Nortel Ethernet Routing Switch 5000 Series

Fundamentals

Release: 6.0
Document Revision: 01.01

www.nortel.com

NN47200-104

Nortel Ethernet Routing Switch 5000 Series
Release: 6.0
Publication: NN47200-104
Document status: Standard
Document release date: 12 November 2008

Printed in Canada and the United States of America

Contents

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 foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. **General**

   — 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).

— 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.

— 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.

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

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

— 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.

New in this release

The following sections detail what's new in *Nortel Ethernet Routing Switch 5000 Series Fundamentals* (NN47200-104) for Release 6.0.

Other changes

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

User interfaces

Information about the acquisition, installation, and basic operation of the user interfaces is consolidated in this document from other documents.

Feature Licensing

Basic information about acquiring, generating, installing, and transferring feature licenses is consolidated in this document from other documents.

Configuration files

Fundamental information about working with configuration files is consolidated in this document from other documents.

Supported standards and RFCs

Lists of standards and Request For Comments supported on the switch are consolidated from other documents into a single source for easy reference.

NNCLI quick reference

A new chapter, Quick reference for basic NNCLI tasks, presents frequently used Nortel Networks Command Line Interface (NNCLI) commands for reference.

Document changes

This document is modified to meet Nortel Customer Documentation Standards. For more information about these standards, see *Nortel Ethernet Routing Switch 5000 Series Documentation Roadmap* (NN47200-103).

Introduction

This document is a new publication resulting from restructuring of the Nortel Ethernet Routing Switch 5000 Series Release 6.0 documentation suite.

For easy reference, basic information about user interfaces, feature licenses, use and management of configuration files, and standards and Request for Comments (RFC) supported on the 5000 Series switches appears in this document. A new reference section, Quick reference for basic NNCLI tasks, is included as a single source for frequently used NNCLI commands.

Navigation

- "User interface fundamentals" (page 15)
- "Feature licensing fundamentals" (page 51)
- "Configuration files fundamentals" (page 61)
- "Supported standards and Request for Comments" (page 75)
- "Quick reference for basic NNCLI tasks" (page 77)

User interface fundamentals

This chapter provides basic information to help you understand the interfaces you can use to configure and manage a Nortel Ethernet Routing Switch. Available features depend on switch model and configuration.

Navigation

NNCLI concepts

Nortel Networks Command Line Interface (NNCLI) is a text-based interface you can usefor switch configuration and management. A common command line interface (CLI), NNCLI follows the industry standard for device management across Nortel products.

NNCLI command modes occur in order of increasing privileges, each based on user logon permission level. Logon password determines user logon permission level.

You can access NNCLI directly through a console connection, remotely through a dial-up modem connection, or in-band through a Telnet session.

You can use NNCLI interactively or you can load and run NNCLI scripts using the configure network command, manually loading the script in the console menu, or automatically loading the script at startup. For more information about automatic configuration download, see "Downloading a configuration file automatically at startup" (page 64).

Navigation

NNCLI command modes

This section describes the use and purpose of NNCLI command modes.

NNCLI command modes separate basic user tasks from control and management of the switch.

NNCLI command modes are

- User Executive
- Privileged Executive
- Global Configuration
- Interface Configuration
- Router Configuration

NNCLI command mode access is determined by access permission levels and password protection.

If no password is set, you can enter NNCLI in User Executive mode and perform the **`enable`** command to move to the next level, Privileged Executive mode.

However, if you have read-only access, you cannot progress beyond User Executive mode, the default mode.

If you have read-write access you can progress from the default mode through all of the available modes.

User Executive mode is the default NNCLI command mode and the initial access mode. Also known as exec mode, it is the most restrictive NNCLI mode with only basic commands available—for example, show, ping and logoff. User Executive commands are available in the other modes.

Privileged Executive mode is an unrestricted mode that can display all switch settings. If you are logged on with write access, you can access all configuration modes and commands that affect switch operation from Privileged Executive mode.

In Privileged Executive mode, also known as privExec mode, you can perform basic switch level management tasks; for example, downloading software images, setting passwords, and starting the switch. Privileged EXEC mode commands are also available in Global, Interface, and Router configuration modes.

Global Configuration mode, also known as config mode, provides commands you can use to set and display general switch configurations such as IP address, Simple Network Management Protocol (SNMP) parameters, Telnet access, and Virtual Local Area Networks (VLAN).

Interface Configuration mode, also known as ifconfig mode, provides commands you can use to configure parameters for each port or VLAN such as speed, duplex mode, and rate limiting.

Router Configuration mode, also known as config-router mode, provides commands you can use to configure routing parameters for Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Virtual Router Redundancy Protocol (VRRP).

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 Executive 5530-24TFD>	No entrance command, default mode	**exit** or **logout**
Privileged Executive 5530-24TFD#	**enable**	**exit** or **logout**
Global Configuration 5530-24TFD(config)#	From Privileged EXEC mode, enter **configure**	To return to Privileged EXEC mode, enter **end** or **exit** To exit NNCLI completely, enter **logout**
Interface Configuration 5530-24TFD(config-if)#	From Global Configuration mode: To configure a port, enter **interface fastethernet <port number>** To configure a VLAN, enter **interface vlan <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-router)#	From Interface Configuration mode: To configure RIP, enter	To return to Global Configuration mode, enter **exit**

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

NNCLI help

This section describes help available in NNCLI.

Help is available at all levels of NNCLI.

Command list

To determine whether a command is available from the current mode, you can obtain a list of all commands available from the prompt.

Obtaining the command list

Perform this procedure to obtain a list of available NNCLI commands.

Procedure Steps

Step	Action
1	At the prompt, enter a question mark (**?**).

--End--

Command options

NNCLI can display command options that you can use to focus command results.

Obtaining command options

Perform this procedure to obtain a list of options for a command.

Procedure Steps

Step	Action
1	At the prompt, enter a portion of a command followed by a space and a question mark (**?**).

--End--

Command names

If you are unsure about the correct name of a command, you can enter a partial command name and NNCLI displays the closest match.

Obtaining a command name

Perform this procedure to obtain a correct command name.

Procedure Steps

Step	Action
1	At the prompt, enter a portion of the command name.
2	Press **Tab**.

--End--

Example of obtaining a command name

Procedure Steps

Step	Action
1	At the prompt, enter **`down`**.
2	Press **Tab**.
	The system displays `download`.

--End--

Command modes

This section describes help available for NNCLI commands and modes.

You can use the help {commands | modes} command to obtain a list of NNCLI command modes and the mode access commands, or to obtain a list of commands organized by mode—each command in this list is accompanied by a short explanation.

The help {commands | modes} command is available in all NNCLI command modes.

Obtaining NNCLI command modes

Perform this procedure to obtain a list of NNCLI command modes with mode access commands.

Procedure Steps

Step	Action
1	At the prompt, enter **help modes**.

--End--

Obtaining NNCLI commands listed by mode

Perform this procedure to obtain a list of NNCLI commands organized by mode.

Procedure Steps

Step	Action
1	At the prompt, enter **help commands**.

--End--

Keystroke shortcuts

This section provides key combinations you can use to make NNCLI navigation easier.

The following table describes the keystroke shortcuts.

Key combination	Function
Ctrl+A	Start of line
Ctrl+B	Back 1 character
Ctrl+C	Abort command
Ctrl+D	Delete the character indicated by the cursor
Ctrl+E	End of line
Ctrl+F	Forward 1 character
Ctrl+H	Delete character left of cursor (**Backspace** key)
Tab	Command or parameter completion
Ctrl+K and **Ctrl+R**	Redisplay line
Ctrl+N or **Down arrow**	Next history command
Ctrl+P or **Up arrow**	Previous history command
Ctrl+T	Transpose characters
Ctrl+U	Delete entire line
Ctrl+W	Delete word to left of cursor
Ctrl+X	Delete all characters to left of cursor

Key combination	Function
Ctrl+z	Exit Global Configuration mode to Privileged EXEC mode
?	Context sensitive help
Esc+C and **Exc+U**	Capitalize character at cursor
Esc+l	Change character at cursor to lower case
Esc+B	Move back 1 word
Esc+D	Delete 1 word to the right
Esc+F	Move 1 word forward

NNCLI access procedures

Perform the procedures in this section to access NNCLI.

Access prerequisites

- Connect to the switch—directly with a console cable connected to the switch console port, or through Telnet.
- To connect to the switch remotely, through Telnet, enable remote access and ensure that the switch IP address is valid.
- Use a terminal or a PC with a terminal emulator as the NNCLI command station.
- If you use a console cable and console port, ensure that the terminal emulation program conforms to settings in the following table.

Property	Value
Baud Rate	9600 bps
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Terminal Protocol	VT100 and VT100/ANSI

Opening an NNCLI session

Procedure Steps

Step	Action
1	Connect to the switch.
2	Enter the password, if applicable.
3	At the NNCLI Banner Screen, enter **CTRL+Y**.
4	To access NNCLI, from the main menu, press **c** or scroll to **Command Line Interface** .

5 Press **Enter**.

--End--

Device Manager concepts

This section provides information to obtain, install, start, and use Device Manager to configure and manage the switch.

Navigation

- "Interface components" (page 22)
- "Online help" (page 33)
- "Device Manager procedures" (page 33)

Device Manager is a graphical user interface application you can use to configure and manage the switch. The application provides a real time graphical representation of the switch front panel and provides network access to monitor and configure devices.

Because Device Manager is a client application that resides on a computer, you must install the application before you can use it.

You can download Device Manager from the Nortel Web site. The Java Runtime Environment (JRE) is bundled with Device Manager software and does not require a separate installation.

Device Manager uses the Simple Network Management Protocol (SNMP) to configure and manage devices.

Interface components

This section describes Device Manager interface components and their use in the application.

The Device Manager window includes the following parts:

- Menu bar: access command menus
- Toolbar: quick access to common commands
- Device view: shows a graphic representation of the device status
- Status bar: displays error messages and other information

Menu bar

The following table describes the Menu bar commands.

Command	Description
Device	Opens a device, refreshes the device view, rediscovers a device, and sets the polling and SNMP properties. From the Device menu you can also open and view the Trap Log, SysLog, and Log and establish a Telnet or SSH connection to the currently open device.
Edit	Opens edit dialog boxes for the objects selected in the device view. From the Edit menu you can also open dialog boxes to manage files and run diagnostic tests, and enable SNTP, SNMPv3 and related configurations.
Graph	Opens statistics dialog boxes for the selected object.
VLAN	Opens dialog boxes for managing VLANs, Spanning Tree Groups (STG), MultiLink Trunking (MLT), and Link Aggregation Control Protocol (LACP).
IP Routing	Opens configuration dialog boxes to set up IP routing functions, including ARP, OSPF, RIP, VRRP, DHCP, UDP Forwarding, and Policies, for the switch, .
IPv6	Opens configuration dialog boxes to set up IPv6 and IPv6 TCP/UDP
QoS	Opens configuration and monitoring dialog boxes for Quality of Service or Differentiated Services.
Serviceability	Opens configuration dialog boxes for IPFIX and RMON.
Actions	Opens the Home page for the Web-based management session.
Help	Opens online Help topics for Device Manager and provides a legend for the port colors in the Device view.

Toolbar

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

The following table describes the Toolbar buttons and provides Menu bar equivalents.

Button	Name	Description	Menu bar equivalent
	Open Device	Opens the Open Device dialog box	Device > Open
	Refresh Device Status	Refreshes the device view information	Device > Refresh Status
	Trap Log	Opens the trap log	Device > Trap Log

Button	Name	Description	Menu bar equivalent
	Help	Opens online Help in a Web browser	Help > Device
	Edit Selected	Displays configuration data for the selected chassis object	Edit > Unit Edit > Chassis Edit > Port
	Graph Selected	Opens statistics and graphing dialog boxes for the selected object	Graph > Chassis Graph > Port
	Globe	Opens a Web-based management session	Actions > Open Home Page
	Telnet	Opens a Telnet session	Device > Telnet
	SSH	Opens an SSH session	Device > SSH Connection
	Alarm Manager	Opens the RMON Alarm Manager	Serviceability > Rmon> Alarm Manager

Status bar

Device Manager provides a status bar to display error and information messages from the software applications. These messages are unrelated to the managed device.

Device view

The Device view is a graphical representation of switch hardware operating status. You can use Device view to perform management tasks on specific objects. If you choose a device from the Device menu, the Device view appears.

Objects in the Device view are

- a stand-alone switch; called a unit in the menus and dialog boxes
- a switch stack; called a chassis in the menus and dialog boxes
- a port

Device view object selection

Perform these procedures to select objects in Device view.

Selecting a single object in Device view

Procedure Steps

Step	Action
1	To select a single object in Device view, a port for example, click the edge of the object.

--End--

Selecting multiple objects in Device view

Procedure Steps

Step	Action
1	To select multiple objects of the same type, for example a block of contiguous ports, click and hold the right mouse button and drag the pointer across the objects to select the group of ports.
2	To select multiple ports, or switches in the stack, **Ctrl+click** on the objects.

--End--

Selecting all ports in a stand-alone switch or stack
Procedure Steps

Step	Action
1	To select all the ports in a stand-alone switch or in a stack, from Device Manager menu bar choose **Edit > Select > Ports**.

--End--

Selecting all switch units in a stack
Procedure Steps

Step	Action
1	To select all units in a stack, from Device Manager menu bar choose **Edit > Select > Units**.

--End--

Selecting an entire stack
Procedure Steps

Step	Action
1	To select an entire stack, from Device Manager menu bar choose **Edit > Select > Chassis**.

--End--

LEDs and ports

LED color in Device view mirrors the physical switch LEDs except that LEDs in Device view do not blink.

Ports in Device view are also color coded to demonstrate port status. To see the port color legend, from Device Manager menu bar choose **Help > Legend**.

The following table describes the port color codes.

Color	Description
Green	Port is operating
Red	Port was manually disabled
Orange	Port has no link
Light Blue	Port is in standby mode—not supported in all switch models
Dark Blue	Port test in progress—not supported in all switch models

Color	Description
Gray	Port is unmanageable
Purple	Port is in loopback testing mode—not supported in all switch models

Shortcut menus

This section describes the port and switch shortcuts.

The switch shortcut menu provides access to basic switch hardware information and graph dialog boxes.

The port shortcut menu provides a faster path to edit and graph a port.

Shortcut menus procedures

Perform the following procedure to access the shortcut menu.

Accessing shortcut menus

Procedure Steps

Step	Action
1	To access the shortcut menu for objects in the Device view, right click the object.

--End--

Variable definitions

Variable	Value
Unit shortcuts	
Edit	Opens a read-only dialog box that provides basic switch hardware information.
Show Port Tooltip	If you mouse over a port in the front panel view, the system displays a window containing the port name and speed. **Show port tooltip** is enabled by default.
Refresh Port Tooltip	Refreshes the port tooltip information. To update the tooltip display, from Device Manager menu bar choose **Edit > Port**, and then click **Refresh Port Tooltip**.
Refresh PoE status	Refreshes port PoE status—not all switch models are equipped with PoE.
Unit #	Displays the unit number.
Port shortcuts	
Disable	Shuts a port down administratively—port color changes to red in the Device view.
Enable	Brings a port up administratively.

Variable	Value
Edit	Opens a dialog box to set port operating parameters.
Graph	Opens a dialog box to display port statistics and display statistics as a graph.

Objects in Device view

You can edit objects in the Device view from the Toolbar or from the Shortcut menu.

After you change a screen value, the value displays in bold.

Changes are not applied to the running configuration until you click Apply.

After changes are applied to a field, you can display the new information.

Object editing procedures

Perform the following procedures to edit objects in the Device view.

Selecting an object to edit from the toolbar
Procedure Steps

Step	Action
1	On the toolbar, click **Edit Selected**.

--End--

Selecting an object to edit from the shortcut menu
Procedure Steps

Step	Action
1	From the shortcut menu, choose **Edit**. After you change a screen value, the value appears in bold.

--End--

Applying changes to the running configuration
Procedure Steps

Step	Action
1	To apply changes to the running configuration, after you change a screen value, you must click **Apply** because the system does not apply changes to the running configuration automatically .

--End--

Displaying updated information
Procedure Steps

Step	Action
1	To display new, applied information, click **Refresh**.

--End--

Statistics and graphs

Device Manager tracks a wide range of statistics for each switch, stack, and port. The system updates statistics based on the poll interval

You can view and graph statistics for single or multiple objects and export statistics to other applications.

This section describes the types of statistics and graphs and the graph dialog box buttons, explains how to view statistics and how to export statistics to other applications.

The data tables in the statistics dialog boxes list the counters, or categories of statistics, gathered by the system for the specified object.

For example, the categories for ports include Interface, Ethernet Errors, Bridge, and RMON.

Each category can be associated with six types of statistics.

The following table describes the types of statistics.

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

Using Device Manager, you can create the following types of graphs:

- line
- area
- bar
- pie

Graph type selection buttons appear at the bottom of the statistics window.

Use the buttons at the top of the graph window to change the orientation, scale, or graph type.

The following table describes the graph dialog box buttons.

Button	Name	Description
	Stacked	Stacks data quantities instead of displaying them side-by-side

Button	Name	Description
	Horizontal	Rotates the graph 90 degrees
	Log Scale	Changes the scale of the x axis from numeric to logarithmic
	Line Chart	Converts an area graph or bar graph to a line graph
	Area Chart	Converts a line graph or bar graph to an area graph
	Bar Chart	Converts a line graph or area graph to a bar graph

Statistics and other applications

Perform this procedure to export statistics to other applications.

Exporting statistics

Procedure Steps

Step	Action
1	To export statistics to a tab-separated file format and import that file to other applications, click the **Export data** button in the tool at the bottom of the Statistics window.

--End--

Graph view methods

You can view graphs from Device Manager statistics using the toolbar, shortcut menu, or the main menu.

Viewing statistics as graphs using the toolbar

Procedure Steps

Step	Action
1	Select the object(s) to graph.
2	On the toolbar, click **Graph Selected**.

3 From the **Statistics** window, select a statistics group tab to view.

4 On the data table, click the right mouse button, and then drag the pointer over the cells to select cells in the same row or column to graph.

5 To select a graph type, click one of the graph buttons at the bottom of the graph window.

6 To print a copy of the graph, click **Print**.

--End--

Viewing statistics as graphs using the shortcut menu
Procedure Steps

Step	Action
1	Select the object(s) to graph.
2	From the shortcut menu, choose **Graph**.
3	From the **Statistics** window, select a statistics group tab to view.
4	On the data table, click the right mouse button, and then drag the pointer over the cells to select cells in the same row or column to graph.
5	To select a graph type, click one of the graph buttons at the bottom of the graph window.
6	To print a copy of the graph, click **Print**.

--End--

Viewing statistics as graphs using the main menu
Procedure Steps

Step	Action
1	Select the object(s) to graph.
2	From Device Manager menu bar, for a stack choose **Graph > Chassis** or, for a port, choose **Graph > Port**.
3	From the **Statistics** window, select a statistics group tab to view.
4	On the data table, click the right mouse button, and then drag the pointer over the cells to select cells in the same row or column to graph.
5	To select a graph type, click one of the graph buttons at the bottom of the graph window.

6	To print a copy of the graph, click **Print**.

--End--

Online help

Online help is context-sensitive and appears in the Web browser.

On Device Manager toolbar, click **Help** to display online help.

Device Manager procedures

Perform the procedures in this section to get, install, and use Device Manager to configure and manage the switch.

Prerequisites

- You must install the application before you can use it because Device Manager is a client application that resides on a computer.

Obtaining Device Manager

Perform this procedure to download Device Manager.

Downloading the application

Procedure Steps

Step	Action
1	Open a Web browser.
2	Enter http://support.nortel.com/support
3	Choose **Support & Training**.
4	Select **Software Downloads**.
5	Select **Network Management**.
6	From **Switches & Routers**, select **Java Device Manager**.
7	Click the latest version.
8	Download the appropriate version for your system.

--End--

Installing Device Manager

Perform the procedures in this section to install Device Manager on a computer. Procedures for two operating systems are included: Microsoft Windows environment and UNIX environment.

Prerequisites for Device Manager installation

Following are general Device Manager installation requirements:

- Before you install a new Device Manager version, Nortel recommends that you remove existing Device Manager versions. Multiple versions of Device Manager can exist on one system, but each version must reside in a separate location.
- If you decide to retain previous versions of Device Manager, you must choose a different folder for the installation process
- To remove existing versions of Device Manager, use the Uninstall DM option. The system created the Uninstall DM option in the Windows Start menu during installation.

Following are the minimum requirements to install Device Manager in a Windows environment:

- Ensure that all previous versions of the software are uninstalled
- Install the new application version in a new directory.
- Use one of these operating systems: Windows NT, Windows 95, Windows 98, Windows 2000, Windows XP, Windows 2003, or Windows Vista.
- Ensure that your CPU is Pentium II 350 MHz or greater.
- Ensure that your computer memory has 256 MB DRAM or better.
- Ensure that your hard drive has at least 300 MB of available space.

Following are the minimum requirements to install Device Manager in a UNIX environment:

- Use one of these operating systems: Sun Solaris 2.8x or higher or Linux Kernel 2.2 or higher.
- Ensure that your computer memory has 128 MB DRAM or better.
- Ensure that your hard drive temporary directory has at least 4 MB of memory.
- Ensure that your hard drive installation directory has at least 300 MB of memory.
- If you use SPARC versions 5.8, 5.9, or 5.10, you must install Sun Solaris operating system patches before installing Device Manager. For more information about obtaining and installing the patch, see "Installing a Sun Solaris patch" (page 35).

Perform this procedure to install a patch for SPARC versions 5.8, 5.9, and 5.10.

Installing a Sun Solaris patch

Procedure Steps

Step	Action
1	On the Solaris workstation, enter the uname -1 command to determine the installed Solaris version.
2	Open a Web browser window and type **sunsolve.sun.com** to access the Sun Microsystems technical support Web site.
3	Follow the directions on the Web page to find and install the appropriate patch.

--End--

Installing from a Windows environment

Procedure Steps

Step	Action
1	To install Device Manager in a Windows environment, close all programs.
2	Locate the downloaded executable Device Manager file on the local computer.
3	Double-click the executable file to start the installation process—file name example, jdm_xxx.exe (xxx represents the software version number_.
4	After the installation programs loads, read and follow the instructions on the **Introductory** window and click **Next**.
5	Read and accept the license agreement and click **Next**.
6	Nortel recommends that you choose the **Typical installation** option on the **Windows Choose Install Sets** window but, if you require a more specialized installation, choose one of the other options, and then click **Next**.
7	On the **Windows Choose Install Folder** window, type a local file system location to install the application. You can also click **Choose** to select a location or click **Restore Default Folder** to restore the default installation location.
8	Click **Next** to proceed.
9	Select a location for Start menu icon placement and click **Next**.
10	Confirm your selections on the **Pre-Installation Summary** window and click **Install** to begin installation.
11	If changes are required, click **Previous** to return to the appropriate location.

12	After the installation process completes, click **Done**.

--End--

Installing from a UNIX environment

Procedure Steps

Step	Action
1	To install Device Manager in a UNIX environment, close all programs. If you use SPARC version 5.8, 5.9, or 5.10, see Device Manager installation prerequisites.
2	Locate the downloaded executable Device Manager file on the local computer.
3	Double-click the executable file to start the installation process.
4	After the installation programs loads, read and follow the instructions on the Introductory screen and click **Next**.
5	Read and accept the license agreement and click **Next**.
6	Nortel recommends that you choose the **Typical installation** option on the **UNIX Choose Install Sets** window but, if you require a more specialized installation, select one of the other options, and then click **Next**.
7	On the **UNIX Choose Install Folder** window type a local file system location to install the application. You can also click **Choose** to select a location or click **Restore Default Folder** to restore the default installation location. Click **Next** to proceed.
8	Confirm your selections on the **Pre-Installation Summary** window and click **Install** to begin installation.
9	If changes are required, click **Previous** to return to the appropriate location and make the changes.
10	After the installation process completes, click **Done**.

--End--

The following table provides the UNIX Device Manager file naming conventions

Operation system	File name
Sun Solaris	jdm_XXXX_solaris_sparc.sh
Linux	jdm_XXXX_linux.sh
XXXX in the file names represents the software version number	

Removing a previous version

Perform this procedure to remove existing Device Manager software.

Prerequisites

- No Uninstall DM option appears in the Windows Start menu.

Uninstalling Device Manager without the Uninstall DM option

Procedure Steps

Step	Action
1	Go to Device Manager software folder.
2	Open the **`UninstallerData`** subfolder.
3	Run the file **`Uninstall Java Device Manager.exe`**.

--End--

Starting Device Manager

Perform the procedures in this section to start Device Manager in Windows and in UNIX environments.

Starting from a Windows environment

Procedure Steps

Step	Action
1	From the **Windows** task bar, choose **Start**.
2	Click **Programs**.
3	Select **Java Device Manager**.
4	Select **DM**.

--End--

Starting from a UNIX environment

Procedure Steps

Step	Action
1	In a UNIX environment, verify that Device Manager installation directory appears in your search path.
2	Enter **`./JDM`**.

--End--

Configuring Device Manager properties

Device Manager uses the Simple Network Management Protocol (SNMP) to configure and manage devices.

Perform the following procedures to set Device Manager properties to configure communication parameters; for example, the polling interval, timeout, and retry count.

Setting properties before access

Procedure Steps

Step	Action
1	To set Device Manager properties for the first time, from Device Manager menu bar, choose **Device > Properties > Current**.
2	Configure the properties in the Properties window.
3	Click **OK**.

--End--

Setting properties after access

Procedure Steps

Step	Action
1	To set Device manager properties after you access a device, from Device Manager menu bar choose **Device > Properties > Devices**.
2	Select the IP address of a device from the Properties Device List.
3	Click **Edit**.
4	Configure the properties in the Properties window.
5	Click **OK**.

--End--

Variable definitions

Variables		Description
Polling	Status Interval	Interval at which the system gathers statistics and status information. For a full stack, set this interval to between 120 and 300 seconds.
	Hotswap Detect every	The frequency at which Device Manager polls for hot swap module information. This value relates to the Status Interval value. For example, if the status Interval is set to 120, and the value for Hotswap Detect every is 2, Device Manager polls the hot swap modules every 240 seconds. For less hot swap polling, set the value to poll every 2 or 3 intervals.
	Enable	Enables (true) or disables (false) periodic polling of the device for updated status. If you disable polling, the chassis status updates only after you choose **Device > Refresh Status**.
SNMP	Retry Count	The number of times Device manager sends the same polling request if a response is not returned. The normal setting is 3 to 4 retries.
	Timeout	Length of each retry of each polling waiting period. If you access the device over a slow connection, increase the timeout interval and change the Retransmission Strategy to superlinear.
	Trace	Choose **Trace** to trace SNMP queries.
	Listen for traps	If selected (enabled), Device Manager listens for traps from the device. If you operate Device Manager from a UNIX platform, to receive traps you must log in as root. The system sends traps in SNMP V2c format, but you can select SNMP V1 trap format for compatibility with older network management systems.
	Max Traps in Log	The specified number of traps in the trap log. The default is 500.
	Trap Port	Specifies the UDP port that Device Manager uses to listen for SNMP traps. The default port is 162.
	Listen for Syslogs	Allows Device Manager to listen to the syslog.
	Confirm row deletion	If selected (enabled), Device Manager displays a confirmation dialog box before deleting a row or entry from a table.
	Default Read Community	Specifies the Default Read Community string. To edit the string, highlight the current value and type over it.
	Default Write Community	Specifies the the Default Write Community string. To edit the string, highlight the current value and type over it.

Variables		Description
Application Control	Application launch with ring tone	Enabled by default, you can modify this field only during configuration of Device Manager default properties, not during configuration of properties for devices.
	Save SNMPv3 Devices Open Last	Disabled by default, if you enable this field the system displays a security warning message because, if you set SNMPv3 devices to open last, users can access the device without entering the SNMPv3 security criteria. If you disable this field, the system erases all SNMPv3 device data saved previously and displays a warning message. You can modify this field only during configuration of Device Manager default properties, not during configuration of properties for devices.
Web Management	Http Port	Specifies the application HTTP port. The default port is 80. To access the Device Home Page using the Web, ensure that the HTTP Port attribute matches the switch configuration. If you change the port number, the system prompts you with a warning message.
Application Launch from JDM	Telnet	Default Telnet is the preset for the operating system. To define a specific Telnet, choose **User-Defined** and specify the Telnet path and parameters.
	SSH	Default SSH is preset in Device Manager. To define a specific SSH, choose **User-Defined** and specify the SSH client path and parameters.

Opening a switch with Device Manager

Perform the procedures in this section to use Device Manager to open a device.

Prerequisites

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

Opening a device

Procedure Steps

Step	Action
1	Start Device Manager.
2	From Device Manager menu, choose **Open > Device** or press **CTRL+O** to open the **Open > Device** window.
3	Enter the switch information on the **Open Device** window.
4	Click **Open**.

--End--

Variable definitions

Variable	Value
Authentication Password	Required if V3 is enabled—specify the current authentication password.
Authentication Protocol	Required if V3 is enabled— identify the authentication protocol used.
Context Name	Specify the context name.
Device Name	A required field, you can enter an IP address or DNS name for the device.
Privacy Password	Required if V3 is enabled—specify the current privacy password.
Privacy Protocol	Required if V3 is enabled—identify the privacy protocol.
Read Community	A required field, you can use the default community string if it is enabled in **Properties Use default community strings**. The default value is public, displayed as ******. The entry is case sensitive.
Use default community strings in properties	If selected, Device Manager uses the default community strings in **Device > Properties**.
User Name	Required if V3 is enabled—enter the name of the user in this field.
v3 Enabled	If selected, the **Open Device** window displays SNMPv3 options.
Write Community	A required field, you can use default community string if it is enabled in **Properties Use default community strings**. The default value is public, displayed as ******. The entry is case sensitive.

Telnet to a switch using Device Manager

Perform these procedures to initiate a Telnet session from Device Manager to the console interface for a switch or stack.

Establishing a Telnet connection from Device Manager main menu

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Device > Telnet**.
2	Follow the instructions on the Telnet screen to continue using NNCLI with the device.

--End--

Establishing a Telnet connection from Device Manager toolbar

Procedure Steps

Step	Action
1	On the toolbar, click the **Telnet** icon.
2	Follow the instructions on the Telnet screen to continue using NNCLI with the device.

--End--

Open an SSH connection to the switch with Device Manager

Perform this procedure to initiate a Secure Shell (SSH) connection to the console interface for a switch or stack.

Prerequisite

- Device must be SSH capable.
- SSH must be enabled.

Establishing an SSH connection

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Device > SSH Connection**.
2	On the toolbar, click **SSH**.

--End--

Trap log

Perform these procedures to configure and view the SNMP trap log.

Prerequisites

- Set the maximum number of trap entries. The default is 500.
- If you use a UNIX platform, log in as root to receive traps.
- If another application uses port 162, disable the other application and restart Device Manager because Device Manager receives traps on port 162 by default.

Setting the maximum number of trap entries for the trap log

Procedure Steps

Step	Action
1	To set the maximum number of trap entries, choose **Device > Properties> Current** from Device Manager menu bar.
2	In **Max Traps In Log**, enter the maximum number of traps to be collected in the trap log.
3	Click **OK**.

--End--

Setting the trap port

Procedure Steps

Step	Action
1	To set the trap port, choose **Device > Properties > Current** from Device Manager menu bar.
2	Deselect **Listen for Traps**.
3	Close **Device > Properties > Current**.
4	Open **Device > Properties > Current**.
5	Select **Listen for traps**.
6	In **Trap Port**, enter the trap port number (Port 162 is the default).
7	Click **OK**.

--End--

Viewing the trap log
Procedure Steps

Step	Action
1	To view the Trap Log, click **Trap Log** on the toolbar or, from Device Manager main menu, choose **Device > Trap Log**.

--End--

Exporting the trap log to a file
Procedure Steps

Step	Action
1	To export the Trap Log to a file, choose **Device > Trap Log** from Device Manager main menu or, from the toolbar, click **Trap Log**.
2	Click **Export** and follow the instructions in the window.

--End--

Accessing Web-based management from Device Manager

Perform this procedure to go to Web-based management from Device Manager.

Opening Web-based management
Procedure Steps

Step	Action
1	To open Web-based management from Device Manager, choose **Actions** from the main menu.
2	Click **Open Home Page**.

--End--

Web-based management concepts

Web-based management is a browser-based application for switch configuration and management. Web-based management requires no separate installation process.

Prerequisites

- Install Microsoft Internet Explorer 4.0 or later, or Netscape Navigator 4.5.1 or later on your management computer.

Navigation

Opening a Web-based management session

Perform this procedure to access Web-based management for a switch.

Prerequisites

- Ensure that the switch has a valid, reachable IP address. Use **`ping`** to verify the IP address or Telnet to the switch IP.
- If the switch is not Layer 3 enabled, ensure that the device can access the management VLAN of the switch, either through a direct connection to a port in the management VLAN or through Layer 3 devices between the device and the switch.

Procedure Steps

Step	Action
1	Open a new Web browser window.
2	In the **Web browser Address** field, type the switch or stack IP address.
3	Press **Enter**.
4	Enter the case-sensitive user name: **RO** for read-only access, **RW** for read-write access.
5	If the system is password protected, enter the password.

--End--

Interface layout

This section describes the common layout of the Web-based management windows.

Each window is divided into two sections: the menu on the left side of the pane, and the management page on the right side of the pane.

Menu

The menu contains the main units of work and their corresponding options. Some options are available only if the switch is part of a stack configuration and are not displayed if a switch is stand-alone.

To use the menu, click a main header; the corresponding options appear in a tree beneath. To display the associated management page, click an option in the tree.

Attention: Nortel recommends that you use the interface navigation tools. The Web browser navigation tools can interfere with the logical navigation of Web-based management.

The following table describes Device Manager Menu options.

Main heading	Options	Description
Summary	Stack Information † Switch Information Identify Unit Numbers † Stack Numbering †	Use Summary to view information about the current state of the switch or stack
Configuration	IP IPv6 System Remote Access SNMVPv1 SNMPv3 ‡ SNMP Trap MAC Address Find MAC Address Port Management High Speed Flow Control Software Download Boot Image Load License File Ascii Config Download Ascii Config Upload Configuration File Console/Comm Port PoE Management (not all switch models are PoE capable) ‡ RTC Time Configuration	Configures switch or stack operation
Fault	RMON Alarm RMON Event RMON Event Log System Log	Configures RMON alarms and events, and view event and system logs
Statistics	Port Port Error Summary Interface Ethernet Errors Transparent Bridging RMON Ethernet RMON History	Use Statistics to view statistics for switch functions

Main heading	Options	Description
Applications	Port Mirroring Rate Limiting EAPOL Security MAC Address Security ‡ IGMP ‡ VLAN ‡ Spanning Tree ‡ MultiLink Trunk Link Aggregation ‡ IP Fix QoS ‡ ADAC ‡	Configures and manages switch applications
Administration	System Information Quick Start Mib Web Page Security ‡ CPU/Memory Utilization Logout Reset Reset to Default	Configure and manage administrative items
Support	Help Release Notes Manuals Upgrade	Access to support facilities
† These options are available only if the switch is part of a stack. ‡ These options have additional, associated options.		

The following table describes Device Manager Menu icons.

Icon	Description
	Collapsed menu title. Click the icon to expand the menu and view all associated options.
	Expanded menu title. All options associated with the menu title display underneath. Click the icon to collapse the menu and hide associated options.
	Menu option. Click the icon to see the management page associated with the menu option.
	Menu option with hyperlink to related pages.

Icon	Description
	Menu option associated with an action. Actions have no associated management page and occur immediately.
	Link to Nortel home page. Click this icon to open a new Web browser window and load the Nortel home page.

Management page

The Management page is the work area. If you select a menu item, the associated Management page appears on the right side of the screen.

Management pages contain one of more of the elements in the following table.

Field	Description
Display	Display fields display preexisting values or statistical information. Display fields are read-only and the background is dim. If the information in the field is highlighted in blue and underlined, it is a hyperlink to a related Management page.
Input	Use input fields to enter or change information. The background of Input fields is white and you can edit them.
Check Box	Use check boxes to set parameters on or off. If a box is blank, the parameter is disabled. Select the check box to change the parameter state.
Icons and buttons	Icons and buttons on a Management page represent actions. Click the icon or button to initiate the action.

Management page icons and buttons are described in the following table.

Icon/button	Name	Description
	Submit	Submits information to the switch. If the Submit button is present, click it to submit changes.
	Modify	Opens a modification page for the data row.
	View	Opens a read-only statistics page for the data row.
	Delete	Deletes the data row.

	Help	Opens Help for the current Management page in a new Web browser window.
	Context-sensitive Help	Opens Help for the current data item in a new Web browser window

Feature licensing fundamentals

This chapter provides information to help you understand, install, and manage feature licensing. Review this section before you use licensed features or before you make changes to the license configuration.

Navigation

Feature licenses

This section describes the types of licenses and lists the features that require a license. You purchase switches and licenses separately.

To enable certain features, Nortel Ethernet Routing Switches support

- an Advanced License
- a Trial License

Licenses support the following features:

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

To enable Advanced License features on an Ethernet Routing Switch 5000 Series, you must

- purchase an Advanced License Kit
- generate a license file on the Nortel electronic licensing portal
- install a license file on the switch

Each License Kit contains

- a Software License Certificate
- a License Authorization Code (LAC) for a specific number of licenses

The License Certificate contains printed instructions that describe how to

- deposit license entitlements (LACs) into a license bank
- enter switch MAC addresses
- generate the license file
- install the license file on a switch to unlock licensed features

You can install a one time Trial License to enable licensed features on a switch for 30 days. You can obtain the trial license on the Nortel Web site. Configure Trial License Support through Nortel Networks Command Line Interface (NNCLI) or the ASCII Configuration Generator (ACG). Software monitors and tracks the trial version of the feature license.

At the end of the 30 day trial period, the system disables all of the licensed features except Split MultiLink Trunking (SMLT). To prevent loop formation, SMLT remains active until you reset the stack or unit.

To minimize network impact, the following events occur prior to Trial License expiry:

- Five days prior to license expiration the system sends a trap. Nortel recommends that you manually disable SMLT and remove cabling loops after you receive the first trap because, after you reset the stack or unit, a loop forms if you do not disable ports participating in the InterSwitch Trunk (IST).
- One day prior to license expiration the system sends a second trap.
- The system sends a final trap at license termination.
- The system disables all licensed features, except SMLT, after it sends the final trap.

See the following table for the text of the traps you receive prior to, and at, Trial License termination.

Days prior to Trial License termination	Trap text
Five	`Trap: bsnTrialLicenseExpiration: Trial license 1 will expire in 5 day(s).`
One	`Trap: bsnTrialLicenseExpiration: Trial license 1 will expire in 1 day(s).`
At Trial License termination	`Trap: bsnTrialLicenseExpiration: Trial license 1 has expired.`

License file generation

This section describes what you must do after you purchase a License Kit.

After you purchase a License Kit, you must generate the license file on the Nortel licensing portal at www.nortellicensing.com. The Nortel licensing portal acts as a license bank—an electronic repository for all license entitlements and licenses.

The License Certificate in the License Kit contains the License Authorization Code (LAC). After you enter the LAC on the licensing portal, the system deposits license entitlements into your license bank. Then you can use one or more switch MAC addresses to generate a license file. Because the system generates the software license file based on the switch MAC address, the license file must contain the authorized MAC addresses of the switches where the license file is installed.

You can generate an individual license file with one or multiple switch MAC addresses and you can add MAC addresses to the same license file at a later time. One license file can support up to 1000 unique MAC addresses.

To support licensed features in a switch stack, ensure that you generate the license from the MAC address of the base unit.

To ensure that licensed features continue to operate if the Base Unit (BU) in a switch stack fails, Nortel recommends that you also enter the MAC address of the Temporary Base Unit (TBU), in addition to the MAC address of the BU, when you generate a license file for a stack of two or more switches.

You can purchase License Kits in combinations. For example, to enable licensed features for 22 MAC addresses, order one AL1016001 kit and one AL1016002 kit. The two kits provide licenses for a total of 22 MAC addresses.

The following table provides the License Kit order codes, license type descriptions, and number of licenses supported for each license kit.

Part number/order code	License type and description	Number of switches or MAC addresses supported
AL1016001	Ethernet Routing Switch 5000 Advanced License Kit, for 1 switch/stack. Enabled features: IPFIX, SMLT, OSPF, ECMP, VRRP and PIM-SM (one license required per stack or standalone unit).	1 switch/stack (2 MAC addresses)
AL1016002	Ethernet Routing Switch 5000 Advanced License Kit, for up to 10 switches/stacks. Enabled features: IPFIX, SMLT, OSPF, ECMP, VRRP and PIM-SM (one license required per stack or standalone unit).	10 switches/stacks (20 MAC addresses)
AL1016003	Ethernet Routing Switch 5000 Advanced License Kit, for up to 50 switches/stacks. Enabled features: IPFIX, SMLT, OSPF, ECMP, VRRP and PIM-SM (one license required per stack or standalone unit).	50 switches/stacks (100 MAC addresses)
AL1016004	Ethernet Routing Switch 5000 Advanced License Kit, for up to 100 switches/stacks. Enabled features: IPFIX, SMLT, OSPF, ECMP, VRRP and PIM-SM (one license required per stack or standalone unit).	100 switches/stacks (200 MAC addresses)

Once you receive the license file, to access licensed features, you must install the license file on the switch.

Generating a license

Perform this procedure to generate a license file.

Prerequisites

- Purchase a License Kit containing a License Certificate with a License Authorization code (LAC). For more information, contact your Nortel sales representative.
- Ensure that a properly configured TFTP server resides in your network.
- Assign IP addresses to all switches.
- Obtain the switch base MAC addresses for the switches that use licensed features—perform the NNCLI command **`show sys-info`** to obtain base MAC addresses.
- Ensure that your browser does not automatically decompress the compressed binary license file.
- After you create the license file at the site identified in the License Kit, you must specify a file name; example: building100_ers5000.lic.

License file names must conform to the following restrictions:

- maximum of 63 alphanumeric characters
- lower case only
- no spaces or special characters permitted
- underscore (_) permitted
- doc (.) and a three character file extension required

If you need to include multiple MAC addresses in a license file, use a text-based file that conforms to the following rules:

- ASCII file format
- one MAC address on a line
- no other characters, spaces, or special characters permitted
- MAC addresses in hexadecimal, capitalized format, each pair of characters separated by colons: example, (XX:XX:XX:XX:XX:XX)
- file must contain correct MAC addresses—incorrect MAC addresses result in licensed features not working on designated units
- number of MAC addresses must not exceed the number of MAC addresses allowed for the LAC entered for a file as described in the following table:

Procedure Steps

Step	Action
1	Use a Web browser to go to the Nortel licensing portal at www.nortellicensing.com.
2	Type your contact information in the required boxes.
3	Create a new license bank or provide details of an existing license bank.
4	Select an E-mail notification option to receive newly generated licenses—after the system generates the license file, it is sent by e-mail to the address you specified.
5	Enter the License Authorization Code provided on the License Certificate.
6	Click **Submit**, and then wait for the confirmation message.
7	After you receive the confirmation message, click **Go to License Bank to Download License**.
8	In the License Bank window, select the LAC for the license you want to generate.
9	Click **Generate License**.
10	In the Generate License window, enter the MAC address of the switch or the MAC address of the Base Unit (BU) and Temporary

Base Unit (TBU) of the stack, or a text file that contains a list of MAC addresses, enter the license file name, and enter additional details as required.

11 Click **Generate License File**.

--End--

License file installation

This section describes what you must do after you generate the license file.

After you obtain the license file, you must install the license file on the switch to unlock the licensed features.

You can install a license file in flash memory or on a TFTP server.

Provided that you name the license file in accordance with accepted file naming conventions, you can apply your choice of file name and extension to a license file generated on the Nortel licensing portal.

Do not specify a license file location—the system records and stores the license file name while you copy the license file to the switch.

Installing a license file using NNCLI

Perform this procedure to use NNCLI to install a license file on a switch.

Attention: If you reset the switch to default, you must reinstall the license file on the switch, and restart the switch, to reactivate the licensed features. The reset removes the software license from the switch because the system stores the license file in nonvolatile random access memory (NVRAM).

Prerequisites

- Store the license on a TFTP server.
- Ensure that you have the correct license file—the license file contains the MAC address of the switch where you are installing the license.
- Ensure that your browser does not automatically decompress the compressed binary license file.

Procedure Steps

Step	Action
1	At the Privileged Executive command prompt, enter **copy tftp license <A.B.C.D> <WORD>**.
2	Restart the switch.

Attention: Nortel recommends that you schedule switch restart during a normal maintenance window.

--End--

Variable definitions

Variable	Value
<A.B.C.D>	TFTP server address
<WORD>	Software license file name on the TFTP server

Displaying an existing software license using NNCLI

Perform this procedure to display the license installed on the switch.

Procedure Steps

Step	Action
1	At any command prompt, enter **show license { <1-10> | all}**

--End--

Variable definitions

Variable	Value
<1-10>	Displays the selected licenses
all	Displays all licenses

Deleting an existing license using NNCLI

Perform this procedure to delete the software license file from the switch.

Procedure Steps

Step	Action
1	At the Privileged Executive command prompt, enter `clear license { <1-10> | all}`

--End--

Variable definitions

Variable	Value
`<1-10>`	Displays the selected licenses
`all`	Displays all licenses

Installing a license file using Device Manager

Perform this procedure to use Device Manager to install a license file on a switch.

Procedure Steps

Step	Action
1	From Device Manager main menu bar, choose **Edit > File System**.
2	Click **License File**.
3	In **TftpServerInetAddressType**, select the system IP version.
4	In **TftpServerInetAddress**, enter the TFTP server IP address.
5	In **LicenseFileName**, enter the software license file name.
6	In **LicenseFileAction**, select **dnldLicense**.
7	Click **Apply**.
8	The system generates a restart warning message; click **Yes** to restart the switch and then activate the license, or click **No** to cancel license installation.

--End--

Variable definitions

Variable	Value
TftpServerInetAddressType	The system IP version
TftpServerInetAddress	TFTP server IP address
LicenseFileName	Name of the license file
LicenseFile Action	Select **dnldLicense** to download the license file

License file transfer

This section describes some situations that can require license transfer.

Under the following conditions, you need to transfer a license on the Nortel Licensing portal:

- replacement of failed switch with a new MAC address
- incorrect MAC address entered on the Nortel License portal during license file generation
- the system displays an error message indicating that you exceed the number of MAC address swaps for a license—for each License authorization Code (LAC) you can swap up to 10% of the MAC addresses; contact Nortel Technical Support to obtain a new LAC

Transferring a license

Perform this procedure to transfer a license from one switch to another.

Procedure Steps

Step	Action
1	In the Web browser, go to the Nortel licensing portal at www.nortellicensing.com.
2	Click **License Bank**.
3	Enter your user name and password.
4	In the **License Bank**, select the License Authorization Code (LAC) entry associated with the license type.
5	Click **View Details**.
6	Select a transaction that contains the license file name from the switch you are replacing.
7	Click **Replace Switch**.
8	In **Step 1: Enter Replacement MAC Address**, enter the new MAC address.
9	In **Step 2: select the MAC Address to Replace**, select the entry for the MAC address that you want to replace.
10	Click **Replace Switch MAC**. If you exceed the MAC replacement threshold, a message appears confirming that the MAC swap is unsuccessful.
11	Select a different LAC entry and try again. If no other LAC entries appear in the list, contact Nortel Technical Support.
12	After the system displays *MAC swap successful*, click **Return to License Bank Details**.

13 Select the transaction that contains the license file name with the new MAC address.

14 Click **Download**.

--End--

Configuration files fundamentals

This chapter provides fundamental information about working with configuration files.

Configuration files are ASCII text files that allow the administrator to quickly change switch configuration.

Procedures to manage binary configuration files are included in the Device Manager section.

Navigation

NNCLI configuration files

This section provides procedures that you can use to display, store, and retrieve configuration files, and to save the current configuration by using Nortel Networks Command Line Interface (NNCLI). Procedures for Universal Serial Bus (USB) devices apply only to switch models with USB ports.

Navigation

Viewing the current configuration

Perform this procedure to display the current configuration.

Procedure Steps

Step	Action
1	At the command prompt, enter **enable** to enter the Privileged EXEC NNCLI mode.
2	At the prompt, enter **show running-config**.

--End--

Saving the current configuration

Perform this procedure to save the current configuration to a TFTP server or USB device.

Procedure Steps

Step	Action
1	At the command prompt, enter **enable** to enter the Privileged EXEC NNCLI mode.
2	At the prompt, enter **copy running-config {tftp | (usb) [u2]} address <A.B.C.D> filename <name>**.

--End--

Variable definitions

Variable	Value
address <A.B.C.D>	Specifies the TFTP server IP address.
filename <name>	Specifies the configuration file name.
{tftp | usb}	Specifies whether to save the file to a TFTP server or a USB mass storage device—not all switch models have a USB port.

Saving the current configuration to flash memory

Perform this procedure to save the current configuration to flash memory (NVRAM).

Procedure Steps

Step	Action
1	At the command prompt, enter **enable** to enter the Privileged EXEC NNCLI mode.

2	At the prompt, enter **copy config nvram**.

--End--

Restoring a system configuration from a USB device

Perform this procedure to copy a configuration stored on a USB device.

Procedure Steps

Step	Action
1	At the command prompt, enter **enable** to enter the Priviliged EXEC NNCLI mode.
2	At the prompt, enter **copy usb config filename <name>**.

--End--

Restoring a system configuration from a TFTP server

Perform this procedure to copy a configuration stored on a TFTP server.

Procedure Steps

Step	Action
1	At the command prompt, enter **enable** to enter the Priviliged EXEC NNCLI mode.
2	At the prompt, enter **copy tftp config address <A.B.C.D> filename <name>**.

--End--

Copying a stack unit configuration to a stand-alone switch

Perform this procedure to copy a stack unit configuration to a stand-alone switch.

Procedure Steps

Step	Action
1	At the command prompt, enter **enable** to enter the Privileged EXEC NNCLI mode.
2	At the prompt, enter **copy tftp config unit address <A.B.D.C> filename <name> unit <unit number>**.

--End--

Variable definitions

Variable	Value
address <A.B.C.D>	Specifies the TFTP IP address.
filename <name>	Specifies the configuration file name.
unit <unit number>	Specifies the stack unit number.

Downloading a configuration file automatically at startup

Perform this procedure to download a configuration automatically at switch startup.

Procedure Steps

Step	Action
1	At the command prompt, enter **enable** to enter the Privileged EXEC NNCLI mode.
2	At the prompt, enter the **configure network load-on-boot {disable | use-bootp |use-config} address <A.B.C.D> filename <name>** command to configure a switch or stack to automatically load a configuration file.

--End--

Variable definitions

Variable	Value
load-on-boot {disable | use-bootp | use-config}	Specifies the setting to automatically load a configuration file while the system starts. **disable** disables the automatic loading of the configuration file. **use-bootp** specifies loading the ASCII configuration file at startup and using BootP to obtain values for the TFTP address and file name. **use-config** specifies loading the ASCII configuration file at startup and using the locally configured values for the TFTP address and file name. If you omit the variables, the system immediately downloads and runs the ASCII configuration file.

Device Manager configuration files

This section provides Device Manager procedures you can use to manage configuration files.

You can use these procedures to

- save the current ASCII configuration file on a TFTP server
- save the current ASCII configuration on a USB storage device
- retrieve an ASCII configuration file, from a TFTP server, to apply to a switch
- retrieve an ASCII configuration file, from a USB storage device, to apply to a switch
- save a binary configuration file
- retrieve a binary configuration file
- manually save the current configuration to flash memory

Procedures for USB storage devices apply only to switch models with USB ports.

Navigation

- "Storing the current ASCII configuration file on a TFTP server" (page 65)
- "Storing the current ASCII configuration file on a USB device" (page 66)
- "Downloading an ASCII configuration file from a TFTP server" (page 66)
- "Downloading an ASCII configuration file from a USB device" (page 67)
- "Downloading an ASCII configuration file automatically " (page 67)
- "Storing a binary configuration file on a TFTP server" (page 67)
- "Storing a binary configuration file on a USB device" (page 68)
- "Downloading a binary configuration file from a TFTP server" (page 68)
- "Downloading a binary configuration file from a USB device" (page 69)
- "Saving the current configuration to flash memory manually" (page 69)

Storing the current ASCII configuration file on a TFTP server

Perform this procedure to save the current ASCII configuration file on a TFTP server.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit > File System**.
2	Click **Ascii Config File** .
3	In **TftpServerInetAddress**, type the TFTP server address.
4	In **AsciiConfigFilename**, type the configuration file name.

5	In **AsciiConfigManualUpload**, click **uploadNow**.
6	Click **Apply**.

--End--

Storing the current ASCII configuration file on a USB device

Perform this procedure to save the current ASCII configuration file on a USB device.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit > File System**.
2	Click **Ascii Config File** .
3	In **TftpServerInetAddress**, type the configuration file name.
4	In **UsbTargetUnit**, enter the stack unit number where the USB device is inserted.
5	In **AsciiConfigManualUpload**, click **uploadToUsb**.
6	Click **Apply**.

--End--

Downloading an ASCII configuration file from a TFTP server

Perform this procedure to download an ASCII configuration file from a TFTP server.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit >File System**.
2	Click **Ascii Config File**.
3	In **TftpServerInetAddress**, type the TFTP server IP address.
4	In **AsciiConfigFilename**, type the configuration file name.
5	In **AsciiConfigManual-Download**, click **downloadNow** to transfer the file from the TFTP server to the switch.
6	Click **Apply**.

--End--

Downloading an ASCII configuration file from a USB device

Perform this procedure to download an ASCII configuration file from a USB device.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit >File System**.
2	Click **Ascii Config File**.
3	In **TftpServerInetAddress**, type the configuration file name.
4	In **UsbTargetUnit**, enter the stack unit number where the USB device is inserted.
5	In **AsciiConfigManual-Download**, click **downloadFromUsb** to transfer the file from the USB device to the switch.
6	Click **Apply**.

--End--

Downloading an ASCII configuration file automatically

Perform this procedure to download an ASCII configuration automatically at switch startup.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit > File System**.
2	Click **AsciiConfigFile**.
3	In **TftpServerInetAddress**, type the TFTP server IP address.
4	In **AsciiConfigFilename**, type the configuration file name.
5	From **AsciiConfigAutoDownload**, click the appropriate download option: **disabled** to disable automatic download, **useBootp** to obtain TFTP server connection settings, or **useConfig** to use the TFTP settings on screen to connect to the TFTP server.
6	Click **Apply**.

--End--

Storing a binary configuration file on a TFTP server

Perform this procedure to store a binary configuration file on a TFTP server.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit > File System**.
2	Click **Config/Image/Diag file**.
3	In **TftpServerInetAddress**, enter the TFTP server IP address.
4	In **BinaryConfigFilename**, enter the configuration file name.
5	In **Action**, click **upldConfig**.
6	Click **Apply**.

--End--

Storing a binary configuration file on a USB device

Perform this procedure to store a binary configuration file on a USB device.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit > File System**.
2	Click **Config/Image/Diag file**.
3	In **BinaryConfigFilename**, enter the configuration file name.
4	In **UsbTargetUnit**, enter the stack unit number or, for a stand-alone switch, enter 0.
5	In **Action**, click **upldConfigtoUsb**.
6	Click **Apply**.

--End--

Downloading a binary configuration file from a TFTP server

Perform this procedure to download a binary configuration file from a TFTP server.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit > File System**.
2	Click **Config/Image/Diag file**.
3	In **TftpServerInetAddress**, enter the TFTP server IP address.

4 In **BinaryConfigFilename**, enter the configuration file name.

5 In **Action**, click **dnldConfig**.

6 Click **Apply**.

--End--

Downloading a binary configuration file from a USB device

Perform this procedure to download a binary configuration file from a USB device.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit > File System**.
2	Click **Config/Image/Diag file**.
3	In **BinaryConfigFilename**, enter the configuration file name.
4	In **UsbTargetUnit**, enter the stack unit number where the USB is inserted.
5	In **Action**, click **dnldConfigFromUsb**.
6	Click **Apply**.

--End--

Saving the current configuration to flash memory manually

Perform this procedure to save the current configuration to flash memory manually.

Procedure Steps

Step	Action
1	From Device Manager main menu, choose **Edit > File System**.
2	Click **Save Configuration**.
3	Deselect **AutosavetoNvramEnabled** to disable automatic flash memory storage of the current configuration.
4	In **Action**, select **copyConfigToNvram**.
5	Click **Apply**.
6	Click **Refresh** to check progress of the configuration download.

--End--

Web-based management configuration files

This section provides the Web-based management procedures you can use to upload or download configuration files.

Procedures for USB storage devices apply only to switch models with USB ports.

Navigation

Storing a configuration file on a TFTP server

Perform this procedure to store a configuration on a TFTP server.

Procedure Steps

Step	Action
1	From the Web-based management main page, choose **Configuration > Configuration** file.
2	In **Configuration Image Filename**, enter the name of the configuration file.
3	In **Select Target**, choose **TFTP Server**.
4	In **TFTP Server IP Address**, enter the TFTP server IP address.
5	In **Copy Configuration Image To Target**, select **Yes**.
6	In **Retrieve Configuration Image From Target**, select **No**.
7	Click **Submit**.

--End--

Storing a configuration file on a USB device

Perform this procedure to store a configuration file on a Universal Serial Bus (USB) storage device.

Procedure Steps

Step	Action
1	From the Web-based management main page, choose **Configuration > Configuration File**.
2	In **Configuration Image Filename**, enter the configuration file name.
3	In **Select Target**, select **USB**.
4	In **Copy Configuration Image to Target**, select **Yes**.
5	In **Retrieve Configuration Image From Target**, select **No**.
6	Click **Submit**.

--End--

Retrieving a configuration file from a TFTP server

Perform this procedure to download a configuration file from a TFTP server.

Procedure Steps

Step	Action
1	From the Web-based management main page, choose **Configuration > Configuration File**.
2	In **Configuration Image Filename**, enter the configuration file name.
3	In **Select Target**, select **TFTP**.
4	In **TFTP Server IP Address**, enter the TFTP server IP address.
5	In **Copy Configuration Image To Target**, select **No**.
6	In **Retrieve Configuration Image from Target**, select **Yes**.
7	Click **Submit**.

--End--

Retrieving a configuration file from a stack unit switch to a stand-alone switch

Perform this procedure to download a configuration file from a stack unit switch to a standalone switch.

Procedure Steps

Step	Action
1	From the Web-based management main page, choose **Configuration > Configuration File**.
2	In **Copy Configuration Image To Target**, select **No**.
3	In **Retrieve Configuration Image from Target**, select **Yes**.
4	In **Select Target**, select a USB number to copy the configuration from.
5	Click **Submit**.

--End--

Retrieving a configuration file from a USB device

Perform this procedure to download an ASCII configuration file from a Universal Serial Bus (USB) storage device.

Procedure Steps

Step	Action
1	From the Web-based management main page, choose **Configuration > Ascii Config Download**.
2	Select **Ascii Configuration USB File Download Setting**.
3	In **Select Target**, select **USB**.
4	In **Ascii Configuration file**, type the name of the configuration file.
5	In **Retrieve Configuration File from Target**, select **Yes**.
6	Click **Submit**.
7	View the *Last Manual Configuration Status* field for the outcome of the operation.

--End--

Retrieving a configuration file through HTTP

Perform this procedure to download an ASCII configuration file using HTTP.

Procedure Steps

Step	Action
1	From the Web-based management main page, choose **Configuration > Ascii Config Download**.
2	Select **Ascii Configuration File Download Setting**.
3	In **Ascii Configuration File**, type the configuration file name, including the full local path or you can click **Browse** to locate the configuration file.
4	Click **Submit**.
5	View the *Last Manual Configuration Status* field for the outcome of the operation.

--End--

Supported standards and Request for Comments

This chapter lists the standards and Request for Comments (RFC) supported by the switch.

Navigation

Standards

The standards in the following list are supported on the switch:

- IEEE 802.1D (Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (Virtual Local Area Network, VLAN, Tagging)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1X (Extensible Authentication Protocol over LAN, EAPOL)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gibabit Ethernet over Copper)
- IEEE 802.3x (Flow Control)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.1ab (Link Layer Discovery Protocol)

RFCs

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

- RFC 791 (IP)
- RFC 894 (IP over Ethernet)

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

Quick reference for basic NNCLI tasks

Use this chapter as a quick reference for frequently used Nortel Networks Command Line Interface (NNCLI) tasks.

For more information about using NNCLI, see "User interface fundamentals" (page 15).

For detailed configuration information, see the function-specific configuration documents for this product.

For a list of documents, see *Nortel Ethernet Routing Switch 5000 Series Documentation Roadmap* (NN47200-103).

Navigation

- "Enable NNCLI as the default interface" (page 83)
- "Disable the switch front user interface (UI) button" (page 83)
- "Check a configuration" (page 83)

Connect to the switch

Switch connection options are

- remote
- console

The following table lists the access method for three types of connection.

Secure Shell (SSH) enabled	SSH not enabled	Console access available
Remote access	Telnet access	Normal console connection access

Start NNCLI from the main menu

To start a configuration using the NNCLI, choose Command Line Interface from the main menu.

At the prompt, perform the commands in the following table.

Command	Purpose
`enable`	Enter configuration mode
`config t`	Start configuration

NNCLI command modes

NNCLI provides command modes to separate basic user tasks from control and management of the switch.

NNCLI command modes are

- User Executive (exec mode)
- Privileged Executive (privExec mode)
- Global Configuration (config mode)
- Interface Configuration (ifconfig mode)
- Router Configuration (config-router mode)

You must use the correct mode to perform certain functions.

For more information about NNCLI, see "NNCLI concepts" (page 15).

Use factory default configuration

To restart the switch using the factory default configuration, perform the commands in the following table.

Command	Purpose
`exit`	Exit the configuration mode
`boot default`	Return a switch, or switches, to factory default configuration

Configure the management IP address

To configure and verify the Management IP Address, perform the commands in the following table.

Command	Purpose
`ip address <IP> netmask <mask>`	Set the management IP and mask
`ip default-gateway <default gateway IP>`	Set the default gateway IP address
`ping <default gateway IP>`	Verify connectivity
`show ip`	Verify configuration

Configure Simple Network Management Protocol (SNMP)

To configure SNMP, perform the commands in the following table.

Command	Purpose
`snmp-server enable`	Enable SNMP (the default setting is disabled)
`snmp-server authentication-trap enable`	Enable authentication traps
`snmp-server community ro`	Set the read-only community name (requirement: enter community string twice)
`snmp-server community rw`	Set the read-write community name (requirement: enter community string twice)
`snmp-server contact "whatever you want"`	Set contact information
`snmp-server location "<Building & Closet #>`	Set building name and closet information
`snmp-server name "<switch IP address>"`	Maintain coherent Syslog messages
`snmp-server host <host IP> <communit y>`	Set IP address of trap receiver
`show sys-info`	Verify configuration
`show snmp host`	Verify configuration

Configure VLANs and tagged uplinks

To configure Virtual Local Area Networks (VLAN) and tagged uplinks, perform the commands in the following table.

Command	Purpose
Vlan configcontrol automatic	Automatically delete old VLANs and update PVID after you add a VLAN to an untagged port (the setting appears at the bottom of the VLAN configuration information).
vlan ports <uplink port> tagging tagall	Enable tagging on the uplink.
vlan ports <uplink port> filter-untagged-frame enable	Discard untagged frames.
vlan ports ALL filter-unregistered-frame disable	Break Spanning Tree Protocol (STP) for Voice over Internet Protocol (VoIP).
vlan create <VID> type port	Create the port based VLAN and assign the 802.1q identifier.
vlan name <VID> <name>	Name the VLAN according to conventions.
vlan members add <VID> <port listing>	Add ports to appropriate VLANs.
vlan mgmt <VID>	Set the management VLAN.
vlan members remove 1 ALL	Remove all ports from VLAN 1.
vlan ports <uplink port> pvid <VID>	Set the PVID on the uplink.
show vlan	Verify VLAN configuration.
show vlan interface info	Verify configuration of PVID and port type.

Configure Internet Group Management Protocol (IGMP)

To configure IGMP, perform the commands in the following table.

Command	Purpose
vlan igmp <VID> snooping enable	Enable IGMP snooping on each appropriate VLAN
vlan igmp <VID> proxy enable	Enable IGMP proxy on each appropriate VLAN
show vlan igmp <VID>	Show IGMP information for each appropriate VLAN

Configure a port

To configure a port, perform the commands in the following table.

Command	Purpose
interface fastEthernet <end-user port list>	Enter configuration mode at the interface level where you can configure multiple ports, excluding uplink ports, simultaneously.

Command	Purpose
auto-negotiation-advertisements 10-full 10-half 100-full 100-half pause-frame	Set 10/100 ports to advertise only 10Mb/s half-duplex and 100Mb/s half-duplex.
default auto-negotiation-advertisement	Advertise Gigabit for Gigabit ports because Custom Autonegotiation Advertisements (CANA) is not appropriate for Gigabit ports.
poe poe-shutdown	Power Over Ethernet (PoE) is on by default; use this command to disable PoE on non-PoE ports.
no poe-shutdown	Enable PoE for AP ports.
shutdown <port>	Disable unused ports.
spanning-tree learning fast	Set fast spanning tree learning on access ports.
name <port name>	Name uplink ports. If you need dual uplinks, Nortel recommends that you add a second switch, in a stack, and use port 48 of the second switch as the second uplink.
qos dhcp snooping enable interface-type access	Enable Dynamic Host Configuration Protocol (DHCP) Snooping and drop incoming DHCP replies on specified ports.
Exit	Terminate port configuration.
interface fastEthernet <uplink port>	Enter configuration mode at the interface level to configure port 48 as an uplink port .
speed auto	Enable autonegotiate.
spanning-tree learning <normal or disable>	Depending on the upstream switch location, set spanning tree to normal or disabled.
name UP-<Switch IP Address>-<Slot>/<Port>	Example: UP-128.206.95.254-1/2
qos dhcp snooping enable interface-type core	Enable DHCP Snooping with DHCP replies.
Exit	Terminate uplink configuration.
show interfaces all	Display interface settings.

Configure passwords

To configure NNCLI passwords, perform the commands in the following table.

Command	Purpose
cli password serial local	Set the switch or stack to use local passwords for serial port access.
cli password telnet local	Set the switch or stack to use local passwords for telnet access.

Command	Purpose
no password security	Remove password complexity and change frequency restrictions.
cli password read-only	Set the read-only password (you must enter the password twice).
cli password read-write	Set the read-write password.

Configure Secure Shell (SSH)

To configure SSH, perform the commands in the following table.

Command	Purpose
ssh pass-auth	Enable password authentication for SSH. To use SSHv2 for switch access, ensure that you use SecureCRT 4.1 or later, Putty, or Linux SSH.
ssh	Enable SSH support.
show ssh global	Display SSH settings.

Configure Telnet

To disable Telnet access, at the prompt enter the command **telnet-access disable**

Configure Simple Network Time Protocol (SNTP)

To configure SNTP, perform the commands in the following table.

Command	Purpose
sntp server primary address <IP address>	Set SNTP server address where <IP address> is the address of the SNTP server in decimal notation.
sntp enable	Enable SNTP.
show sntp	Display SNTP settings SNTP . The SNTP default setting is Greenwich Mean Time (GMT).

Configure log settings

To configure log settings, perform the commands in the following table.

Command	Purpose
logging volatile overwrite	Allow log to roll over if the buffer is full.
logging remote address <syslog server IP>	Set syslog server.
logging remote level informational	Log all events.
logging remote enable	Enable syslogging.

Configure Secure Socket Layer (SSL)

To configure SSL, perform the commands in the following table.

Command	Purpose
ssl certificate	Create a certificate for use on the next startup or SSL reset. For switches that include a secure Web server (for example, Ethernet Routing Switch 5510), Nortel recommends that you replace the generic certificate with a new certificate generated by the **ssl certificate** command.
ssl	Enables SSL server.
show ssl	Displays SSL settings.

Configure access control

To configure access control, perform the commands in the following table.

Command	Purpose
ipmgr source-ip 1 <trusted net> mask <mask>	Enables management from the trusted net.
ipmgr source-ip 2 <trusted net2> mask <mask>	Enables management from trusted net 2.
show ipmgr	Displays access control configuration.

Enable NNCLI as the default interface

To designate NNCLI as the default interface, perform the commands in the following table.

Command	Purpose
exit	Exit configuration mode to return to the enable prompt.
cmd-interface cli	Set NNCLI as the default command interface.

Disable the switch front user interface (UI) button

To disable the UI button on the switch front, at the prompt enter the command

No ui-button enable

Check a configuration

To display the switch configuration, at the prompt enter the command

show running-config

Nortel Ethernet Routing Switch 5000 Series

Fundamentals

Printed in Canada and the United States of America
Release: 6.0
Publication: NN47200-104
Document status: Standard
Document revision: 01.01
Document release date: 12 November 2008

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

www.nortel.com

NORTEL