.
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—

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 Device Manager menu bar, choose Edit, Diagnostics, 802.1ab, LLDP .
The LLDP dialog box appears with the Globals tab displayed. |
| 2 | Click the Unknown TLV tab.
The Unknown TLV tab appears.

"Unknown TLV tab fields" (page 205) describes the Unknown 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—

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 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 fields](#)" (page 205) 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—

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 207)
- "Local Protocol VLAN tab" (page 207)
- "Local VLAN Name tab" (page 208)
- "Local Protocol tab" (page 209)
- "Neighbor VLAN Id tab" (page 210)
- "Neighbor Protocol VLAN tab" (page 211)
- "Neighbor VLAN Name tab" (page 212)
- "Neighbor Protocol tab" (page 213)

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 | <p>From 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.</p> <p>"Procedure" (page 207) describes the Local VLAN Id tab fields.</p> |
|---|---|

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—

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 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. "Procedure" (page 207) 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—

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 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.

"Procedure" (page 208) 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—

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 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.

"Procedure" (page 209)"Procedure" (page 209) describes the Local Protocol tab fields.

Local Protocol tab fields

Field	Description
PortNum	Port number.

Field	Description
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—

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 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 fields" \(page 210\)](#) 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—

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 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 fields" (page 211) 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.

Field	Description
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—

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 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 fields" (page 212) 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.

Field	Description
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—

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 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 fields" (page 213) 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.
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—

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 214)
- "Local PoE tab" (page 215)
- "Local Link Aggregate tab" (page 216)
- "Local Max Frame tab" (page 217)
- "Neighbor Port Auto-negotiation tab" (page 217)
- "Neighbor PoE tab" (page 218)
- "Neighbor Link Aggregate tab" (page 220)
- "Neighbor Max Frame tab" (page 221)

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
------	--------

- | | |
|---|---|
| 1 | <p>From Device Manager menu bar, choose Edit, Diagnostics, 802.1ab, Port dot3.</p> <p>The LLDP_Port_dot3 dialog box appears with the Local Port Auto-negotiation tab displayed.</p> <p>"Local Port Auto-negotiation tab fields" (page 214) describes the Local Port Auto-negotiation tab fields.</p> |
|---|---|

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.

Field	Description
AutoNegAdvertisedCap	This object contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the local port on the system.
OperMauType	A value that indicates the operational MAU type of the given port on the local system.

—End—

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 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 fields](#)" (page 215) 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.

Field	Description
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—

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 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 tab fields" (page 216) 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—

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 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 fields" (page 217) 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—

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 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 fields" (page 218) 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—

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 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 fields" (page 219) 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 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.

Field	Description
PowerPairs	This object contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the remote port. <ul style="list-style-type: none"> • signal • spare
PowerClass	This object contains the value of the pethPsePortPowerClassifications object (defined in IETF RFC 3621) for the remote port. <ul style="list-style-type: none"> • class0 • class1 • class2 • class3 • class4

—End—

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 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 220) 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.

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.
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—

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 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 fields" (page 221) 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.

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.
MaxFrameSize	Maximum Frame Size for the remote port.

—End—

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 222)
- "Local Location tab" (page 223)
- "Local PoE PSE tab" (page 227)
- "Neighbor Capabilities tab" (page 227)
- "Neighbor Policy tab" (page 228)
- "Neighbor Location tab" (page 230)
- "Neighbor PoE tab" (page 232)
- "Neighbor PoE PSE tab" (page 233)
- "Neighbor PoE PD tab" (page 234)
- "Neighbor Inventory tab" (page 236)

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 | <p>From Device Manager menu bar, choose Edit, Diagnostics, 802.1ab, Port med.</p> <p>The LLDP_Port_med dialog box appears with the Local Policy tab displayed.</p> <p>"Local Policy tab fields" (page 223) describes the Local Policy tab fields.</p> |
|---|--|

Local Policy tab fields

Field	Description
PortNum	Port number.
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—

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 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 fields" (page 224) describes the Local Location tab fields.

Local Location tab fields

Field	Description
PortNum	Port number.
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—

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.
2	Click the Location Details button. The Coordinate Based Location dialog box opens. 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).
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.

2 Click the **Location Detail** button.

The Civic Address Location dialog box opens.

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
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 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 fields" (page 227) 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—

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 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 fields" (page 228) 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.
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—

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 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 fields" (page 229) 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.
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

Field	Description
	operation. In this case, both the VLAN ID and the Layer 2 priority fields are ignored, and only the DSCP value has relevance.

—End—

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 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 fields" (page 230) 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.

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 advertised by the remote device. The parsing of this information is dependent on the location subtype.

—End—

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. |
| 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.
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 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 fields" (page 232) 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.
PoeDeviceType	Defines the type of Power-via-MDI (Power over Ethernet) advertised by the remote device: <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—

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 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 fields" (page 233) 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.

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.
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. low: indicates that the device advertises its power priority as low, see RFC 3621.

—End—

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 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 fields" (page 235) 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—

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 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 fields" (page 236) 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.
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.

Field	Description
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—

Configuring Auto Unit Replacement

Use the following procedure to configure the Auto Unit Replacement (AUR) feature.

Procedure steps

Step	Action
1	Select Edit > Chassis from the menu. The Chassis dialog box appears.
2	Click the AUR tab.
3	Enable Auto Unit Replacement by selecting the AutoUnitReplacementEnabled check box.
4	Enable Auto Unit Replacement saving by selecting the AutoUnitReplacementSaveEnabled check box.
5	Enter a value for forced saves in the AutoUnitReplacementForceSaves field.
6	Enter a value for AUR restore in the AutoUnitReplacementRestore field.
7	Click Apply .

—End—

Configuring local time zone

Set the local time zone on the Ethernet Routing Switch 5000 Series.

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 Ethernet Routing Switch 5000 Series.

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 with Device Manager

This section describes topology diagnostic information available in Device Manager through the following tabs:

- "Topology tab" (page 239)
- "Topology Table tab" (page 239)

Topology tab

To view topology information:

From Device Manager menu bar, select **Edit, Diagnostics, Topology**.

The **Topology** dialog box appears with the **Topology** tab displayed.

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.

Topology Table tab

To view more topology information:

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

- | | |
|---|---|
| 1 | From 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—

Configuring IPv6 with Device Manager

You can configure IPv6 with Device Manager.

Configuring IPv6 global properties with Device Manager

Use the following procedure to configure IPv6 global properties with Device Manager:

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

- | | |
|---|--|
| 1 | Click the IPv6 tab in Device Manager.

<i>The IPv6 dialog box appears with the Globals tab displayed.</i> |
| 2 | Enter the global properties in the boxes. |

- 3 Click **Apply** to save the changes.
- 4 Click **Refresh** to display updated information.

—End—

Job aid Use the data in this table to help you configure the Globals tab.

Table 17
Variable definitions

Variable	Definition
AdminEnabled	Check this box to enable the administration function.
OperEnabled	True or false
Forwarding	notForwarding or Forwarding
DefaultHopLimit	Default number of hops: 30
IcmpNetUnreach	
IcmpRedirectMsg	True or false
IcmpErrorInterval	Time to wait before sending an ICMP error message. A value of 0 means the system does not send an ICMP error message. Value: 0 to 2147483647 ms
IcmpErrorQuota	Default value: 1
MulticastAdminStatus	True or false

Viewing an IPv6 interface ID to a VLAN with Device Manager

Use the following procedure to view an IPv6 interface ID to a VLAN to learn the ID.

Prerequisite

You must configure a VLAN before you can give the VLAN an interface identifier, or an IPv6 address. The Nortel Ethernet Routing Switch 5000 Series switches support port-based and protocol-based VLANs. For more information about configuring VLANs, see *Nortel Ethernet Routing Switch 5000 Configuration — VLANs, Spanning Tree and Multi-Link Trunking*, NN47200-501.

Viewing an IPv6 interface ID to a VLAN

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

- | | |
|---|--|
| 1 | From Device Manager menu bar, click the IPv6 tab.
<i>The IPv6 dialog box appears with the Globals tab displayed.</i> |
|---|--|

- 2 Click the **Interfaces** tab.
*The **Interface** tab appears.*
- 3 View the parameters.

—End—

Job aid Use the data in this table to help you understand the Interfaces tab.

Table 18
Variable definitions

Variable	Definition
IfIndex	Identifies a physical interface or a logical interface (VLAN). For a VLAN, it is the Ifindex of the VLAN.
Identifier	Specifies the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
IdentifierLength	Specifies the length of the interface identifier in bits.
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.
Vlanid	Identifies the Virtual LAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag.
Type	Specifies Unicast, the only supported type.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. The default value is 1280.
PhysAddress	Specifies the media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address.
AdminStatus	Specifies whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true).
OperStatus	Specifies whether the operation status of the interface is up or down.
ReachableTime	Specifies the time (in milliseconds) that a neighbor is considered reachable after receiving a reachability confirmation.

Variable	Definition
RetransmitTime	Specifies the RetransmitTime, which is the time (in milliseconds) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.
MulticastAdminStatus	Specifies the multicast status as either True or False.

Graphing IPv6 statistics with Device Manager

Use the following procedure to display graphical representations of IPv6 statistics with Device Manager:

Step	Action
1	From Device Manager menu bar, click the IPv6 tab. <i>The IPv6 dialog box appears with the Globals tab displayed.</i>
2	Click the Interfaces tab. <i>The Interface tab appears.</i>
3	Select an interface.
4	Click the Graph button. <i>The IPv6 Interface Stats window opens.</i>
5	Click on the information that you want to see as a graph.
6	Click on a graph button to see the data in a line chart, area chart, bar chart or pie chart.
7	Click the Clear Counters button to reset all values to 0.

—End—

Job aid The following table defines the variables for the **Graph** button:

Table 19
Graph button variables

Variable	Definition
AbsoluteValue	Counter value.
Cumulative	Total value seen since dialog displayed.
Average/sec	Average value.
Minimum/sec	Minimum value seen.

Variable	Definition
Maximum/sec	Maximum value seen.
LastValue/sec	Last value seen.
InReceives	Number of packets received.
InHrdErrors	Number of incoming errors.
InNoRoutes	Number of incoming undefined routes.
InAddrErrors	Number of incoming address errors.
InUnknownProtos	Number of incoming unknown protocols.
InTruncatedPkts	Number of incoming truncated packets.
InDiscards	Number of discarded incoming packets.
InDelivers	Number of delivered incoming packets.
OutForwDatagrams	Number of outgoing forwarded datagrams.
OutRequests	Number of outgoing requests.
OutDiscards	Number of discarded outgoing packets.
OutFragOKs	Number of accepted fragmented outgoing packets.
OutFragFails	Number of failed fragmented outgoing packets.
OutFragCreates	Number of fragmented outgoing packets created.
ReasmReqds	Number of reasm packets required.
ReasmOKs	Number of reasm packets accepted.
ReasmFails	Number of reasm packets failed.
InMcastPkts	Number of incoming multicast packets.
OutMcastPkts	Number of outgoing multicast packets.
Poll Interval	Set the poll interval. <ul style="list-style-type: none"> • none • 2s • 5s • 10s • 30s • 1m • 5m • 30m

Variable	Definition
	<ul style="list-style-type: none"> 1h

Configuring an IPv6 address for a switch or stack with Device Manager

Use the following procedure to configure an IPv6 address for a switch or stack with Device Manager.

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

- | | |
|---|--|
| 1 | Click the IPv6 tab in Device Manager.
<i>The IPv6 dialog box appears with the Globals tab displayed.</i> |
| 2 | Click the Interfaces tab.
<i>The Interface tab appears.</i> |
| 3 | Click the Insert button.
<i>The IPv6, Insert Interfaces window appears.</i> |
| 4 | Fill in the parameters. |
| 5 | Click Insert to save the changes. |
| 6 | Click Close to return to the IPv6 screen. |

—End—

Job aid The following table defines the variables for the Insert Interfaces window:

Table 20
IPv6 variables and definitions

Variable	Definition
IfIndex	Identifies a physical interface or a logical interface (VLAN). For a VLAN, it is the Ifindex of the VLAN.
Identifier	Specifies the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
IdentifierLength	Specifies the length of the interface identifier in bits.

Variable	Definition
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. Value: 1280 to 9600
AdminStatus	Specifies whether the administration status of the interface is enabled (true) or disabled (false).
ReachableTime	Specifies the time (in milliseconds) that a neighbor is considered reachable after receiving a reachability confirmation. Value: 0 to 36000000 ms
RetransmitTime	Specifies the RetransmitTime, which is the time (in milliseconds) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Value: 0 to 36000000 ms

Setting IPv6 static routes with Device Manager

Use the following procedure to set IPv6 static routes:

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

- | | |
|---|--|
| 1 | Click the IPv6 tab in Device Manager.
<i>The IPv6 dialog box appears with the Globals tab displayed.</i> |
| 2 | Click the Static Routes tab.
<i>The Static Routes tab appears.</i> |
| 3 | Click the Insert button.
<i>The IPv6, Insert Static Routes window appears.</i> |
| 4 | Fill in the parameters. |
| 5 | Click Insert to save the changes. |
| 6 | Click Close to return to the IPv6 screen. |

—End—

Job aid The following table defines the variables for the Insert Static Routes window:

Table 21
Static Routes variables

Variable	Description
Dest.	Enter the destination IPv6 address.
PrefixLength	Enter the prefix length.
NextHop	Enter the IPv6 address for the next hop to create the default gateway.
IfIndex	Click the VLAN button to select the IfIndex for your VLAN.

Viewing the neighbor cache with Device Manager

View the neighbor cache to discover information about neighbors in your network. Neighbor cache in IPv6 is similar to the IPv4 Address Resolution Protocol (ARP) table. The neighbor cache is a set of entries for individual neighbors to which traffic was sent recently. You make entries on the neighbor on-link unicast IP address, including information such as the link-layer address. A neighbor cache entry contains information used by the Neighbor Unreachability Detection algorithm, including the reachability state, the number of unanswered probes, and the time the next Neighbor Unreachability Detection event is scheduled.

View neighbor cache

Step	Action
1	From Device Manager menu bar, click the IPv6 tab. <i>The Ipv6 dialog box appears with the Globals window displayed.</i>
2	Click the Neighbors tab. <i>The Neighbors window appears.</i>
3	View the values in each field.

—End—

Job aid Use the data in this table to help you view the Neighbors tab.

Table 22
Variable definitions

Variable	Definition
IfIndex	A unique value to identify a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN.
NetAddress	The IPv6 address corresponding to the media-dependent physical address.
PhysAddress	The media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address.
Interface	Either a physical port ID or the Multi-Link Trunking port ID. This entry is associated either with a port or with the Multi-Link Trunking in a VLAN.
LastUpdated	The value of sysUpTime at the time this entry was last updated. If this entry was updated prior to the last reinitialization of the local network management subsystem, this object contains a zero value.
Type	<p>The type of mapping is as follows:</p> <ul style="list-style-type: none"> • Dynamic type—indicates that the IP address to the physical address mapping is dynamically resolved using, for example, IPv4 ARP or the IPv6 Neighbor Discovery Protocol. • Static type—indicates that the mapping is statically configured. • Local type—indicates that the mapping is provided for the interface address. <p>The default is static.</p>
State	<p>Specifies the Neighbor Unreachability Detection state for the interface when the address mapping in this entry is used. If Neighbor Unreachability Detection is not in use (for example, for IPv4), this object is always unknown. Options include the following:</p> <ul style="list-style-type: none"> • reachable—confirmed reachability • stale—unconfirmed reachability

Variable	Definition
	<ul style="list-style-type: none"> • delay—waiting for reachability confirmation before entering the probe state • probe—actively probing • invalid—an invalidated mapping • unknown—state cannot be determined • incomplete—address resolution is being performed

Configuring the IPv6 neighbor cache with Device Manager

Use the following procedure to configure the IPv6 neighbor cache with Device Manager:

Step Action

- 1 From Device Manager menu bar, click the **IPv6** tab.
*The Ipv6 dialog box appears with the **Globals** window displayed.*
- 2 Click the **Neighbors** tab.
*The **Neighbors** window appears.*
- 3 Click the **Insert** button.
*The **IPv6, Insert Neighbours** window opens.*
- 4 Fill in the required information.
- 5 Click **Insert** to save your changes.

—End—

Job aid The following table lists the fields in the **IPv6, Insert Neighbours** window.

Table 23
IPv6, Insert Neighbours variables

Variable	Definition
IfIndex	A unique value to identify a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN.

Variable	Definition
NetAddress	The IPv6 address corresponding to the media-dependent physical address.
PhysAddress	The media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address.
Interface	Either a physical port ID or the Multi-Link Trunking port ID. This entry is associated either with a port or with the Multi-Link Trunking in a VLAN.

Displaying IPv6 interface ICMP statistics with Device Manager

Use the following procedure to display the IPv6 interface ICMP statistics with Device Manager:

Step Action

- 1 From Device Manager menu bar, click the **IPv6** tab.
*The Ipv6 dialog box appears with the **Globals** window displayed.*
 - 2 Click the **ICMP Stats** tab.
*The **ICMP Stats** window appears.*
 - 3 Click **Clear Counters** to reset the statistics.
 - 4 Set the Poll interval.
-

—End—

Job aid The following table lists the fields in the **ICMP Stats** window.

Table 24
ICMP Stats variables

Variable	Definition
InMsgs	Number of ICMP messages received.
InErrors	Number of ICMP error messages received.
OutMsgs	Number of ICMP messages sent.
OutErrors	Number of ICMP error messages sent.
Poll Interval	Sets polling interval. Value: 2 to 60 s.

Displaying ICMP message statistics with Device Manager

Use the following procedure to display the IPv6 interface ICMP message statistics with Device Manager:

Step	Action
1	From Device Manager menu bar, click the IPv6 tab. <i>The Ipv6 dialog box appears with the Globals window displayed.</i>
2	Click the ICMP Msg Stats tab. <i>The ICMP Msg Stats window appears.</i>
3	Click Refresh to update the ICMP message statistics.

—End—

Job aid The following table lists the fields in the **ICMP Msg Stats** window.

Table 25
ICMP Msg Stats variables

Variable	Definition
Type	Type of packet received or sent.
InPkts	Number of packets received.
OutPkts	Number of packets sent.

Displaying IPv6 TCP global properties with Device Manager

Use the following procedure to display IPv6 TCP global properties with Device Manager:

Step	Action
1	From Device Manager menu bar, click IPv6, TCP/UDP . <i>The Ipv6TcpUdp dialog box appears with the TCP Globals window displayed.</i>
2	Click Refresh to update the information.

—End—

Job aid The following table lists the fields in the **TCP Globals** window.

Table 26
TCP Globals variables

Variable	Definition
RtoAlgorithm	Algorithm identifier.
RtoMin	Minimum value in milliseconds.
RtoMax	Maximum value in milliseconds.
MaxConn	Maximum number of connections.

Displaying IPv6 TCP connections with Device Manager

Use the following procedure to display IPv6 TCP connections with Device Manager:

Step	Action
1	From Device Manager menu bar, click the IPv6, TCP/UDP tab. <i>The Ipv6TcpUdp dialog box appears with the ICMP Globals window displayed.</i>
2	Click the TCP connections tab. <i>The TCP connections window appears.</i>
3	Click Refresh to update the information.

—End—

Job aid The following table lists the fields in the **TCP connections** window.

Table 27
TCP connections variables

Variable	Definition
LocalAddressType	Type of local address (IPV6 or IPV4).
LocalAddress	Local address.
LocalPort	Local port IP.
RemAddress Type	Type of remote address (IPV6 or IPV4).
RemAddress	Remote address.
RemPort	Remote port number.
State	State <ul style="list-style-type: none"> • Enabled • Disabled

Displaying IPv6 TCP listeners with Device Manager

Use the following procedure to display IPv6 TCP listeners with Device Manager:

Step	Action
1	From Device Manager menu bar, click the IPv6, TCP/UDP tab. <i>The Ipv6TcpUdp dialog box appears with the ICMP Globals window displayed.</i>
2	Click the TCP listeners tab. <i>The TCP listeners window appears.</i>
3	Click Refresh to update the information.
—End—	

Job aid The following table lists the fields in the **TCP listeners** window.

Table 28
TCP listeners variables

Variable	Definition
LocalAddressType	Type of local address (IPV6 or IPV4).
LocalAddress	Local address.
Local Port	Local port number.

Displaying IPv6 UDP endpoints with Device Manager

Use the following procedure to display IPv6 UDP endpoints with Device Manager:

Step	Action
1	From Device Manager menu bar, click the IPv6, TCP/UDP tab. <i>The Ipv6TcpUdp dialog box appears with the ICMP Globals window displayed.</i>
2	Click the UDP Endpoints tab. <i>The UDP Endpoints window appears.</i>
3	Click Refresh to update the information.
—End—	

Job aid The following table lists the fields in the **UDP Endpoints** window.

Table 29
UDP Endpoints variables

Variable	Definition
LocalAddressType	Type of local address (IPV6 or IPV4).
LocalAddress	Local address.
Local Port	Local port number.
RemoteAddressType	Type of remote address (IPV6 or IPV4).
RemoteAddress	Remote address.
RemotePort	Remote port number.
Instance	Distinguishes between multiple processes connected to the UDP endpoint.
Process	Displays the ID for the UDP process.

Configuring PoE with Device Manager

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 5000 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 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.

—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.

The following table "PoE tab items for a single unit" (page 256) 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.
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—

Copying the license file

Use Device Manager to copy the license file to the 5000 Series Nortel Ethernet Routing Switch.

Step	Action
1	From Device Manager menu select Edit, File System . The FileSystem dialog box appears.
2	Click the License File tab. The License File tab appears.
3	In the TftpServerInetAddressType field, select the address type, IPv4 or IPv6.
4	In the TftpServerInetAddress field, enter the TFTP server address in the format selected in the previous step.
5	In the LicenseFileName field, enter the software license filename for the TFTP server.
6	In the UsbTargetUnit field, select the target location using an integer ranging 0-9. 0 specifies TFTP retrieval. 1-8 are used to specify USB in a stack unit. 9 is used to specify a standalone unit.
7	In the LicenseFileAction field, select dnldLicense .
8	Click Apply .
9	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.
10	To reboot the switch, choose Edit, Chassis
11	Under the System tab, select the reboot option and click Apply .

—End—

Customizing NNCLI banner

Banner tab

The Banner tab controls NNCLI banner display.

To configure the Banner Control, use the following procedure:

Step	Action
1	Open the Edit Chassis screen in the manner detailed at the beginning of this section.
2	Select the Banner tab.

—End—

The following table 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 5000 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.

Custom Banner tab

The Custom Banner tab customizes NNCLI 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. |
-

—End—

The following table 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.

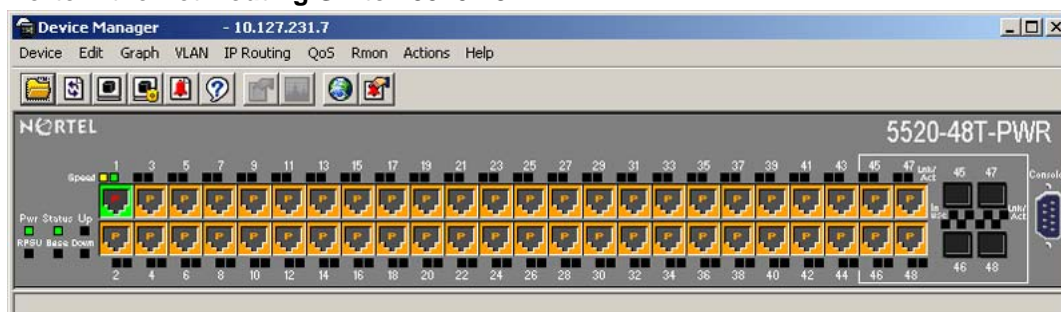
Field	Description
Id	Identifies the line of text within a custom banner
Line	Displays a one line of a fifteen line banner. If the line contains non-printable ASCII characters, then the line is rejected and an error message returned.

Viewing PoE ports with Device Manager

The Front Panel view of 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 259) 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 259) 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.

System configuration with Web-based management

The modules in this section provide procedures that allow you to configure your system with Web-based management.

Configuration files in Web-based management

Web-based management provides tools for the storage and retrieval of configuration files.

For details, see the following topics:

- ["Storing and retrieving a configuration file through TFTP or USB" \(page 260\)](#)
- ["Retrieving a configuration file through HTTP or USB" \(page 262\)](#)

Storing and retrieving a configuration file through TFTP or USB

The **Configuration File Download/Upload** page in Web-based management is used to store or retrieve a configuration file.

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 Web-based management.
2	Complete the fields on this page that are relevant to the file upload process. "File upload fields" (page 260) 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 or 5600 Series, 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.

Field	Description
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 Web-based management.
- 2 Complete the fields on this page that are relevant to the file download process. "[File download fields](#)" (page 261) 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 or 5600 Series, 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.

Field	Description
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 Ethernet Routing Switch 5000 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.

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 5000 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 Web-based management. |
| 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 or 5600 Series switches 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 Web-based management.
2	In the table entitled Ascii Configuration USB File Download Setting (present only on 5530-24TFD and 5600 Series switches), supply the necessary information in the fields provided to complete the file download. " Ascii USB file download fields " (page 263) 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.

General Switch Administration with Web-based management

This section contains information about the following topics:

- "[Viewing stack information](#)" (page 264)
- "[Viewing summary switch information](#)" (page 265)
- "[Changing stack numbering](#)" (page 266)
- "[Identifying unit numbers](#)" (page 267)
- "[Configuring BootP, DHCP, IP, and gateway settings](#)" (page 267)

- ["Modifying system settings" \(page 275\)](#)
- ["Managing remote access by IP address" \(page 276\)](#)
- ["Configuring the Real-Time Clock" \(page 277\)](#)

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.
—End—	

The following table 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.
	Serial Number	The serial number of the base unit.
Stack Inventory	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.
	Unit	The unit number assigned to the device by the network manager. For more information about stack numbering, see "Changing stack numbering" (page 266) .
	Description	The description of the device or its subcomponent.
	Pluggable port	The SFP GBICs connected to the switch.

Section	Fields	Description
	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.

The following table 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 266).
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.
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.

The following table 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. |
| 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.

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 describes the items on the IP screen.

IP page items

Section	Item	Range	Description
Boot Mode Setting	BootP Request Mode	BootP When Needed	<p>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.</p> <p>Note: This is the default.</p>
		BootP Always	<p>Choose this mode to inform the switch, each time it boots, to ignore any manually configured network parameters and send BootP requests. This setting disables remote management if no BootP server is set up for the switch.</p>
Boot Mode Setting (continued)		<p>BootP Disabled Choose this mode to inform the switch, each time it boots, to use the IP configuration parameters manually configured. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.</p>	<p>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.</p> <p>Note: This mode causes the same operation for DHCP.</p>
		<p>BootP or Last Address</p>	<p>Choose this mode to inform the switch, at each start up, to obtain the IP configuration with BootP. If the BootP requests fail, the switch uses the last network parameters successfully obtained through BootP, stored in 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</p>	

Section	Item	Range	Description
			process, change the BootP request mode to any of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.
		DHCP When Needed	Choose this mode to inform the switch to send DHCP requests when the switch has no manually configured IP address. If the switch has manually configured network parameters, the switch uses these values instead
		DHCP Always	Choose this mode to inform the switch to ignore any manually configured network parameters and send DHCP requests when the switch starts. This setting disables remote management if no DHCP server is set up for the switch.
		DHCP or Last Address	Choose this mode to inform the switch, at each start, to obtain the IP configuration with DHCP. If the DHCP requests fail, the switch uses the last network parameters successfully obtained through DHCP, stored in non-volatile memory. Note: Valid parameters obtained when the switch uses BootP/DHCP replace current information stored in the non-volatile memory.
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.

Section	Item	Range	Description
	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.
- NNCLI control and ACG support
- Device Manager 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> |
|---|--|


```
Granted Lease Time: 65535 seconds
```

- 2 Use the `renew dhcp` command to renegotiate the lease time with the DHCP Server.

```
55XX(config)#renew dhcp
```

```
55XX(config)#show ip dhcp client lease
```

```
Configured Lease Time: 60 seconds
```

```
Granted Lease Time: 60 seconds
```

—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 - Device Manager configuration You can configure the DHCP Client from Device Manager. Use **Edit, Chassis** and **BootMode**.

DHCP BootMode options

Option	Description
dhcp	Corresponds to DHCP Always mode.
dhcpWhenNeeded	Corresponds to DHCP When Needed mode.
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**.

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 Web-based management System Information home page.

To configure system settings:

Step	Action
1	Open the System screen by selecting Configuration, System from the menu.

The following table describes the items on the **System** screen.

System page items

Item	Description
System Description	The factory set description of the hardware and software versions.
System Object ID	The character string that the vendor created to uniquely identify this device.
System Up Time	The elapsed time since the last network management portion of the system was last reinitialized. Note: This field is updated only when the screen is redisplayed.
System Contact	Type a character string to create the contact information for the network manager or the selected person to contact regarding switch operation; for example, 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 IPv4 addresses and 50 IPv6 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.

The following table 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 IPv4 addresses and 50 source IPv6 addresses.
	SNMP/Access	Allowed Disallowed	Enables SNMP access.
	SNMP/Use List	Yes No	Restricts SNMP access to the specified 50 source IPv4 addresses and 50 source IPv6 addresses.
	Web Page/Access		Displays allowed Web Interface access.
	Web/Use List	Yes No	Restricts Web Interface access to the specified 50 source IPv4 addresses and 50 source IPv6 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.

Section	Item	Range	Description
	Allowed Source Mask	A.B.C.D	Enter the source IP mask you want to allow switch access.
Allowed Source IPv6 address and prefix length	Allowed Source IPv6 Address	WORD	Enter the source IPv6 address you want to allow switch access.
	Allowed Prefix Length	<1-128>	Enter the source IPv6 prefix length 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.
- 2 In the fields provided, configure the Real Time Clock. "[Real Time Clock fields](#)" (page 277) 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—

Changing switch software in Web-based management

To change the software version running on the switch with Web-based management, follow this procedure:

Step	Action
1	Navigate to the Software Download Management page by selecting Configuration, Software Download from the menu.
2	In the provided fields, specify the information needed to complete the software download procedure.
3	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.

Job aid

Software download page fields

Field	Description
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	The target from which the software images are downloaded. Select either TFTP Server, USB1 or USB2 as the download target. This field is only present for 5530-24TFD or 5600 Series switches.

Field	Description
TFTP Server IP Address	The IP address of the TFTP Server to be used in the software download. You can use either an A.B.C.D or IPv6 address. This field is only present for 5530-24TFD or 5600 Series switches.
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. • Primary: Download the Primary image. • Secondary: Download the Secondary image. • Diagnostics: Perform a download of the diagnostics image specified in the Diagnostics Image File Name field. • Primary Image If Newer: Perform a download of the software image specified in the Primary Image File Name field only if it is newer than the current image. • Secondary Image If Newer: Perform a download of the software image specified in the Secondary Image File Name field only if it is newer than the current image. • Download Primary without Reset: Perform a download of the specified software image and do not reset the switch at the end of the process. • Download Secondary without Reset: Perform a download of the specified software image and do not reset the switch at the end of the process. • Download Diagnostic without Reset: Perform a download of the specified software image and do not reset the switch at the end of the process.

Configuring PoE with Web-based management

The following sections detail PoE configuration and management with Web-based management:

- ["Configuring power management on the switch" \(page 279\)](#)
- ["Configuring power management for the ports" \(page 281\)](#)

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 280).
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 280) 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.

Item	Description
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 282).
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 282) 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.

Configuring IPv6 with Web-based management

Use the following procedures to perform basic configuration tasks for IPv6 with Web-base management:

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

- | | |
|---|---|
| 1 | Log in to Web-based management. |
| 2 | Click Configuration, IPv6 .
<i>The IPv6 screen opens.</i> |
| 3 | Enter the information in the boxes. |
| 4 | Click Submit to save your changes. |

—End—

Job aid

The following table lists the variables on the IPv6 screen.

Table 30
IPv6 variables

Variable	Definition
IPv6 Setting	
In-Band Stack IPv6 Address	Global stack IPV6 address.
In-Band Switch IPv6 Address	Global switch IPv6 Address.
Link Local Address	Local Address derived from the interface ID.
Default Gateway	Default gateway IPv6 address.
Global Admin Status Setting	

Variable	Definition
Global Admin Status	Set the global administration status. <ul style="list-style-type: none"> • Enabled • Disabled
Management Interface Admin Status Setting	
Management Interface Admin Status	Set the management interface administration status. <ul style="list-style-type: none"> • Enabled • Disabled

Managing remote access by IP address with Web-based management

Modifying system settings with Web-based management

Setting user access limitations with Web-based management

Web-based management 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" \(page 285\)](#)
- ["Setting the Telnet password" \(page 287\)](#)
- ["Setting the Console password" \(page 288\)](#)
- ["Configuring RADIUS authentication" \(page 289\)](#)

Setting the Web password

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

Step	Action
1	<p>Select the password type from the Web/Telnet Switch Password Type list. Three options are available in the Web/Telnet Switch Password Type list:</p> <ul style="list-style-type: none"> • None <p>This selection indicates that no password is required for users accessing the switch through Web-based management.</p>



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 289) 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/Telnet 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 can also be changed on this screen.

—End—

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, Web/Telnet** from the main menu and follow this procedure:

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

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

- **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 289) 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 **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: You can also change the **Web/Telnet Stack Password** settings on this screen.

—End—

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 289) 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 **Console 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: You can also change the **Console Stack Password** settings on this screen.

—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 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—

Configuration reference

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 291) outlines the factory default configuration settings present in a switch in a factory default state.

Factory default configuration settings

Setting	Factory Default Configuration Value
Unit Select switch	non-Base
Unit	1
BootP Request Mode	BootP When Needed
In-Band Stack IP Address	0.0.0.0 (no IP address assigned)
In-Band Switch IP Address	0.0.0.0 (no IP address assigned)
In-Band Subnet Mask	0.0.0.0 (no subnet mask assigned)
Default Gateway	0.0.0.0 (no IP address assigned)
Read-Only Community String	public
Read-Write Community String	private
Trap IP Address	0.0.0.0 (no IP address assigned)
Community String	Zero-length string
Authentication Trap	Enabled
Autotopology	Enabled
sysContact	Zero-length string
sysName	Zero-length string
sysLocation	Zero-length string

Setting	Factory Default Configuration Value
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
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

Setting	Factory Default Configuration Value
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
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

Setting	Factory Default Configuration Value
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 type	None
Console Stack Password type	None
Telnet/Web Stack Password type	None
Telnet/Web Switch Password type	None
Console Read-Only Switch Password	Passwords are user for non-SSH software images and userpasswd for SSH software images.
Console Read-Write Switch Password	Passwords are secure for non-SSH software images and securepasswd for SSH software images.
Console Read-Only Stack Password	Passwords are user for non-SSH software images and userpasswd for SSH software images.
Console Read-Write Stack Password	Passwords are secure for non-SSH software images and securepasswd for SSH software images.
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

Setting	Factory Default Configuration Value
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
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)
Allowed Source IPv6 Address and Allowed Prefix Length (50 user-configurable fields)	First field: ::/0 (no IPv6 address assigned)
	Remaining 49 fields: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 (any IPv6 address is allowed)
Image Filename	Zero-length string

Setting	Factory Default Configuration Value
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

Index

A

AAUR 149
 access 98, 276
 address field 67
 address source field 67
 AdminState field 168, 170
 Agent Auto Unit Replacement 149
 Allowed Source IP field 276
 Allowed Source Mask field 277
 AUR
 configuring with Device Manager 237
 configuring with NNCLI 148
 auto-MDI X 38
 autonegotiation 69
 description 38
 autopolarity 38
 autosense description 38
 Autotopology
 configuring with NNCLI 73
 autotopology command 73
 available power 256

B

banner command 146
 Banner tab 257
 Base tab 183
 BaseNumPorts field 169, 171, 255
 boot command 100
 Bootp 26
 BootP 66
 configuring 267
 modes 101
 request modes 268

bootp field 67
 BootP Request Mode field 268
 Bridge parameter
 Base tab
 BridgeAddress field 184
 NumPorts field 184
 Type 184
 Forwarding tab
 Address field 186
 Port field 186
 Status field 186
 broadcast traffic 77

C

CANA 39
 configuring with NNCLI 86
 chassis
 configuration, editing 165
 Clock
 configuring with NNCLI 105
 configuration
 PoE, by port 178
 PoE, switch parameters 254
 configuration files
 in Device Manager 158
 in NNCLI 93
 in Web-based management 260
 connecting external power source 46
 console password
 setting with Web-based management 288
 ConsumptionPower field 256
 Custom Autonegotiation Advertisements 39

D

daylight saving time
 configure 238
DC power source
 connection 46
default autotopology command 74
default duplex command 72
default flowcontrol command 76
Default Gateway field 270
default ip address unit command 68
default ipbootp server command 102
default management interface
 setting 97
default rate-limit command 78
default speed command 70
default telnet-access command 100
default-gateway field 67
Descr field 168, 169, 255
Description field 264
DHCP 36
dhcp client lease field 67
DNS
 configuring with NNCLI 89
duplex command 71
duplex mode 69
Dynamic Host Configuration Protocol
 (DHCP) 36

E

external power source
 connecting 46

F

factory default configuration 291
feature license file
 configuring with Device Manager 256
 configuring with NNCLI 150
Firmware Version field 265
flow control 75
flowcontrol command 75
Forwarding tab 185, 185

G

gateway 63
gateway addresses, configuring 267

GBIC information
 displaying 147
GBIC ports 164
Gigabit Ethernet 75

H

hardware description 264, 265
hardware information
 displaying 147
Hardware Version field 265

I

Identify Unit Numbers page 267
IEEE 802.3u standard 38
In-Band Stack IP Address field 269
In-Band Subnet Mask field 269
In-Band Switch IP Address field 269
In-Use field 270
Interface tab 174
interfaces
 displaying 69
IP address 63, 64, 65, 67, 68, 267
 for each unit 67, 267
ip address command 64
IP Address field 264, 265
ip address unit command 67
IP blocking
 configuring with NNCLI 62
ip bootp server command 101
ip default-gateway command 66
IP gateway address 267
IP manager list 276
IP page 267
IpAddress field 169, 171

L

Last BootP field 270
LEDs 267
LLDP
 configuring with Device Manager 188
 Configuring with NNCLI 122
local time zone
 configure 237
Location field 169, 170
LstChng field 168, 170

M

MAC address 265
 MAC Address field 264, 266
 Mac Address field 265
 Manufacturing Date Code field 264, 265
 MDAs 75
 Module Description field 265
 multicast traffic 77

N

netmask 64, 67
 network administrator
 contact information 275, 275
 New Unit Number field 266
 no autotopology command 74
 no banner command 147
 no flowcontrol command 76
 no ip address command 65
 no ip address unit command 68
 no ip bootp server command 102
 no ip default-gateway 66
 no rate-limit command 78
 no telnet-access command 99
 no web-server command 152
 NotificationControlEnable field 256
 numbering
 stacks 266
 unit 265, 266, 267
 NVRAM 60

O

Operational State field 264, 265
 OperState field 169, 171, 174
 OperStatus field 256

P

passwords
 setting with NNCLI 152
 ping command 88
 Pluggable port 264
 PoE
 available power 256
 configuration, editing 254
 configuring with Device Manager 259
 configuring with NNCLI 143

 configuring with Web-based
 management 279
 error codes 46
 port settings 178
 power being used 256
 status codes 46
 traps 256, 256
 PoE tab 178
 PoE tab for a single unit 255
 Port dialog box 174
 ports 69
 graphing 174
 Power 178
 power being used 256
 Power field 256
 power status 265
 Power Status field 265
 Power tab for a single unit 255
 power usage traps 256
 PowerDetectionMethod fieldtroubleshooting
 power detection method 256
 PowerPairs field 256

Q

quick configuration 61

R

RADIUS authentication
 configuring with NNCLI 154
 Rate Limit tab 179
 rate-limit command 77
 rate-limiting 77
 Real Time Clock
 configuring with NNCLI 85
 Real-time clock
 configuring with Web-based
 management 277
 RelPos field 169
 requirements
 remote access 97

S

security 98
 serial number 255
 Serial Number field 264, 265
 SerNum field 168, 171, 255

- setting TFTP parameters with NNCLI 16
 - show banner command 146
 - show interfaces command 69
 - show ip command 66
 - show rate-limit command 77
 - shutdown command 102
 - Simple Network Time Protocol 79
 - Simple Network Time Protocol (SNTP) 36
 - Simple Network Time Protocol tab 186
 - SNMP Access field 276
 - SNMP Use List field 276
 - SNTP 36, 79
 - configuring with Device Manager 186
 - configuring with NNCLI 79
 - setting daylight saving time 238
 - setting time zone 237
 - SNTP tab 186
 - software
 - updating 16
 - updating with Device Manager 156
 - updating with NNCLI 91
 - updating with Web-based management 278
 - Software Version field 264, 265
 - software versions 264
 - speed 69
 - speed command 70
 - Stack Information page 264
 - stack information, viewing 264
 - Stack Numbering page 266
 - Stack Numbering Setting table 266
 - stack numbering, configuring 266
 - stacking 264, 266
 - replacing units 266
 - static|custom field 146
 - subnet mask 64, 67
 - summary options
 - changing stack numbering 266
 - identifying unit numbers 267
 - viewing
 - stack information 264
 - switch information 265
 - Switch administration with NNCLI 57
 - switch configuration 60
 - switch information
 - viewing 265
 - Switch Information page 265
 - System Contact field 275
 - System Description field 264, 275
 - System Location field 275
 - system location, naming 275
 - System Name field 275
 - system name, configuring 275
 - System Object ID field 275
 - System page 275
 - system settings
 - modifying 275
 - system contact 275
 - system location 275
 - system name 275
 - System Up Time field 275
- ## T
- Target Replacement Setting field 266
 - Target Unit to Replace field 266
 - TDR
 - configuring with NNCLI 72
 - TDR tab 180
 - Telnet 97, 98
 - Telnet Access field 276
 - telnet command 88
 - Telnet password
 - setting with Web-based management 287
 - Telnet Use List field 276
 - telnet-access command 98
 - terminal setup 96
 - testing cables 72
 - TLVs
 - IEEE 802.1 organizationally-specific 54
 - IEEE 802.3 organizationally-specific 54
 - Management 53
 - Organizationally-specific for MED devices 54
 - topology information
 - viewing with Device Manager 239
 - Topology tab 239
 - Topology Table tab 239
 - TotalNumPorts 169, 171
 - TotalNumPorts field 255
 - traffic
 - Gigabit Ethernet 75
 - rate-limiting 77
 - Transparent tab 184

traps 256
 power 256
troubleshooting
 access 65, 68, 97, 276
 DC power source 46
 external power source 46
 PoE 179, 255
 PoE tab 254
 power pairs 256
Type field 168, 255

U

Unit field 264, 265
unit number 265, 266
 identifying 267
 numbering
 units 264
Unit tab 165

updating software 16
UsageThreshold field 256
user access limitations
 setting with NNCLI 152
 setting with Web-based Management 285

V

Ver field 168, 171, 255
VlanIds 186

W

Web Page Access field 276
Web password
 setting with Web-based management 285
Web quick start 37
Web Use List field 276
web-server command 151

Nortel Ethernet Routing Switch 5000 Series

Configuration — System

Copyright © 2005-2008, Nortel Networks
All Rights Reserved.

Publication: NN47200-500
Document status: Standard
Document version: 04.02
Document date: 12 December 2008

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

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

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

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

Sun, Solaris, and Java - are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

SPARC is a trademark of SPARC International, Inc.

UNIX is a trademark of X/Open Company, Ltd.

All other trademarks are the property of their respective owners.

