Part No. 217105-A
June 2005

4655 Great America Parkway
Santa Clara, CA 95054

System Configuration Guide

Nortel Ethernet Switches 460 and 470
Software Release 3.6

NORTEL

International regulatory statements of conformity

This is to certify that the Nortel Ethernet Switches 460 and 470 were evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC - Electromagnetic Emissions – CISPR 22, Class A
- EMC - Electromagnetic Immunity – CISPR 24
- Electrical Safety – IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed below.

National electromagnetic compliance (EMC) statements of compliance

FCC statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

ICES statement (Canada only)

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Nortel Ethernet Switches 460 and 470) do not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Nortel Ethernet Switches 460 and 470) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

CE marking statement (Europe only)

EN 55 022 statements

This is to certify that the Nortel Ethernet Switches 460 and 470 are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

Caution: This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case the user may be required to take appropriate measures.

EN 55 024 statement

This is to certify that the Nortel Ethernet Switches 460 and 470 are shielded against the susceptibility to radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of
EN 55 024 (CISPR 24).

CE Declaration of Conformity

This product conforms to the provisions of the R&TTE Directive 1999/5/EC.

VCCI statement (Japan/Nippon only)

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI statement for Ethernet Switches 460 and 470 (Taiwan only)

This is a Class A product based on the standard of the Bureau of Standards, Metrology and Inspection (BSMI) CNS 13438, Class A.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

MIC notice for Ethernet Switches 460 and 470 (Republic of Korea only)

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Ministry of Information and Communications (MIC). This device may not be sold for use in a non-business application.

Observe the Regulatory Marking label on the bottom surface of the chassis for specific certification information pertaining to this model. Each model in the Ethernet Switch Series which is approved for shipment to/usage in Korea is labeled as such, with all appropriate text and the appropriate MIC reference number.

National safety statements of compliance

CE marking statement (Europe only)

EN 60 950 statement

This is to certify that the Nortel Ethernet Switches 460 and 470 are in compliance with the requirements of EN 60 950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance.

NOM statement Ethernet Switches 460 and 470 (Mexico only)

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Méxicana (NOM):

Exporter:	Nortel Networks, Inc. 4655 Great America Parkway Santa Clara CA 95054 USA
Importer:	Nortel Networks de México, S.A. de C.V. Avenida Insurgentes Sur #1605 Piso 30, Oficina Col. San Jose Insurgentes Deleg-Benito Juarez México D.F. 03900
Tel:	52 5 480 2100
Fax:	52 5 480 2199
Input:	Ethernet Switch 460, Ethernet Switch 470
	100 - 120 VAC 16A 50 to 60 Hz
	200 - 240 VAC 12 A 50 to 60 Hz

Información NOM (unicamente para México)

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Méxicana (NOM):

Exportador:	Nortel Networks, Inc. 4655 Great America Parkway Santa Clara, CA 95054 USA
Importador:	Nortel Networks de México, S.A. de C.V. Avenida Insurgentes Sur #1605 Piso 30, Oficina Col. San Jose Insurgentes Deleg-Benito Juarez México D.F. 03900
Tel:	52 5 480 2100
Fax:	52 5 480 2199
Embarcar a:	Ethernet Switch 460, Ethernet Switch 470
	100 - 120 VAC 16A 50 to 60 Hz
	200 - 240 VAC 12 A 50 to 60 Hz

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 MERCHANTABLITITY 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**
    a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government,

the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-Odd entities) and 48 C.F.R. 227.7202 (for Odd entities).

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

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

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

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

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

Revision History

Date Revised	Version	Reason for revision
June 2005	1.0	Created new document structure and incorporated new features for Ethernet Switch Release 3.6 software.

Contents

Figures

Tables

Preface

About this guide

This guide provides information about configuring and managing basic switching features on the Ethernet Switch 460 and Ethernet Switch 470.

Network management tools and interfaces

The following are the management tools and interfaces available with the switch (for basic instructions on these tools, refer to the *System Configuration Guide* (217105-A)):

- Console interface

  The console interface (CI) allows you to configure and manage the switch locally or remotely. Access the CI menu and screens locally through a console terminal attached to your Ethernet Switch, remotely through a dial-up modem connection, or in-band through a Telnet session.

- Web-based management

  You can manage the network from the World Wide Web and can access the web-based Graphical User Interface (GUI) through the HTML-based browser located on your network. The GUI allows you to configure, monitor, and maintain your network through web browsers. You can also download software using the web.

- Java-based Device Manager

  The Device Manager is set of Java-based graphical network management applications that is used to configure and manage Ethernet Switches 460 and 470.

- Command Line Interface (CLI)

  The CLI is used to automate general management and configuration of the Ethernet Switches 460 and 470. Use the CLI through a Telnet connection or through the serial port on the console.

- Any generic SNMP-based network management software.

  You can use any generic SNMP-based network management software to configure and manage Ethernet Switches 460 and 470.

- Telnet

  Telnet allows you to access the CLI and CI menu and screens locally using an in-band Telnet session.

- SSH

  Secure Shell (SSH) is a client/server protocol that can provide a secure remote login with encryption of data, username, and password. For details on SSH connections, refer to *Configuring and Managing Security* (217104-A).

- Nortel Enterprise Policy Manager

  The Nortel Enterprise Policy Manager (formerly Optivity Policy Services) allows you to configure the Ethernet Switches 460 and 470 with a single system.

Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, bridging, and IP
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies

Before using this guide, you must complete the installation procedures discussed in *Installing the Nortel Ethernet Switch 460-24T-PWR* (213318-C) or *Installing the Nortel Ethernet Switch 470* (217108-A).

Text conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `ip default-gateway <XXX.XXX.XXX.XXX>`, you enter `ip default-gateway 192.32.10.12`
braces ({ })	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is `http-server {enable|disable}` the options are `enable` or `disable`.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is `show ip [bootp]`, you can enter either `show ip` or `show ip bootp`.
`plain Courier text`	Indicates command syntax and system output. Example: `TFTP Server IP Address:  192.168.100.15`
vertical line |	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is `cli password <serial|telnet>`, you must enter either `cli password serial` or `cli password telnet`, but not both.
H.H.H.	Enter a MAC address in this format (XXXX.XXXX.XXXX).

Related publications

For more information about managing or using the switches, refer to the following publications:

- *Release Notes for the Ethernet Switch 460 and 470 Switch Software Version 3.6* (217103)
- *Installing the Nortel Ethernet Switch 460-24T-PWR* (213318-C)
- *Installing the Nortel Ethernet Switch 470* (217108-A)
- *Configuring and Managing Security* (217104-A)
- *Configuring Quality of Service, and IP Filtering* (217106-A)
- *System Monitoring Guide* (217107-A)
- *Configuring IP Multicast Routing Protocols* (217459-A)
- *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (312865-C)

You can print selected technical manuals and release notes free, directly from the Internet. Go to www.nortel.com/support. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems web site to download a free copy of the Adobe Acrobat Reader.

Obtaining technical assistance

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

If you purchased a Nortel service program, contact one of the following Nortel Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Technical Solutions Centers is available from the www.nortel.com/callus URL.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www.nortel.com/erc URL.

Chapter 1
About Ethernet Switches 460 and 470

This chapter provides an introduction to Ethernet Switch Release 3.6 software. This version of the software supports the following devices:

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

This chapter gives you information on the following topics:

Features

New Features

Auto-Detection and Auto-Configuration (ADAC) of Nortel IP Phones

Auto-Detection and Auto-Configuration (ADAC) of Nortel IP Phones allows a switch to perform the automatic configuration of the switch ports and virtual local area networks (VLAN) required for the transmission of signal and voice between the Nortel IP Phones and the switch.

For more information on ADAC, refer to *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A).

Auto Unit Replacement

The Auto Unit Replacement (AUR) feature provides the user with 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 can be restored to the new unit.

For more information on Auto Unit Replacement, refer to "Stacking" on page 293.

EAPOL Security enhancements

Prior to Release 3.6 software, Extensible Authentication Protocol over LAN (EAPOL) Authentication (802.1x) supported Port Based User Access. At any time, only one user (MAC) could be authenticated on a port and the port could be assigned to only one port-based VLAN.

With Release 3.6 software, EAP supports two modes for authentication:

- Single Host with Single Authentication (SHSA) and Guest VLANs
- Multiple Host (MAC) with Multiple Authentication (MHMA)

SHSA is the default mode, in which only one device or user on that port can complete EAP Authentication. However, Guest VLANs can also be configured for access to the port. Any active VLAN can be made a Guest VLAN.

With MHMA, multiple devices, each with a different MAC address, are allowed on a port. Each device must complete EAP Authentication for the port to allow traffic with the corresponding MAC address.

For more information on the EAPOL Security enhancements, refer to *Configuring and Managing Security* (217104-A).

MAC address-based security auto-learning

The MAC address-based security auto-learning feature provides the ability to add allowed MAC addresses in the MAC Security Table automatically without user intervention. The user specifies the number of addresses (1 to 25) per port to be added in the table. The switch then forwards traffic only for those MAC addresses that are included in the Security Table on the specified ports.

For more information on the MAC address-based security auto-learning, refer to *Configuring and Managing Security* (217104-A).

Scaling of STP to 16

Spanning Tree Protocol (STP) now supports 16 STP instances, up from eight. For more information on Spanning Tree Protocol, refer to *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A).

Multiple STG support for MLT

Tagged MultiLink Trunking (MLT) groups can now be assigned to multiple spanning tree groups (STG). The MLT can have different learning settings for different spanning tree groups. However, all port members of a particular MLT group must be assigned to the same STGs.

For more information on Multiple STG support for MLT, refer to *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A).

VLACP

Virtual Link Aggregation Control Protocol (VLACP), an LACP extension, is a Layer 2 handshaking protocol that provides end-to-end failure detection between two physical Ethernet interfaces. It allows the switch to detect unidirectional or bidirectional MLT failures.

For more information on VLACP, refer to *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A).

PVST+

Per-VLAN Spanning Tree Plus (PVST+) is the Cisco proprietary implementation of the spanning tree protocol. In addition to the existing Nortel MSTG, Release 3.6 software provides support for PVST+. As a result, users now have the option of running Spanning Tree Protocol in a multivendor network, especially with Cisco switches.

For more information on support for PVST+, refer to *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A).

SSL Web-based management

Secure Socket Layer (SSL) is available to provide security for the Web-based management system. It allows access to Web-based management using a secure https session. The user must enable SSL for the browser through the Command Line Interface (CLI).

For more information on SSL Web-based management, refer to *Configuring and Managing Security* (217104-A).

Password Security

The Password Security feature applies stricter rules to govern user passwords than normal. When the Password Security feature is running, user passwords:

- must be between 10 and 15 printable characters
- can no longer be viewed as clear text, appearing as 15 asterisks (*) in the user interfaces

- expire over a configurable period of time

For more information on the Password Security feature, refer to *Configuring and Managing Security* (217104-A).

Failed Login Attempt Trap

The new Simple Network Management Protocol (SNMP) trap, bsnLoginFailure, sends an SNMP trap for each failed login attempt due to a user/password mismatch, provided that at least one trap receiver is configured on the switch or stack. Also, with an SSH-enabled image, the system generates a trap when Digital Signature Algorithm (DSA) authentication fails due to key mismatch. No trap is generated when the login fails due to a wrong configuration of the RADIUS server, or when the client IP is not in the allowed IP list.

The Failed Login Attempt trap is now included in the list of supported SNMP traps in *Configuring and Managing Security* (217104-A).

Command history audit log

Starting with Release 3.6 software, Ethernet Switches 460 and 470 save the last 100 commands entered to a command history log in NVRAM. The switch periodically copies the history from NVRAM to the syslog server.

Each log entry consists of:

- a timestamp (sysUpTime or real clock time, if available)
- the source of the command (for example, console interface and unit or Telnet and IP)
- the text of the command itself

If a user resets the switch to factory defaults, the switch saves the command history (in this case, the history also contains the reset command).

You must configure a syslog server in order to save all of the command history. If you do not configure a syslog server, the switch loses the commands when they begin to wrap in the NVRAM buffer.

The `show audit log` CLI command displays the command history audit log stored in NVRAM. For more details, see *Configuring and Managing Security* (217104-A).

CLI command enhancements

The following describe additional CLI command enhancements.

help commands mode command

The `help commands mode` command displays the list of commands available on the device, either for the current mode of operation or as a complete list of all the commands available on the device. (See "help commands mode command" on page 162.)

help modes command

The `help modes` command displays information regarding available CLI modes on the switch. (See "help modes command" on page 164.)

shutdown command

The `shutdown` command resets the switch one to ten minutes after saving the configuration. Users are informed that they have between one and ten minutes to unplug the switch; otherwise, the switch is reset. (See "shutdown command" on page 168.)

The shutdown command is also available from the Console Interface. (See "shutdown command" on page 168.)

show system verbose command

The `show system verbose` command displays additional system characteristics, including the status of switch fans, the power status, and the serial number of the switch.

Detailed fan status information is now also available to users through the Console Interface, Web-based management, SNMP, and Device Manager (JDM). (See "show system verbose command" on page 176.)

show tech command

The `show tech` command displays detailed system and configuration information for technical support purposes. (See "show tech command" on page 178.)

show interfaces gbic-info command

The `show interfaces gbic-info` command displays hardware specifications for Gigabit Interface Converters (GBIC) on the switch. (See "show interfaces gbic-info command" on page 178.)

Detailed GBIC information is now also available to users through the Console, Web-based management, and SNMP when the GBIC is plugged in.

Copper GBIC support

A full-sized GBIC is supported. This GBIC supports 1000BaseT and works only on Ethernet Switch 470 units.

General Features

Ethernet Switch Release 3.6 software provides many useful features.

The following are the general features supported by the switch:

Ethernet

- 10BaseT
- 100BaseT
- 1000BaseT
- 1000BaseGBIC

Layer 2

- 802.1q VLANs
- IGMP Snooping
- 802.1d Spanning Tree
- Nortel Multiple Spanning Tree
- 802.1s Multiple Spanning Tree
- 802.1w Rapid Spanning Tree

QoS

- Filtering
- Flow metering
- Traffic Shaping

Management

- Telnet
- HTTP/HTTPS
- SSH
- SNMP/SNMP V3

Hardware Description

The Nortel Ethernet Switches provide policy-enabled networking features to optimize consistent performance and behavior of network traffic. The Differentiated Services (DiffServ) network architecture offers varied levels of service for different types of data traffic. DiffServ lets you designate a specific level of performance on a per-packet basis.

This section provides information on the following Ethernet Switches:

- "Ethernet Switch 460-24T-PWR" on page 53
- "Ethernet Switch 470-24T" on page 67
- "Ethernet Switch 470-48T" on page 81

Ethernet Switch 460-24T-PWR

This section describes the Ethernet Switch 460-24T-PWR and covers the following topics:

General Description

The Ethernet Switch 460-24T-PWR is an IEEE 802.3af-compliant 24-port 10/100 stackable Ethernet switch.

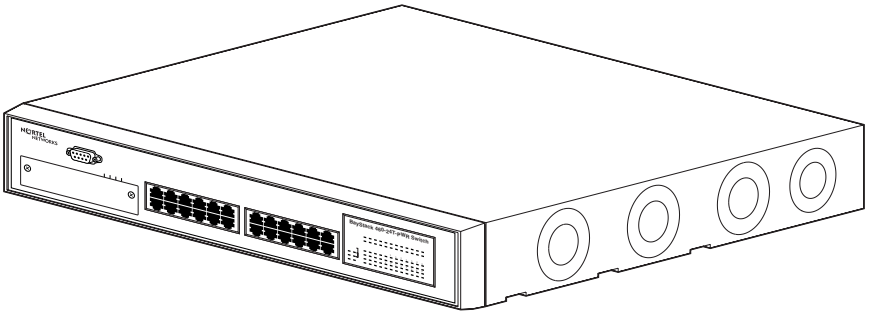
It has a Media Dependent Adapter slot that supports various types of media, including 1000BaseT and GBICs. It also provides support for a redundant power supply unit or an uninterruptible power supply (RPSU/UPS) module.

The Ethernet Switch 460-24T-PWR can detect and power IEEE 802.3af compliant network devices connected on the front ports, such as IP phones, wireless access points, and video devices, among others. The switch automatically supplies the DC voltage required by each connected appliance at the current level required for that particular device.

Physical Description

Figure 1 depicts the front and side views of the Ethernet Switch 460-24T-PWR.

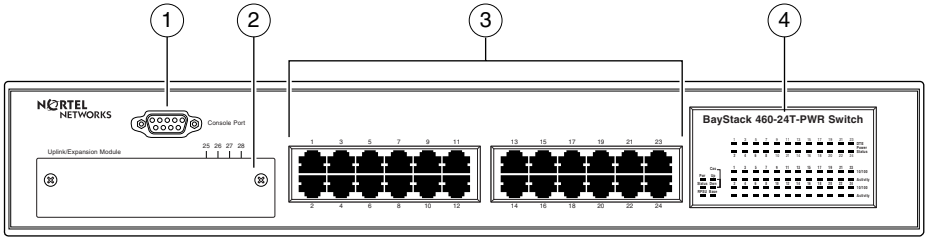
Figure 1 Ethernet Switch 460-24T-PWR



Front Panel

Figure 2 shows the front panel configuration for the Ethernet Switch 460-24T-PWR. Table 1 describes the front panel components.

Figure 2 Ethernet Switch 460-24T 10/100/1000 front panel



460-24T-PWR Switch

10829EA

Table 1 Ethernet Switch 460-24T-PWR 10/100/1000 front panel description

Legend	Description
1	Console port
2	Uplink/expansion slot
3	Port connectors
4	LED display panel

Note: The 24 panel ports are colored red to signify that they can carry power as well as data.

Console port

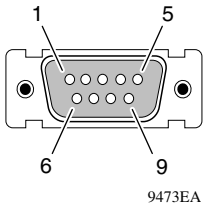
The console port allows you to access the Console Interface (CI) screens and customize your network using the supplied menus and screens.

The console port is a DB-9, RS-232-D male serial port connector. You can use this connector to connect a management station or console/terminal to the Ethernet Switch 460-24T-PWR by using a straight-through DB-9 to DB-9 standard serial port cable. You must use a VT100/ANSI-compatible terminal to provide cursor control and to enable the cursor and functions keys.

See *Installing the Nortel Ethernet Switch 460-24T-PWR* (213318-C) for more information.

Table 2 describes the components of the console port.

Table 2 Console port description

Connector	Pin number	Signal
	1	Carrier detect (not used)
	2	Transmit data (TXD)
	3	Receive data (RXD)
	4	Data terminal ready (not used)
	5	Signal ground (GND)
	6	Not used
	7	Request to send (not used)
	8	Not used
	9	Ring indicator (not used)

Note: The console port is configured as a data communications equipment (DCE) connector. Ensure that your RS-232 cable pin-outs are configured for DCE connections.

The console port default settings are: 9600 baud with 8 data bits, 1 stop bit, and no parity as the communications format, with flow control set to Enabled.

Console/Serial Cable

To connect to the console port of the Ethernet Switch 460-24T-PWR, use a straight-through serial cable with a DB-9 female connector for the Ethernet Switch unit, and the appropriate connector for your PC.

The console/serial cable to connect from a PC with a male DB-9 serial port to the Ethernet Switch is available to order using the following information:

Description	Order number
Console cable for use with Ethernet Switch and Passport 8300 switches.	AL2011013

Uplink/Expansion slot

The Uplink/Expansion slot allows you to attach optional Media Dependent Adapters (MDA) that support a range of media types.

Table 3 describes the MDAs supported by the Ethernet Switch 460-24T-PWR.

Table 3 MDAs supported by Ethernet Switch 460-24T-PWR

Description	Order number
450-1SX 1-port 1000BASE-SX Single PHY MDA	AL2033005
450-1SR 1-port 1000BASE-SX Redundant PHY MDA	AL2033006
450-1LX 1-port 1000BASE-LX Single PHY MDA	AL2033007
450-1LR 1-port 1000BASE-LX Redundant PHY MDA	AL2033008
BayStack 450-1 GBIC MDA	AL2033009
BPS2000-4TX 4-port 10/100 MDA	AL2033011
BPS2000-4FX 4-port 100BASE-FX MDA w/mini MT-RJ-type connectors	AL2033012
BPS2000-2FX 2-port 100BASE-FX MDA w/SC-type connectors	AL2033013
BPS2000 1-port 1000BASE-T MDA	AL2033014
BPS2000 2-port 1000BASE-T MDA	AL2033015
BPS2000 2-port SFP GBIC MDA	AL2033016

MDA compatibility

Note: The MDA do not supply power to PoE (Power Over Ethernet) devices. Only unit ports, 1-24 can supply power to PoE devices.

The switch provides support for many Nortel MDAs that use a variety of media, including Gigabit Interface Converters (GBICs) and CWDM.

Refer to *Installing Media Dependent Adapters (MDA)s* (302403) and *Installing Gigabit Interface Converters, SFPs, and CWDM SFP Gigabit Interface Converters* (312865) for more information on installation, technical specifications, connectors, and cabling for the GBIC MDAs. Contact your Nortel representative for a complete listing of compatible MDAs.

Port Connectors

The Ethernet Switch 460-24T-PWR uses 24 10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors.

The 10BASE-T/100BASE-TX port connectors are configured as Media Dependent Interface Crossover (MDI-X). These ports connect straight cables to the Network Interface Card (NIC) in a node or server, similar to a conventional Ethernet repeater hub.

If you are connecting to an Ethernet hub or Ethernet switch, use a crossover cable unless an MDI connection exists on the associated port of the attached device.

The Ethernet Switch 460-24T-PWR uses autosensing ports designed to operate at 10 Mbps (megabits per second) or at 100 Mbps, depending on the connecting device.

These ports support the IEEE 802.3u autonegotiation standard, which means that when a port is connected to another device that also supports the IEEE 802.3u standard, the two devices negotiate the best speed and duplex mode.

The 10BASE-T/100BASE-TX switch ports also support half and full-duplex modes of operation.

Note: Autonegotiation is enabled by default on the front panel 10/100BASE-TX ports.

The 10BASE-T/100BASE-TX RJ-45 ports can connect to 10 Mbps or 100 Mbps Ethernet segments or nodes.

Auto-MDI/MDI-X

The 10/100BASE-TX port connectors supports auto-MDI/MDI-X. Typical MDI-X ports connect straight-through cables to the NIC in a node or server, similar to a conventional Ethernet repeater hub. However, with the auto-MDI/MDI-X feature and autonegotiation enabled, you can still use straight-through cables while connecting to an Ethernet hub or switch. The port operates as a standard MDI-X port if autonegotiation is disabled on a port.

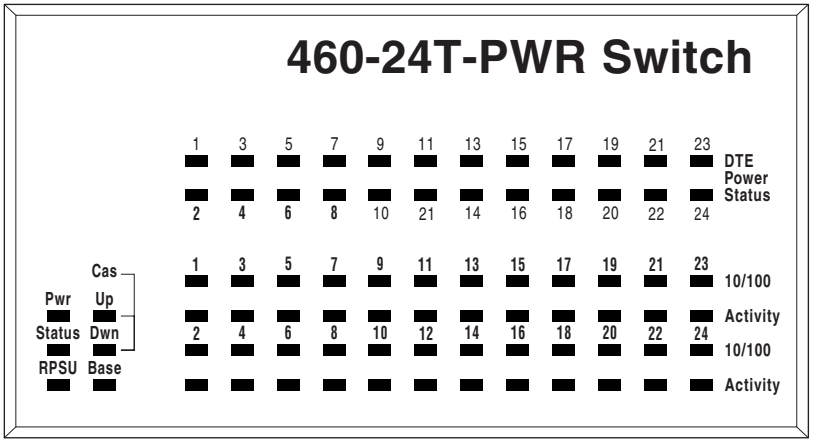
Auto-polarity

The Ethernet Switch 460-24T-PWR supports auto-polarity. With autonegotiation enabled, auto-polarity can automatically reverse the polarity of a pair of pins from positive to negative or negative to positive. This corrects the polarity of the received data if the port detects that the polarity of the data is reversed due to a wiring error.

LED display panel

Figure 3 shows the Ethernet Switch 460-24T-PWR LED display panel. Table 4 on page 60 provides a description of the LEDs.

Figure 3 Ethernet Switch 460-24T-PWR LED display panel



10856EA

Table 4 Ethernet Switch 460-24T-PWR System LED descriptions

Label	Type	Color	State	Meaning
Pwr	Power status	Green	On	DC power is available to the switch's internal circuitry.
			Off	No AC power to switch or power supply failed.
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A nonfatal error occurred during the self-test (this includes disabled fans).
			Off	The switch failed the self-test.
RPSU	RPSU Status	Green	On	The switch is connected to the RPSU and can receive power if needed.
			Off	The switch is not connected to the RPSU or the RPSU is not on.
Up	Stack Mode	None	Off	The switch is in stand-alone mode.
		Green	On	The switch is connected to the **Up (Cascade A Out)** connector on the *upstream* unit.
		Amber	On	This unit has detected a problem with the switch connected to the **Up (Cascade A Out)** connector. In order to maintain the integrity of the stack, this unit has bypassed its upstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green		Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.
Down	Stack Mode	None	Off	The switch is in stand-alone mode.
		Green	On	The switch is connected to the **Down (Cascade A In)** connector on the *downstream* unit.
		Amber	On	This unit has detected a problem with the switch connected to the **Down (Cascade A In)** connector. In order to maintain the integrity of the stack, this unit has bypassed its upstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green	Blinking	Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.

Label	Type	Color	State	Meaning
Base	Base mode	Green	On	The switch is configured as the stack base unit.
			Off	The switch is not configured as the stack base unit (or is in stand-alone mode).
			Blinking	Stack configuration error: indicates that multiple base units or no base units are configured in the stack.
		Amber	On	This unit is operating as the stack configuration's temporary base unit. This condition occurs automatically if the base unit (directly downstream from this unit) fails. If this happens, the following events take place: • The two units directly upstream and directly downstream from the failed unit automatically wrap their cascade connectors and indicate this condition by lighting their **Up** and **Down** LEDs. • If the temporary base unit fails, the next unit directly downstream from this unit becomes the new temporary base unit. This process can continue until there are only two units left in the stack configuration. This automatic failover is a temporary safeguard only. If the stack configuration loses power, the temporary base unit will not power up as the base unit when power is restored. For this reason, you should always assign the temporary base unit as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced.
DTE Power Status	DTE power status		Off	No DTE/PoE device is detected.
		Green	On	DTE/PoE device is detected and power is applied.
		Amber	On	DTE/PoE power fault or short circuit.
			Blinking	DTE/PoE device is detected, but there is insufficient power to turn on the device.
10/100	Link status and speed		Off	The communications link connection is bad or there is no connection to this port.
		Green	On	Valid communications link established at 100 Mbps.
		Amber	On	Valid communications link established at 10 Mbps.
		Green or Amber	Blinking	The corresponding port is management disabled.
Activity	Port activity	Green	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

Cooling fans

Four cooling fans are located on one side of the Ethernet Switch 460-24T-PWR to provide cooling for the internal components.

When you install the switch, allow enough space on both sides of the switch for adequate air flow. For more information on installing the switch, see *Installing the Nortel Ethernet Switch 460-24T-PWR* (213318-C).

Back panel

Figure 4 shows the back panel of the Ethernet Switch 460-24T-PWR. Table 5 describes the various parts of the back panel.

Figure 4 Ethernet Switch 460-24T-PWR back panel

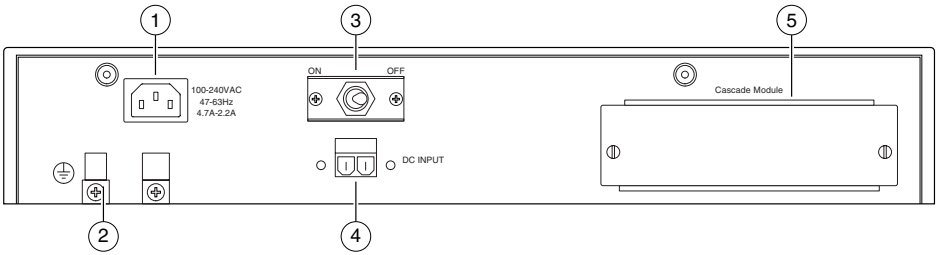


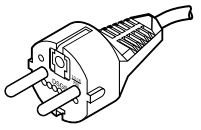
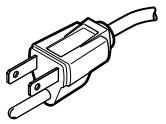
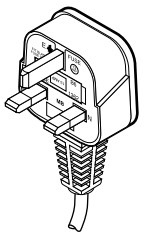
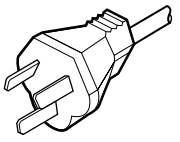
Table 5 Ethernet Switch 460-24T-PWR back panel description

Legend	Description
1	AC Power Receptacle
2	Ground lug
3	DC ON/OFF switch (for optional external power source)
4	DC connector receptacle (for optional external power source)
5	Cascade Module slot

AC power receptacle

The AC power receptacle accepts a variety of AC power cords. Ensure that you have the proper power cord for your region. Any cord used must have a CEE-22 standard V female connector on one end and must meet the IEC 320-030 specifications. Table 6 lists specifications for international power cords.

Table 6 International power cord specifications

Country/Plug description	Specifications	Typical plug
Continental Europe: • CEE7 standard VII male plug • Harmonized cord (HAR marking on the outside of the cord jacket to comply with the CENELEC Harmonized Document HD-21)	220 or 230 VAC 50 Hz Single phase	 228FA
U.S./Canada/Japan: • NEMA5-15P male plug • UL recognized (UL stamped on cord jacket) • CSA certified (CSA label secured to the cord)	100 or 120 VAC 50–60 Hz Single phase	 227FA
United Kingdom: • BS1363 male plug with fuse • Harmonized cord	240 VAC 50 Hz Single phase	 229FA
Australia: • AS3112-1981 Male plug	240 VAC 50 Hz Single phase	 230FA

Ground lug

The ground lug allows you to attach a grounding wire. Attach a 12-gauge wire to this lug and connect it to the chassis ground (on the rack), especially if you are using only an external power source.

DC ON/OFF switch

The DC ON/OFF switch allows you to manually turn off power from the optional external power source to the Ethernet Switch 460-24T-PWR. This switch serves as a safety feature only; if you encounter problems you can immediately switch off the power supply from the external power source by moving this switch to the Off mode.

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

DC connector receptacle

This is the receptacle into which you plug the optional external power source, either an Ethernet Switch Power Supply Unit 10 (PSU) or a Network Energy Source (NES) unit. This receptacle requires a 2-pin cable. This 2-pin cable comes with a NES unit and must be ordered separately for an Ethernet Switch Power Supply Unit 10.

You can use the Ethernet Switch 460-24T-PWR in various configurations. These configurations depend on three interrelated items:

- Physical power source
- DC source type configuration
- DC source configuration

For an optional external power source, you can use either an Ethernet Switch Power Supply Unit 10 or an NES. Contact your Nortel representative for more information about the Ethernet Switch Power Supply Unit 10 or the NES unit.

The DC Connector receptacle provides the following three options to power the switch:

- Internal power source only
- External power source only
- Internal power source plus external power source

The Ethernet Switch 460-24T-PWR supports two external power source options:

- Ethernet Switch Power Supply Unit 10
- NES

Cascade Module slot

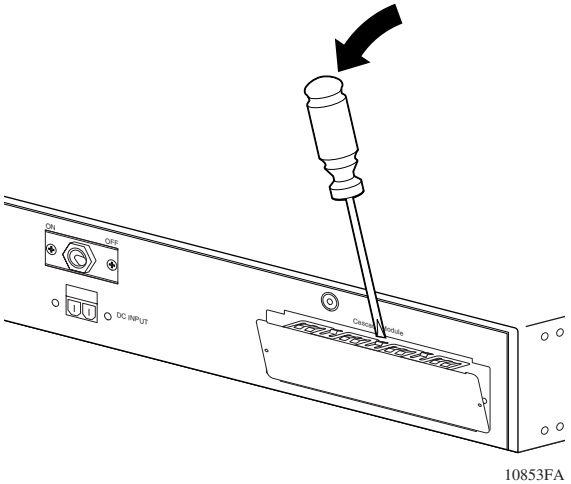
The Cascade Module slot allows you to attach an optional BayStack 400-ST1 Cascade Module to the switch.

You can connect up to eight switches into a redundant stack configuration. Installation instructions are provided with each BayStack 400-ST1 Cascade Module.

For more information, see *Installing the BayStack 400-ST1 Cascade Module* (304433). Use a flathead screwdriver to remove the filler panel that covers the Cascade Module slot.

Figure 5 shows how to remove a cascade filler panel.

Figure 5 Removing the cascade module filler panel



Up (Cascade A Out) connector

The Up (Cascade A Out) connector provides an attachment point for connecting the Ethernet Switch 460-24T-PWR unit to another unit through the cascade cable. A return cable from the Cascade A Out connector of another unit to the Cascade A In connector of this unit completes the stack connection.

Unit Select switch

The Unit Select switch (up = Base) determines the base unit for the stack configuration. The Unit Select switch status is displayed on the LED display panel of the Ethernet Switch 460-24T-PWR. When the Unit Select switch is in the Base (up) position, all other Unit Select switches in the stack configuration must be set to Off (down).

Down (Cascade A In) connector

Down (Cascade A In) connector provides an attachment point for accepting a cascade cable connection from an adjacent unit in the stack. A return cable from the Cascade A Out connector of this unit to the Cascade A In connector of the adjacent unit completes the stack connection.

Table 7 Cascade Cable and Cascade Module ordering information

Description	Order number
BayStack 400-SRC Cascade Return Cable (1 meter)	AL2018001
BayStack 400-SSC Spare Cascade Cable (18 inch)	AL2018002
BayStack 400-SRC Cascade Return Cable (3 meter)	AL2018004
BayStack 400-ST1 Cascade Module (includes cascade cable)	AL2033010

Ethernet Switch 470-24T

This section introduces the Ethernet Switch 470-24T and covers the following topics:

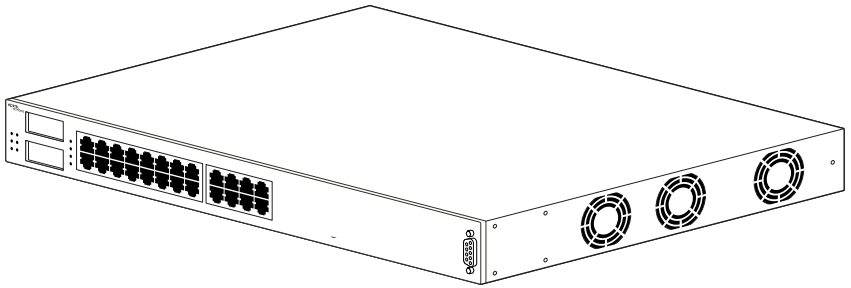
General Description

The Ethernet Switch 470-24T is a 24-port 10/100/1000 stackable Ethernet switch. It has two Gigabit Interface Converter (GBIC) slots and provides support for a redundant power supply unit/uninterruptible power supply (RPSU/UPS) module.

Physical Description

Figure 6 depicts the front and side views of the Ethernet Switch 470-24T.

Figure 6 Ethernet Switch 470-24T

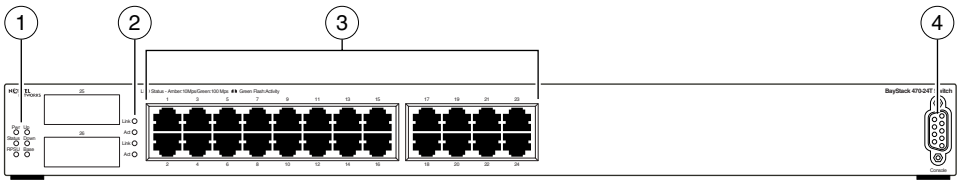


10772FB

Front Panel

Figure 7 shows the front panel configuration for the Ethernet Switch 470-24T. Table 8 describes the front panel components.

Figure 7 Ethernet Switch 470-24T front panel



10773EB

Table 8 Ethernet Switch 470-24T front panel description

Legend	Description
1	System LED display panel
2	GBIC slots and LEDs
3	10/100 port connectors and LEDs
4	Console port

System LED display Panel

Figure 8 shows the Ethernet Switch 470-24T LED display panel.

Figure 8 Switch LED display panel

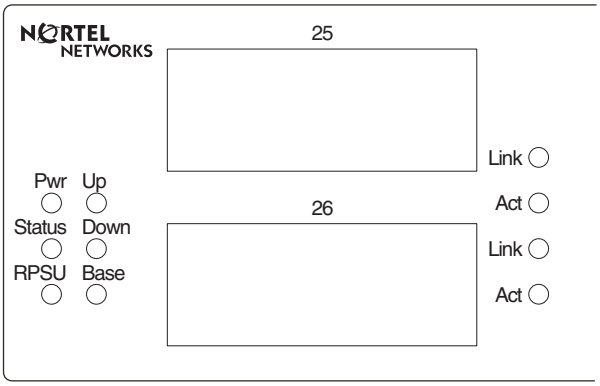


Table 9 provides a description of the Ethernet Switch 470-24T LEDs.

Table 9 Ethernet Switch 470-24T switch LED descriptions

Label	Type	Color	State	Meaning
Pwr	Power status	Green	On	DC power is available to the switch internal circuitry.
			Off	No AC power to switch or power supply failed.
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A non-fatal error occurred during the self-test (this includes malfunctioning fans).
			Off	The switch failed the self-test.
RPSU	RPSU Status	Green	On	The switch is connected to the RPSU and can receive power if needed.
			Off	The switch is not connected to the RPSU or RPSU is not on.

Table 9 Ethernet Switch 470-24T switch LED descriptions

Label	Type	Color	State	Meaning (Continued)
Up	Stack Mode	None	Off	The switch is in stand-alone mode.
		Green	On	The switch is connected to the **Up (Cascade A Out)** connector on the *upstream* unit.
		Amber	On	This unit has detected a problem with the switch connected to the **Up (Cascade A Out)** connector. In order to maintain the integrity of the stack, this unit has bypassed its upstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green		Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.
Down	Stack Mode	None	Off	The switch is in stand-alone mode.
		Green	On	The switch is connected to the **Down (Cascade A In)** connector on the *downstream* unit.
		Amber	On	This unit has detected a problem with the switch connected to the **Down (Cascade A In)** connector. In order to maintain the integrity of the stack, this unit has bypassed its upstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green	Blinking	Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.

Table 9 Ethernet Switch 470-24T switch LED descriptions

Label	Type	Color	State	Meaning (Continued)
Base	Base mode	Green	On	The switch is configured as the stack base unit.
			Off	The switch is not configured as the stack base unit (or is in stand-alone mode).
			Blinking	Stack configuration error: indicates that multiple base units or no base units are configured in the stack.
		Amber	On	This unit is operating as the stack configuration's ***temporary base unit***. This condition occurs automatically if the base unit (directly downstream from this unit) fails. If this happens, the following events take place: • The two units directly upstream and directly downstream from the failed unit automatically wrap their cascade connectors and indicate this condition by lighting their **Up** and **Down** LEDs. • If the temporary base unit fails, the next unit directly downstream from this unit becomes the new temporary base unit. This process can continue until there are only two units left in the stack configuration. This automatic failover is a temporary safeguard only. If the stack configuration loses power, the temporary base unit will not power up as the base unit when power is restored. For this reason, you should always assign the temporary base unit as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced.

GBIC slots and LEDs

The Ethernet Switch 470-24T has two GBIC slots that can accommodate standard-sized GBICs.

Table 10 describes the GBICs supported by the Ethernet Switch 470-24T.

Table 10 GBICs supported by the Ethernet Switch 470-24T

GBIC	Connector	Order number	Note
1000Base-T	RJ-45 connector	AA1419042	Copper GBIC
1000Base-SX	SC connector	AA1419001	Short wavelength/ distance 550 m

GBIC	Connector	Order number	Note
1000Base-LX	SC connector	AA1419002	Long wavelength/ distance 5 km
1000Base-XD	SC connector	AA1419003	Extended distance 50 km
1000Base-ZX	SC connector	AA1419004	Extended distance 70 km
1000BaseWDM	SC connector	From AA1419017 to AA1419024	1470 nm to 1610 nm (in 20 nm intervals)

Figure 9 shows the Ethernet Switch 470-24T GBIC slots and LEDs. Table 11 provides a description the LEDs.

Figure 9 Ethernet Switch 470-24T LED descriptions

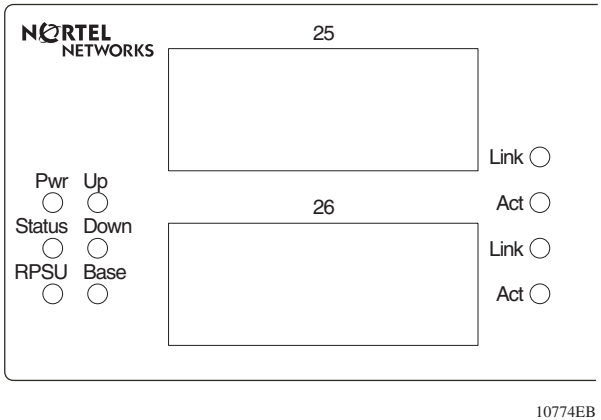


Table 11 Ethernet Switch 470-24T GBIC slot and LED descriptions

Label	Type	Color	State	Meaning
Link	Link status	Green	On	Valid communications link established.
			Off	The communications link connection is bad or there is no connection to this port.
			Blinking	The corresponding port is management disabled.
Activity	Port activity	Green	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

10/100 Port Connectors and LEDs

The Ethernet Switch 470-24T provides you with 24 10/100BASE-TX RJ-45 (8-pin modular) Ethernet port connectors.

The Ethernet Switch 470-24T uses autosensing ports designed to operate at 10 Mbps or 100 Mbps, depending on the connecting device. These ports support the IEEE 802.3u standard. This means that when a port is connected to another device that also supports the IEEE 802.3u standard, the two devices can negotiate at the best speed and duplex mode.

Figure 10 shows the LEDs associated with the 10/100 port connectors in an Ethernet Switch 470-24T. Table 12 provides a description of the LEDs.

Figure 10 Port LEDs

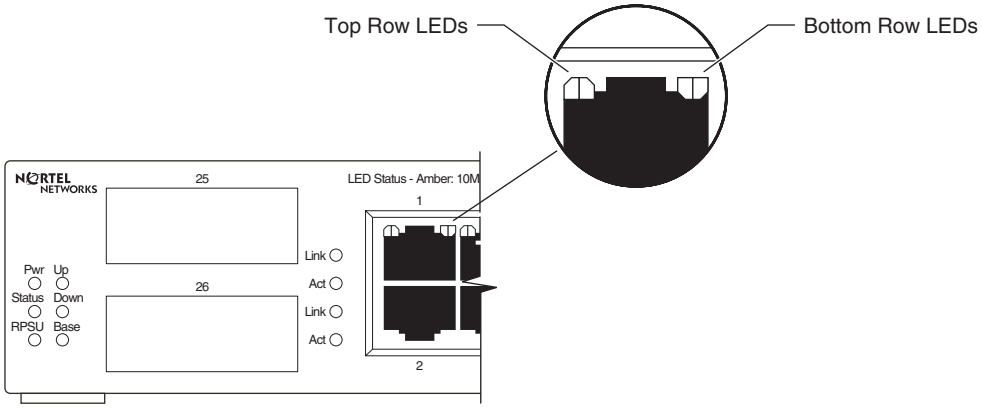


Table 12 10/100 port connector LEDs

Label	Type	Color	State	Meaning
Status (Left)	Link status and speed	None	Off	The communications link connection is bad or there is no connection to this port.
		Green	On	Valid communications link established at 100 Mbps.
		Amber	On	Valid communications link established at 10 Mbps.
		Green or Amber	Blinking	The corresponding port is management disabled.
Activity (Right)	Port activity	Green	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

Auto-MDI/MDI-X

The 10/100BASE-TX port connectors support auto-MDI/MDI-X.

Typical MDI-X ports connect over straight-through cables to the Network Interface Card (NIC) in a node or server, similar to a conventional Ethernet repeater hub. However, with the auto-MDI/MDI-X feature and autonegotiation enabled, you can still use straight-through cables while connecting to an Ethernet hub or switch. If autonegotiation is disabled on a port, that port operates as a standard MDI-X port.

Auto-polarity

The Ethernet Switch 470-24T supports auto-polarity. With autonegotiation enabled, auto-polarity can automatically reverse the polarity of a pair of pins from positive to negative or negative to positive. This corrects the polarity of the received data if the port detects that the polarity of the data is reversed due to a wiring error.

Console port

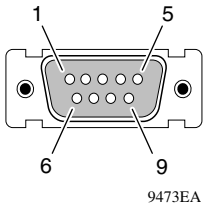
The console port allows you to access the Console Interface (CI) screens and customize your network using the supplied menus and screens.

The console port is a DB-9, RS-232-D male serial port connector.

You can use this connector to connect a management station or console/terminal to the Ethernet Switch unit by using a straight-through DB-9 to DB-9 standard serial port cable.

Figure 13 describes the pin-out assignments for the console port.

Table 13 Console port description

Connector	Pin number	Signal
	1	Carrier detect (not used)
	2	Transmit data (TXD)
	3	Receive data (RXD)
	4	Data terminal ready (not used)
	5	Signal ground (GND)
	6	Not used
	7	Request to send (not used)
	8	Not used
	9	Ring indicator (not used)

Note: The console port is configured as a Data Communications Equipment (DCE) connector. Ensure that your RS-232 cable pin-outs are configured for DCE connections.

The console port default settings are: 9600 baud with 8 data bits, 1 stop bit, and no parity as the communications format, with flow control set to Enabled.

Console/Serial Cable

To connect the console port of the Ethernet Switch unit, use a straight-through serial cable with a DB-9 female connector for the Ethernet Switch unit, and the appropriate connector for your PC. The console/serial cable to connect from a PC with a male DB-9 serial port to the Ethernet Switch is available to order using the following information:

Description	Order number
Console cable for use with Ethernet Switch and Passport 8300 switches.	AL2011013

Cooling fans

Three cooling fans are located on one side of the Ethernet Switch 470-24T to provide cooling for the internal components. When you install the switch, ensure you allow enough space on both sides of the switch for adequate air flow.

See *Installing the Ethernet Switch 470* (217108-A) for detailed information.

Back panel

The switch back panel is shown in Figure 11. Table 14 provides a description of the components of the back panel.

Figure 11 Ethernet Switch 470-24T back pane

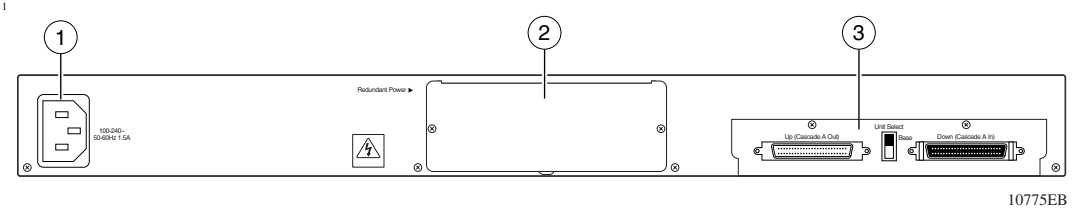


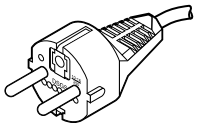
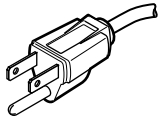
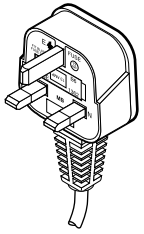
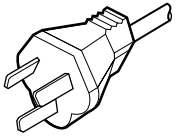
Table 14 Ethernet Switch 470-24T back-panel descriptions

Legend	Description
1	AC power receptacle
2	RPSU slot
3	Cascade Module connector

AC power receptacle

The AC power receptacle accepts a variety of AC power cords. Ensure you have the proper power cord for your region. Any cord used must have a CEE-22 standard V female connector on one end and must meet the IEC 320-030 specifications. Table 15 on page 78 lists the specifications for international power cords.

Table 15 International power cord specifications

Country/Plug description	Specifications	Typical plug
Continental Europe: • CEE7 standard VII male plug • Harmonized cord (HAR marking on the outside of the cord jacket to comply with the CENELEC Harmonized Document HD-21)	220 or 230 VAC 50 Hz Single phase	 228FA
U.S./Canada/Japan: • NEMA5-15P male plug • UL recognized (UL stamped on cord jacket) • CSA certified (CSA label secured to the cord)	100 or 120 VAC 50–60 Hz Single phase	 227FA
United Kingdom: • BS1363 male plug with fuse • Harmonized cord	240 VAC 50 Hz Single phase	 229FA
Australia: • AS3112-1981 Male plug	240 VAC 50 Hz Single phase	 230FA

UPS/RPSU Slot

The redundant power supply slot provides a space for the -48 V DC-to-DC converter. The -48 V DC-to-DC converter allows you to connect a backup power supply unit to the Ethernet Switch 470-24T.

Nortel provides an optional redundant power supply unit (RPSU) for this purpose. The Ethernet Switch Power Supply Unit 10 is a hot-swappable power supply unit that provides uninterrupted operation to as many as four Ethernet Switch 470-24T units, in the event that any of the switch power supplies fail.

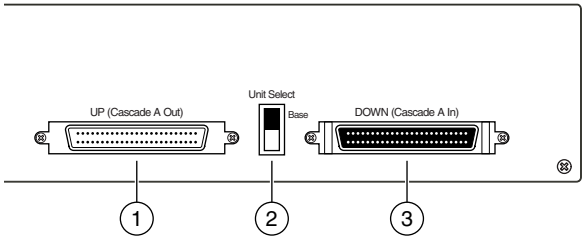
The Ethernet Switch Power Supply Unit 10 has a powerful, modular, redundant, and uninterruptible power supply (UPS) functionality in a single chassis. It provides scalable power redundancy and protection to your networking equipment. The modules fit into the right-hand side of the rear of the chassis. The UPS and associated battery pack module fit into the front of the chassis. For further information, refer to the *Installation and Reference for the BayStack 10 Power Supply Unit* (208296-C). Contact your Nortel sales representative for more information.

Built-in Cascade Connector

The Ethernet Switch 470-24T provides a fail-safe stacking environment using built-in Cascade Connectors. You can connect up to eight Ethernet Switches to provide uninterrupted connectivity for up to 384 ports. The entire stack is manageable as a single unit.

The front panel components of the built-in Cascade Connector are shown in Figure 12. Component descriptions follow the figure.

Figure 12 Built-in Cascade Connector components



1 = Cascade Up
2 = Unit Select switch
3 = Cascade Down

10693EB

UP (Cascade A Out) connector

The UP (Cascade A Out) connector provides an attachment point for connecting this unit to another unit through the cascade cable. A return cable from the Cascade A Out connector of another unit to the Cascade A In connector of this unit completes the stack connection.

Unit Select switch

The Unit Select switch (up = Base) determines the base unit for the stack configuration. The Unit Select switch status is displayed on the Ethernet Switch 470-24T LED display panel. When the Unit Select switch is in the Base (up) position, all other Unit Select switches in the stack configuration must be set to Off (down).

Down (Cascade A In) connector

Provides an attachment point for accepting a cascade cable connection from an adjacent unit in the stack. A return cable from the Cascade A Out connector of this unit to the Cascade A In connector of the adjacent unit completes the stack connection.

Replacement Cascade Cables

Table 16 provides the order numbers for the Replacement Cascade Cables.

Table 16 Replacement cascade cables

Description	Order number
BayStack 400-SRC Cascade Return Cable (1 meter)	AL2018001
BayStack 400-SSC Spare Cascade Cable (18 inch)	AL2018002
BayStack 400-SRC Cascade Return Cable (3 meter)	AL2018004

Ethernet Switch 470-48T

This section introduces the Ethernet Switch 470-48T and covers the following topics:

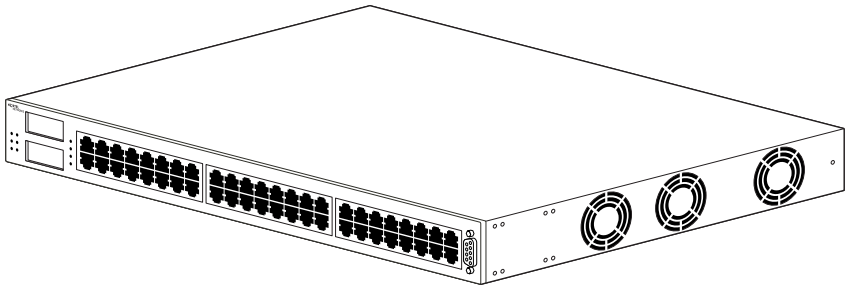
General Description

The Ethernet Switch 470-48T is a 48-port 10/100 stackable Ethernet switch. It has two Gigabit Interface Converter (GBIC) slots and provides support for a redundant power supply unit/uninterruptible power supply (RPSU/UPS) module.

Physical Description

Figure 13 depicts the front and side views of the Ethernet Switch 470-48T.

Figure 13 Ethernet Switch 470-48T 10/100/1000

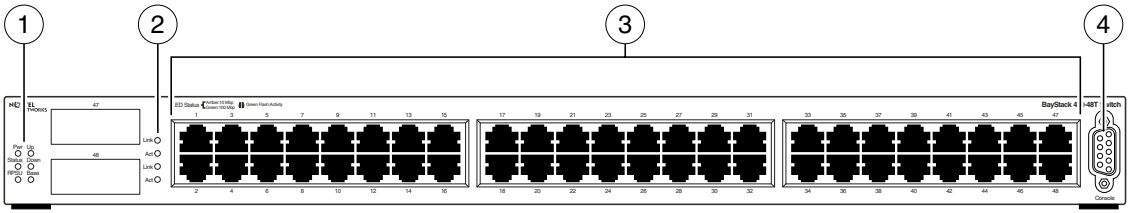


10772FA

Front Panel

Figure 14 shows the front panel configuration for the Ethernet Switch 470-48T. Table 17 describes the front panel components.

Figure 14 Ethernet Switch 470-48T 10/100/1000 front panel.



10773EA

Table 17 Ethernet Switch 470-48T front panel description

Legend	Description
1	System LED display panel
2	GBIC slots and LEDs
3	10/100 port connectors and LEDs
4	Console port

System LED display Panel

Figure 15 shows the Ethernet Switch 470-48T LED display panel. Table 18 provides a description of the LEDs.

Figure 15 Ethernet Switch 470-48T LED display panel

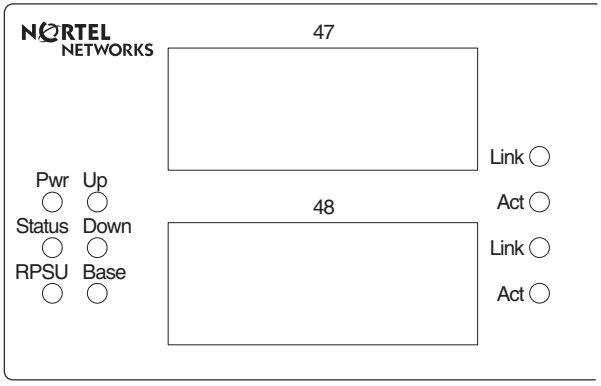


Table 18 Ethernet Switch 470-48T LED descriptions

Label	Type	Color	State	Meaning
Pwr	Power status	Green	On	DC power is available to the switch internal circuitry.
			Off	No AC power to switch or power supply failed.
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A non-fatal error occurred during the self-test (this includes malfunctioning fans).
			Off	The switch failed the self-test.
RPSU	RPSU Status	Green	On	The switch is connected to the RPSU and can receive power if needed.
			Off	The switch is not connected to the RPSU or RPSU is not on.

Label	Type	Color	State	Meaning
Up	Stack Mode	None	Off	The switch is in stand-alone mode.
		Green	On	The switch is connected to the **Up (Cascade A Out)** connector on the *upstream* unit.
		Amber	On	This unit has detected a problem with the switch connected to the **Up (Cascade A Out)** connector. In order to maintain the integrity of the stack, this unit has bypassed its upstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green		Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.
Down	Stack Mode	None	Off	The switch is in stand-alone mode.
		Green	On	The switch is connected to the **Down (Cascade A In)** connector on the *downstream* unit.
		Amber	On	This unit has detected a problem with the switch connected to the **Down (Cascade A In)** connector. In order to maintain the integrity of the stack, this unit has bypassed its upstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green	Blinking	Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.

Label	Type	Color	State	Meaning
Base	Base mode	Green	On	The switch is configured as the stack base unit.
			Off	The switch is not configured as the stack base unit (or is in stand-alone mode).
			Blinking	Stack configuration error: indicates that multiple base units or no base units are configured in the stack.
		Amber	On	This unit is operating as the stack configuration's ***temporary base unit***. This condition occurs automatically if the base unit (directly downstream from this unit) fails. If this happens, the following events take place: • The two units directly upstream and directly downstream from the failed unit automatically wrap their cascade connectors and indicate this condition by lighting their **Up** and **Down** LEDs. • If the temporary base unit fails, the next unit directly downstream from this unit becomes the new temporary base unit. This process can continue until there are only two units left in the stack configuration. This automatic failover is a temporary safeguard only. If the stack configuration loses power, the temporary base unit does not power up as the base unit when power is restored. For this reason, you must always assign the temporary base unit as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced.

GBIC slots and LEDs

The Ethernet Switch 470-48T has two Gigabit Interface Converter (GBIC) slots that can accommodate standard-sized GBICs.

The GBICs supported by the Ethernet Switch 470 are described in Table 19.

Table 19 GBICs supported by Ethernet Switch 470-48T

GBIC	Connector	Order number	Note
1000Base-T	RJ-45 connector	AA1419042	Copper GBIC
1000Base-SX	SC connector	AA1419001	Short wavelength/ distance 550 m
1000Base-LX	SC connector	AA1419002	Long wavelength/ distance 5 km
1000Base-XD	SC connector	AA1419003	Extended distance 50 km
1000Base-ZX	SC connector	AA1419004	Extended distance 70 km
1000BaseWDM	SC connector	From AA1419017 to AA1419024	1470 nm to 1610 nm (in 20 nm intervals)

Figure 15 on page 83 shows the GBIC LED panel and Table 20 provides a description of the LEDs.

Table 20 Ethernet Switch 470-48T 10/100/1000 GBIC LED descriptions

Label	Type	Color	State	Meaning
Link	Link status	Green	On	Valid communications link established.
			Off	The communications link connection is bad or there is no connection to this port.
			Blinking	The corresponding port is management-disabled.
Activity	Port activity	Green	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

10/100 Port Connectors and LEDs

The Ethernet Switch 470-48T provides the user with 48 10/100BASE-TX RJ-45 (8-pin modular) Ethernet port connectors.

The Ethernet Switch 470-48T uses autosensing ports designed to operate at 10 Mbps or 100 Mbps, depending on the connecting device. These ports support the IEEE 802.3u standard. This means that when a port is connected to another device that also supports the IEEE 802.3u standard, the two devices negotiate at the best speed and duplex mode.

Figure 16 shows the LEDs associated with the 10/100 port connectors in an Ethernet Switch 470-48T. Table 21 on page 88 provides a description of the LEDs.

Figure 16 Port LEDs

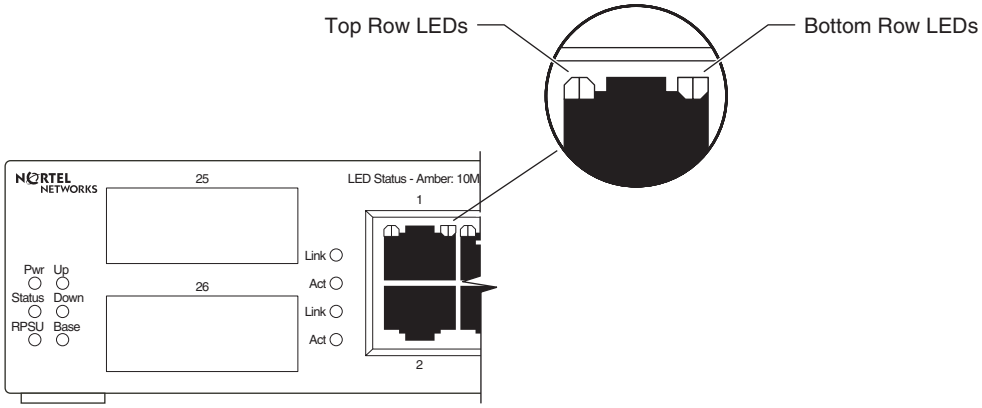


Table 21 10/100 port connector LEDs

Label	Type	Color	State	Meaning
Status (Left)	Link status and speed	None	Off	The communications link connection is bad or there is no connection to this port.
		Green	On	Valid communications link established at 100 Mbps.
		Amber	On	Valid communications link established at 10 Mbps.
		Green or Amber	Blinking	The corresponding port is management disabled.
Activity (Right)	Port activity	Green	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

Auto-MDI/MDI-X

The 10/100BASE-TX port connectors supports auto-MDI/MDI-X.

Typical MDI-X ports connect over straight-through cables to the network interface card (NIC) in a node or server, similar to a conventional Ethernet repeater hub. However, with the auto-MDI/MDI-X feature and autonegotiation enabled, you can still use straight-through cables while connecting to an Ethernet hub or switch. If autonegotiation is disabled on a port, that port operates as a standard MDI-X port.

Auto-polarity

The Ethernet Switch 470-48T supports auto-polarity. With autonegotiation enabled, auto-polarity can automatically reverse the polarity of a pair of pins from positive to negative or negative to positive. This corrects the polarity of the received data if the port detects that the polarity of the data is reversed due to a wiring error.

Console port

The console port allows you to access the Console Interface (CI) screens and customize your network using the supplied menus and screens.

The console port is a DB-9, RS-232-D male serial port connector.

You can use this connector to connect a management station or console/terminal to the Ethernet Switch 470-48T by using a straight-through DB-9 to DB-9 standard serial port cable. You must use a VT100/ANSI-compatible terminal (for cursor control and to enable cursor and functions keys) to use the console port. See *Installing the Ethernet Switch 470* (213318-C) for more information.

Note: The console port is configured as a Data Communications equipment (DCE) connector. Ensure that your RS-232 cable pin-outs are configured for DCE connections.

The console port default settings are: 9600 baud with 8 data bits, 1 stop bit, and no parity as the communications format, with flow control set to enabled.

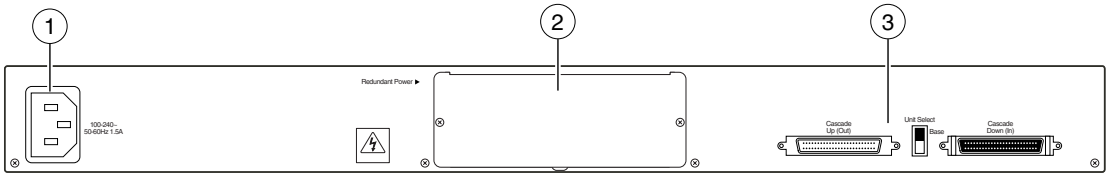
Cooling fans

Three cooling fans are located on one side of the Ethernet Switch 470-48T to provide cooling for the internal components. When you install the switch, ensure you allow enough space on both sides of the switch for adequate air flow. See *Installing the Ethernet Switch 470* (213318-C) for detailed information.

Back panel

The switch back panel is shown in Figure 17. Table 22 on page 90 provides a description of the components of the back panel.

Figure 17 Ethernet Switch 470-48T back panel



10775EA

Table 22 Ethernet Switch 470-48T back panel description

Legend	Description
1	AC Power Receptacle
2	UPS/RPSU Slot
3	Cascade Module Connector

AC power receptacle

The AC power receptacle accepts a variety of AC power cords. Ensure you have the proper power cord for your region. Any cord used must have a CEE-22 standard V female connector on one end and must meet the IEC 320-030 specifications. Table 23 lists specifications for international power cords.

Table 23 International power cord specifications

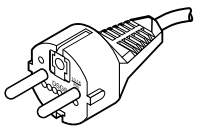
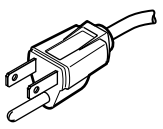
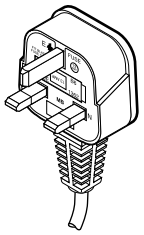
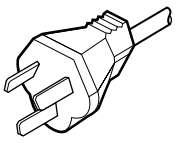
Country/Plug description	Specifications	Typical plug
Continental Europe: • CEE7 standard VII male plug • Harmonized cord (HAR marking on the outside of the cord jacket to comply with the CENELEC Harmonized Document HD-21)	220 or 230 VAC 50 Hz Single phase	 228FA
U.S./Canada/Japan: • NEMA5-15P male plug • UL recognized (UL stamped on cord jacket) • CSA certified (CSA label secured to the cord)	100 or 120 VAC 50–60 Hz Single phase	 227FA

Table 23 International power cord specifications (Continued)

Country/Plug description	Specifications	Typical plug
United Kingdom: • BS1363 male plug with fuse • Harmonized cord	240 VAC 50 Hz Single phase	 229FA
Australia: • AS3112-1981 Male plug	240 VAC 50 Hz Single phase	 230FA

UPS/RPSU Slot

The redundant power supply slot provides a space for the -48 V DC-to-DC converter. The -48 V DC-to-DC converter allows you to connect a backup power supply unit to the Ethernet Switch 470-48T.

Nortel provides an optional RPSU for this purpose. The Ethernet Switch Power Supply Unit 10 is a hot-swappable power supply unit that provides uninterrupted operation to as many as four Ethernet Switch 470-48T units, in the event that any of the switch power supplies fail.

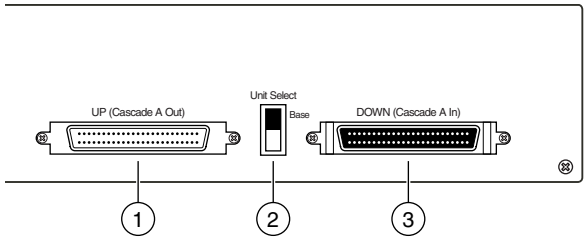
The Ethernet Switch Power Supply Unit 10 has a powerful, modular redundant and uninterruptible power supply (UPS) functionality in a single chassis. It provides scalable power redundancy and protection to your networking equipment. The modules fit into the right-hand side of the rear of the chassis. The UPS and associated battery pack module fit into the front of the chassis. For further information, refer to *Installation and Reference for the BayStack 10 Power Supply Unit* (208296-C). Contact your Nortel sales representative for more information.

Built-in Cascade Connector

Ethernet Switches 470-48T provide a fail-safe stacking environment using built-in Cascade Connectors. You can connect up to eight Ethernet Switches to provide uninterrupted connectivity for up to 384 ports. The entire stack is manageable as a single unit.

The front panel components of the built-in Cascade Connector are shown in Figure 18. This figure describes the components of the built-in Cascade Connector.

Figure 18 Built-in Cascade Connector



1 = Cascade Up
2 = Unit Select switch
3 = Cascade Down

10693EB

UP (Cascade A Out) connector

The UP (Cascade A Out) connector provides an attachment point for connecting this unit to another unit via the cascade cable. A return cable from another unit's Cascade A Out connector to this unit's Cascade A In connector completes the stack connection.

Unit Select switch

The Unit Select switch (up = Base) determines the base unit for the stack configuration. The Unit Select switch status is displayed on the Ethernet Switch 470-48T LED display panel. When the Unit Select switch is in the Base (up) position, all other Unit Select switches in the stack configuration must be set to Off (down).

DOWN (Cascade A In) connector

The DOWN (Cascade A In) connector provides an attachment point for accepting a cascade cable connection from an adjacent unit in the stack. A return cable from this unit's Cascade A Out connector to the adjacent unit's Cascade A In connector completes the stack connection.

Replacement Cascade Cables

Table 24 describes the Replacement Cascade Cables.

Table 24 Replacement Cascade Cables

Description	Order number
BayStack 400-SRC Cascade Return Cable (1 meter)	AL2018001
BayStack 400-SSC Spare Cascade Cable (18 inch)	AL2018002
BayStack 400-SRC Cascade Return Cable (3 meter)	AL2018004

SNMP MIB support

The Ethernet Switches 460 and 470 support an SNMP agent with industry-standard Management Information Bases (MIB), as well as private MIB extensions. This ensures compatibility with existing network management tools.

With SNMP management, you can configure SNMP traps to generate automatically on individual ports for conditions, such as an unauthorized access attempt or changes in the operating status of a port.

For more information on the supported SNMP MIBs for Ethernet Switches 460 and 470, see *Configuring and Managing Security* (217104-A).

SNMP trap support

The Ethernet Switches 460 and 470 support an SNMP agent with industry-standard SNMPv1 traps, as well as private SNMPv1 trap extensions.

For information on configuring SNMP, see *Configuring and Managing Security* (217104-A).

Supported standards and RFCs

This section lists the standards and Requests for Comments (RFC) supported by the Ethernet Switches 460 and 470.

Standards

The following IEEE Standards contain information relevant to the Ethernet Switches 460 -24T, 470-24T, and 470-48T:

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1w (RSTP)
- IEEE 802.1s (MSTP)
- IEEE 802.3af DRAFT (Power) for the Ethernet Switch 460-24T-PWR only

RFCs

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

- IanaIfType.mib (IANAifType MIB)
- RFC 1213.mib (MIB-II)
- RFC 2011.mib (IP MIB)
- RFC 2012.mib (TCP MIB)
- RFC 2013.mib (UDP MIB)
- RFC 2021.mib (RMON2 MIB)
- RFC 2576.mib (SNMP Community MIB)
- RFC 2665.mib (EtherLike MIB)

- RFC 2737.mib (Entity MIB)
- RFC 2819.mib (RMON MIB)
- RFC 2863.mib (IF MIB)
- RFC 2940.mib (COPS Client MIB)
- RFC 3289.mib (Diffserv MIB)
- RFC 3289tc.mib (Diffserv DSCP TC)
- RFC 3291.mib (INET Address MIB)
- RFC 3411.mib (SNMP Framework MIB)
- RFC 3413-tgt.mib (SNMP Target MIB)
- RFC 3413-notif.mib (SNMP Notification MIB)
- RFC 3414.mib (SNMP User-based SM MIB)
- RFC 3415.mib (SNMP View-based ACM MIB)
- RFC 3418.mib (SNMPv2 MIB)
- RFC 3621.mib (Power Ethernet MIB)
- RFC 3826.mib (SNMP USM AES MIB)

Network configuration

This section describes how to use the Ethernet Switch 460 or 470 to connect workstations, personal computers (PC), and servers to each other by connecting these devices directly to the switch, through a shared media hub connected to the switch, or by creating a virtual LAN (VLAN) through the switch.

To determine which version of the Ethernet Switch software is running, use the Console Interface (CI) menus or the Web-based management system:

- CI menus—From the main menu of the console, choose Systems Characteristics menu. The software currently running is displayed in sysDescr.
- Web-based management system—Open the System Information page, which is under Administration on the main menu. The software currently running is displayed in the sysDescription field.

Network configuration examples

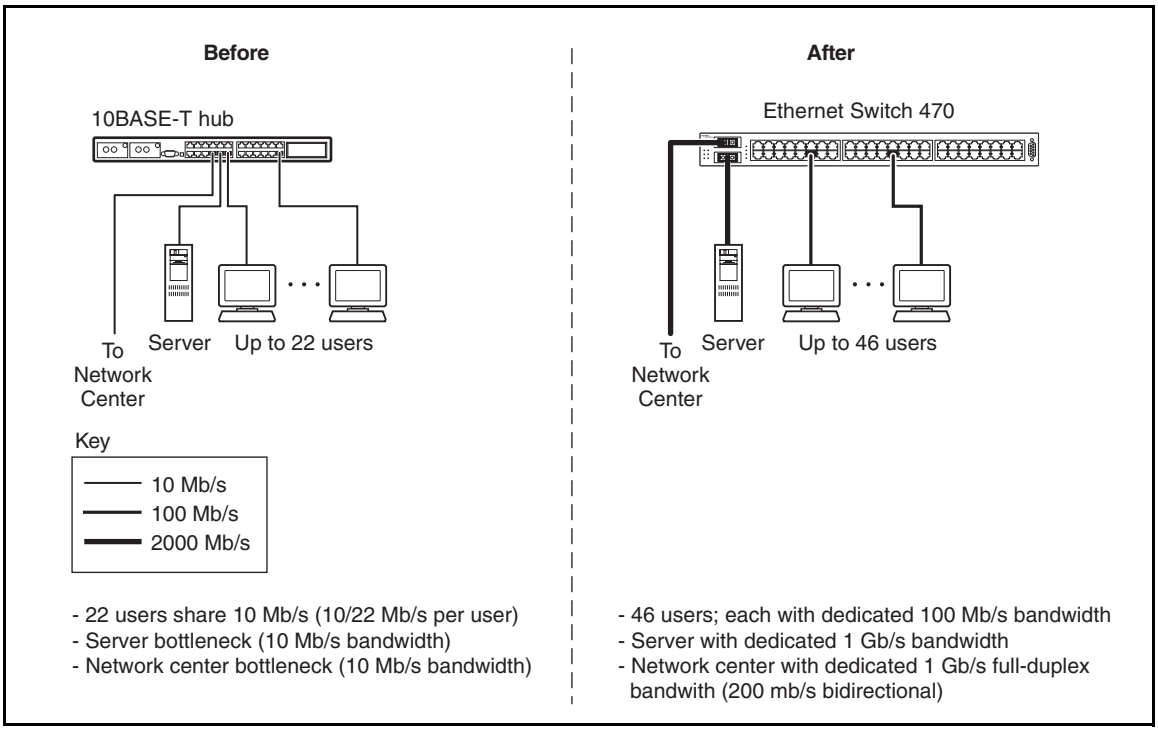
This section provides four network configuration examples using the Ethernet Switches 460 and 470. In these examples, the packet classification feature can be used to prioritize the traffic of the network to ensure uninterrupted traffic of critical applications.

- "Desktop switch application"
- "Segment switch application" on page 97
- "High-density switched workgroup application" on page 99

Desktop switch application

Figure 19 shows an Ethernet Switch 470 used as a desktop switch, where desktop workstations are connected directly to switch ports. This configuration provides dedicated 100 Mb/s connections to the network center, the server, and as many as 46 users.

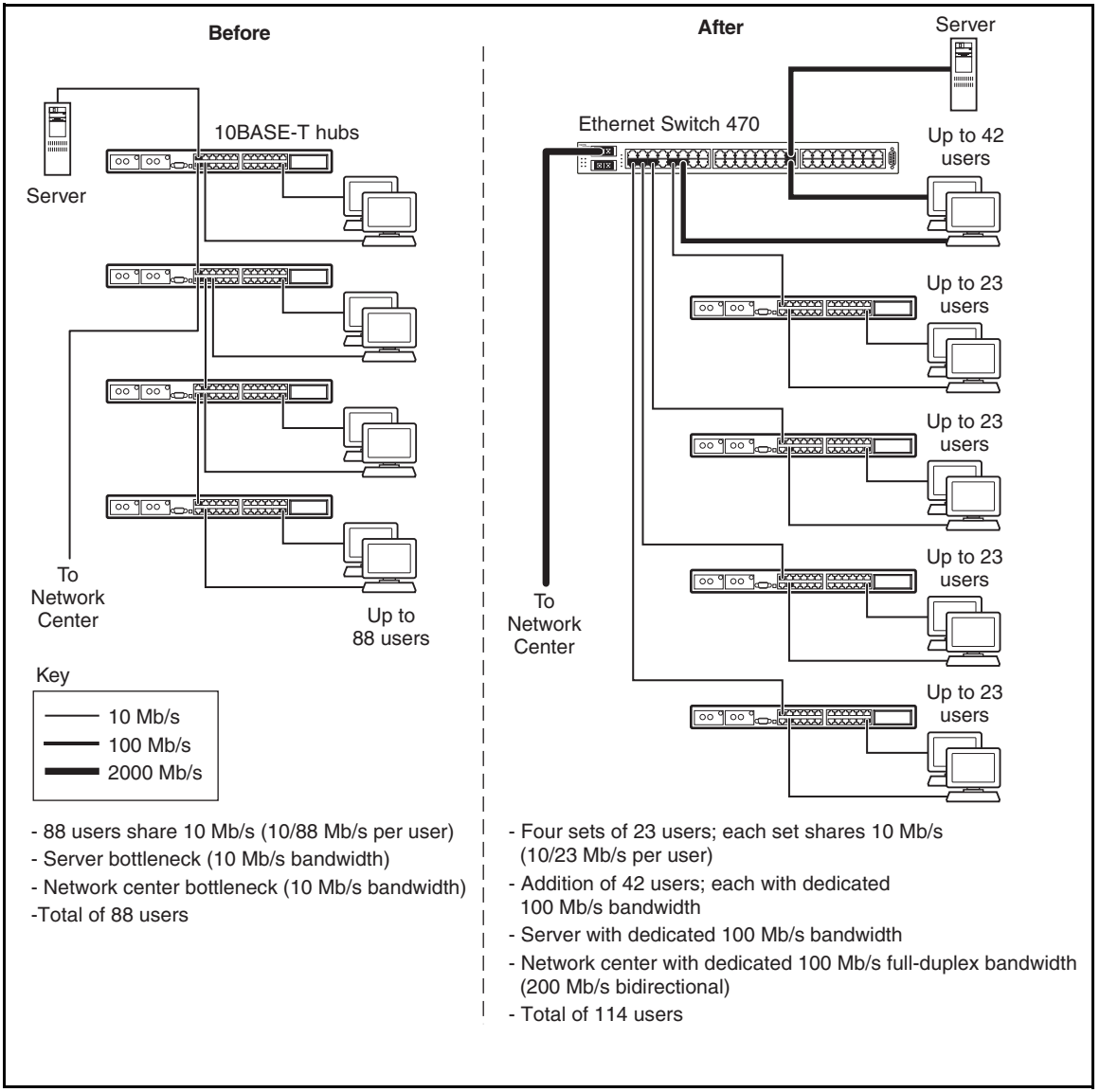
Figure 19 Ethernet Switch 470 used as a desktop switch



Segment switch application

Figure 20 on page 98 shows an Ethernet Switch 470 used as a segment switch to alleviate user contention for bandwidth, and to eliminate server and network bottlenecks. Before segmentation, 88 users had a total bandwidth of only 10 Mb/s available. After segmentation, 92 users have 40 Mb/s, four times the previous bandwidth, and 22 dedicated 100 Mb/s connections have been added. This configuration can be extended to add more segments without degrading performance.

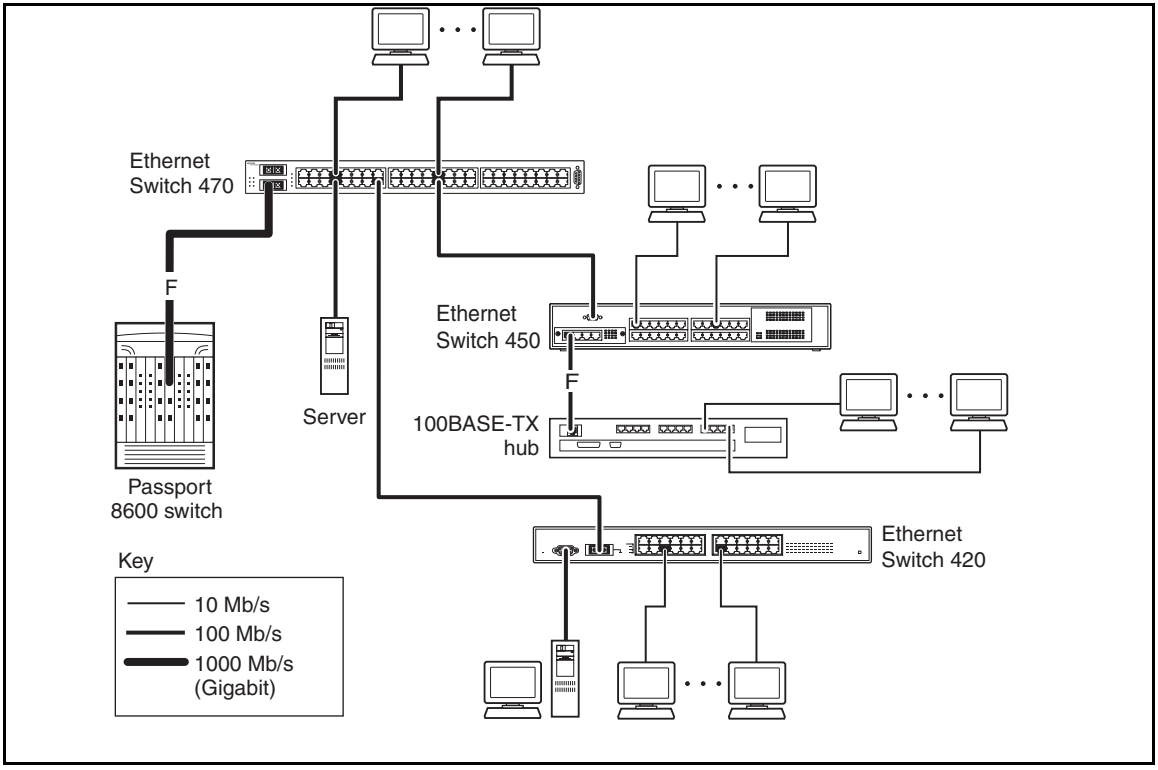
Figure 20 Ethernet Switch 470 used as a segment switch



High-density switched workgroup application

Figure 21 shows an example of using an Ethernet Switch 470 with a high-speed (gigabit) connection to a Nortel Passport™ 8600 switch. Ethernet Switches 450 and 420 are also shown in this example of a high-density switched workgroup.

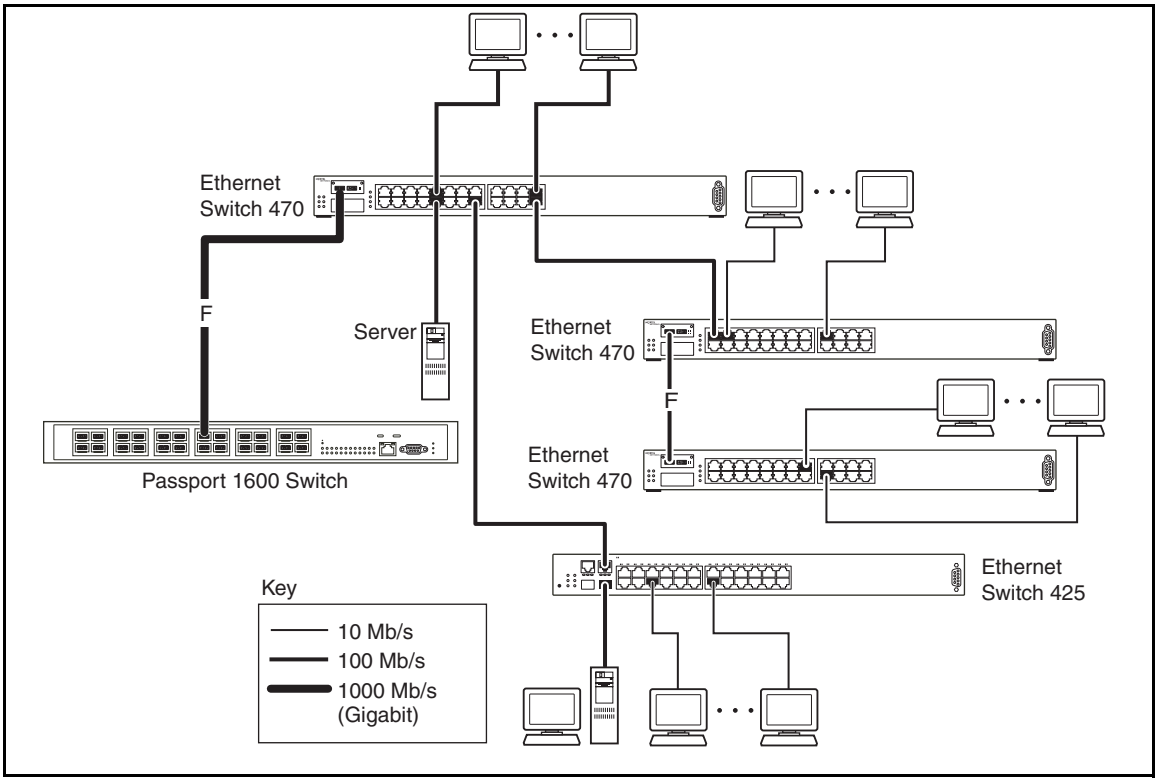
Figure 21 Configuring power workgroups and a shared media hub



As shown in Figure 22 on page 100, the Passport 1600 switch is used as a backbone switch, connecting to an Ethernet Switch 470 with a GBIC for maximum bandwidth. The Ethernet Switch 425 and the other Ethernet Switches 470 have 100 Mb/s connections to the first 470 and a 100 Mb/s server, as well as 10 Mb/s connections to DTE (data terminal equipment).

See the Nortel support web page www.nortel.com/support for online documentation about the Nortel Passport 8600 switch and the Passport 1600 switch, as well as the Ethernet Switches 420, 425, 450, and 470.

Figure 22 Configuring power workgroups and a shared media hub



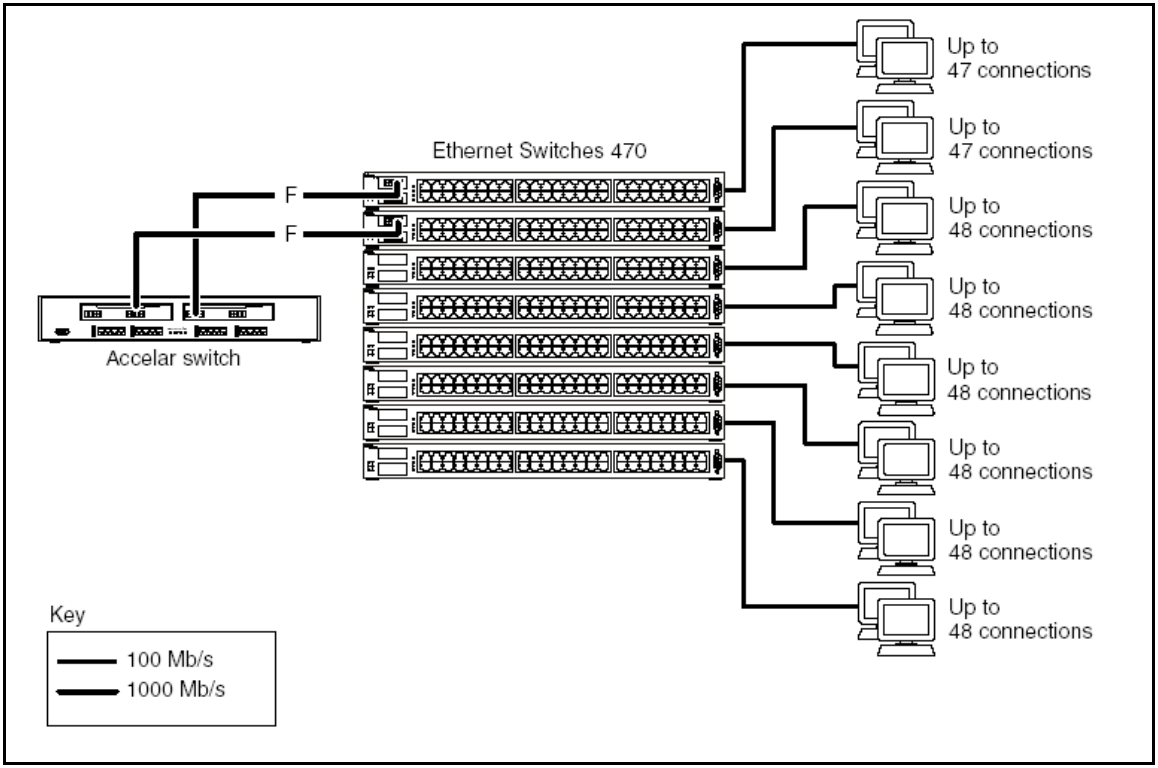
Fail-safe stack application

Figure 23 shows an example of eight Ethernet Switches 470 that are stacked together as a single managed unit. If any single unit in the stack fails, the remaining stack remains operational, without interruption.

The Accelar 1100 switch is used as a backbone switch, connecting to the switches with an optional (1000BASE-SX) GBIC for maximum bandwidth.

For an overview of the fail-safe stacking feature for the Ethernet Switches 460 and 470, see "Stacking" on page 293.

Figure 23 Fail-safe stack example for Ethernet Switch 470



Ethernet Switch stack operation

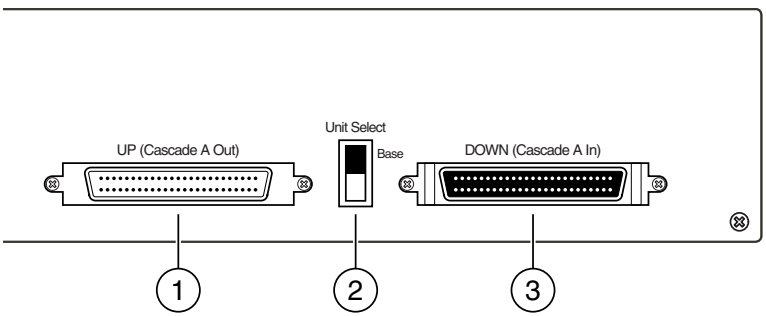
Ethernet Switches provide fail-safe stackability using built-in or optional cascade connectors. You can connect up to eight Ethernet Switches together to provide uninterrupted connectivity for 384. You can manage the entire stack of switches as a single unit.

This section discusses the following stacking topics:

Built-in Cascade Connector

The front panel components of the built-in Cascade Connector are shown in Figure 24.

Figure 24 Built-in Cascade Connector components



1 = Cascade Up
2 = Unit Select switch
3 = Cascade Down

10693EB

Cascade A Out connector

Provides an attachment point for connecting this unit to another unit through the cascade cable. A *return* cable from the Cascade A Out connector of another unit to the Cascade A In connector of this unit completes the stack connection (see the example shown in Figure 25 on page 104).

Unit Select switch

The Unit Select switch (up = Base) determines the *base unit* for the stack configuration (see "Base unit" on page 107). The Unit Select switch status is displayed on the Ethernet Switch LED display panel. When the Unit Select switch is in the Base (up) position, all other Unit Select switches in the stack configuration must be set to Off (down).

Cascade A In connector

Provides an attachment point for accepting a cascade cable connection from an adjacent unit in the stack. A *return* cable from the Cascade A Out connector of this unit to the Cascade A In connector of the adjacent unit completes the stack connection (see the example shown in Figure 25 on page 104).

Figure 25 Connecting cascade cables

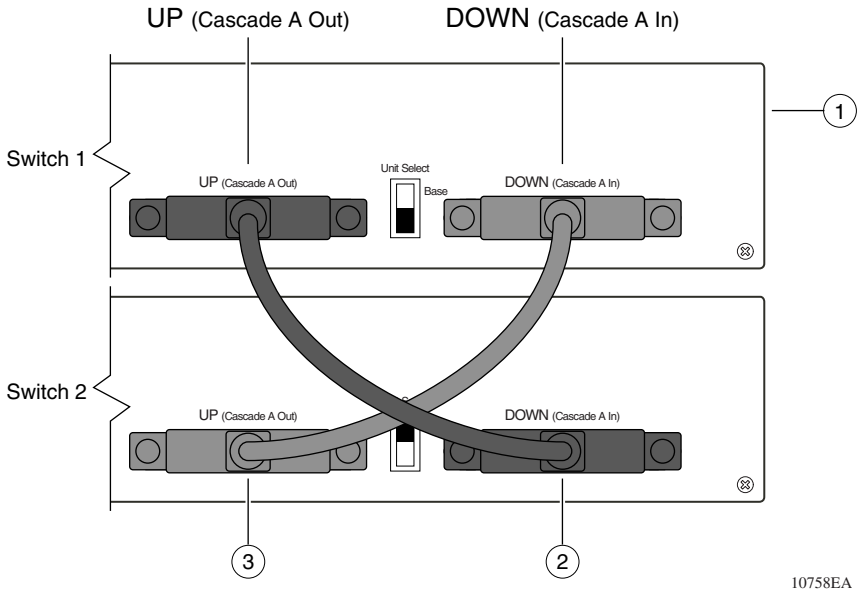


Table 25 describes legends used in the figure.

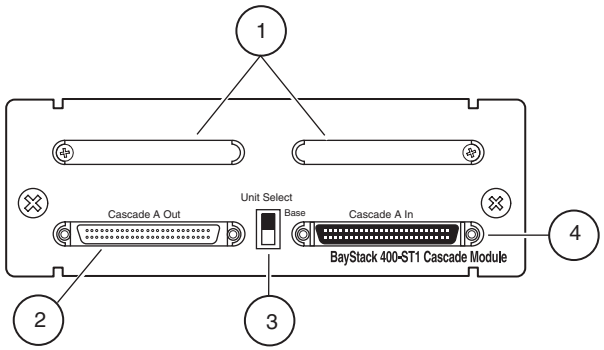
Table 25 Connecting cascade cable

Legend	Description
1	Base unit
2	AL 2018002 cascade cable
3	AL 2018002 cascade cable (used for return)

BayStack 400-ST1 Cascade Module

The front panel components of the BayStack 400-ST1 Cascade Module are shown in Figure 26. Component descriptions follow the figure.

Figure 26 BayStack 400-ST1 Cascade Module front panel components



1 = Blank connectors (unused)
2 = Cascade A Out connector
3 = Unit Select switch
4 = Cascade A In connector

BS0031B

Cascade A Out connector

Provides an attachment point for connecting this unit to another unit via the cascade cable. A *return* cable from the Cascade A Out connector of another unit to the Cascade A In connector of this unit completes the stack connection (see the example shown in Figure 27 on page 106).

Unit Select switch

The Unit Select switch (up = Base) determines the *base unit* for the stack configuration (see "Base unit" on page 107). The Unit Select switch status is displayed on the Ethernet Switch LED display panel. When the Unit Select switch is in the Base (up) position, all other Unit Select switches in the stack configuration must be set to Off (down).

Cascade A In connector

Provides an attachment point for accepting a cascade cable connection from an adjacent unit in the stack. A *return* cable from the Cascade A Out connector of this unit to the Cascade A In connector of the adjacent unit completes the stack connection (see the example shown in Figure 27).

Figure 27 Connecting cascade cables

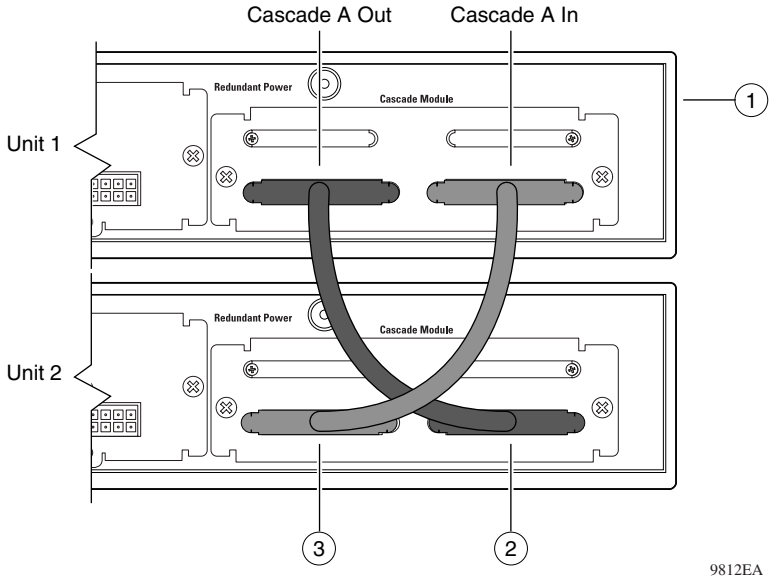


Table 26 describes the legends used in the figure.

Table 26 Connecting cascade cables

Legend	Description
1	Base unit
2	303978-A cascade cable
3	303978-A cascade cable (used for return)

Base unit

Note: For stacking three or more units (maximum 8 units per stack), order the optional 1 meter (39.27 inch) cascade max-return cable (order number AL2018001).

The base unit is the unique stack unit that you configure with the Unit Select switch on the front panel of the BayStack 400-ST1 Cascade Module. One Ethernet Switch 460 or 470 in the stack must be configured as the base unit; all other units in the stack must have their Unit Select switch set to Off. You can assign any single Ethernet Switch 460 or 470 as the base unit.

The physical ordering of all of the other units in the stack is determined by the position of the base unit within the stack. This is important for management applications that view the physical ordering of the units within the stack.

Some characteristics of the base unit are described in the following sections.

Initial installation

During the initial installation of the stack, the software automatically determines the physical order of all units in the stack according to the position of the base unit within the stack. Thereafter, the individual units maintain their original unit numbering, even if you change the position of one or more units in the stack. (Refer to "Using the Console Interface" on page 131 for information on renumbering the units using the Console Interface (CI) menus and to "Administering the switch using Web-based management" on page 477 for information on renumbering the units using the Web-based management system.)

For example, when you initially power up the stack, the base unit becomes unit 1 and the unit that the base unit connects to (via the Cascade A Out cable) becomes unit 2 (and the next unit is unit 3 and so on), until the maximum stack configuration (up to 8 units) is reached. If you change the base unit to another unit in the stack, the new base unit keeps its original unit number in the stack.

Stack MAC address

When the switch is participating in a stack configuration, a stack MAC address is automatically assigned during the stack initialization. The base unit MAC address, with a software offset, is used for the stack MAC address.

For example, if the base unit's MAC address is 00-00-82-99-44-00, and the stack software offset is `1F`, then the stack MAC address becomes:

00-00-82-99-44-1F

If another unit in the stack is assigned as the base unit, the MAC address of the *new* base unit (with offset) now applies to the stack configuration. The original stack IP address still applies to the new base unit.

Temporary base unit

If an assigned base unit fails, the next unit in the stack order automatically becomes the new *temporary base unit*. This change is indicated by the base LED on the temporary base unit LED display panel turning on (amber).

This automatic failover is a temporary safeguard only. If the stack configuration loses power, the temporary base unit will not power up as the base unit when power is restored. For this reason, you should always assign the temporary base unit as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced.

Note: If you do not reassign the temporary base unit as the new base unit, and the temporary base unit fails, the next unit directly downstream from this unit becomes the new temporary base unit. This process can continue until there are only two units left in the stack configuration.

Identify Unit Numbers

When you choose Identify Unit Numbers from the main menu, the console returns the message:

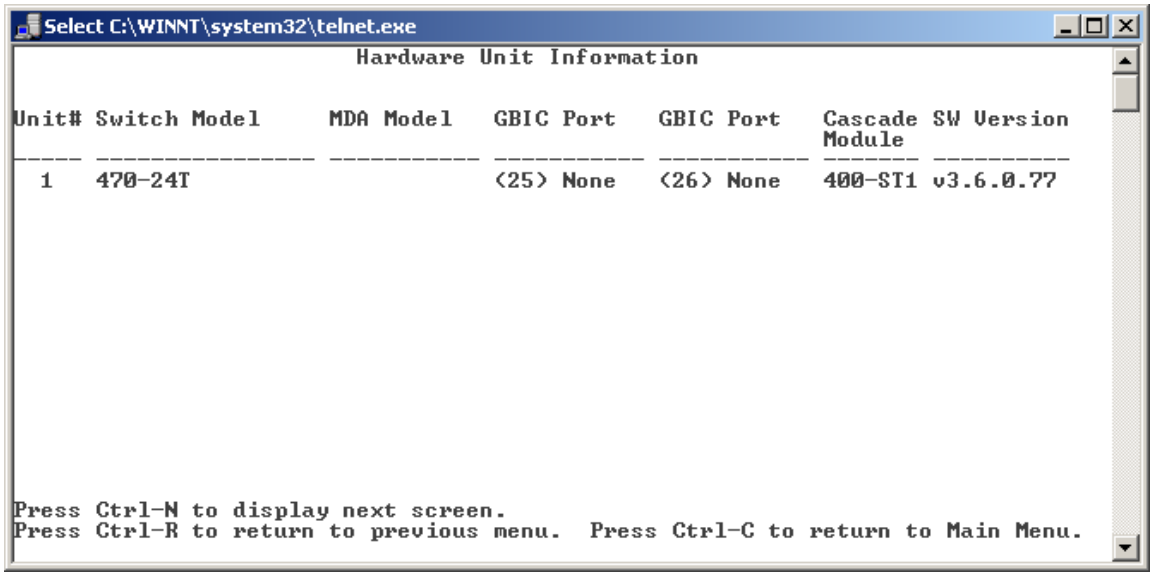
`Port LEDs lit on the front panel of the switch correspond to` its unit number.

Hardware Unit Information screen

The Hardware Unit Information screen (Figure 28) lists the switch models. In addition, this screen displays the software version running on the hardware. To open the Hardware Unit Information screen:

- Choose Display Hardware Units (or press h) from the main menu.

Figure 28 Hardware unit information screen



Removing a unit from the stack

If a unit is removed from the stack (therefore operating in stand-alone mode), the following switch configuration settings revert back to the settings configured before the unit became a member of the stack:

- IP address
- Password: console, Web, Telnet, SNMP (including Device Manager)
- Stack operational mode
- SNMP community strings

Stack configurations

As shown in Figure 29 on page 111, the cascade connectors and cables on the BayStack 400-ST1 Cascade Module front panel provide the ability to stack up to 8 switches. With BPS-2000 MDAs installed in each switch, the stack can accommodate a maximum of 224 switch ports.

Since stack parameters are associated with the base unit (see "Base unit" on page 107), the physical stack order depends on the base unit's position and whether the stack is configured *stack up* or *stack down.*

Stack up configurations

In Figure 29 on page 111, data flows from the base unit (unit 1) to the next switch, which is assigned as unit 2, and continues until the last switch in the stack is assigned as unit 8. The physical order of the switches is *from bottom to top* (unit 1 to unit 8).

Figure 29 Stack up configuration example

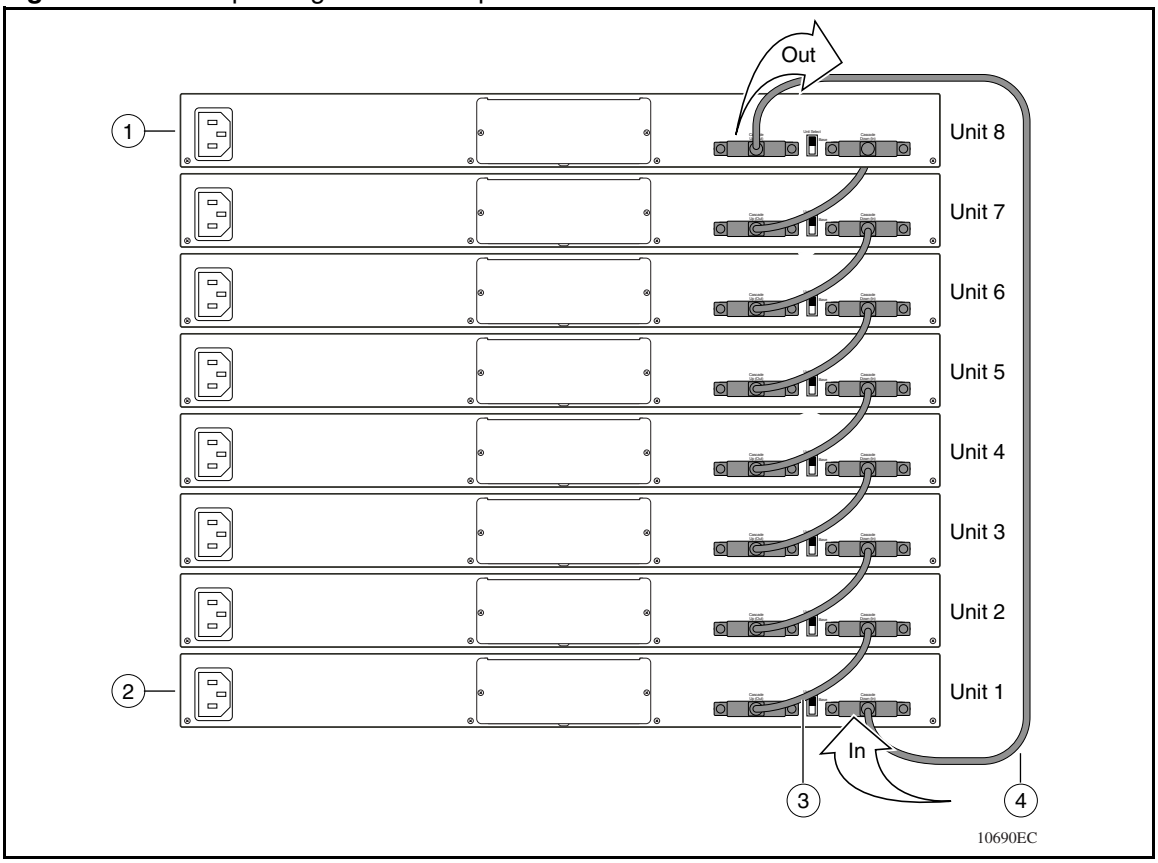


Table 27 describes the stack up configuration illustration references.

Table 27 Stack up configuration description

1	Last unit
2	Base unit
3	Cascade Cable (AL2018001 - 1 foot) Cascade Cable (AL2018002 - 18 inches) - Not shown
4	Cascade Cable (AL2018004 - 3 meters)

Stack down configurations

In Figure 30, data flows from the base unit (unit 1) to the next switch, which is assigned as unit 2, and continues until the last switch in the stack is assigned as unit 8. The physical order of the switches is *from top to bottom* (unit 1 to unit 8).

Figure 30 Stack down configuration example

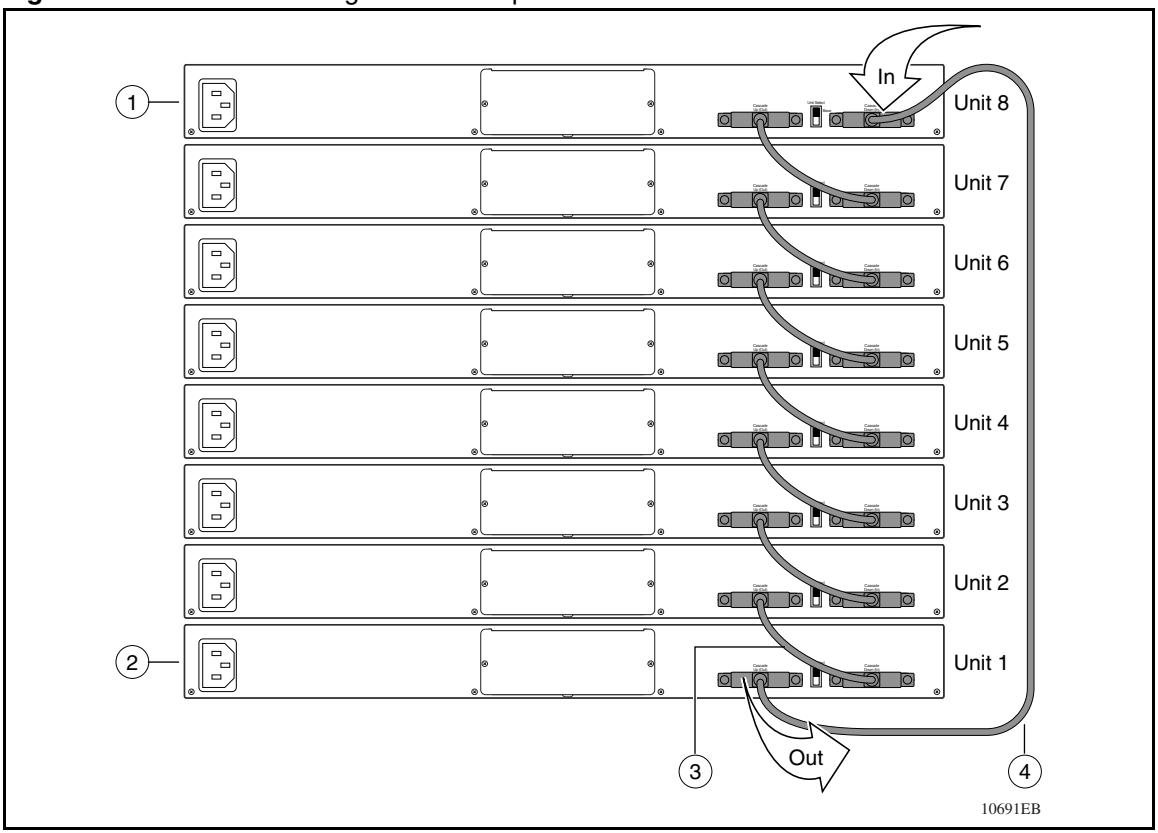


Table 28 describes the stack down configuration illustration references.

Table 28 Stack down configuration description

1	Base unit
2	Last unit
3	Cascade cable (part number 303978-A)
4	Cascade max-return cable (part number 303979-A)

Certain Network Management Station (NMS) applications assume a stack down configuration for the graphical user interface (GUI) that represents the stack (see Figure 30).

Note: For this reason, Nortel recommends that you always configure the top unit in the stack as the base unit.

In any stack configuration, the following applies:

- You can access and manage the stack using a Telnet connection, the Web-based management interface, or any generic SNMP management tool through any switch port that is part of the stack configuration.
- When stacking three or more switches, use the longer (1-meter) cascade max-return cable (part number 303979-A) to complete the link from the last unit in the stack to the base unit.

Redundant cascade stacking feature

Ethernet Switches 460 and 470 allow you to connect up to eight units into a redundant cascade stack. If any single unit fails or if a cable is accidently disconnected, other units in the stack remain operational, without interruption.

Figure 31 on page 114 shows an example of how a stack configuration reacts to a failed or powered-down unit in the stack configuration:

1. As shown in Figure 31 on page 114, unit 3 becomes non-operational.

   This result can be due to a failed unit or simply because the unit was powered down.

2. Unit 2 and unit 4, directly upstream and downstream from unit 3, sense the loss of link signals from unit 3.

   a. Units 2 and 4 automatically loop their internal stack signals (A and B).

   b. The Cas Up LED for unit 2 and the Cas Dwn LED for unit 4 turn on (amber) to indicate that the stack signals are looped.

3. The remaining stack units remain connected.

Although the example shown in Figure 31 shows a failed unit causing the stack to loop signals at the points of failure (A and B), the system reacts the same way if a cable is removed.

Figure 31 Redundant cascade stacking feature

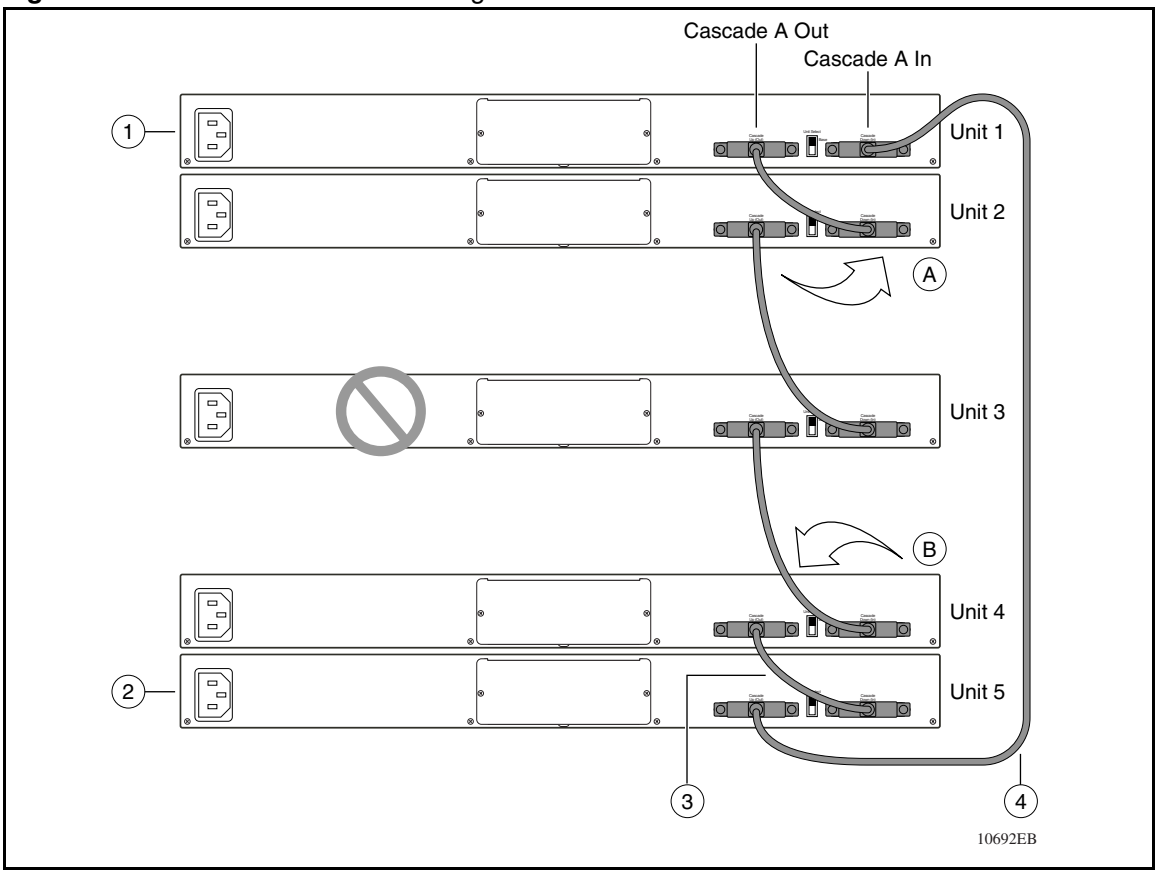


Table 29 describes the redundant cascade stacking illustration references.

Table 29 Redundant cascade stacking descriptions

Legend	Description
1	Base unit
2	Last unit
3	Cascade cable (AL 2018002 - 18 inches)
4	Cascade max-return cable (AL 2018004 - 3 meters)

Faulty unit and cable detection

The stack manager can detect the scenario whereby a unit appears good to its neighboring units (its up and downstream clocks are good), but the data packets it transmits or receives are corrupted or missing. In such a scenario, the stack falls apart and the ring check does not succeed.

This triggers the “Ring Discovery” algorithm whereby units are polled both downstream and upstream individually to isolate the point of failure. When the failure is isolated, the bad unit or cables are wrapped out.

In the case where a cable has bad data pins, the stack ports where the cable is connected are wrapped out. On a unit that has its IN port connected to the bad cable, the system log shows “IN stack port wrapped; check for bad cable or unit” and its downstream LED stays amber.

Similarly, on the unit that has its OUT port connected to the bad cable, the system log shows “OUT stack port wrapped; check for bad cable or unit” and its upstream LED stays amber. When replacing a bad cable with a good one, at least one unit should be rebooted so that the stack manager on the base unit detects a unit coming in and re-runs the stack.

Accessing the system through text-based interfaces

This section describes the following topics:

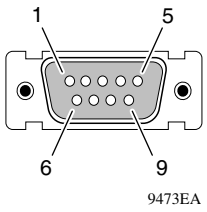
Configuring the Console Port

The console or the serial port provides a physical-layer connection by using the standard RS-232 protocol to connect the Ethernet Switch unit to a terminal or Personal Computer (PC). A connection through the console port allows the network manager to gain access to the Console Interface (CI) and Command Line Interface (CLI).

The console port is a DB-9, RS-232-D male serial port connector. You can use this serial port to connect a management station or terminal to the Ethernet Switch unit by using a straight-through DB-9 to DB-9 standard serial port cable.

Refer to Table 30 for the pin-out assignments for the console port.

Table 30 Console Port Pin-outs

Connector	Pin number	Signal
	1	Carrier detect (not used)
	2	Transmit data (TXD)
	3	Receive data (RXD)
	4	Data terminal ready (not used)
	5	Signal ground (GND)
	6	Not used
	7	Request to send (not used)
	8	Not used
	9	Ring indicator (not used)

Note: The console port is configured as a data communications equipment (DCE) connector. Ensure that your RS-232 cable pin-outs are configured for DCE connections.

Console port serial cable requirements

To connect the console port of the Ethernet Switch unit, use a straight-through serial cable with a DB-9 female connector for the Ethernet Switch unit, and the appropriate connector for your PC. The console/serial cable to connect from a PC with a male DB-9 serial port to the Ethernet Switch is available to order using the following information:

Table 31 Console cable ordering information

Description	Order number
Console cable for use with Ethernet Switch and Passport 8300 switches.	AL2011013

Default port configuration settings

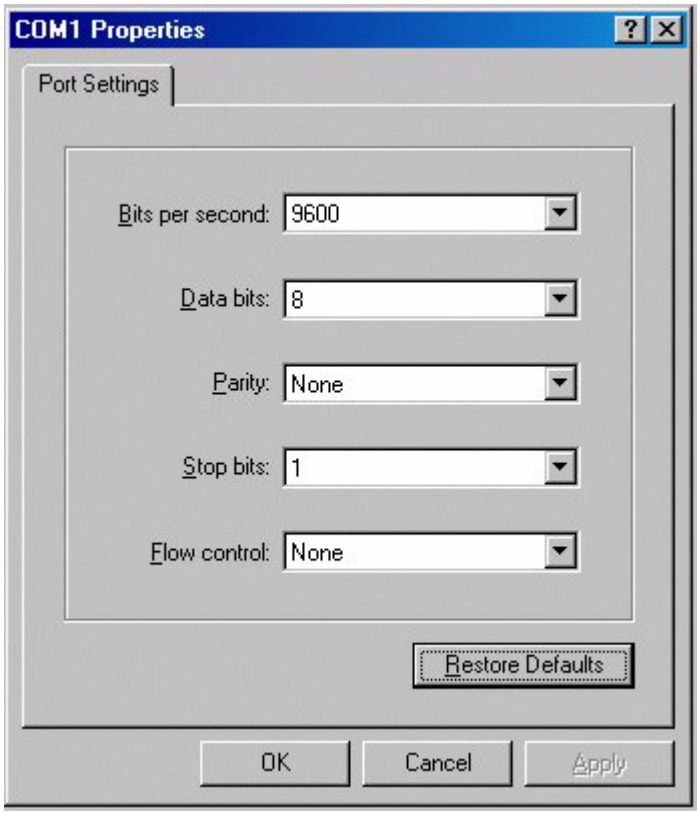
In order to utilize the serial port, you must have a terminal or PC with terminal emulation software attached to the console port. The default communications settings for the console port are as follows (see Figure 32 on page 118):

- 8 Data Bits
- 1 Stop Bit
- No Parity
- 9600 BPS
- No flow control

While there is no need to set the flow control on the terminal, the text-based interfaces react to the XOFF (CTRL-S) and XON (CTRL-Q) characters. Pressing the XOFF character causes the Ethernet Switch unit to stop sending data to the connected terminal or PC.

Pressing the XON character signals the switch to send characters to the connected device. Pressing XON causes the switch to immediately send characters that are stored in the output buffer, and to then resume normal operation.

Figure 32 HyperTerminal communication port settings



Configuring the console port using the user interface

The Console Port Speed parameter is the only console port setting that the network manager can configure. All other console port configuration parameters are fixed and cannot be changed by the user.

Table 32 indicates whether the user has read (r), read-write (rw), or no access to the parameters through the listed user interface.

Table 32 Console port parameters interface support matrix

Parameter	Default	Menu Interface	CLI	Web	Device Manager
Speed / Bits per second	9600	rw	rw	rw	no
Data bits	8	r	no	r	no
Parity	1	r	no	r	no
Stop bits	None	r	no	r	no
Flow Control	Xon/Xoff	no	no	no	no

Configuring the console port using the Console Interface

The Console/Comm Port Configuration screen, shown in Figure 33 on page 120, allows you to configure and modify the console port parameters and security features of a switch.

To open the Console/Comm Port Configuration screen, choose Console/Comm Port Configuration from the main menu, or press “o” on the keyboard.

Figure 33 Console/Comm Port Configuration screen

```
                    Console/Comm Port Configuration



Comm Port Data Bits:                    8 Data Bits
Comm Port Parity:                       No Parity
Comm Port Stop Bits:                    1 Stop Bit
Console Port Speed:                     [ 9600 Baud  ]



Console Switch Password Type:           [ None                  ]
Console Stack Password Type:            [ None                  ]
Telnet/WEB Switch Password Type:        [ None                  ]
Telnet/WEB Stack Password Type:         [ None                  ]
Console Read-Only Switch Password:      [ user ]
Console Read-Write Switch Password:     [ secure ]
Console Read-Only Stack Password:       [ user ]
Console Read-Write Stack Password:      [ secure ]



RADIUS Password Fallback:               [ No  ]
Primary RADIUS Server:                  [ 0.0.0.0 ]
```

Table 33 describes the Console/Comm Port Configuration screen fields.

Table 33 Console/Comm Port Configuration parameters

Field	Description
Comm Port Data Bits	A read-only field that indicates the current console/comm port data bit setting.
Comm Port Parity	A read-only field that indicates the current console/comm port parity setting.
Comm Port Stop Bits	A read-only field that indicates the current console/comm port stop bit setting.

Table 33 Console/Comm Port Configuration parameters (Continued)

Field	Description
Console Port Speed	Allows you to set the console/comm port baud rate to match the baud rate of the console terminal. Default Value: 9600 Baud Range: 2400 Baud, 4800 Baud, 9600 Baud, 19200 Baud, 38400 Baud
	Caution: If you choose a baud rate that does not match your console terminal baud rate, you will lose communication with the configuration interface when you press [Enter]. If communication is lost, set your console terminal to match the new service port setting.
	Achtung: Bei Auswahl einer Baud rate, die nicht mit der Baudrate des Konsolenterminals übereinstimmt, geht die Kommunikation mit der Konsolenschnittstelle verloren, wenn Sie die Eingabetaste drücken. Stellen Sie in diesem Fall das Konsolenterminal so ein, daß es mit der neuen Einstellung der Service-Schnittstelle übereinstimmt.
	Attention: Si vous sélectionnez un débit différent de celui de votre terminal, vous perdrez le contact avec l'interface de votre console dès que vous appuierez sur [Entrée]. Pour restaurer la communication, alignez le débit de votre terminal sur le nouveau débit de votre port de service.
	Precaución: Si selecciona una velocidad de transmisión que no coincide con la velocidad de transmisión del terminal de la consola, perderá la comunicación con el interfaz de la consola al pulsar [Intro]. Si se pierde la comunicación, ajuste el terminal de la consola para que coincida con el nuevo valor del puerto de servicio.
	Attenzione: Nel caso in cui si scelga una velocità di trasmissione non corrispondente a quella del terminale della console, la comunicazione con l'interfaccia della console cadrà premendo il tasto [Invio]. Se la comunicazione cade, impostare il terminale della console in modo tale che corrisponda alla nuova impostazione della porta di servizio.
	注意: コンソール・ターミナルのボー・レートに合っていないボー・レートを選択すると、[Enter]を押したときに、コンソール・インタフェイスとの通信が途切れてしまいます。この場合には、新しいサービス・ポート設定に合うようにコンソール・ターミナルを設定してください。

Troubleshooting

If you encounter any problems while connecting to the serial port of the device, execute the following steps:

- Check that the Ethernet Switch unit is turned on.
- Check that you are using the correct communications port on your device.
- Check that all cables are tightly connected and that you are using the appropriate straight-through cable.
- Check that your communications software is set up according to the recommended configuration outlined in "Default port configuration settings" on page 117: 8 Data Bits, 1 Stop Bit, No Parity, 9600 bps, No flow control.
- Verify the speed of the port by connecting to the device through a Telnet connection and navigating to the appropriate screen.
- Change the speed setting on the port to match the setting of the serial port on the Ethernet Switch unit. Possible values include: 2400, 4800, 9600, 19200, 38400.
- Verify the integrity of the cable by using it to connect to another device or by checking it with a the receptacle into which you plug.
- Depress the XON (CTRL-Q) key in case you inadvertently suspended operation of the console port by depressing the XOFF (CTRL-S) key.

Usage guidelines

To prevent unauthorized access, ensure that:

- The device connected to the console port is logged out of the system when not in use.
- The console port is configured as a data communications equipment (DCE) connector. Ensure that your RS-232 cable pin-outs are configured appropriately.

Telnet Access

The Ethernet Switch unit provides in-band management access through the Telnet protocol. By default, Telnet access is enabled. The unit allows TCP connections on port 23.

Telnet client support

The Telnet client allows you to Telnet to a host or UNIX machine. One Telnet client session at a time is supported.

Telnet command

The `telnet` command allows you to establish a Telnet session to a remote system using either the system IP address or hostname.

Managing Telnet Access

The Ethernet Switch unit allows you to customize Telnet access to the device. The parameters that you can control are:

- Login Timeout
- Login Retries
- Inactivity Timeout
- Event Logging
- Access Control List

IP manager list

You can limit access to the management features of the Ethernet Switch unit by defining the IP addresses that are allowed access to the switch.

The features provided by the IP manager list are:

- Definitions of up to 50 IP addresses and masks that are allowed
- Options to enable or disable access for Telnet, SNMP, and the Web-based management system

Configuring user interface support for Telnet Access using the IP Manager

The IP manager Telnet Access configuration parameters are available through a number of interfaces.

Table 34 indicates whether the user has read (r), read-write (rw), or no access to the parameter through the listed interface.

Table 34 Configuring user Interface support for Telnet access

Parameter	Default	Menu Interface	CLI	Web	Device Manager
Access	Enabled	rw	rw	rw	no
Event Logging	All	rw	rw	no	no
Inactivity Timeout	15 minutes	rw	rw	no	no
Login Retries	3	rw	rw	no	no
Login Timeout	1 minute	rw	rw	no	no
Use Access Control List	Yes	rw	rw	rw	no

For more information on configuring the IP manager list, see *Configuring and Managing Security* (217104-A).

Troubleshooting

If you encounter any problems while accessing the Ethernet Switch unit through the Telnet protocol, do the following to diagnose the problem:

- Check that you are targeting the correct IP address and that your Telnet program is configured to target TCP port 23.
- Check that the IP address, subnet mask, and default gateway parameters are correctly configured on the Ethernet Switch unit and the management station.
- Ping the target device to ensure your management workstation can reach it.
- Eliminate all Telnet access restrictions to minimize complexity.
- Check that Telnet access is enabled on the Ethernet Switch unit.

- Ensure that the IP address of the management station is allowed to Telnet to the device.

Usage Guidelines

Refer to the following guidelines when configuring Telnet access on the Ethernet Switch unit.

- The Console Interface, CLI, and Web-based interface support up to 50 IP Address/Mask combinations.
- When Telnet access is disabled, the unit allows devices to connect to port 23, and then immediately resets the connection.
- If your network uses dynamic IP addresses, it can be better to define a range of IP addresses that are allowed to access the unit instead of defining specific IP addresses.

Using remote logging

The remote logging feature provides an enhanced level of logging by replicating system messages onto a syslog server. System log messages from several switches can be collected at a central location, eliminating the need for the network manager to query each switch individually to interrogate the log files.

You must configure the remote syslog server and set up the unit to log informational messages to this remote server. The UDP packet is sent to port 514 of the configured remote syslog server.

Once the IP address is in the system, you can send the syslog messages to the remote syslog server. If a syslog message is generated prior to capturing the IP address of the server, the system stores up to ten messages that are sent once the IP address of the remote server is on the system.

You can configure this feature by:

- enabling remote logging
- specifying the IP address of the remote syslog server
- specifying the severity level of the messages that you want to send to the remote server

For details, see *System Monitoring Guide* (217107-A).

Configuring terminal emulation software

If you are using a PC, you must have terminal emulation software that can send, receive, and interpret the screen formatting and cursor control commands required by the Console Interface and CLI.

The terminal emulation software is required if you are connecting to the device through the serial port or through a Telnet connection.

Set your terminal emulation parameters as follows:

- VT100 Arrows
- VT100 Terminal Emulation
- Backspace set to Del

Other optional terminal emulation configuration parameters are useful. This includes adding a line delay of 1 second, when sending an ASCII text file to the switch through the terminal emulator, and marking the option to “Wrap lines that exceed the terminal width” (see Figure 34 on page 127).

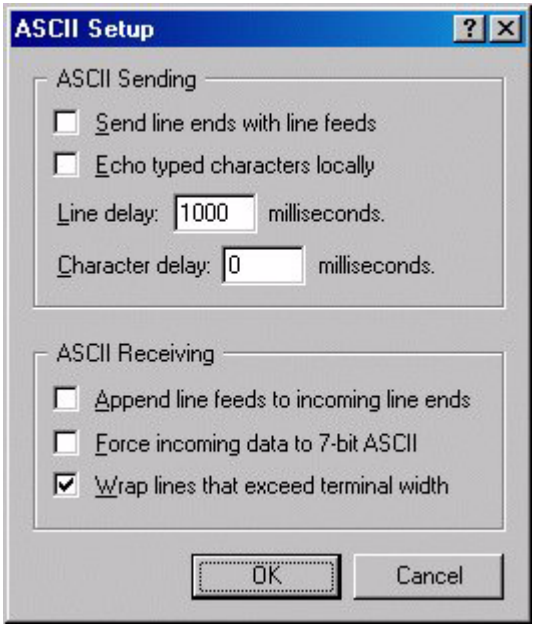
Line Delay

Some CLI commands allow you to make extensive configuration changes with only one command. The system can take some time to execute these commands; so, if you are going to paste a series of commands to the device as an ASCII text file through the terminal emulator, you can be forced to delay between each command in order for the system to process the commands. Note that this restriction does not exist if you use the built-in ASCII Configuration Download feature.

Wrapping lines that exceed terminal width

Some of the output — particularly from the system log — can exceed the width of your terminal screen. In order to see all the text sent to the display device when this condition occurs, you can configure the terminal emulator to automatically wrap the text to the next line by enabling the **Wrap lines that exceed terminal width** option.

Figure 34 HyperTerminal ASCII setup configuration panel



Management Interface Support

The Nortel Ethernet Switches that are shipped directly from the factory are ready to operate in any 10BASE-T or 100BASE-TX standard network.

Before you start working on any switch, you must assign an IP address to the switch. You can set the address by using the console port or BootP, which resides on the switch. You can manage the switch using one of the following network management tools and interfaces:

- "Console Interface"
- "Web-based management"
- "Device Manager" on page 129
- "Command Line Interface (CLI)" on page 129
- "Simple Network Management Protocol" on page 129
- "Other" on page 130

Console Interface

The Console Interface (CI) allows you to configure and manage the switch locally or remotely.

You can access the CI menu and screens in one of the following methods:

- locally through a console terminal attached to your switch
- remotely through a dial-up modem connection
- in-band through a Telnet session

For information about the Console Interface, see Chapter 2, "Using the Console Interface," on page 131.

Web-based management

You can manage the network from the Web-based Graphical User Interface (GUI) through an HTML-based browser located on your network.

The GUI allows you to configure, monitor, and maintain your network through Web browsers. You can also download software by using the Web-based management interface.

For information about Web-based management, see Chapter 5, "Using the Web-based management interface," on page 229.

Device Manager

The Device Manager is a set of Java-based graphical network management applications used to configure and manage the Ethernet Switch 460/470.

For more information on the Device Manager, see Chapter 4, "Installing and using Device Manager software," on page 181.

Command Line Interface (CLI)

The CLI is used to automate general management and configuration of the Ethernet Switch. Use the CLI through a Telnet connection or through the serial port on the console.

For more information on the CLI commands, see Chapter 3, "CLI Basics," on page 153.

SSH

Secure Shell (SSH) is a client/server protocol that can provide a secure remote login with encryption of data, username, and password. For details on SSH connections, refer to *Configuring and Managing Security* (217104-A).

Simple Network Management Protocol

You can use any generic Simple Network Management Protocol (SNMP)-based network management software to configure and manage an Ethernet Switch unit.

Other

You can also interact with Ethernet Switches using the Nortel Enterprise Policy Manager (formerly Optivity Policy Services).

Chapter 2
Using the Console Interface

You can manage the switch with the following tools:

- Java Device Manager (JDM)
- Web-based management system
- Command Line Interface (CLI)
- Console Interface (CI menus)

For more information on using the JDM, refer to Chapter 4, “Installing and using Device Manager software,” on page 181.

For more information on using the Web-based management system, refer to Chapter 5, “Using the Web-based management interface,” on page 229.

For more information on using the CLI menus, refer to Chapter 3, “CLI Basics,” on page 153.

For information about SNMP, see your network management documentation.

This chapter describes how to configure and manage the Ethernet Switch 460/470 using the menu-driven Console Interface (CI).

Note: When you power up or reset the switch, it runs a self-test, then displays the Nortel logo banner. Press [Ctrl]-Y to access the 460 or 470 main menu.

This chapter covers the following topics:

- "Switch Configuration Menu screen" on page 139
- "Port Configuration screen" on page 142
- "High Speed Flow Control Configuration screen" on page 144
- "System Log screen" on page 149

To find out which version of the Ethernet Switch 460 or 470 software is running, use the Console Interface (CI) menus or the Web-based management system:

- CI menus—From the main menu of the console, choose Systems Characteristics menu. The software currently running is displayed in sysDescr.
- Web-based management system—Open the System Information page, which is under Administration on the main menu. The software currently running is displayed in the sysDescription field.

Accessing the Console Interface menus and screens

The Console Interface is an easy-to-use menu system that provides you with access to the most frequently used configuration parameters, commands, and utilities.

You can access the CI menus and screens locally through a console terminal attached to your Ethernet Switch 460 or 470, remotely through a dial-up modem connection, or in-band through a Telnet session.

Note: If you have a properly configured BootP server in your network, it detects the IP address; you do not need to configure the IP address.

Using the Console Interface menus and screens

The CI menus and screens provide options that allow you to configure and manage the Ethernet Switch 460 or 470. Help prompts at the bottom of each menu and screen explain how to enter data in the highlighted field, and how to navigate the menus and screens.

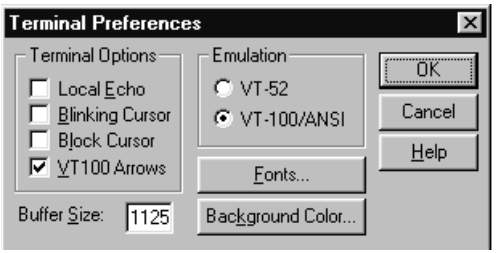
The Console Port default settings are: 9600 baud with eight data bits, one stop bit, and no parity as the communications format, with flow control set to disabled.

Some CI screen options allow you to toggle among several possible values; other options allow you to set or modify a parameter.

Using Telnet to access the CI menus and screens

When you use Telnet to access the CI menus and screens, set the terminal Preferences to VT100 Arrows and VT-100/ANSI and as shown in Figure 35.

Figure 35 Terminal preference settings



Navigating the CI menus and screens

Use the following methods to navigate the CI menus and screens.

To select a menu option:

1. Use the arrow keys to highlight the option name.
2. Press [Enter].

   The option takes effect immediately after you press [Enter].

Alternatively, you can press the key corresponding to the underlined letter in the option name. For example, to select the Switch Configuration option in the main menu, press the w key. Note that the text characters are not case-sensitive.

Note: In some instances, the underscore is not displayed in the option menu. When this is the case, pressing the associated key still selects the appropriate option.

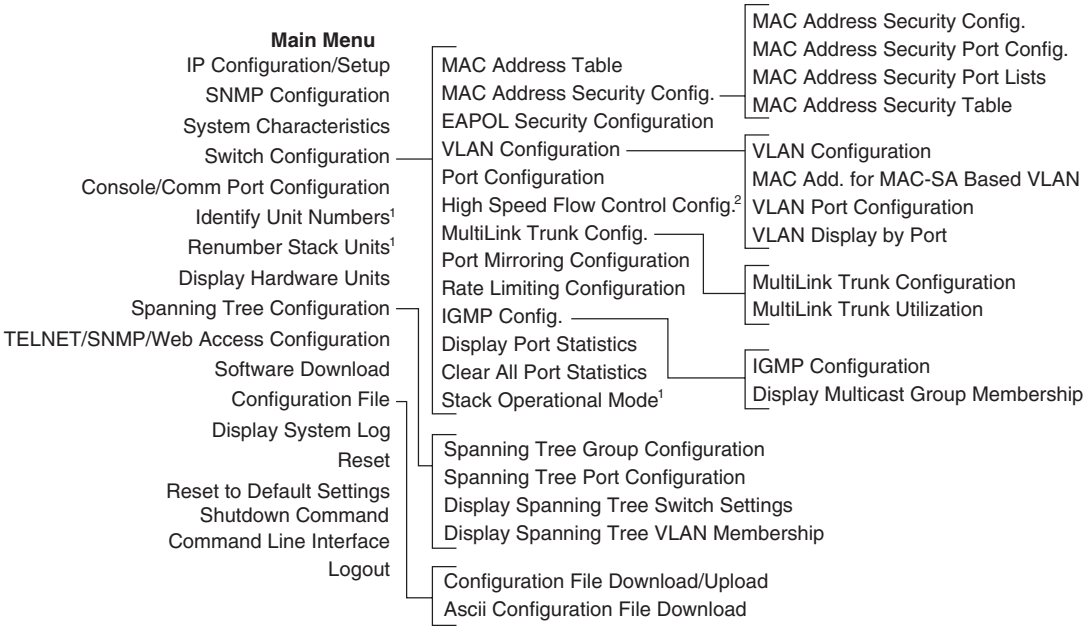
Additional navigation aids follow:

- To toggle between values in a form:
  - Use the spacebar to highlight the value.
  - Press [Enter].
- To clear a string field:
  - Position the cursor in the string field.
  - Press [Ctrl]-K.
- To return to the previous menu, press [Ctrl]-R.
- To go to the next screen in a series, press [Ctrl]-N.
- To return to the main menu at any time, press [Ctrl]-C.
- Press [Backspace] to delete entered text.
- Options that appear in brackets (for example, [Enabled]) are user-configurable options.

Screen fields and descriptions

Figure 36 on page 135 shows a map of the CI screens. The remainder of this chapter describes the CI screens and their fields, beginning with the main menu.

Figure 36 Map of Console Interface screen



[1] Only appears when the switch is participating in a stack configuration.
[2] Only appears when a gigabit MDA is installed in one or more units in a stack configuration.

The CI screens for your specific switch model show the correct model name in the main menu screen title, and the correct number of ports and port types in the Port Configuration screen.

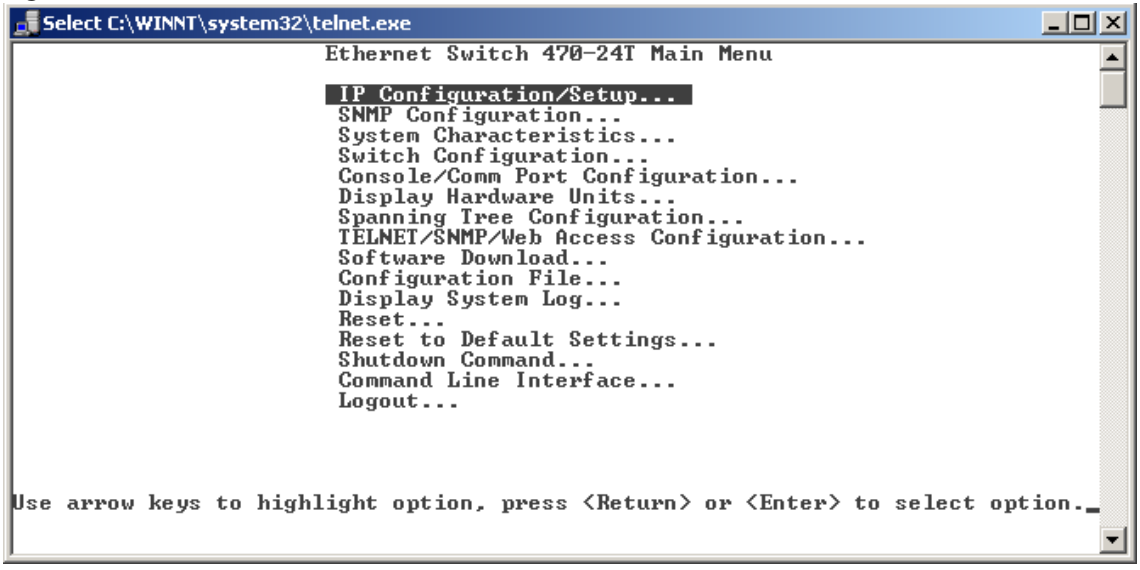
Note: The field values shown in the CI screens in this section are provided as examples only.

Console Interface Main Menu

This section describes the options available from the CI main menu. Figure 37 displays the CI main menu. The CI screens and submenus for these options are described throughout this document.

Note: Some menu options shown in example of main menu and in other examples do not appear on your screen, depending on the switch options installed. However, the full menu options are shown in the screen examples and described in the following sections.

Figure 37 Console Interface main menu



Description of Main Menu Components

Table 35 describes the Console Interface main menu options.

Table 35 Console interface Main Menu options

Option	Description
IP Configuration/ Setup...	Displays the IP Configuration/Setup screen (see Figure 89 on page 243). This screen allows you to set or modify IP configuration parameters and to ping other network devices.
SNMP Configuration...	Displays the SNMP Configuration screen (see *Configuring and Managing Security* (217104-A)). This screen allows you to set or modify the SNMP read-only community and read-write community strings, enable or disable the authentication trap, set the IP address of trap receivers, and set the trap community strings.
System Characteristics...	Displays the System Characteristics screen (see "Managing System Characteristics" on page 255). This screen allows you to view switch characteristics, including number of resets, power status, hardware and software version, MAC address, GBIC information, firmware version, date of manufacture, and hardware deviation number. This screen also contains three user-configurable fields: sysContact, sysName, and sysLocation.
Switch Configuration...	Displays the Switch Configuration Menu screen (see "Switch Configuration Menu screen" on page 139). This menu provides the following configuration options: MAC Address Table, MAC Address-Based Security, EAPOL Security Configuration, VLAN Configuration, Port Configuration, High Speed Flow Control, MultiLink Trunk Configuration, Port Mirroring Configuration, Rate Limiting Configuration, IGMP Configuration, Display Port Statistics, and Clear All Port Statistics.
Console/Comm Port Configuration...	Displays the Console/Comm Port Configuration screen (see "Configuring the Console Port" on page 116). This screen allows you to configure and modify the console/Comm port parameters, including the console port speed and password settings for the switch.
Identify Unit Numbers	Displays the following message at the bottom of the Main Menu: Port LEDs lit on the front panel of the switch correspond to its unit number.
Renumber Stack Units...	Displays the Renumber Stack Units screen (see "Renumbering stack units" on page 301). This screen allows you to reset the unit numbers within a stack.
Display Hardware Units	Displays the Display Hardware Unit Information screen (see "Hardware Unit Information screen" on page 109). This screen displays the switch model and the software version running.
Spanning Tree Configuration...	Displays the Spanning Tree Configuration Menu (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)). This menu provides the following options: Spanning Tree Group Configuration, Spanning Tree Port Configuration, Display Spanning Tree Switch Settings, and Display Spanning Tree VLAN Membership.

Table 35 Console interface Main Menu options (Continued)

Option	Description
TELNET/SNMP/Web Access Configuration...	Displays the TELNET/SNMP/Web Access Configuration screen (see *Configuring and Managing Security* (217104-A)). This screen allows you to set your switch to enable a user at a remote console terminal to communicate with the switch as if the console terminal is directly connected to it. You can have up to ten active Telnet sessions running at one time in a switch configuration. You can use the Command Line Interface (CLI), JDM, Web-based management system, or these menus with a Telnet session. This screen also allows you to set the switch to allow up to 50 IP addresses to access the switch using either these management systems or SNMP access
Software Download...	Displays the Software Download screen (see "Software Management using the Console Interface" on page 264). This screen allows you to revise the switch software image that is located in non-volatile flash memory (NVRAM).
Configuration File...	Displays the Configuration File Menu screen (see "Configuration Management" on page 268). This menu provides the following options: Configuration File Download/Upload and ASCII Configuration File Download.
Display System Log	Displays the System Log screen (see "System Log screen" on page 149).
Reset	Resets the switch with the current configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch; enter No to abort the option: • When you select this option, the switch resets, runs a self-test, then displays the Nortel logo screen. Press [Ctrl]-Y to access the Ethernet Switch 460 or 470 main menu.
Reset to Default Settings	Resets the switch to the factory default configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch to the factory default configuration settings; enter No to abort the option: • When you select this option, the switch resets, runs a self-test, then displays the Nortel logo screen. Press [Ctrl]-Y to access the switch main menu. **NOTE**: The following items do NOT reset: Reset Count, and Reason for Last Reset.
	Caution: If you choose the Reset to Default Settings option, all of your configured settings will be replaced with factory default settings when you press [Enter]
	Achtung: Bei Auswahl des Befehls zur Rücksetzung auf die Standardeinstellungen werden alle von Ihnen konfigurierten Einstellungen durch die werkseitigen Standardeinstellungen ersetzt, wenn Sie die Eingabetaste drücken.
	Attention: Si vous restaurez la configuration usine, votre configuration courante sera remplacée par la configuration usine dès que vous appuierez sur [Entrée].

Table 35 Console interface Main Menu options (Continued)

Option	Description
	Precaución: Si selecciona el comando Restaurar valores predeterminados, todos los valores de configuración se sustituirán por las valores predeterminados en fábrica al pulsar [Intro].
	Attenzione: Nel caso in cui si selezioni la reimpostazione dei valori di default, tutte le impostazioni configurate verranno sostituite dai default di fabbrica premendo il tasto [Invio].
	注意：「デフォルトの設定にリセット」コマンドを選択すると、現在のコンフィグレーションされた設定は、[Enter]を押したとき、工場出荷時の設定に変更されます。
Shutdown command	Allows the switch to be safely shut down and powered off. Once the shutdown command is initiated, the switch saves the current configuration and instructs the user to power off the switch within the specified time period (one to ten minutes); otherwise, the switch is reset. When the command is initiated in the Console Interface, the following message appears: `It is safe to poweroff the switch, it will reset in xxx seconds.`
Command Line Interface	Allows a properly authorized user to initiate a CLI management session. Refer to Chapter 3, “CLI Basics,” on page 153, for information on using the CLI.
Logout	Allows a user in a Telnet session or a user working at a password-protected console terminal to terminate the session.

Switch Configuration Menu screen

The Switch Configuration Menu screen (Figure 38 on page 140) allows you to set or modify your switch configuration.

Note: The High Speed Flow Control Configuration option appears only when an optional GBIC is installed.

From the main menu, choose Switch Configuration (or press w) to open the Switch Configuration Menu screen (Table 36 on page 140).

Figure 38 Switch Configuration Menu screen

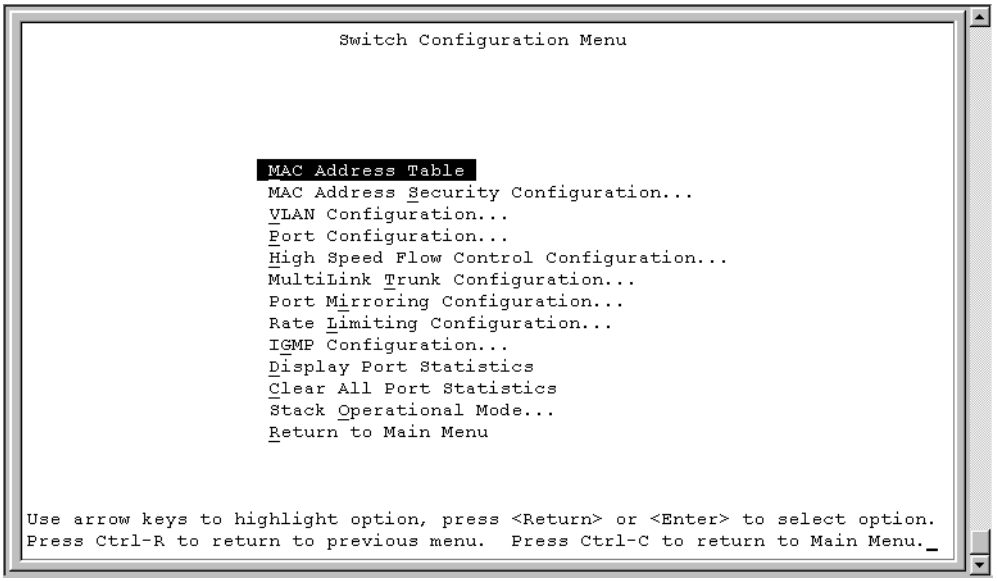


Table 36 describes the Switch Configuration Menu screen options.

Table 36 Switch Configuration Menu screen options

Option	Description
MAC Address Table	Displays the MAC Address Table screen (see *Configuring and Managing Security* (217104-A)). This screen allows you to view all MAC addresses and the associated ports or trunks that the switch has learned, or to search for a particular MAC address (to see if the switch has learned the address).
MAC Address Security Configuration...	Displays the MAC Address Security Configuration menu (see *Configuring and Managing Security* (217104-A)). This screen allows you to set up the MAC address security feature and provides the following options: MAC Address Security Configuration, MAC Address Security Port Configuration, MAC Address Security Port Lists, and MAC Address Security Table. This menu allows you to enable and disable security features on the port and trunk levels.
EAPOL Security Configuration...	Displays the EAPOL Security Configuration menu (see *Configuring and Managing Security* (217104-A)). This screen allows you to set up Extensible Authentication Protocol over LAN (EAPOL)-based security.

Table 36 Switch Configuration Menu screen options (Continued)

Option	Description
VLAN Configuration...	Displays the VLAN Configuration Menu (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)). This menu allows you to create and modify VLANs and enable the automatic PVID feature. It provides the following options: VLAN Configuration, MAC Addresses for MAC-SA Based VLAN, VLAN Port Configuration, and VLAN Display by Port.
Port Configuration...	Displays the Port Configuration screen (see "Port Configuration screen" on page 142). This screen allows you to configure a specific port or ports.
High Speed Flow Control Configuration...	Selectable only when an optional GBIC is installed in the Uplink Module slot. When the GBIC is installed, selecting this option displays the High Speed Flow Control Configuration screen (see "High Speed Flow Control Configuration screen" on page 144)
MultiLink Trunk Configuration...	Displays the MultiLink Trunk Configuration Menu (for details, see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)). This menu allows you to create and modify trunks, and to monitor the bandwidth utilization of configured trunks. It provides the following options: MultiLink Trunk Configuration and MultiLink Trunk Utilization.
Port Mirroring Configuration...	Displays the Port Mirroring Configuration screen (see *System Monitoring Guide* (217107-A)). This screen allows you to designate a single switch port as a traffic monitor for up to two specified ports or addresses.
Rate Limiting Configuration...	Displays the Rate Limiting Configuration screen (see "Rate Limiting Configuration screen" on page 147). This screen allows you to limit the forwarding rate of broadcast and multicast packets.
IGMP Configuration...	Displays the IGMP Configuration screen (see *Configuring IP Multicast Routing Protocols* (217459-A)). This screen allows you to optimize multicast traffic by setting up IGMP port memberships that filter multicast on a per port basis.
Display Port Statistics	Displays the Port Statistics screen (see *System Monitoring Guide* (217107-A)). This screen allows you to view detailed information about any switch port.

Table 36 Switch Configuration Menu screen options (Continued)

Option	Description
Clear All Port Statistics	Allows you to clear all port statistics. This option is followed by screen prompts that present a choice of actions. Choose one of the following: • Yes, to clear all port statistics for all switch ports • No, to abort the option
Stack Operational Mode	Displays the stack operational mode screen, which provides information about the types of switches in your stack. See "Stacking" on page 293 for details. • The Pure Stack Mode is the only possible operational mode. The Hybrid Stack Mode is not supported in this release.

Port Configuration screen

The Port Configuration screen (Figure 39 on page 143) allows you to configure specific switch ports or all switch ports. You can enable or disable the port status of specified switch ports, set the switch ports to autonegotiate for the highest available speed of the connected station, or set the speed for selected switch ports (autonegotiation is not supported on fiber optic ports).

You can disable switch ports that are trunk members; however, the screen prompts for verification of the request before completing the action. Choosing [Yes] disables the port and removes it from the trunk.

Note: The Autonegotiation fields, the Speed fields, and the Duplex fields are independent of MultiLink Trunking, rate limiting, VLANs, IGMP Snooping, and the STP.

To open the Port Configuration screen:

➨ Choose Port Configuration (or press p) from the Switch Configuration Menu screen.

Figure 39 Port Configuration screen

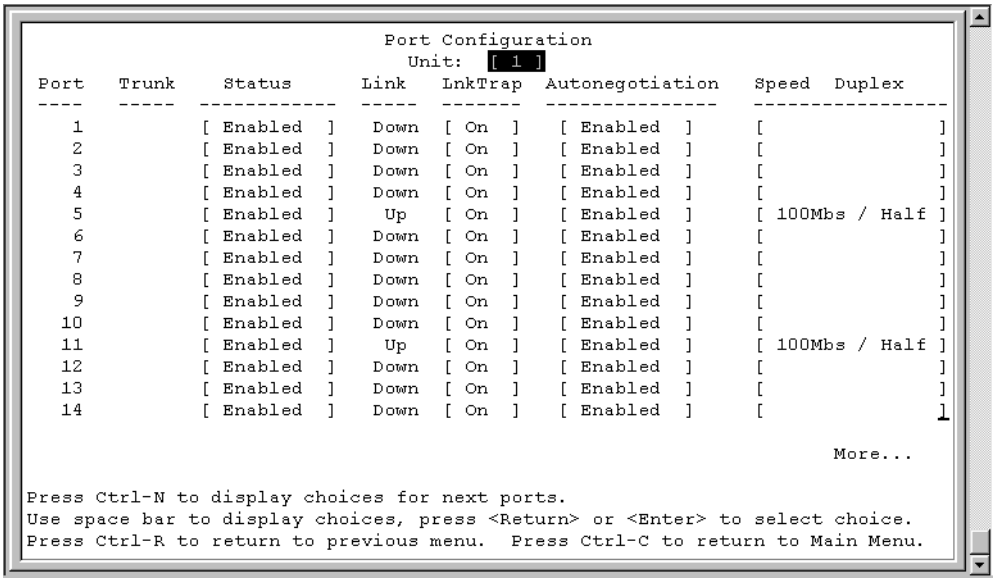


Table 37 describes the Port Configuration screen fields.

Table 37 Port Configuration screen fields

Field	Description
Port	Indicates the switch port numbers that correspond to the field values in that row of the screen (for example, the field values in row 2 apply to switch port 2). The values that you set in the *Switch* row will affect all switch ports.
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)).
Status	Allows you to disable any of the switch ports. You can also use this field to control access to any switch port. Default Value Enabled Range Enabled, Disabled
Link	A read-only field that indicates the current link state of the corresponding port, as follows: • Up: The port is connected and operational. • Down: The port is not connected or is not operational.

Table 37 Port Configuration screen fields (Continued)

Field	Description
LnkTrap	Allows you to control whether link up/link down traps are sent to the configured trap sink from the switch. Default Value On Range On, Off
Autonegotiation	When enabled, sets the corresponding port speed to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode. **NOTE**: This field is disabled for GBIC ports. Default Value Enabled Range Enabled, Disabled
Speed/Duplex*	Allows you to manually configure any port to support an Ethernet speed of 10 Mb/s or 100 Mb/s, in half- or full-duplex mode. This field is set (by default) to 100 Mb/s, full-duplex for gigabit ports only. **NOTE**: Use the High Speed Flow Control Configuration screen (next) to set autonegotiation for all gigabit ports. Default Value 100Mbs/Half (when Autonegotiation is Disabled) Range 10Mbs/Half, 10Mbs/Full, 100Mbs/Half, 100Mbs/Full

* Fiber optic ports can only be set to 100 Mb/s/Half or 100 Mb/s Full.

High Speed Flow Control Configuration screen

The High Speed Flow Control Configuration screen (Figure 40 on page 145) allows you to set the port parameters for installed GBIC ports. Use this screen to set autonegotiation for all gigabit ports.

➨ Choose High Speed Flow Control Configuration (or press h) from the Switch Configuration Menu screen to open the High Speed Flow Control Configuration screen.

Figure 40 High Speed Flow Control Configuration

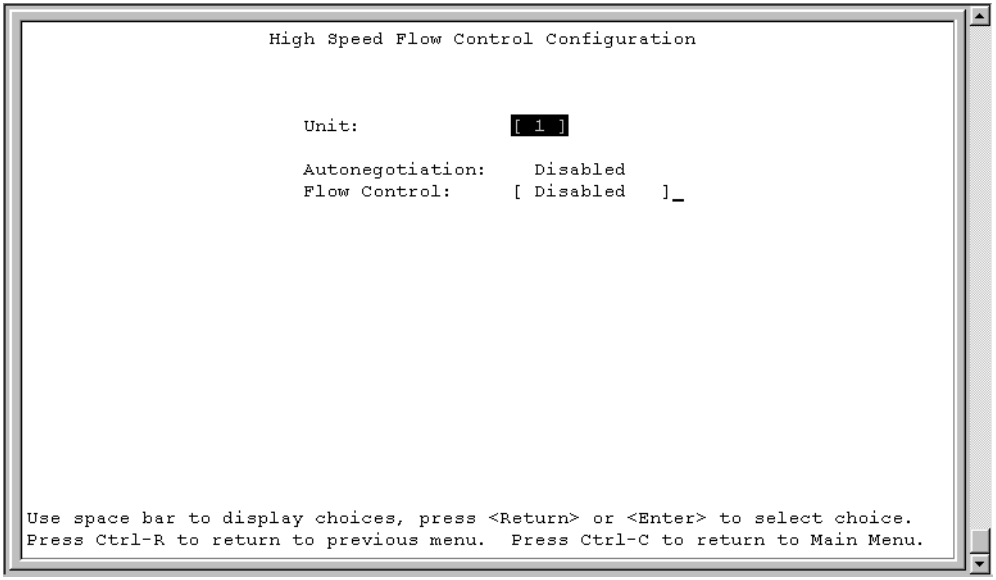


Table 38 describes the High Speed Flow Control Configuration screen fields.

Table 38 High Speed Flow Control Configuration Screen Fields

Field	Description
Unit	Allows you to select the unit number (when stacking is configured) to view or configure. To view or configure another unit, type its unit number and press [Enter], or press the space bar to toggle the unit numbers (the system only displays a screen for units configured with a Gigabit MDA).
Autonegotiation	When enabled, the port only advertises support for 100 Mb/s operation, in full-duplex mode. **NOTE:** This field is disabled for all GBIC ports. Default Value Disabled Range Not applicable

Table 38 High Speed Flow Control Configuration Screen Fields (Continued)

Field	Description
Flow Control	Allows you to control traffic and avoid congestion on the GBIC port. Two modes are available (see "Choosing a high speed flow control mode" on page 146 for details about the two modes). The Flow Control field cannot be configured unless you set the Autonegotiation field value to Disabled. Default Value Disabled Range Disabled, Symmetric, Asymmetric
Preferred Phy	Allows you to choose a preferred Phy port; the other Phy port reverts to backup. Default Value Right Range Right, Left
Active Phy	Indicates the operational Phy port. Default Value: None Range: None, Right, Left

Choosing a high speed flow control mode

The High Speed Flow Control feature allows you to control traffic and avoid congestion on the Gigabit full-duplex link. If the receive port buffer becomes full, the switch issues a flow-control signal to the device at the other end of the link to suspend transmission. When the receive buffer is no longer full, the switch issues a signal to resume the transmission. You can choose Symmetric or Asymmetric flow control mode.

Symmetric mode

This mode allows both the GBIC port and its link partner to send flow control pause frames to each other.

When a pause frame is received (by either the GBIC port or its link partner), the port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frame is received. Both devices on the link must support this mode when it is selected.

Asymmetric mode

This mode allows the link partner to send flow control pause frames to the GBIC port. When a pause frame is received, the receiving port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frame is received.

In this mode, the GBIC port is disabled from transmitting pause frames to its link partner. Use this mode when the GBIC port is connected to a buffered repeater device.

Rate Limiting Configuration screen

The Rate Limiting Configuration screen allows you to limit the forwarding rate of broadcast and multicast packets.

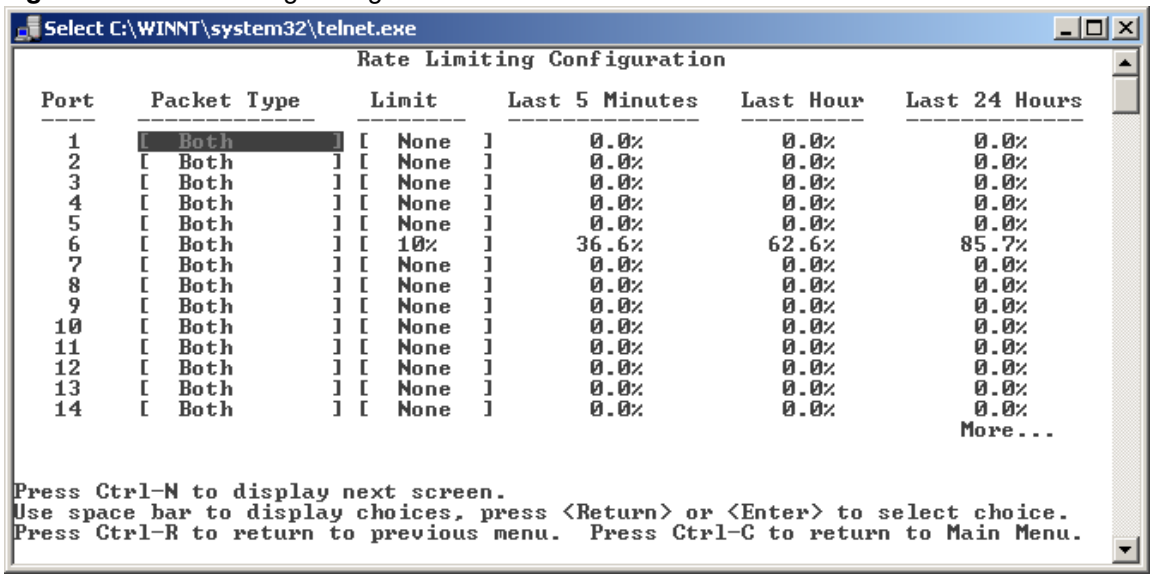
Figure 41 shows a sample Rate Limiting Configuration screen.

Note: If a port is configured for rate limiting, and it is a MultiLink Trunk member, all trunk member ports implement rate limiting. Also, if a trunk member implements rate limiting and the port is disabled from rate limiting, all trunk members are disabled from rate limiting.

To open the Rate Limiting Configuration screen:

- Choose Rate Limiting Configuration (or press l) from the Switch Configuration Menu screen.

Figure 41 Rate Limiting Configuration screen



You can use this screen to view the percentage of either packet type (or both packet types) received on each port.

When the volume of either packet type is high, placing severe strain on the network (often referred to as a *storm*), you can set the forwarding rate of those packet types to *not exceed* a specified percentage of the total available bandwidth. The percentage you set refers to the total available bandwidth, not to a percentage of current traffic. Table 39 on page 149 describes the Rate Limiting Configuration screen fields.

Table 39 Rate Limiting Configuration screen fields

Field	Description
Port	Indicates the switch port numbers that correspond to the field values in that row of the screen (for example, the field values in row 2 apply to switch port 2). Note that the values applied in the Switch affect all switch ports.
Packet Type	Allows you to select the packet types for rate-limiting or viewing. Default Value Both Range Both, Multicast, Broadcast
Limit	Sets the percentage of port bandwidth allowed for forwarding the packet types specified in the Packet Type field. When the threshold is exceeded, any additional packets (specified in the Packet Type field) are discarded*. Default Value None Range None, 10%, 9%, 8%, 7%, 6%, 5%, 4%, 3%, 2%, 1%
Last 5 Minutes	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) received by the port in the last 5 minutes. This field provides a running average of network activity and is updated every 15 seconds. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.
Last Hour	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) received by the port in the last hour. This field provides a running average of network activity and is updated every 5 minutes. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.
Last 24 Hours	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) received by the port in the last 24 hours. This field provides a running average of network activity and is updated every hour. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.

* Rate-limiting is disabled if this field is set to None. This allows you to select and view the percentage of specific packet types present in the network, without inadvertently limiting the forwarding rate.

System Log screen

The System Log screen (Figure 42 on page 150) displays or clears messages obtained from system non-volatile memory or dynamic memory.

System Log messages operate as follows:

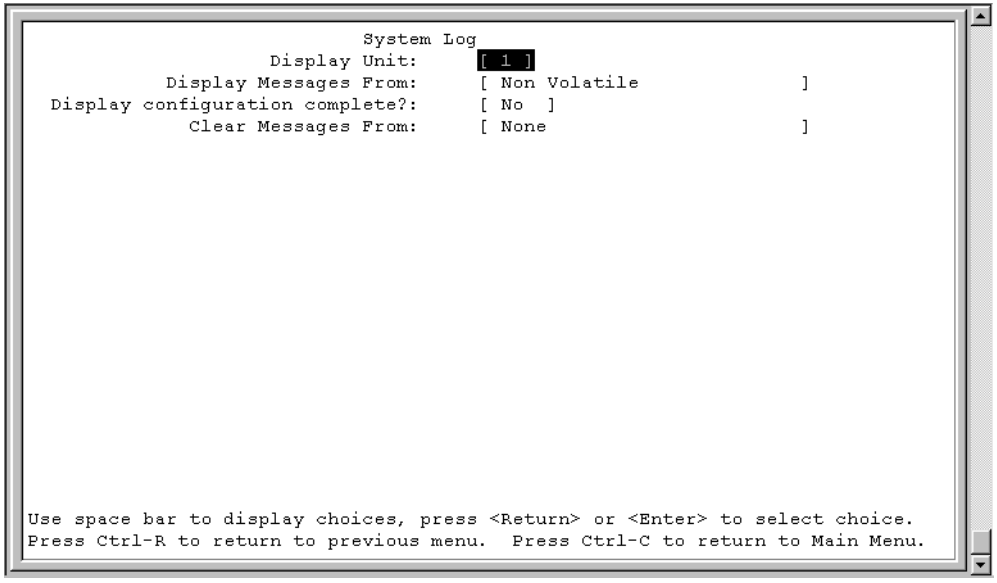
- Non-volatile memory messages are retrievable after a system reset.

- Messages can be viewed while the system is operational.
- All non-volatile and dynamic memory messages are timestamped.
- When you restart your system, the system deletes dynamic memory messages.
- After a reset, the system copies all messages stored in non-volatile memory to dynamic memory. The messages copied to dynamic memory are timestamped to zero (0).

To open the System Log screen:

- Choose Display System Log (or press y) from the main menu.

Figure 42 System Log screen



Displaying most recent log entry first

This option allows you to view the system log with the most recent entry displayed first; the rest of the log entries are listed in reverse chronological order.

Table 40 describes the System Log screen fields.

Table 40 System Log screen fields

Field	Description
Display Messages From	This field allows you to select the memory source your messages are obtained from. Choose Non Volatile, Volatile, or Volatile + Non Volatile. Use the spacebar to toggle between the options. Default Non Volatile RangeNon Volatile, Volatile + Non Volatile
Display configuration complete?	This field allows you to determine whether the configuration information received from non-volatile or dynamic memory (depending on what is selected in the Display Messages From field) is complete. Use the spacebar to toggle between the options. DefaultNo RangeNo, Yes
Clear Messages From	This field allows you to clear the information messages from dynamic or non-volatile memory or both. If you clear dynamic messages, existing non-volatile messages are copied into dynamic memory. After a system reset, all existing non-volatile messages are copied to dynamic memory. Use the spacebar to toggle between the options. DefaultNone RangeNone, Non Volatile, Volatile + Non Volatile

Troubleshooting

Do the following if you have problems navigating in or displaying the Console Interface menu system:

- Ensure that your terminal emulation software configuration is consistent with the guidelines presented earlier in this chapter.

Usage guidelines

- In the Console Interface, configure the terminal for 24 rows by 80 columns.

Chapter 3
CLI Basics

The Command Line Interface (CLI) is a management tool that provides methods for configuring, managing, and monitoring the operational functions of the Ethernet Switches 460 and 470. You access the CLI through a direct connection to the switch console port, or remotely using Telnet. For a complete, alphabetical list of CLI commands, refer to Appendix B, "CLI Command List," on page 525.

Note: When you power up or reset the switch, it runs a self-test, then displays the Nortel logo banner on the Console Interface. Press [Ctrl]-Y to access the Ethernet Switch 460 or 470 main menu.

This chapter discusses the following CLI topics:

Accessing the CLI

You access the CI menus using Telnet or a direct connection to the switch from a terminal or personal computer (PC). You can use any terminal or PC with a terminal emulator as the CLI command station. Be sure the terminal has the following features:

- 9600 bits per second (b/s), 8 data bits, 1 stop bit, no parity, no flow control
- Serial terminal-emulation program such as Terminal or Hyperterm for Windows NT* or Hyperterm for Windows* 95 or Windows 98
- Cable and connector to match the male DTE connector (DB-9) on the switch console port, with the DCE/DTE switch on the switch management module set to DTE
- Under Terminal Options, VT100 Arrows checked in the Terminal Preferences window, and Block Cursor unchecked; under Emulation, VT-100/ANSI checked

To access the CLI:

1 When you access the switch, the Nortel banner appears (Figure 43).

Figure 43 Ethernet Switch banner

```
 ###      ###  ############   ##########  ############# ########### ###
 ####     ### ############# ############ ############# ########### ###
 #####    ### ###        ### ###       ###       ###       ###          ###
 ######   ### ###        ### ###       ###       ###       ###          ###
 ### ###  ### ###        ### ############       ###       #########    ###
 ###  ### ### ###        ### ###########        ###       #########    ###
 ###   ###### ###        ### ###   ###          ###       ###          ###
 ###    ##### ###        ### ###    ###         ###       ###          ###
 ###     #### ############# ###     ###       ###      ########### ###########
 ###      ###  ###########  ###      ###      ###      ########### ###########

*******************************************************
*Ethernet Switch 470-48T
*Nortel
*Copyright (c) 1996-2005,  All Rights Reserved
*BOSS 3.6
*HW:#01      FW:3.0.0.5   SW:v3.6.0  ISVN: 2
*************************************************************
Enter Ctrl-Y to begin.
```

2 Press [Ctrl]+Y, and the Main Menu appears on the console screen (Figure 44) with the top line highlighted.

Figure 44 Main Menu for Switch Console Interface

```
                        Ethernet Switch 470-24T Main Menu

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

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

3 Using the Down Arrow key, scroll down to Command Line Interface, and press [Enter]. The CLI cursor appears as one of the following depending on your switch product number:

```
460-24T-PWR>
470-24T>
470-48T>
```

The > sign at the end of the name of the switch indicates that the CLI opens in User EXEC mode. Refer to "CLI command modes" on page 156 to select the command mode you want to use (and are authorized to use).

CLI command modes

Most CLI commands are available only under a certain command mode. The switch has the following four command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration

The User EXEC mode is the default mode; it is also referred to as exec. This command mode is the initial mode of access upon first powering-up the switch. In this command mode, the user can access only a subset of the CLI commands; however, the commands in this mode are available while the user is in any of the other four modes. The commands in this mode provide basic functionality, such as ping and logout.

Commands in the Privileged EXEC mode are available to all other modes except the User EXEC mode. The commands in this mode allow you to perform basic switch-level management tasks, such as downloading the software image, setting passwords, and booting the switch. The Privileged EXEC mode is also referred to as privExec mode.

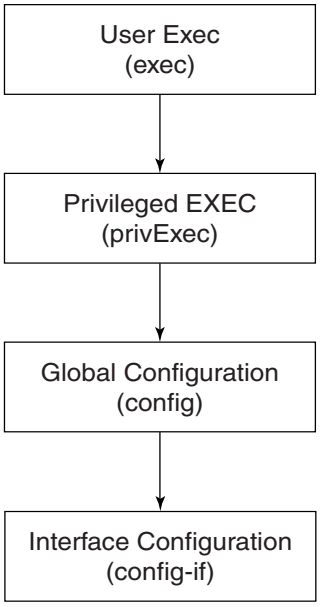
The last two command modes allow you to change the configuration of the switch. Changes made in these command modes are immediately applied to the switch configuration and saved to non-volatile memory (NVRAM).

The Global Configuration commands allow you to set and display general configurations for the switch, such as the IP address, SNMP parameters, Telnet access, and VLANs. The Global Configuration mode is also referred to as config mode.

The Interface Configuration commands allow you to configure parameters for each port, such as speed, duplex mode, and rate limiting. The Interface Configuration mode is also referred to as config-if mode.

Figure 45 on page 157 provides an illustration of the hierarchy of CLI command modes.

Figure 45 CLI command mode hierarchy



You can see a specific value for each command mode at the prompt line, and you can use specific commands to enter or exit each command mode (Table 41). Additionally, you can only enter command modes from specific modes and only exit to specific command modes.

Table 41 Command mode prompts and entrance/exit commands

Command mode	Prompt	Enter/exit command

User EXEC (exec)	`460-24T-PWR>`
	`470-24T>`
	`470-48T>`
		• Default mode, automatically enter
		• `logout` or `exit` to quit CLI

Privileged EXEC (privExec)	`460-24T-PWR#`
	`470-24T#`
	`470-48T#`
		• `enable` to enter from User EXEC mode
		• `logout` or `exit` to quit CLI

Table 41 Command mode prompts and entrance/exit commands (Continued)

Command mode	Prompt	Enter/exit command

Global Configuration (config)	`460-24T-PWR(config)#`
	`470-24T(config)#`
	`470-48T(config)#`
		• `configure` to enter from Privileged EXEC mode
		• `logout` to quit CLI;
		`end` or `exit` to exit to Privileged EXEC mode

Interface Configuration (config-if)	`460-24T-PWR(config-if)#`
	`470-24T(config-if)#`
	`470-48T(config-if)#`
		• `interface FastEthernet {<portnum>|all}` to enter from Global Configuration mode
		• `logout` to quit CLI;
		`end` to exit to Privileged EXEC mode;
		`exit` to exit to Global Configuration mode

The prompt displays the switch name, `460-24T-PWR, 470-24T, or 470-48T` and the current CLI command mode.

See Appendix B, "CLI Command List," on page 525 for a complete, alphabetical list of all CLI commands.

The initial command mode in CLI depends on your access level when you log in to the switch CI menus:

- With no password protection, you enter the CLI in userExec mode, and use the `enable` command to move to the privExec command mode.
- If you log in to the CI menus with read-only access, you enter the CLI in userExec mode and cannot access any other CLI command modes.
- If you log in to the CI menus with read-write access, you enter the CLI in privExec mode and can use the appropriate commands to move to the other command modes.

Basic navigation

This section discusses basic navigation within the CLI and between the command modes. The CLI incorporates various shortcut commands and keystrokes to simplify its use. The following topics are covered in this section:

General navigation commands

When you navigate through the CLI, online help is available at all levels. Entering a portion of the command at the prompt, followed by a space and a question mark (`?`), results in a list of all options for that command. Refer to "help command" on page 161 for more information about the specific types of online help.

The system records the last command in a CLI session. However, the last command is not saved across reboots.

Add the word `no` to the beginning of most CLI configuration commands to clear or remove the parameters of the actual command. For example, when you enter the command `ip stack address 192.32.154.126`, you set the IP stack address. However, when you enter `no ip stack address`, the system returns the IP address to zero. See Appendix B, "CLI Command List," on page 525 for an alphabetical list of `no` commands.

Add the word `default` to the beginning of most CLI configuration commands returns the parameters of the actual command to the factory default values. Refer to Appendix B, "CLI Command List," on page 525 for an alphabetical list of `default` commands.

When you enter a portion of the command and press the [Tab] key, the system finds the first unambiguous match of a command and displays that command. For example, if you enter `down`+[Tab], the system displays `download`.

Keystroke navigation

You can change the location of the cursor using the key combinations shown in Table 42.

Table 42 Keystroke navigation

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)
[Ctrl]+I &	Command/parameter completion
[Ctrl]+K & [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 left of cursor
[Ctrl]+X	Delete all characters to left of cursor
[Ctrl]+z	Exit Global Configuration mode (to Privileged EXEC mode)
?	Context-sensitive help
[Esc]+c & [Esc]+u	Capitalize character at cursor

Table 42 Keystroke navigation

Key combination	Function
[Esc]+l	Change character at cursor to lowercase
[Esc]+b	Move back 1 word
[Esc]+d	Delete 1 word to the right
[Esc]+f	Move 1 word forward

help command

The `help` command is in all command modes and displays a brief message about using the CLI help system. The syntax for the `help` command is:

```
help
```

The `help` command has no parameters or variables.

Figure 46 on page 162 shows the output from the `help` command.

Figure 46 `help` command output in privExec mode

```
470-24T#help
Context help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will be empty
and you must backup until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

Keystroke navigation:
    [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)
    [Ctrl]+I & Command/parameter completion
    [Ctrl]+K & [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 left of cursor
    [Ctrl]+X Delete all characters to left of cursor
    [Ctrl]+z Exit Global Configuration mode (to Privileged EXEC mode)
    [Esc]+c & [Esc]+u Capitalize character at cursor
    [Esc]+l Change character at cursor to lowercase
    [Esc]+b Move back 1 word
    [Esc]+d Delete 1 word to the right
    [Esc]+f Move 1 word forward
```

help commands mode command

The `help commands mode` command displays the list of commands available on the device, either for the current mode of operation or as a complete list of all the commands available on the device.

The `help commands mode` command is in all command modes. The syntax for the `help commands mode` command is:

```
help commands [mode {current | exec | privExec | config |
ifconfig}]
```

Table 44 describes the parameters and variables for the `help commands mode` command.

Table 43 `help commands mode` command parameters and variables

Parameters and variables	Description
`{current| exec | privExec | config | ifconfig}`	Specifies the command mode: • current: mode from which the command was entered • exec: User Executive mode • privExec: Privileged Executive mode • config: Global Configuration mode • ifconfig: Interface Configuration mode Note: When you enter the command with no additional parameters, the device displays the list of all commands available on the switch.

Figure 47 on page 164 shows the sample output for the `help commands mode exec` command.

Figure 47 `help commands mode exec` command output

```
-------------------------------------------
User Executive commands
-------------------------------------------
Command    Description
-------------------------------------------
enable     Turn on privileged commands
exit       Exit from the EXEC and end the current session
help       Description of the interactive help system
logout     Exit from the EXEC
ping       Send echo messages
show       Show running system information
telnet     Telnet to another host
terminal   Set terminal line parameters
-------------------------------------------
```

help modes command

The `help modes` command displays information regarding available CLI modes on the switch.

The syntax for the `help modes` command is:

```
help modes
```

The `help modes` command has no parameters or variables.

The `help modes` command is in all command modes.

Figure 48 shows the output from the `help modes` command.

Figure 48 `help modes` command output

```
    Mode                    Short Name      Comments
-----------------------   ----------- ----------------------
User Executive              exec          Default mode
Privileged Executive        privExec      Enter using "enable"
Global Configuration        config        Enter using "configure"
Interface Configuration     ifconfig      Enter using "interface"
```

no command

The `no` command is always used as a prefix to a configuration command, and it negates the action performed by that command. The effect of the `no` command is to remove or to clear the configuration controlled by the specified command. Various `no` commands are in the config and config-if command modes.

Refer to Appendix B, "CLI Command List," on page 525 for an alphabetical listing of all `no` commands.

Note: Not all configuration commands support the `no` prefix command.

default command

The `default` command is always used as a prefix to a configuration command, and it restores the configuration parameters to default values.

Refer to Appendix B, "CLI Command List," on page 525 for an alphabetical listing of all `default` commands.

Note: Not all commands support the `default` prefix command.

logout command

The `logout` command logs you out of the CLI session and returns you to the Main Menu of the Console Interface (CI) menus (Figure 44 on page 155). The syntax for the `logout` command is:

```
logout
```

The `logout` command is in all command modes.

The `logout` command has no parameters or variables.

enable command

The `enable` command changes the command mode from User EXEC to privExec mode. The syntax for the `enable` command is:

```
enable
```

The `enable` command is in the exec command mode.

The `enable` command has no parameters or variables.

Note: You must have read-write access to the switch to use the `enable` command.

configure command

The `configure` command moves you from the privExec command mode to the Global Configuration (config) command mode and identifies the source for the configuration commands. The syntax for the `configure` command is:

```
configure {terminal|network}
```

The `configure` command is in the privExec command mode.

Table 44 describes the parameters and variables for the `configure` command.

Table 44 `configure` command parameters and variables

Parameters and variables	Description
`terminal|network`	Specifies the source for the configuration commands for the switch: • `terminal`—allows you to enter config mode to enter configuration commands • `network`—allows you to set up parameters for auto-loading a script at boot-up or for loading and executing a script immediately

interface command

The `interface` command moves you from the config command mode to the Interface Configuration (config-if) command mode. The syntax for the `interface` command is:

```
interface FastEthernet {<portlist>}
```

The `interface` command is in the config command mode.

Table 45 describes the parameters and variables for the `interface` command.

Table 45 interface command parameters and variables

Parameters and variables	Description
<portlist>	Specifies the portlist you want to be affected by all the commands issued in the config-if command mode.

disable command

The `disable` command returns you to the User EXEC (exec) command mode from the privExec command mode. The syntax for the `disable` command is:

```
disable
```

The `disable` command is in the privExec command mode.

The `disable` command has no parameters or variables.

end command

The `end` command moves you to the priv Exec mode from either the Global Configuration (config) mode or the Interface Configuration (config-if) mode.

The syntax for the `end` command is:

```
end
```

The `end` command has no parameters or variables.

exit command

The `exit` command moves you around the command modes:

- In User EXEC (exec) and Privileged EXEC (privExec) command modes, `exit` allows you to quit the CLI session.
- In Global Configuration (config) mode, `exit` moves you back to the privExec command mode.
- In Interface Configuration (config-if) command mode, `exit` moves you back to the config mode.

The syntax for the `exit` command is:

```
exit
```

The `exit` command has no parameters or variables.

shutdown command

The `shutdown` command allows you to safely shut down and power off the switch. Once the `shutdown` command is initiated, the switch saves the current configuration and instructs users to power off the switch within the specified time period (one to ten minutes); otherwise, the switch is reset.

When the `shutdown` command is initiated in the CLI, the following message appears:

```
It is now safe to poweroff the switch/stack. Autoreset in
<60-600> seconds. Any configuration changes from now until
reset will be lost.
```

The syntax for `shutdown` command is:

```
shutdown minutes-to-wait <1-10>
```

where *<1-10>* specifies the number of minutes that pass before the switch resets itself. The default wait time is set at two minutes.

Note: Any configurations or logins performed on the switch after the `shutdown` command is initiated are not saved into NVRAM and are lost after the reset.

Note: When the `shutdown` command is entered, warning messages appear to all users connected to the switch through the Console Interface. In the CLI, the warning message appears only to the person initiating the `shutdown` command. In the Device Manager and Web-based management interfaces, no warning message appears.

The `shutdown` command is in the privExec command mode.

Numbering ports

The Ethernet Switch 470-24T can operate either in stand-alone mode or in stack mode. The Ethernet Switch 470-24T has 24 10/100 Mb/s ports on the front. Thus, you have a maximum of 26 ports on one Ethernet Switch 470-24T.

The Ethernet Switch 470-48T can operate either in stand-alone mode or in stack mode. The Ethernet Switch 470-48T has 48 10/100 Mb/s ports on the front. Thus, you have a maximum of 48 ports on one Ethernet Switch 470-48T.

The Ethernet Switch 460-24T-PWR can operate either in stand-alone mode or in stack mode. The Ethernet Switch 460-24T-PWR has 24 10/100 Mb/s ports on the front, as well as an uplink slot that allows you to attach a media dependent adapter (MDA). The MDAs available for the uplink can have up to four ports. Thus, you have a maximum of 28 ports on one Ethernet Switch 460-24T-PWR.

Note: The MDAs do not supply power to PoE (Power Over Ethernet) devices. Only unit ports 1 to 24 can supply power to PoE devices.

The CLI uses the variable <*portlist*> when a command specifies one or more ports for the command. The format of the variable <*portlist*> is different if you are working with a stand-alone switch or with a stack.

Note: The variable *portlist* replaces the use of variables *portnum*, *port-num,* and `all` for ports.

Numbering port in stand-alone mode

In stand-alone mode, use the <*portlist*> variable in the following formats:

- A single port number—an integer between 1 through 26
  - Example: `7` means port 7
- A range of port numbers—a pair of port numbers between 1 and 26 separated by a dash
  - Example: `1-3` means ports 1, 2, and 3
  - Example: `5-24` means all ports from port 5 through port 24
- A list of port numbers and/or port ranges, separated by commas
  - Example: `1,3,7` means ports 1, 3, and 7
  - Example: `1-3,9-11` means ports 1, 2, 3, 9, 10, and 11
  - Example: `1,3-5,9-11,15` means ports 1, 3, 4, 5, 9, 10, 11, and 15
- `none` means no ports (not case-sensitive)
- `all` means all the ports on the stand-alone switch, including any MDA ports (not case-sensitive)

You can also use the unit/port convention discussed in "Numbering port in stacked mode" on page 171 with a stand-alone Ethernet Switch 460-24T-PWR as long as the unit number is always 1.

Numbering port in stacked mode

In stacked mode, the value of the `<portlist>` variable must include the number of the unit within the stack, followed by a forward slash (/) and the desired port numbers. The unit numbers are always integers between 1 and 8, and the port numbers are always integers between 1 and 26. You can also use `none`, to indicate none of the ports in the stack, or `all`, to indicate all of the ports in the stack.

In stacked mode, use the `<portlist>` variable in the following formats:

- A single port number—an integer for the unit, followed by /, and an integer for the port number
  - — Example: `1/7` means unit 1 port 7
  - — Example: `3/24` means unit 3, port 24
- A range of port numbers—an integer for the unit, followed by /, and integers for the port number between 1 and 26 separated by a dash
  - — Example: `1/1-3` means unit 1, ports 1, 2, and 3
  - — Example: `3/5-26` means unit 3, port 5 through port 26
- A unit with no ports specified—an integer for the unit, followed by /, and the word `none` (not case-sensitive)
  - — `3/none` means unit 3 with no ports
- A unit with all ports specified—an integer for the unit, followed by /, and the word `all` (not case-sensitive)
  - — `3/all` means unit 3 with all ports
- A list of port numbers, port ranges, and/or units with all ports or no ports—using the unit/port format—separated by commas
  - — Example: `1/1,2/3,3/7` means unit 1 port 1; unit 2, port 3; and unit 3, port 7
  - — Example: `1/1-3,3/9-11` means unit 1, ports 1, 2, 3; and unit 3, ports 9, 10, and 11
  - — Example: `1/1,4/3-5,5/9-11,7/15` means unit 1, port 1; unit 4, ports 3, 4, 5; unit 5, ports 9, 10, 11; and unit 7, port 15

— Example: `1/3,3/ALL,4/NONE` means unit 1, port 3; unit 3, all ports; and unit 4, no ports

- `none` means no ports in the stack (not case-sensitive)
- `all` means all the ports in the stack, including all MDA ports (not case-sensitive)

To view the unit numbers in the stack, enter the `show stack-info` command (see "show stack-info command" on page 360). You must be in the Privileged EXEC (privExec) mode to enter this command.

Refer to "Stacking" on page 294 for more information on numbering units within the stack.

How to comment and run scripts

You can use the CLI interactively, or you can load and execute CLI "scripts." CLI scripts are loaded in one of the following ways:

- By entering the `configure network` command.
- By manually loading the script in the console menu.
- By automatically loading the script at boot-up

Managing basic system information

This section shows you how to view basic system information, such as the current software version and the stack mode; you can renumber the units within a stack. The following topics are covered:

- "show sys-info command" on page 173
- "show stack-info command" on page 175

Refer to "Stacking" on page 294 for more information on the operation of the stack mode, including unit numbering.

show sys-info command

The `show sys-info` command displays the current system characteristics, which includes Hardware rev, FW rev, date of manufacture (DOM), and Hardware deviation number. The syntax for the `show sys-info` command is:

```
show sys-info
```

The `show sys-info` command is in the privExec command mode.

The `show sys-info` command has no parameters or variables.

Figure 49 on page 174 and Figure 50 on page 175 displays sample output from the `show sys-info` command.

Figure 49 `show sys-info` command output

```
460_24T_PWR#show sys-info
Operation Mode:         Switch
MAC Address:            00-09-97-29-1F-00
Reset Count:            1
Last Reset Type:        Software Download
Power Status:           Primary Power
Autotopology:           Enabled
Current Switch Mode:    L2
Next Boot Switch Mode:  L2
Local MDA Type:         None
PoE Module FW:          7013.2
sysDescr:               Ethernet Switch 460 - 24T - PWR
                        HW:00       FW:3.0.0.5   SW:v3.6.0 ISVN:1
                        Mfg Date:20021102    HW Dev:
Serial #:               SDNIHR007B
sysObjectID:            1.3.6.1.4.1.45.3.49.1
sysUpTime:              12 days, 07:04:49
sysNtpTime:             SNTP not synchronized.
sysServices:            3
sysContact:
sysName:
sysLocation:
```

Figure 50 `show sys-info` command output

```
470_48T#show sys-info
Operation Mode:         Switch
MAC Address:            00-04-38-D5-9F-C0
Reset Count:            1
Last Reset Type:        Software Download
Power Status:           Primary Power
Autotopology:           Enabled
Current Switch Mode:    L2
Next Boot Switch Mode: L2
GBIC Port 47:           None
GBIC Port 48:           None
sysDescr:               Ethernet Switch 470 - 48T
                      HW:#0D     FW:3.0.0.5   SW:v3.6.0.00 ISVN:2
                        Mfg Date:20020717    HW Dev:
Serial #:               ACC1000CP
sysObjectID:            1.3.6.1.4.1.45.3.46.1
sysUpTime:              12 days, 08:43:00
sysNtpTime:             SNTP not synchronized.
sysServices:            3
sysContact:
sysName:
sysLocation:
470_48T#
```

To change the system contact, name, or location, refer to the `snmp-server` command.

show stack-info command

The `show stack-info` command displays the current stack information, which includes unit numbers, MDA and cascade attachments, and software version for all units. The syntax for the `show stack-info` command is:

```
show stack-info
```

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

The `show stack-info` command has no parameters or variables.

Figure 51 displays sample output from the `show stack-info` command.

Figure 51 `show stack-info` command output

```
460-24T-PWR#show stack-info
Unit #  Switch Model       MDA Model    Cascade MDA  SW Version
------  -----------------  -----------  -----------  ------------
1       460-24T-PWR        None         400-ST1      v3.6.0.00
2       460-24T-PWR        None         400-ST1      v3.6.0.00
```

show system verbose command

The `show system verbose` command displays additional system characteristics, including the status of switch fans, the power status, and the serial number of the switch.

The syntax for the `show system verbose` command is:

```
show system verbose
```

If verbose is omitted from the command, a short summary is displayed, similar to the `show sys-info` command.

The `show system verbose` is in the privExec command mode.

Figure 52 on page 177 shows a sample output of the `show system verbose` command.

Figure 52 `show system verbose` command output

```
470_48T (config) # show system verbose

System Information:
            Operation Mode:                 Stack
            Size of Stack:                  2
            Base Unit:                      1
            MAC Address:                    00-0E-40-5D-49-DF
            Reset Count:                    10
            Last Reset Type:                Power Cycle
            Autotopology:                   Enabled
            Current Switch Mode:            L2
            Next Boot Switch Mode:          L2
            sysObjectID:                    1.3.6.1.4.1.45.3.46.1
            sysUpTime:                      0 days, 00:03:50
            sysNtpTime:                     SNTP not synchronized
            sysServices:                    3
            sysContact:
            sysName:
            sysLocation:
Unit #1:    (Base Unit):
            Switch Model:                   Ethernet Switch 470-48T
            MDA Model:                      None
            GBIC Port 47:                   None
            GBIC Port 48:                   None
            Cascade Module:                 400-ST1
            Hardware Version:               #05
            Firmware Version:               3.0.0.5
            Software Version:               v3.6.0.0
            Serial Number:                  SSGDFL0M01
            Manufacturing Date:             20030907
            Power Status:                   Primary
            Fan #1 Status:                  Normal
            Fan #2 Status:                  Normal
            Fan #3 Status:                  Failure
Unit #2:
            Switch Model:                   Ethernet Switch 470-48T
            MDA Model:                      None
            GBIC Port 47:                   None
            GBIC Port 48:                   None
            Cascade Module:                 400-ST1
            Hardware Version:               #05
            Firmware Version:               3.0.0.5
            Software Version:               v3.6.0.0
            Serial Number:                  SSGDFL0M02
            Manufacturing Date:             20030907
            Power Status:                   Primary
            Fan #1 Status:                  Normal
            Fan #2 Status:                  Normal
            Fan #3 Status:                  Failure
```

show tech command

The `show tech` command displays detailed system and configuration information for technical support purposes.

The syntax for the `show tech` command is:

```
show tech
```

The `show tech` command is in the exec command mode.

show interfaces gbic-info command

The `show interfaces gbic-info` command displays hardware specifications for GBICs on the switch.

The syntax for this command is:

`show interfaces gbic-info <portlist>`

where *<portlist>* specifies the GBIC port or ports to display. Omitting this variable shows the details for all GBICs in the stack.

The `show interfaces gbic-info` command is in all command modes.

Figure 53 on page 179 shows a sample output for the `show interfaces gbic-info` command.

Figure 53 `show interfaces gbic-info` command output

```
UNIT #1
 Port  Number       47
 GBIC   Type        XXXXXXX
 Vendor Name        XXXX
 Vendor OUI         12345
 Vendor Part #      12345
 Vendor Revision    X.X
 Vendor Serial #    12345-12345
 HW Options         XXXXXXX
 Date Code          01012010
 Vendor Data        XXXXXXX
```

Chapter 4
Installing and using Device Manager software

Java Device Manager (JDM) is an SNMP-based graphical user interface (GUI) tool designed to manage single devices. To use JDM (also referred to in this manual as Device Manager), you must have network connectivity to a management station running JDM in one of the supported environments.

The JDM software is provided on the software CD as a self-extracting executable file, and is also available from the Nortel web site. This chapter provides instructions for installing the JDM software in a Windows*, UNIX*, or Linux* environment.

In Ethernet Switch Release 3.6 software, the Java Runtime Environment (JRE) is bundled with the JDM software and does not require a separate installation.

This chapter includes the following topics:

JDM installation precautions

The following warnings apply to Device Manager on all operating environments:

- If you have other Nortel switches in your network, and are running earlier versions of JDM software, you must install the newest version of JDM in order to access the switches running the latest software.

- Prior to upgrading JDM, either uninstall your previous version of the Device Manager software, or install the new software to a different directory. (You can have multiple versions of Device Manager stored on your PC or UNIX machine, provided that each version is stored in a separate directory.)

Note: Do not install the JDM to a directory where a previous version of Device Manager software already exists.

- The JDM and Ethernet Switch software versions must match for the correct dialog boxes and information to be shown and accessible. Please refer to the Release Notes for a complete compatibility list.
- JDM saves the IP addresses that are visited to a settings file. A JDM uninstall operation does not remove this settings file.
  - In a Windows environment, the settings file is *dm.ini*, and is created in the JDM install directory.
  - In a Unix environment, the settings file is *~/.jdm/dm.ini*.
  - In a Linux environment, the settings file is *~/.jdm/dm.ini*.
- The *dm.ini* file containing IP addresses visited from a previous JDM version is automatically used by a new JDM version installed in the same directory. You must manually move or copy the *dm.ini* file from a previous version of JDM to a new JDM installation in a different directory.

Installing JDM on Windows

This section includes the following topics:

Windows minimum requirements

The minimum system requirements for installing JDM on Microsoft* Windows NT*, Windows 95, Windows 98, Windows 2000, or Windows XP are:

- 350 MHz or higher Pentium processor
- 256 MB DRAM
- 300 MB space on hard drive

Removing previous versions of JDM on Windows

Note: Removing previous versions of JDM is an optional process. Multiple versions of JDM can exist on one system, as long as each version is in a separate location.

If you decide to allow previous versions of JDM to remain, then you must choose a different folder to use during the installation process.

Remove existing versions of Device Manager software by using the Uninstall DM option that was created in the Windows Start menu during installation.

For example, to remove Device Manager from a Windows XP system using the default program group, choose the following option from the Windows Start menu: All Programs>Nortel>Java Device Manager>Uninstall DM.

If no program group was added to the Windows Start menu during installation, then complete the following steps to remove existing Device Manager software:

1. Navigate to the folder where the JDM software is installed.
2. Open the UninstallerData sub-folder.
3. Run the following file: *Uninstall Java Device Manager.exe*.

Note: If more than one version of Device Manager software is installed, ensure you select the correct software to uninstall.

Installing JDM on Windows from the CD

To access the JDM software from the installation CD:

1. Close all programs.
2. Insert the software CD into your CD-ROM drive.
3. From the Windows Start menu, choose Run.

   The Run dialog box opens.
4. Use Browse to navigate to the drive where the CD-ROM is located.
5. On the CD-ROM drive, locate the \Windows\Device Manager subdirectory.
6. Double-click the *jdm_xxxx.exe* file.

Note: In the file name, *xxxx* represents the current version of the JDM software.

Continue with "Executing the JDM installation software on Windows" on page 185.

Installing JDM on Windows from the web

To obtain the JDM software from the Nortel web site:

1. Go to the following URL:

   http://www.nortel.com/support
2. Select the correct software support page for your product.

   From the Product Finder page:

   a. Select the product family from the first box.

   b. Select the specific product from the second box.

   c. Select Software.

   d. Click Go.

   The software page opens.

3 Click the Java Device Manager version you want.

The Software Detail Information page opens.

4 Click JDM for PC (95/98/NT/2000/XP).

A File Download dialog box opens that asks you to either run this program from its current location or to download the JDM software to your system.

5 Click Save.

A Save As dialog box opens.

6 Choose the directory to which you want to download the software. The software download is a self-extracting .exe file.

7 Click Save to begin the file transfer.

Once the file transfer is complete, continue with step 8.

8 Close all programs.

9 Navigate to the directory on your system where you downloaded the JDM Software.

10 Double-click the *jdm_xxxx.exe* file.

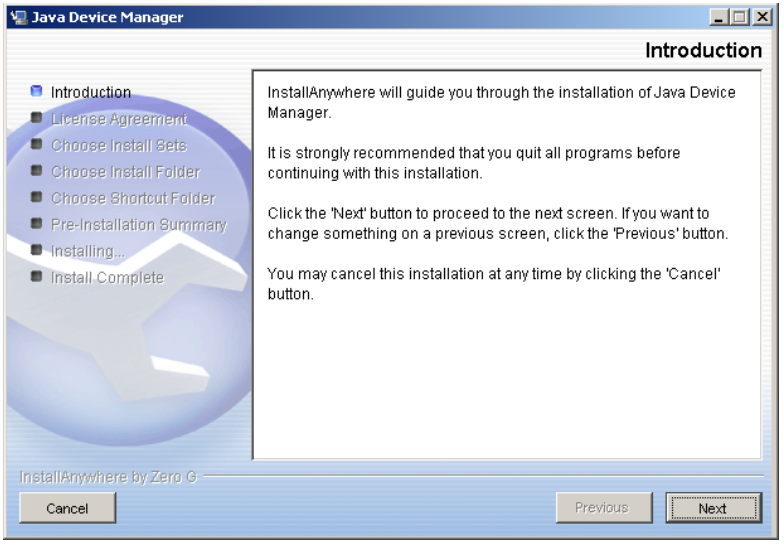
Note: In the file name, *xxxx* represents the current version of the JDM software.

Continue with "Executing the JDM installation software on Windows ".

Executing the JDM installation software on Windows

An install screen opens, followed by a Nortel dialog box. When the InstallAnywhere Introduction dialog box appears (Figure 54 on page 186), you are ready to install the JDM.

Figure 54 InstallAnywhere Introduction dialog box

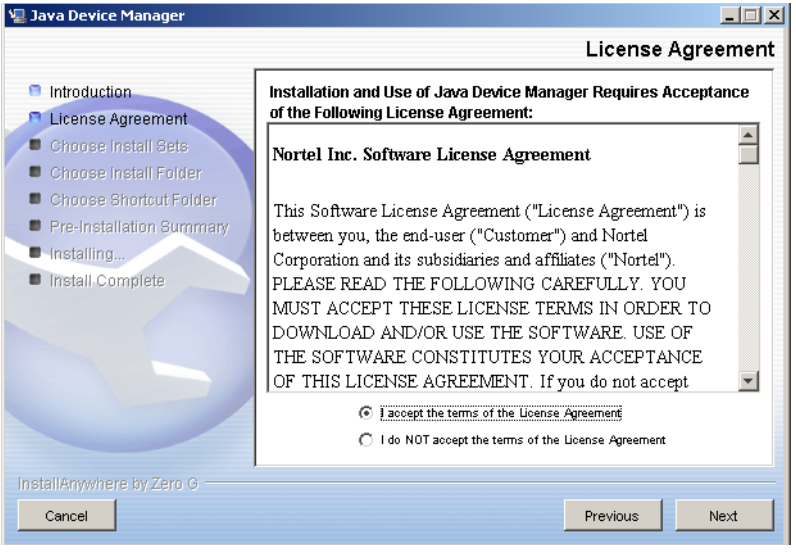


1 Click Next to begin the installation process.

The License Agreement dialog box opens.

2 Click I accept the terms of the License Agreement, as shown in Figure 55.

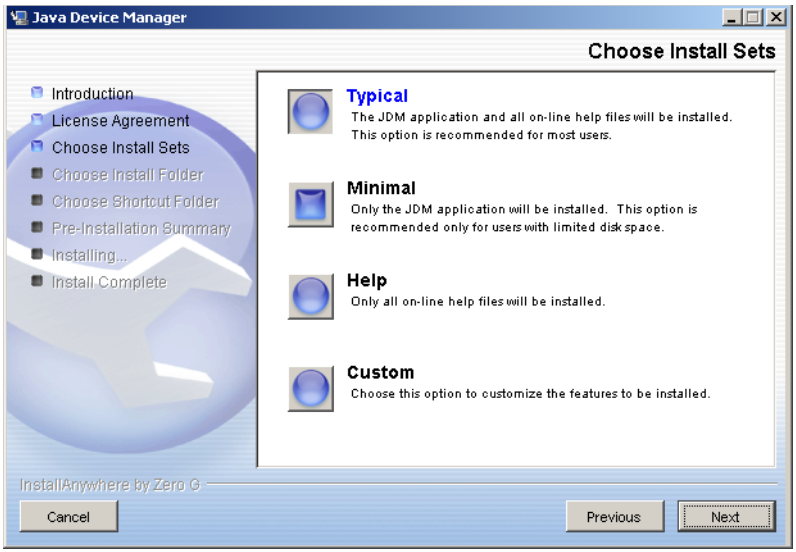
Figure 55 License Agreement dialog box



3 Click Next.

The Choose Install Set dialog box opens, as shown in Figure 56.

Figure 56 Choose Install Set dialog box



4 Do one of the following:

— Select Typical installation to install the common set features, as well as online help.

— Select Minimal installation to select minimal features to install (recommended for those with limited disk space).

— Select Help to install only the online help.

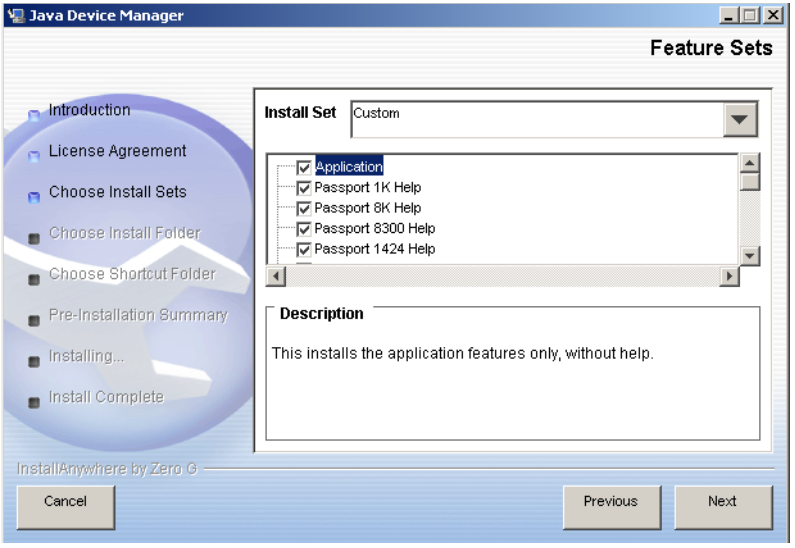
— Select Custom installation to customize the features prior to installation.

5 Click Next.

If you did not select Custom installation in step 4, then the Choose Install Folder dialog box opens. Continue with step 8 on page 189.

If you selected Custom installation in step 4, then the Feature Sets dialog box opens, as shown in Figure 57 on page 188.

Figure 57 Feature Sets dialog box

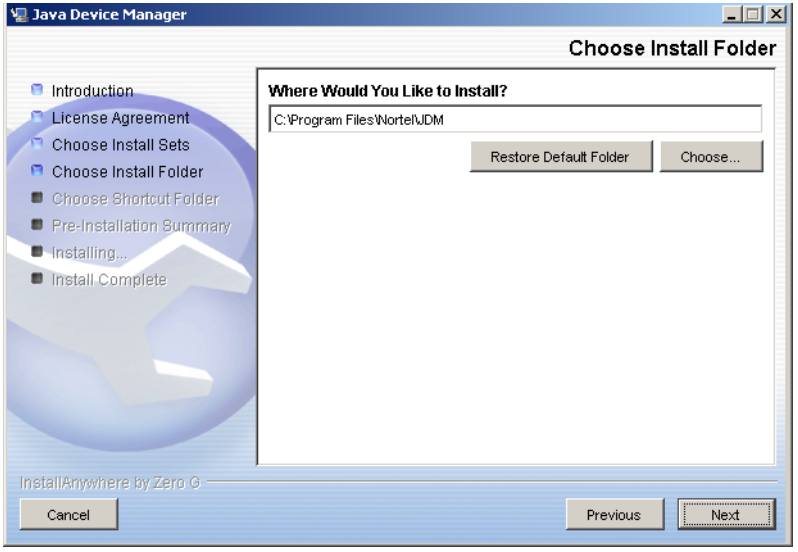


6 Select which features to install from the feature sets list.

7 Click Next.

The Choose Install Folder dialog box opens, as shown in Figure 58.

Figure 58 Choose Install Folder dialog box



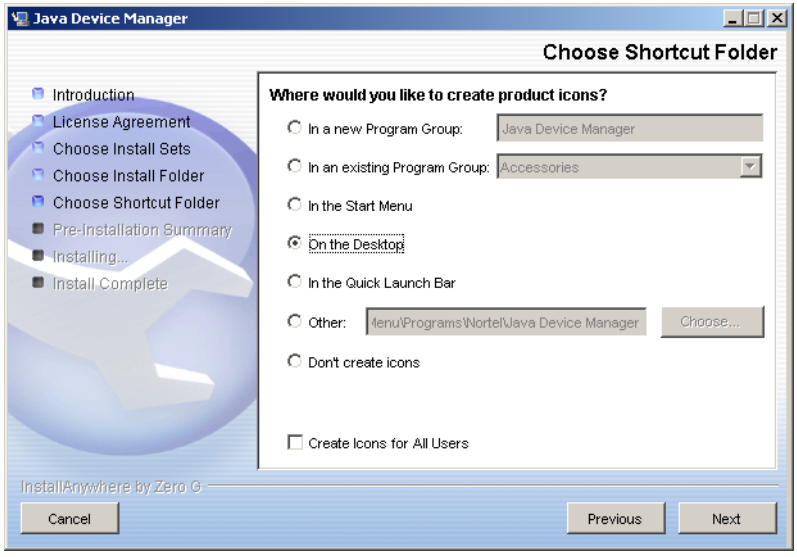
8 Click Restore Default Folder to use the default location for JDM, or click Choose to select a different storage path.

Note: If Device Manager is already installed on your computer, you must choose a storage path that does not conflict with the already existing version.

9 Click Next.

The Choose Shortcut Folder dialog box opens, as shown in Figure 59.

Figure 59 Choose Shortcut Folder dialog box

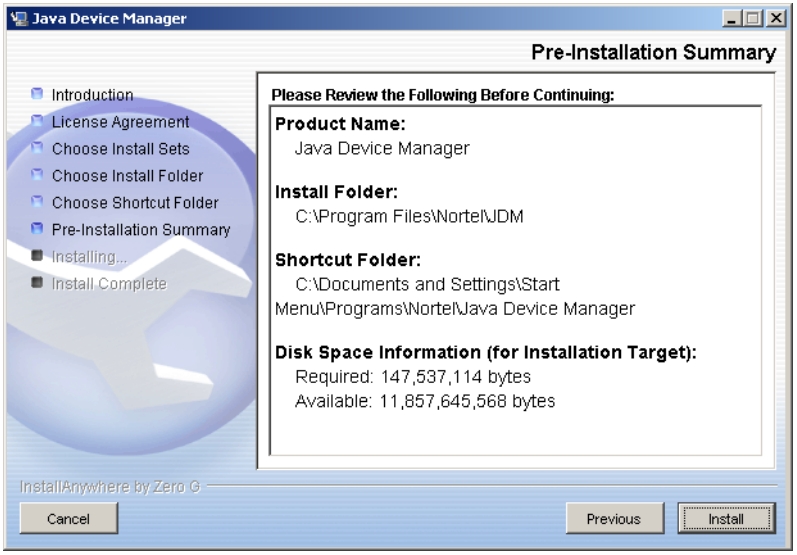


10 Select the desired shortcut path from the list provided.

11 Click Next.

The Pre-Installation Summary dialog box opens, as shown in Figure 60. A summary of the choices you have made is displayed for confirmation.

Figure 60 Choose Shortcut Folder dialog box

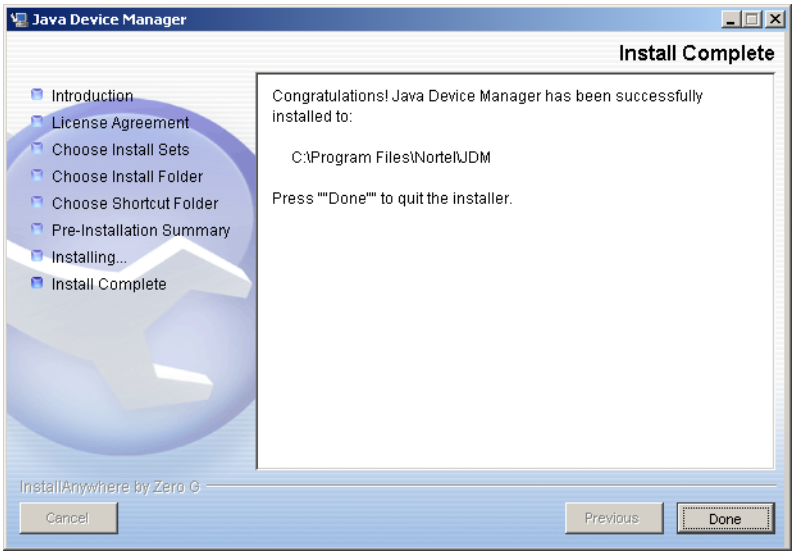


12 Verify the folder, shortcut, and disk space required to install the software. If necessary, click Previous to return to the appropriate dialog box and make changes.

13 Click Install.

The installation process begins. When the installation is complete, the Install Complete dialog box opens, as shown in Figure 61 on page 191.

Figure 61 Install Complete dialog box



14 Click Done to exit the installation.

JDM is now installed on your machine. For instructions on starting the Device Manager software, see "Starting Device Manager" on page 200.

Installing JDM on UNIX or Linux

Note: JDM installation procedures are now standardized across all platforms. In addition, the required Java Runtime Environment (JRE) version 1.4.1 is now part of the JDM installation package and does not require a separate installation. The bundled JRE is used with this JDM only, and does not affect other Java applications on the same system.

Note: Solaris and HP-UX, certain OS patches are required for JDM/JRE to function properly. Please consult SUN or HP to install the appropriate OS patches before launching JDM.

Note: UNIX and Linux systems are case-sensitive. Use lower-case to specify file names, and check to ensure that directories are entered correctly.

This section includes the following topics:

Unix minimum requirements

JDM supports two UNIX platforms and one Linux platform:

- a UNIX SPARC* workstation running the Sun* Solaris* 2.7.x (or higher)
- an HP* workstation running the HP-UX* 11.x operating system (or higher)
- a PC running Linux Kernel 2.2 operating system (or higher)

The minimum system requirements for installing JDM on any Unix or Linux platform are:

- 4 MB available in a temporary directory
- 300 MB free in the directory where you want to install the JDM software
- 128 MB DRAM

Installing JDM on Linux from the CD

To install the Device Manager software to a Linux environment from the CD:

1. Close all programs.
2. Insert the software CD into your CD-ROM drive.
3. Navigate to the Linux/JDM subdirectory on the software CD.
4. Run the *jdm_xxxx_linux.sh* file.

   Continue with "Executing the JDM installation software on UNIX or Linux" on page 196.

Installing JDM on Solaris from the CD

To install the JDM software to a Solaris environment from the CD:

1. Close all programs.
2. Insert the software CD into your CD-ROM drive.

3 Navigate to the Solaris/JDM subdirectory on the software CD.

4 Run the *dm_xxxx_solaris_sparc.sh* file.

Continue with "Executing the JDM installation software on UNIX or Linux" on page 196.

Installing JDM on HP-UX from the CD

To install the JDM software to a HP-UX environment from the CD, follow these steps with the exact syntax:

1 Close all programs.

2 Insert the software CD into your CD-ROM drive.

3 Navigate to the HP-UX/JDM subdirectory on the software CD.

4 Run the *jdm_xxxx_hpux_pa-risc.sh* file.

Continue with "Executing the JDM installation software on UNIX or Linux" on page 196.

Installing JDM on UNIX or Linux from the web

To install the JDM software to a UNIX (Solaris or HP-UX) environment from the web:

1 Go to the following URL:

http://www.nortel.com/support

2 Select the correct software support page for your product.

This requires four steps from the Product Finder page:

a Select the product family from the first box.

b Select the specific product from the second box.

c Select Software.

d Click Go.

The software page opens.

3 Click the Java Device Manager version you want.

The Software Detail Information page opens.

4 Click the appropriate JDM file for you operating environment.

A File Download dialog box opens that asks you to either run this program from its current location or to download the JDM software to your system.

5 Click Save.

A Save As dialog box opens.

6 Choose the directory to which you want to download the software. The software download is a self-extracting .sh file.

7 Click Save to begin the file transfer.

Once the file transfer is complete, continue with step 8.

8 Close all programs.

9 Navigate to the directory on your system where you loaded the JDM software.

10 Make the installation file executable.

For the Solaris environment, make the file executable by entering:

```
chmod a+x dm_xxxx_solaris_sparc.sh
```

For the HP-UX environment, make the file executable by entering:

```
chmod a+x jdm_xxxx_hpux_pa-risc.sh
```

For the Linux environment, make the file executable by entering:

```
chmod a+x jdm_xxxx_linux.sh
```

11 Run the installation file.

For the Solaris environment, run the *dm_xxxx_solaris_sparc.sh* file.

For the HP-UX environment, run the *jdm_xxxx_hpux_pa-risc.sh* file.

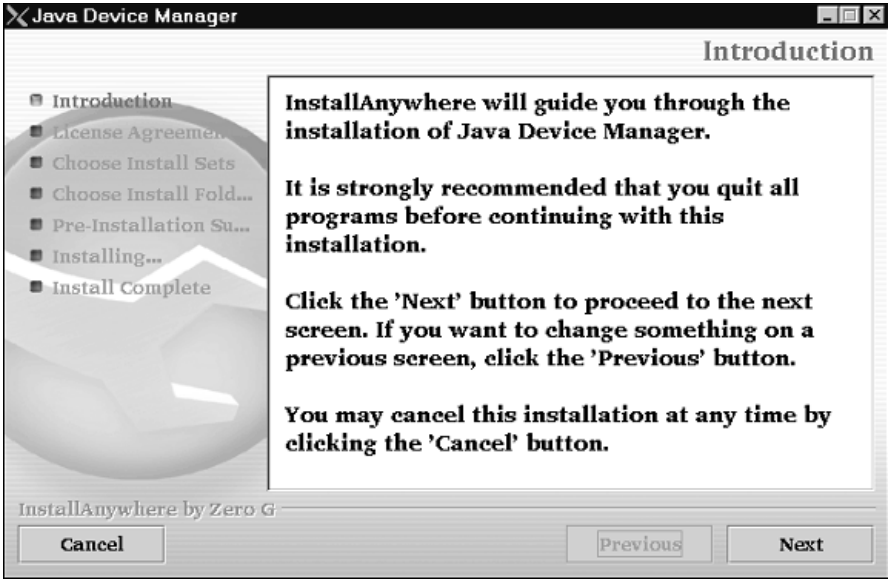
For the Linux environment, run the *jdm_xxxx_linux.sh* file.

Continue with "Executing the JDM installation software on UNIX or Linux" on page 196.

Executing the JDM installation software on UNIX or Linux

An install screen opens, followed by a Nortel dialog box. When the InstallAnywhere Introduction dialog box appears (Figure 62), you are ready to complete the JDM installation.

Figure 62 InstallAnywhere Introduction dialog box



1 Click Next to continue the installation process.

The License Agreement dialog box opens.

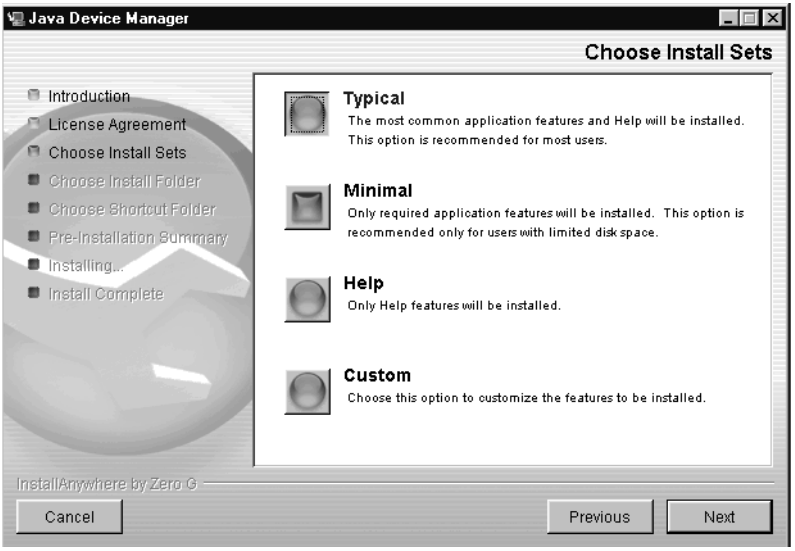
2 Click I accept the terms of the License Agreement, as shown in Figure 63 on page 197.

Figure 63 License Agreement dialog box

3 Click Next.

The Choose Install Set dialog box opens, as shown in Figure 64.

Figure 64 Choose Install Set dialog box



4 Do one of the following:

— Select Typical installation to install the common set features, as well as online help.

— Select Minimal installation to select minimal features to install (recommended for those with limited disk space).

— Select Help to install only the online help.

— Select Custom installation to customize the features prior to installation.

5 Click Next.

If you did not select Custom installation in step 4, then the Choose Install Folder dialog box opens. Continue with step 8 on page 199.

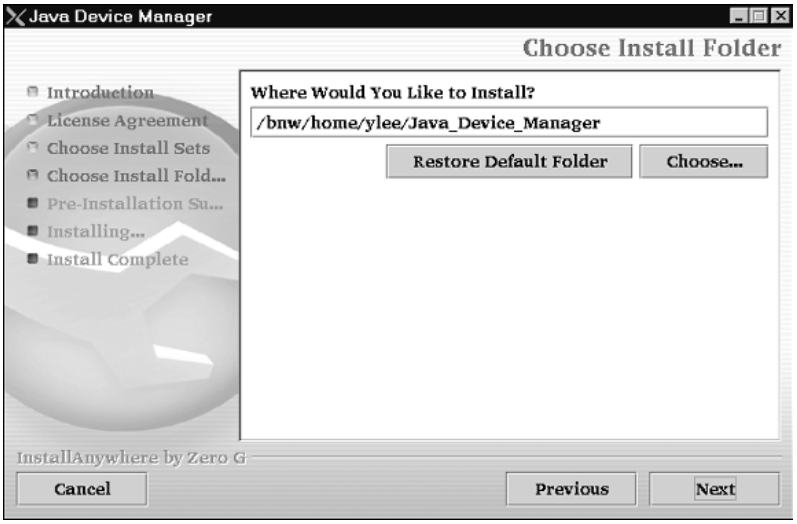
If you selected Custom installation in step 4, then the Feature Sets dialog box opens.

6 Select which features to install from the feature sets list.

7 Click Next.

The Choose Install Folder dialog box opens, as shown in Figure 65.

Figure 65 Choose Install Folder dialog box



8 Click Restore Default Folder to use the default location for JDM, or click Choose to select a storage path.

Note: If Device Manager is already installed on your computer, you must choose a storage path that does not conflict with the already existing version.

9 Click Next.

The Pre-Installation Summary dialog box opens.

10 Verify the folder and disk space required to install the software. If necessary, click Previous to return to the appropriate dialog box and make changes.

11 Click Install.

The installation process begins.

When the installation is complete, the Install Complete dialog box opens, as shown in Figure 66.

Figure 66 Install Complete dialog box

12 Click Done to exit the installation.

JDM is now installed on your machine. For instructions on starting the Device Manager software, see "Device Manager basics" on page 200.

Device Manager basics

This section describes basic procedures for using the Device Manager software. The section includes the following information:

- Instructions to start Device Manager, set the Device Manager properties, and open a device (next)
- A summary of the Device Manager user interface features and how to use them (page 207)
- Instructions to view statistics and display graphs (page 217)
- Instructions to use Device Manager to Telnet to a switch (page 224)
- Information about the trap log (page 225)
- Information about the Web-based management system (page 226)
- Information about online Help (page 227)

Starting Device Manager

To start Device Manager, do one of the following:

- In the Windows* environment, choose All Programs > Nortel > Java Device Manager > DM from the Windows Start menu.
- In a UNIX* environment, verify that the Device Manager installation directory is in your search path. Then type: `JDM`

An abbreviated Device Manager window opens, as shown in Figure 67 on page 201.

Figure 67 Device Manager window

Note: On startup, Device Manager performs a DNS lookup for the machine on which it is running. If the DNS lookup is slow or fails, the initial Device Manager window can take up to 30 seconds to open.

Setting the Device Manager properties

Device Manager uses the Simple Network Management Protocol (SNMP) to configure and manage Ethernet Switches 460 and 470. You can use the Device Manager Properties dialog box to configure important communication parameters such as the polling interval, timeout, and retry count. You can set these parameters at any time before or after you open a device.

To set the Device Manager properties:

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

The Properties dialog box opens (Figure 68 on page 202).

Figure 68 Device Manager Properties dialog box

2 Select properties you want to change and set their values.

3 Click OK.

Table 46 describes the Properties dialog box items.

Table 46 Properties dialog box items

Area	Item	Description
Polling	Status Interval	Interval at which statistics and status information is gathered. For a full stack, set this interval to between 120 and 300 seconds.
	(If Traps, Status Interval)	Interval (in seconds) at which statistics and status information are gathered when traps are enabled. Set this interval relative to the interval specified in the Status Interval field. It is usually 2 or 3 times the value of the Status Interval.
	Hotswap Detect every	The frequency at which Device Manager polls for hot swap module information. This value is in relation to the Status Interval value. For example, if the Status Interval is set to 120, and the value for Hotswap Detect every is 2, Device Manager polls the hot swap modules every 240 seconds. If less frequent hot swap polling is desired, set this value to poll every 2 or 3 intervals.
	Enable	Enables (true) or disables (false) periodic polling of the device for updated status. If polling is disabled, the chassis status is updated only when you click Refresh on the Chassis tab.
SNMP	Retry Count	Number of times Device Manager sends the same polling request if a response is not returned to Device Manager. You may want to set this field to three or four.
	Timeout	Length of each retry of each polling waiting period. When you access the device through a slow link, you may want to increase the timeout interval and then change the Retransmission Strategy to superlinear.
	Trace	The trace field is used to enable and disable SNMP tracing. When Trace is selected, SNMP protocol data units (PDUs) are displayed in the Device > Log dialog box.
	Register for Traps	When selected (enabled), Device Manager automatically registers to received traps when it is launched against a device. **Note:** This property does not apply to Ethernet Switches 460 and 470.
	Listen for Traps	When selected (enabled), Device manager listens for traps from the device.
	Max Traps in Log	The specified number of traps that may exist in the trap log. The default is 500.
	Trap Port	Specifies the UDP port that Device Manager uses to listen for SNMP traps.
	Listen for Syslogs	Enables the Device Manager to listen to the syslog.
	Confirm row deletion	When selected (enabled), Device Manager displays a dialog box for confirmation before deleting a system table row.

Table 46 Properties dialog box items (Continued)

Area	Item	Description
	Default Read Community	Displays the default Read Community type. You can edit this field by highlighting the current value and typing over it.
	Default Write Community	Displays the default Write Community type. You can edit this field by highlighting the current value and typing over it.

Opening a device

"Opening" a device displays the device view. To open the device view, you must enter community strings that determine the access level granted to the device.

Table 47 shows the default access community strings for the Device Manager software.

Table 47 SNMP community string default values

Access level	Description
Read-only	public
Read-write	private

To display the device view:

1 Do one of the following:

- Choose Device > Open.
- Choose Device > Open Last, and select an IP address from the list.
- Click the folder icon in the Device Manager window.

- Press [Ctrl] + O.

The Open Device dialog box opens (Figure 69 on page 205).

Figure 69 Open Device dialog box

Table 48 describes the Open Device dialog box fields.

Table 48 Open Device dialog box fields

Fields	Description
Device Name	Either an IP address or a DNS name for the device, entered by the user.
Read Community	SNMP read community string for the device. Default is `public` (displayed as ******). The entry is case-sensitive.
Write Community	SNMP write community string for the device. Default is `private` (displayed as *******).The entry is case-sensitive.
v3 Enable	When selected (enabled), Open Device dialog box will display SNMPv3 options.
User Name	Indicates the name of the user
Authentication Protocol	Identifies the authentication protocol used: NONE, MD5 or SHA-96.
Authentication Password	Specifies the current authentication password
Privacy Protocol	Identifies the privacy protocol
Privacy Password	Specifies the current privacy password

2 In the Device Name text box, type the DNS name or IP address of the device.

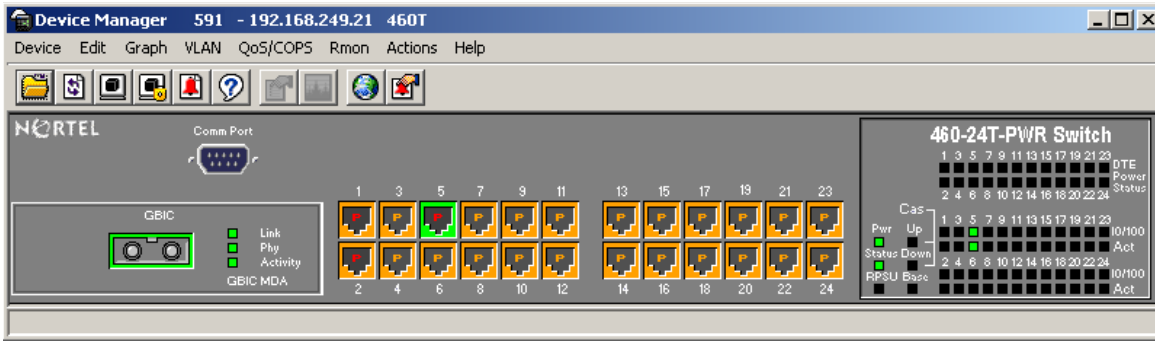
3 In the Read Community and Write Community text boxes, type the proper community strings

4 Click Open.

Device Manager automatically determines what version of software the selected device is running and displays the appropriate Device Manager dialog boxes.

The Device Manager window opens, displaying a dialog box of the device (Figure 70 on page 207) that represents the physical features of the device.

Figure 70 Device view



Note: For additional details on using SNMP with Ethernet Switches 460 and 470, and instructions on how to open a device using SNMPv3, refer to *Configuring and Managing Security* (217104-A).

Device Manager window

The Device Manager window (Figure 71) has the following parts:

- Menu bar
- Toolbar
- Device view

Figure 71 Parts of the Device Manager window

Menu bar

Use the menu bar to set up and operate Device Manager (Table 49).

Table 49 Menu bar commands

Command	Description
Device	Opens a device, refreshes the device view, and sets the polling and SNMP properties. This menu also allows you to open and view the Trap Log, SysLog, and Log. It also allows you to Telnet or open an SSH connection to the device that is currently open.
Edit	Opens edit dialog boxes for the objects selected in the device view. This command also opens dialog boxes for managing files and running diagnostic tests. This command also allows to set SNTP, SNMP v3 and related configurations.
Graph	Opens statistics dialog boxes for the selected object.
VLAN	Opens dialog boxes for managing VLANs, Spanning Tree Groups (STGs, RSTP, MSTP), Multi-Link Trunks and LACP.
QoS/COPS	Opens configuration and monitoring dialog boxes for Quality of Service (QoS), or Differentiated Services, and Common Open Policy Services (COPS).
Rmon	Opens RMON configuration and monitoring dialog boxes.
Actions	Allows you to open the Home page for the Web-based management session.
Help	Opens online Help topics for Device Manager and provides a legend for the port colors in the device view.

Toolbar

The toolbar contains buttons that provide quick access to commonly used commands and some additional actions. Table 50 describes the toolbar buttons.

Table 50 Toolbar buttons

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

Table 50 Toolbar buttons (Continued)

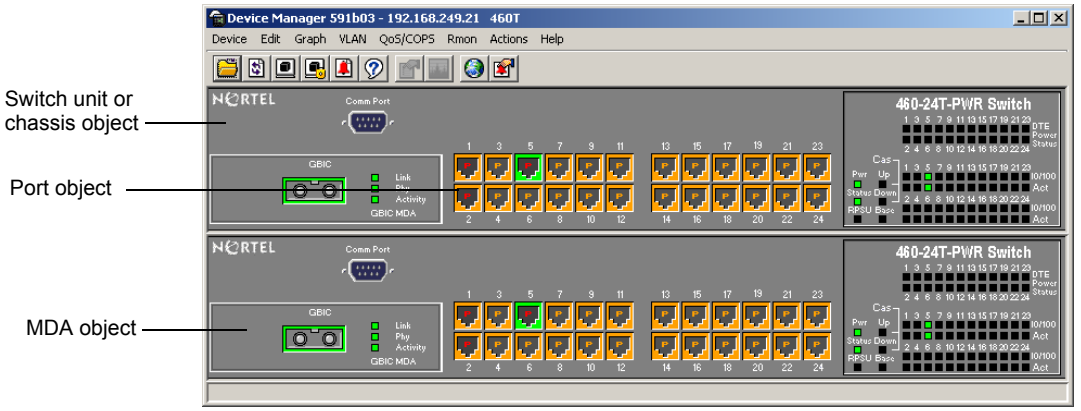
Button	Name	Description	Menu bar equivalent
	Trap Log	Opens the trap log.	Device > Trap Log
	Help	Opens online Help in a Web browser.	Help > Device
	Edit Selected	Displays configuration data for the selected chassis object.	Edit > Unit Edit > Chassis Edit > Port
	Graph Selected	Opens statistics and graphing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

Device view

The device view allows you to determine at a glance the operating status of the various units and ports in your hardware configuration. You also can use the device view to perform management tasks on specific objects.

Figure 72 on page 210 shows the parts of a typical device view.

Figure 72 Objects in the device view



The device view will also display devices that are down in a stack.

The following sections describe how you select and use objects in the device view:

- "Selecting objects," next
- "Selecting a single object" on page 211
- "Selecting multiple objects" on page 211
- "Viewing information about an MDA" on page 211
- "LEDs and ports" on page 213

Selecting objects

The types of objects contained in the device view are:

- A stand-alone switch (called a unit in the menus and dialog boxes)
- A switch stack (called a chassis in the menus and dialog boxes)
- A media dependent adapter (MDA) (called a unit in the menus and dialog boxes)
- A port

Selecting a single object

To select a single object:

➨ Click the edge of the object.

The object is outlined in yellow, indicating that it is selected. Subsequent activities in Device Manager refer to the selected object.

Selecting multiple objects

To select multiple objects of the same type (such as ports or switches of the same type):

➨ Do one of the following:

- For a block of contiguous ports, drag to select the group of ports.
- For multiple ports, MDAs, or switches in the stack, [Ctrl]+ click on the objects.

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

➨ Choose Edit > Select > Ports.

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

➨ Choose Edit > Select > Units.

To select an entire stack:

➨ Choose Edit > Select > Chassis.

Viewing information about an MDA

To view information about an MDA:

1 Select the MDA.

2 Choose Edit > Unit.

The Edit > Unit dialog box opens for the MDA.

The Edit > Unit dialog box describes the MDA installed in the switch (Figure 73).

Figure 73 MDA dialog box

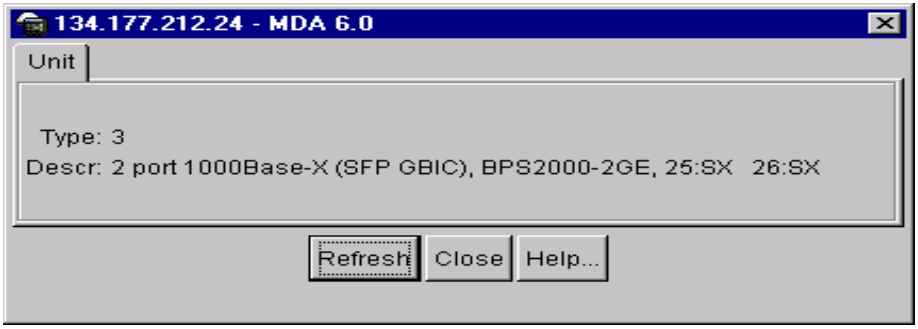


Table 52 describes the MDA dialog box fields.

Table 51 MDA dialog box fields

Field	Description
Type	Type of component or subcomponent installed in the Ethernet Switch 460-24T-PWR.
Descr	Description of the component or subcomponent installed in the Ethernet Switch 460-24T-PWR. If not available, the value is a zero-length string.

Media dependent adapters and port conventions

The conventions on the graphical representation of the switch are different from the actual switch. The colors in the graphical representation of the MDA and ports are color-coded to provide port status.

Table 52 describes the colors in the graphical representation of the MDA and its ports.

Table 52 MDA and MDA port colors

Color	Description
Green	Port is operating.
Red	Port has been manually disabled.

Table 52 MDA and MDA port colors (Continued)

Color	Description
Orange	Port has no link.
Gray	Port is unmanageable.

A blinking LED on an MDA is not indicated in the graphical representation of the switch.

For a full description of switch LEDs, refer to the respective switch user manuals.

LEDs and ports

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

For a full description of the LEDs for the Ethernet Switches 460 and 470, refer to "About Ethernet Switches 460 and 470" on page 45.

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

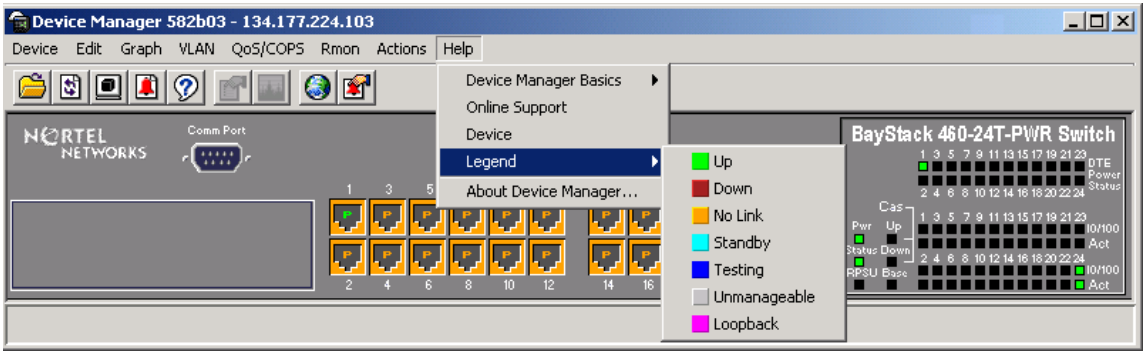
Table 53 shows the status assigned to each color.

Table 53 Port color codes

Color	Description
Green	Port is operating.
Red	Port has been manually disabled.
Orange	Port has no link.
Gray	Port is unmanageable.

In addition, the Help menu provides a legend that identifies the port colors and their meanings.

Figure 74 Color port legend



Shortcut menu

Each object in the device view has a shortcut menu that opens when you right-click a selected object. The Switch shortcut menu provides access to basic hardware information about the switch and to the graphing dialog boxes for the switch.

Figure 75 Switch unit shortcut menu

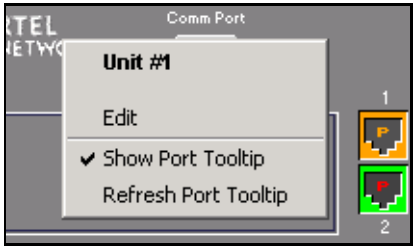


Table 54 describes the commands on the switch unit shortcut menu.

Table 54 Switch unit shortcut menu commands

Command	Description
Edit	Opens a dialog box that provides basic hardware information about the switch.
Refresh Port Tooltip	Refreshes the port tooltip data of the switch. The port tooltip data contains: Slot/Port, PortName, and PortOperSpeed.
Disable Port Tooltip	Disables the port tooltip function of the switch.

The port shortcut menu provides a faster path for editing and graphing a single port; however, you can access the same options using the menu bar or the toolbar.

Figure 76 Port shortcut menu

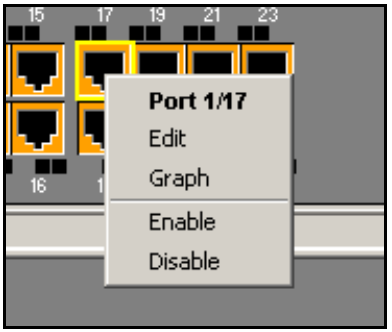


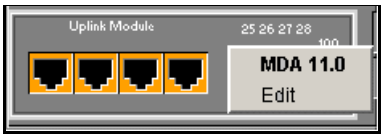
Table 55 describes the commands on the port shortcut menu.

Table 55 Port shortcut menu commands

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

The MDA shortcut menu contains only the Edit command which opens a read-only dialog box with basic hardware information about the MDA.

Figure 77 MDA shortcut menu



Status bar

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

Using the buttons in Device Manager dialog boxes

Table 56 describes buttons in Device Manager dialog boxes. Not all buttons appear in all dialog boxes.

Table 56 Device Manager buttons

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

Editing objects

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

- Select an object and, on the toolbar, click the Edit Selected button.

  The edit dialog box opens for that object.

- From a switch or port shortcut menu, choose Edit. The edit dialog box opens for that object.

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

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

Working with statistics and graphs

Device Manager tracks a wide range of statistics for each switch, the stack (chassis), and each port. You can view and graph statistics for a single object or multiple objects. For information about the statistics tracked for the switch and ports, refer to "Statistics for single and multiple objects" on page 221 and to the *System Monitoring Guide* (217107-A).

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

Types of statistics

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

You can set the polling intervals for each graph from a pull-down menu offering the following choices: None, 2 seconds, 5 seconds, 10 seconds, 30 seconds, 1 minute, 5 minutes, 30, minutes, or 1 hour.

Table 57 describes the types of statistics shown in the statistics dialog boxes.

Table 57 Types of statistics

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

Types of graphs

With Device Manager, you can create line, area, bar, and pie graphs. Figure 78 on page 219, Figure 79 on page 219, Figure 80 on page 220, and Figure 81 on page 220 illustrate the different graph styles, respectively.

Figure 78 Line graph

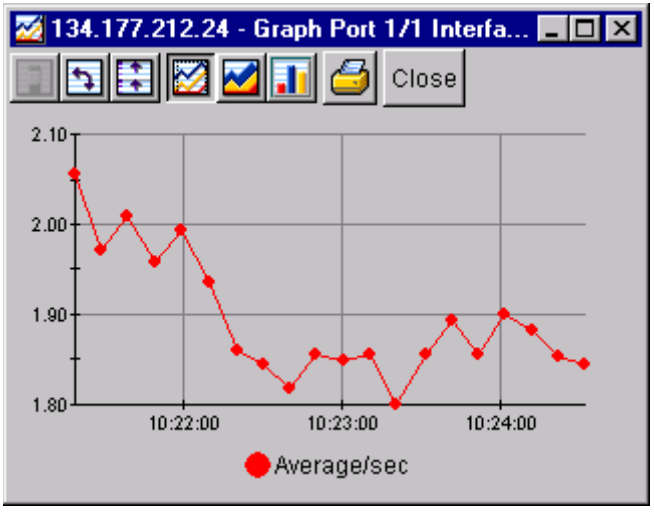


Figure 79 Area graph

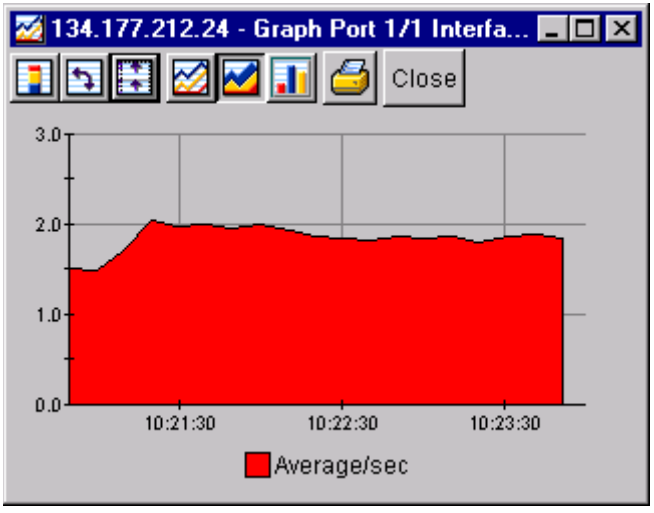


Figure 80 Bar graph

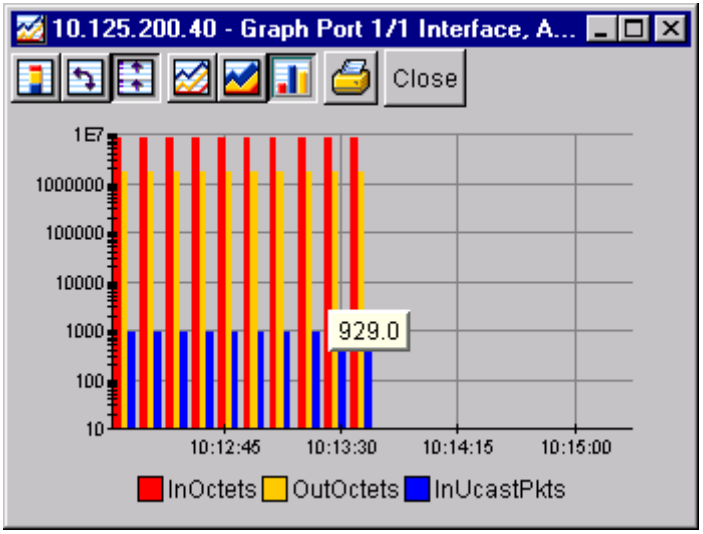
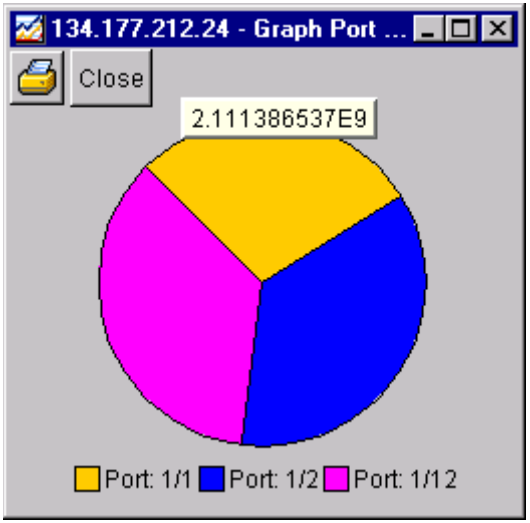


Figure 81 Pie graph

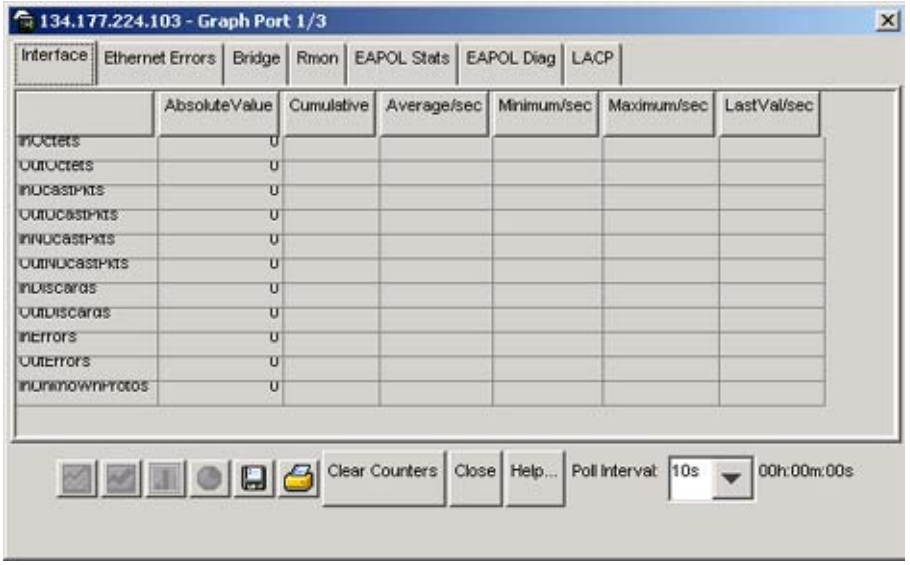


Statistics for single and multiple objects

The statistics dialog box displays statistics for a selected object.

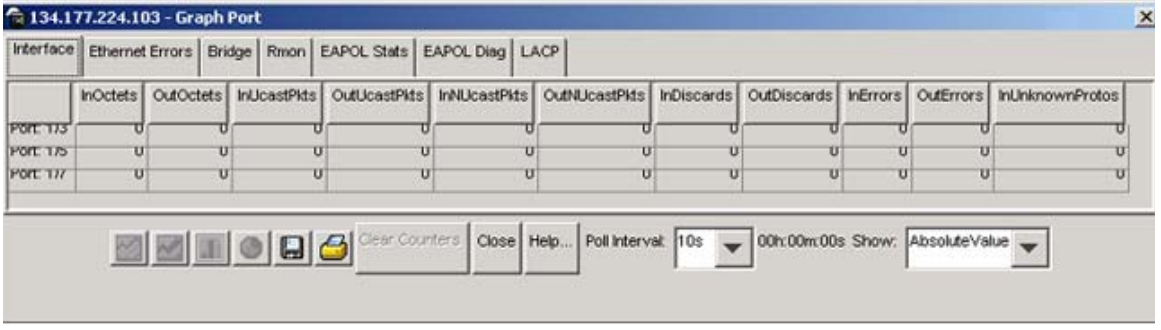
The dialog box for a single object shows all six types of statistics for each counter (Figure 82).

Figure 82 Interface statistics for a single port



The statistics dialog box for multiple objects shows a single type of statistics (Table 57 on page 218) for the selected objects. For example, Figure 83 shows LastValue statistics for the selected ports.

Figure 83 Interface statistics for multiple ports



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

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

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

See "Viewing statistics as graphs," next for instructions on using these buttons.

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

Viewing statistics as graphs

To create a graph for an object:

1 Select the object or objects to be graphed

See "Selecting objects" on page 210 for more information.

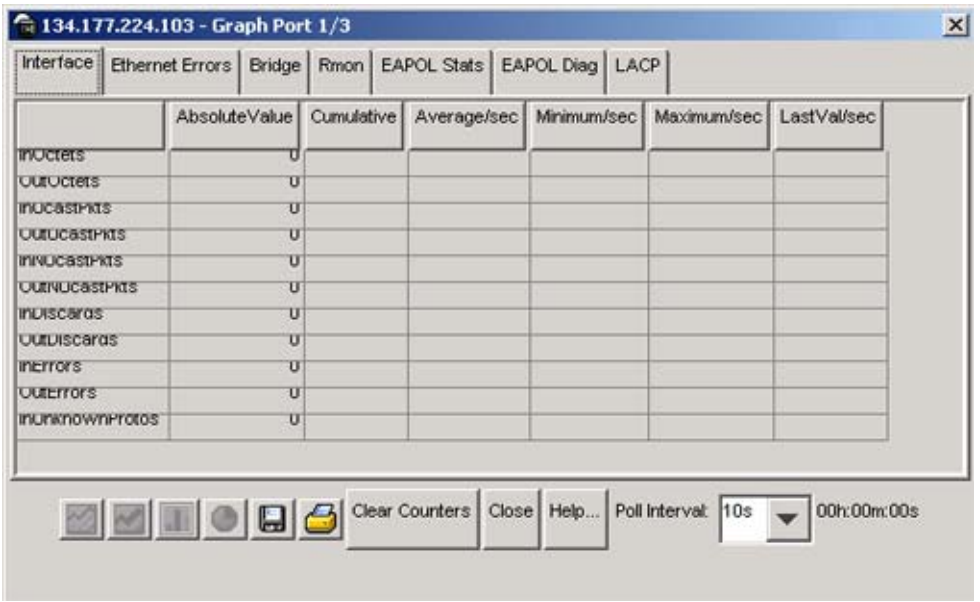
2 Do one of the following:

- On the toolbar, click Graph Selected.

- From the shortcut menu for the object, choose Graph.
- From the main menu, choose Graph > Chassis or Graph > Port.

A statistics dialog box opens with tabs for different categories of statistics for the selected object (Figure 84 on page 223).

Figure 84 Statistics dialog box for a port



3 Select a tab for the group of statistics you want to view.

4 On the displayed data table, drag to select the cells you want to graph. (They must be in the same row or column.)

5 Click one of the graph buttons at the bottom of the dialog box

See "Types of graphs" on page 218 for more information.

A graph dialog box opens for the selected graph type.

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

Buttons at the top of the graph dialog boxes for line, area, and bar graphs allow you to change the orientation of the graph, change the scale, or change the graph type.

Table 58 describes the buttons in the graph dialog boxes.

Table 58 Graph dialog box buttons

Button	Name	Description
	Stacked	Stacks data quantities instead of displaying them side-by-side.
	Horizontal	Rotates the graph 90 degrees.
	Log Scale	Changes the scale of the x-axis (of an unrotated graph) from numeric to logarithmic.
	Line Chart	Converts an area graph or bar graph to a line graph.
	Area Chart	Converts a line graph or bar graph to an area graph.
	Bar Chart	Converts a line graph or area graph to a bar graph.
	Pie Chart	Converts a line, bar, or area graph into pie chart.

Telneting to a switch

From Device Manager, you can initiate a Telnet session to the Console Interface for the switch or stack you are currently accessing.

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

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

  A Telnet window to the switch opens.

Opening an SSH connection to the switch

From Device Manager, you can initiate a Secure Shell (SSH) connection to the Console Interface for the switch or stack you are currently accessing.

To open an SSH connection to a switch:

➨ Do one of the following:

- From the Device Manager main menu, Choose Device > SSH Connection.
- On the toolbar, click the SSH button.

An SSH window to the switch opens.

Note: The SSH connection is established only when the device is SSH capable and enabled. For more information on SSH connections, refer to *Configuring and Managing Security* (217104-A).

Trap log

You can configure an Ethernet Switch to send SNMP generic traps. When Device Manager is running, any traps received are recorded in the trap log. You set the maximum number of entries in the trap log using the Properties window (Figure 68 on page 202). The default number of trap log entries is 500.

To view the trap log:

➨ Do one of the following:

- On the toolbar, click the Trap Log button.

- From the Device Manager Main Menu, choose Device > Trap Log.

Note: When you operate Device Manager from a UNIX platform, you must be logged in as root in order to receive traps.

Using the Export button at the bottom of the screen, you can export the trap log to a separate file that you can save to your system.

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

By default, traps are sent in SNMP V2c format. However, if you are using an older network management system (NMS), one that supports only SNMP V1 traps (HP OpenView), you can specify to send the traps in V1 format.

For more information about traps and trap receivers, refer to *Configuring and Managing Security* (217104-A).

Accessing the Web-based management system

You can access the Web-based management system for the Ethernet Switch from Device Manager.

To access the Web-based management system:

➨ From the Main Menu, choose Actions > Open Home Page.

The Web browser opens to the Web-based management system for the switch. For more information on this system, refer to "Using the Web-based management interface" on page 229.

Online help

Online Help in Device Manager is context-sensitive. You can use a Web browser to display online Help. The Web browser should launch automatically when you click the Help button. If the Help topic you are accessing is not displayed in your browser, exit the existing browser session and click the Help button again.

If, for some reason, the Web browser does not launch, the default locations of the Help files are the directories listed in Table 59.

Table 59 Help file locations

Platform	Default path
Device Manager	<JDM Installation directory> / help / pp8k_basics/dmhelp.html
Device specific help	<JDM Installation directory> /help / falcon / v360.zip. help.html is the home page for the Online Help.

Chapter 5
Using the Web-based management interface

This chapter describes the requirements for using the Web-based management interface, and how to use it as a tool to configure the Ethernet Switches 460 and 470. This chapter covers:

Note: Starting with Release 3.6 software, Secure Socket Layer (SSL) is available to provide security for the Web-based management system. It allows access to the Web-based management using a secure https session. The user must enable SSL for the browser through the Command Line Interface (CLI).

For more information on SSL Web-based management, refer to *Configuring and Managing Security* (217104-A).

Requirements

To use the Web-based management interface, you need the following items:

- A computer connected to any of the network ports
- One of the following web browsers installed on the computer (check the memory requirements):
  - — Microsoft Internet Explorer*, version 4.0 or later (Windows 95/98/NT/XP)
  - — Netscape Navigator*, version 4.51 or later (Windows 95/98/NT/XP and Unix)
- The IP address of the Ethernet Switch
- A web browser optimized for 800 by 600 pixel screen size

Note: The web pages of the Web-based management interface can load at different speeds depending on the web browser you use.

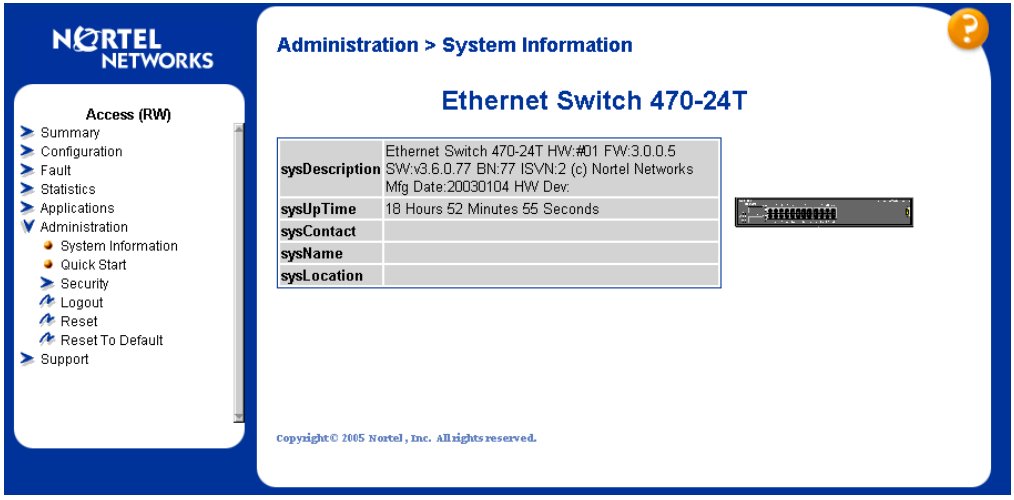
Logging in to the Web-based management interface

Before you log in to the Web-based management interface, use the Console Interface to verify the VLAN port assignments, and to ensure that your switch CPU and your computer are assigned to the same VLAN. If the devices are not connected to the same VLAN, you cannot access the Web-based management system.

To log in to the Web-based management interface, follow these steps:

1. Start your web browser.
2. In the web address field, enter the IP address for your host switch or stack, for example, http://10.30.31.105, and press [Enter]. The home page opens.

Figure 85 Web-based management interface home page

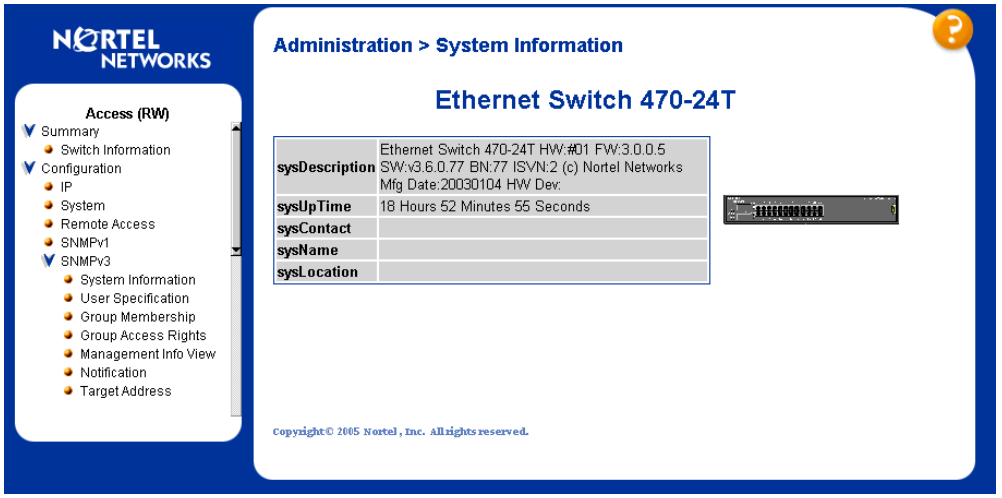


Network security does not yet exist the first time you access the Web-based management user interface. As the system administrator, you must create access parameters and passwords to protect the integrity of your network configurations.

Web page layout

The switch home page (Figure 86) and all successive web pages have a common layout. Each is divided into two sections: the menu and the management page. All web pages are optimized for a 800 x 600 pixel screen size.

Figure 86 Web page layout



Menu

The menu, as shown at left in Figure 86, contains a list of seven main titles and their corresponding options.

To navigate the Web-based management interface menu, click a menu title, and then click one of its options. When you click an option, the corresponding page opens.

Table 60 lists the main headings in the Web-based management user interface and their associated options.

Table 60 Main headings and options

Main menu titles	Options
Summary	Stack Information (stack mode only) Switch Information Identify Unit Numbers (stack mode only) Stack Numbering (stack mode only)
Configuration	IP System Remote Access SNMPv1 SNMPv3* SNMP Trap MAC Address Table Find MAC Address Port Management High Speed Flow Control Software Download Ascii Config Download Configuration File Console/Comm Port
Fault	RMON Threshold RMON Event Log System Log
Statistics	Port Port Error Summary Interface Ethernet Errors Transparent Bridging RMON Ethernet RMON History
Applications	Port Mirroring Rate Limiting EAPOL Security MAC Address Security* IGMP* VLAN* Multilink Trunk* QoS* Cops* ADAC*

Table 60 Main headings and options (Continued)

Main menu titles	Options
Administration	System Information Quik Start Security* Logout Reset Reset to Default
Support	Help Release Notes Manuals Upgrades
*Has additional menus.	

Navigation buttons or icons are provided in the menu to assist you in navigating the Web-based management interface.

Caution: Web browser capabilities, such as page bookmarking, refresh, page forward, and page back, function as they do in any other web site. However, these capabilities do not enhance the functionality of the Web-based management interface. Nortel recommends that you use only the navigation tools provided in the management interface.

Table 61 describes the icons that appear on the menu.

Table 61 Menu icons

Button or icon	Description
	This icon identifies a menu title. Click this icon to display its options.
	This icon identifies a menu title option. Click this icon to display the corresponding page.
	This icon identifies a menu title option with a hyperlink to related pages.

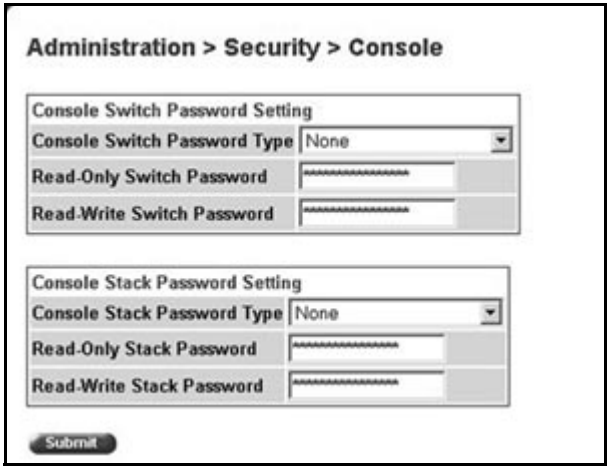
Table 61 Menu icons

	This icon is linked to an action, for example, logout, reset, or reset to system defaults.
	Clicking on the Nortel logo opens the Nortel corporate home page in a new web browser.

Management page

When you click a menu option, the corresponding management page opens. Figure 87 shows the page displayed for the Administration > Security > Console option.

Figure 87 Console page



A page is composed of one or more of the following elements:

- Tables and input forms

  The gray cells in a page indicate read-only information, and white cells indicate input fields.

- Check boxes

  You enable or disable a selection by clicking a check box. When a check mark is displayed in the box, that selection is enabled. You disable a selection by clearing the checked box.

- Icons and buttons

  Icons and buttons perform an action related to the displayed page or the switch, such as opening another page or updating the values shown on the current page. As well, some icons initiate an action, such as reformatting the current displayed data as a bar or pie chart.

Table 62 describes the icons that can appear on a page to assist you in navigation.

Table 62 Page buttons and icons

Icon	Name	Description
	Modify	Accesses a modification page for the selected row.
	View	Accesses a view only statistics page for the selected row.
	Delete	Deletes a row.
	Help	Accesses the Help menu in a new Web browser.
	Item-Specific Help	Accesses the item-specific Help menu in a new Web browser.
		Note: Text within a table that is highlighted blue and underlined is a hyperlink to a related management page.

Chapter 6
System Configuration using the Console Interface

The Console Interface allows you to display and modify the switch configuration while the switch is operating.

This chapter includes information about the system configuration, such as Configuring the switch IP address, downloading and uploading your software, and customizing your system. This chapter covers the following topics:

Configuring the system IP address

There are two ways to configure the IP address of the Ethernet Switch:

- Using a Static IP address
- Using BootP to provide an IP address

The Ethernet Switch unit begins switching as soon as you attach network devices and connect the switch to power. To manage the switch using Telnet or SNMP or to perform TFTP operations, the following IP address parameters must be configured on the device:

- IP Address of the switch or the stack
- IP Subnet mask
- IP Gateway address

Configuring a Static IP Address

The initial static IP address configuration must be performed through the serial or console port of the device. Once an IP address has been configured and is functional, the you may change the IP address configuration through any of the available user interfaces.

Static IP Configuration Requirements

Here are the requirements for configuring a static IP address on the Ethernet Switch:

1. The IP address must not be in use by another system.
2. You must use a serial cable if configuring the static IP address through the console port. If you are configuring the IP address of a stack, please make sure that serial cable is connected to the console port of the base unit.
3. If you are configuring the IP address of the switch through an in-band connection that uses the Ethernet network, make sure that the management station is connected to a port that is a member of the management VLAN.

Static IP address user interface configuration support

The Static IP address parameters may be manipulated through all user interfaces.

Table 63 lists the configuration parameters and the access permissions for the user through the various user interfaces.

Table 63 Static IP address user interface configuration support

Parameter	Default	Menu Interface	CLI	Web	Device Manager
In-Band Stack IP Address	0.0.0.0	rw	rw	rw	rw
In-Band Switch IP Address	0.0.0.0	rw	rw	rw	rw
In-Band Subnet Mask	0.0.0.0	rw	rw	rw	rw
Default Gateway:	0.0.0.0	rw	rw	rw	rw

Configuring a static IP address using the Console Interface

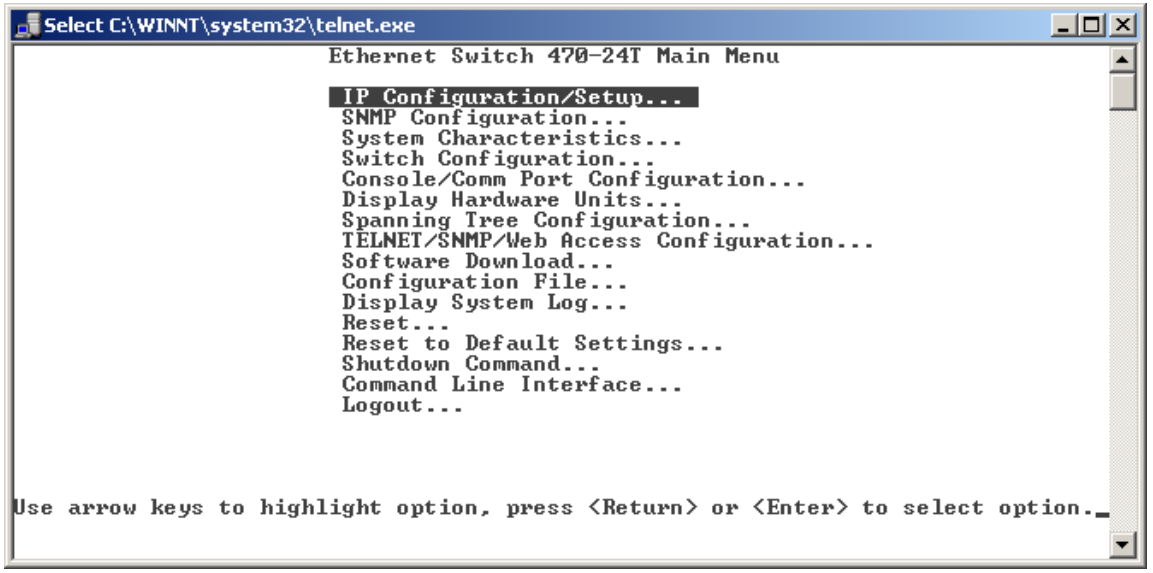
For the initial setup of a stand-alone switch or a stack configuration, you must use the following IP procedures:

1. Connect the terminal to the Console port on the switch.
2. Set the terminal protocol.
3. Connect the switch to power supply.
4. After the Nortel logo is displayed, press [Ctrl]-Y to display the Main Menu.

Note: Initially, the screen displays the Main Menu for a stand-alone switch. But, if the switch is part of a stack configuration, the screen is refreshed within 60 seconds to show the Main Menu for the stack.

5 Select IP Configuration/Setup by choosing IP Configuration/Setup (or pressing i) from the main menu to display the IP Configuration/Setup menu. Table 88 displays the Console Interface Main Menu.

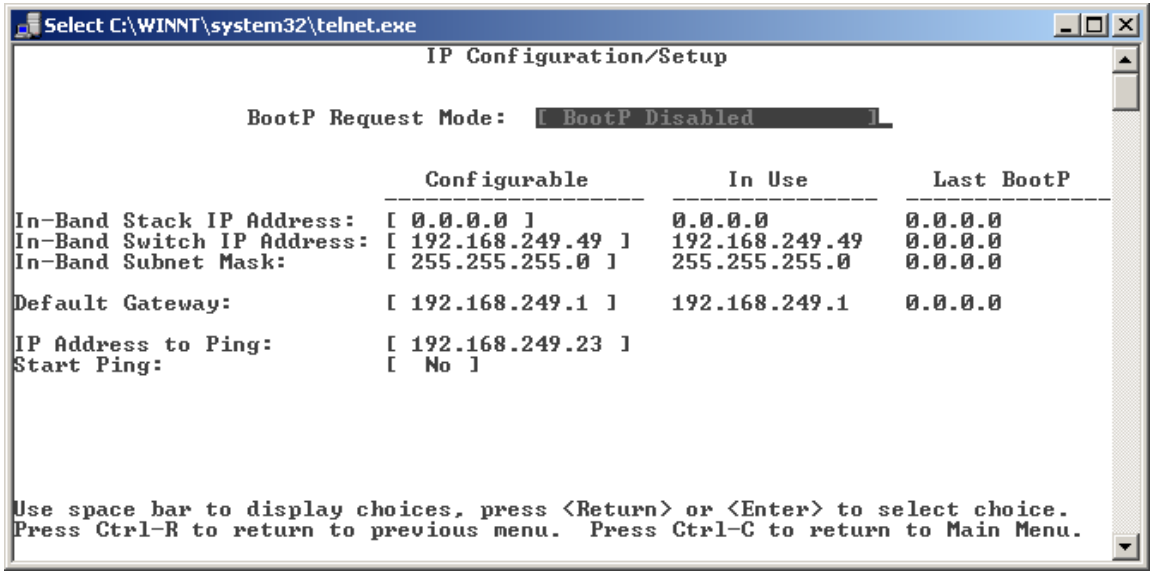
Figure 88 Console Interface Main Menu



6 For a stand-alone switch, in the In-Band Switch IP Address field, enter the IP address of the switch in dotted-decimal notation.

7 For a stack configuration, in the In-Band Stack IP Address field, enter the Stack IP address in dotted decimal notation. Figure 89 displays the IP configuration screen.

Figure 89 IP configuration screen



Note: The default management VLAN in Ethernet Switches 460 and 470 is VLAN1. To manage the switch, ensure the network management station is on the management VLAN, or is connected to the management VLAN.

The In-Band Switch IP address field allows this switch to operate as a stand-alone switch. However, this field is not required for the operation of the stack. You cannot enter the same IP address in both fields (In-Band Stack IP address and In-Band Switch IP address).

If the In-Band Subnet Mask field does not display a value, when you enter the IP address in the In-Band IP address field, the switch software provides an in-use default value for the In-Band Subnet Mask field. This value is based on the class of the IP address specified in the In-Band Switch IP address or the IP-Band Stack address fields.

8 In the Default Gateway field, specify the default gateway address.

Note: If you are stacking Ethernet Switches, ensure that you set one switch as the Base Unit.

9 Press Ctrl+C to return to the main menu.

To reset the Ethernet Switch to factory default values, select Reset to Default values on the main menu, and then press Enter key.

Static IP Address Configuration Parameters

Table 64 IP Configuration/Setup screen fields

Field	Description
Unit	To view or configure an IP address for a specific unit, choose that unit number.
Configurable	Column header for the user-configurable IP configuration fields in this screen.
In Use	Column header for the read-only fields in this screen. The read-only data displayed in this column represents IP configuration that is currently in use.
Last BootP	Column header for the read-only fields in this screen. The read-only data displayed in this column represents IP configuration obtained from the last BootP reply received.
In-Band Stack IP Address	The in-band *stack* IP address field. This field is not required for the operation of the stand-alone switch. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point
In-Band Switch IP Address	The in-band IP address of the switch. . Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point 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.

Table 64 IP Configuration/Setup screen fields (Continued)

Field	Description
In-Band Subnet Mask	The subnet address mask associated with the in-band IP address shown on the screen (see In-Band Switch IP Address field). Network routers use the subnet mask to determine the network or subnet address portion of a host's IP address. The bits in the IP address that contain the network address (including the subnet) are set to 1 in the address mask, and the bits that contain the host identifier are set to 0. Default Value 0.0.0.0 (no subnet mask assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point
Default Gateway	The IP address of the default gateway. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point

Pinging the switch

You can ping from an Ethernet Switch 460 or 470. This makes network management much easier.The ping command tests the network connection to another network device. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device. The local IP address must be set before issuing the ping command.

For more information on the CLI commands, see Chapter 3, "CLI Basics," on page 153.

Troubleshooting

Do the following if you have problems while configuring the IP address parameters on the switch:

- Check is all the IP address parameters are correct.
- Use the PING function on the switch to PING itself.
- Use the PING function on the switch to PING the default gateway.

- Check if the IP address is in use on another device.

Note: The Ping command tests the network connection to another network device. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device. The local IP address must be set before issuing the ping command. For more information on the CLI commands, see Chapter 3, "CLI Basics," on page 153.

Usage guidelines

- A switch IP address can be configured for devices in a stack. That address cannot be active unless the unit disassociates from the rest of the stack.
- When the two units in a stack of two units disassociate with one another, neither unit uses the stack IP address. Both units use the switch IP address that is configured for each unit.

Configuring an IP address using BootP

The BootP or Boot Protocol enables the network manager to administer the IP addresses of network devices from a central location. Along with the IP address, the BootP protocol identifies the default gateway, subnet mask and other configuration parameters that may be managed by the BootP server.

The BootP implementation on Ethernet Switches enables BootP to operate in the following modes:

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

You can retrieve the ASCII configuration file name and configuration server address using BootP.

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

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).

BootP Configuration Requirements

To use the BootP protocol, you need a BootP server that adheres to the IETF standard RFC 951.

That BootP server must be accessible through the Management VLAN. If the BootP server is not located on the same subnet as the Ethernet Switch, but is located on another IP subnet, there must be a router on the local subnet (the subnet with which the Ethernet Switch is associated) that provides BootP Relay functionality as defined in RFC 1532.

BootP User Interface Configuration Support

The BootP parameters may be manipulated through all user interfaces. The following table indicates whether the user has read (r), read-write (rw), or no access to the parameter through the listed user interface.

Table 65 BootP Configuration User Interface Support

Parameter	Default	Menu Interface	CLI	Web	Device Manager
BootP Always		rw	rw	rw	rw
BootP When Needed	default setting	rw	rw	rw	rw
BootP Or Last Address		rw	rw	rw	rw
BootP Disable		rw	rw	rw	rw

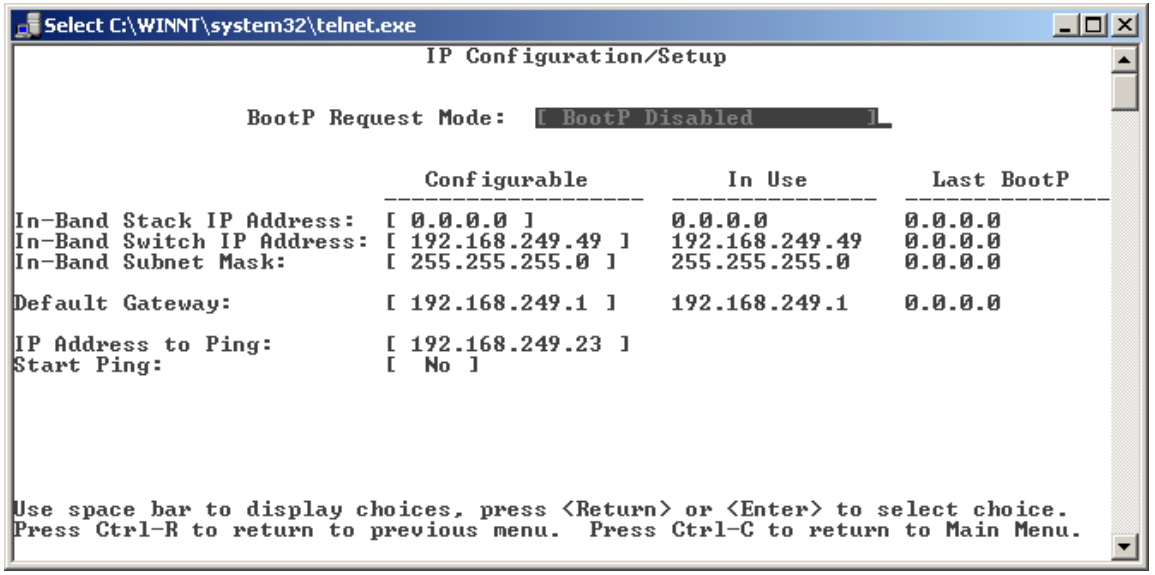
Configuring BootP using the console Interface

Use the following procedure to configure the BootP parameters on the Ethernet Switch:

1. Connect to the device through the serial port or through a Telnet connection.
2. After the Nortel logo is displayed, press [Ctrl]-Y to display the Main Menu.

3 Select IP Configuration/Setup by choosing IP Configuration/Setup (or pressing i) from the main menu to display the IP Configuration/Setup menu. Figure 90 displays the IP configuration using the Console Interface.

Figure 90 IP configuration using the Console Interface



4 Highlight the BootP Request Mode field.

5 Cycle through the various BootP parameters by pressing the spacebar.

6 Press the Enter key to activate the appropriate selection.

Note: The read-only fields in this screen are updated based on the BootP mode specified in the BootP Request Mode field. (See "Configuring an IP address using BootP" on page 247 for more information.)

BootP configuration Parameters

BootP When Needed

Selecting this parameter allows the switch to request an IP address if one has not already been set from the console terminal. This mode is the default mode. When selected, this mode operates as follows:

- When the IP data is entered from the console terminal, the data becomes the in-use address of the switch and BootP requests are not broadcast. The switch can be managed using this in-band IP address.
- When the in-band IP address is not set from the console terminal, the switch broadcasts BootP requests until it receives a BootP reply containing an IP address. If the switch does not receive a BootP reply that contains an IP address, the switch cannot be managed in-band.

  If an IP address is *not* currently in use, these actions take effect immediately. If an IP address *is* currently in use, these actions take effect only after the switch is reset or power cycled.

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.

BootP Always

Selecting this parameter requires the switch to obtain its IP address from the BootP server. If a static IP address is defined, it will be ignored. When this option selected, the switch operates as follows:

- The switch continues to broadcast BootP requests, regardless of whether an in-band IP address is set from the console terminal.
- If the switch receives a BootP reply that contains an in-band IP address, the switch uses this new in-band IP address.
- If the switch does not receive a BootP reply, the switch cannot be managed using the in-band IP address set from the console terminal.

If an IP address is *not* currently in use, these actions take effect immediately. If an IP address *is* currently in use, these actions take effect only after the switch is reset or power cycled.

BootP Disabled

When this parameter is selected, the switch does not use BootP. The switch will operate in the following manner:

- The switch does not broadcast BootP requests, regardless of whether an IP address is set from the console terminal.
- The switch can be managed only by using the in-band switch IP address set from the console terminal.

These actions take effect after the switch is reset or power cycled, even if an IP address is not currently in use.

BootP or Last Address

Selecting this parameter allows the switch to use the last IP address received from the BootP server if the BootP server should become unreachable. When selected, this mode operates as follows:

- When the IP data is entered from the console terminal, the data becomes the in-band address of the switch and BootP requests are not broadcast. The switch can be managed using this in-band IP address.
- When the in-band IP address is not set from the console terminal, the switch broadcasts BootP requests until it receives a BootP reply containing an in-band IP address. If the switch does not receive a BootP reply that contains an in-band IP address within 10 minutes, the switch uses the last in-band IP address it received from a BootP server. This IP information is displayed in the Last BootP column.

If an IP address is *not* currently in use, these actions take effect immediately. If an IP address *is* currently in use, these actions take effect only after the switch is reset or power cycled.

Troubleshooting

Execute the following steps to diagnose your system if it should have issues obtaining an IP address using the BootP protocol:

- Check if the BootP server is accessible to the switch through the management VLAN.

- Check if the BootP server is configured with the proper MAC address of the device.
- Review the last BootP settings on the Console Interface.
- Place a packet analyzer on the network to investigate the problem.

Usage guidelines

Sample bootptab file

This section provides a sample BootP configuration file. The BootP server searches for this file, called bootptab (or BOOTPTAB.TXT, depending on your operating system), which contains the site-specific information (including IP addresses) needed to perform the software download and configuration. You can modify this sample BootP configuration file or create one of your own. A sample BootP configuration file follows:

```
# The following is a sample of a BootP configuration file that was
extracted
# from a Nortel Networks EZ LAN network management application.
Note that
# other BootP daemons can use a configuration file with a different
format.
#
# Before using your switch BootP facility, you must customize your
BootP
# configuration file with the appropriate data.
#
# Blank lines and lines beginning with '#' are ignored.
#
# Legend:
#
# first field -- hostname
# ht -- hardware type
# ha -- host hardware address
# tc -- template host (points to similar host entry)
# ip -- host IP address
# hd -- bootfile home directory
# bf -- bootfile
# EZ dt -- device type
# EZ fv -- firmware version
# EZ av -- agent version
# cs - TFTP server address for ASCII config file (optional)
#
# Fields are separated with a pipe (|) symbol. Forward slashes (/)
are
# required to indicate that an entry is continued to the next line.
#
# Caution
#
# Omitting a Forward slash (/) when the entry is continued to the
next
```

```
# line, can cause the interruption of the booting process or the
# incorrect image file to download. Always include forward slashes
# where needed.
#
# Important Note:
#
# If a leading zero (0) is used in the IP address it is calculated
as an
# octal number. If the leading character is "x" (upper or lower
case),
# it is calculated as a hexadecimal number. For example, if an IP
address
# with a base 10 number of 45 is written as .045 in the BOOTPTAB.TXT
file,
# the Bootp protocol assigns .037 to the client.
#
# Global entries are defined that specify the parameters used by
every device.
# Note that hardware type (ht) is specified first in the global
entry.
#
# The following global entry is defined for an Ethernet device.
Note that this
# is where a client's subnet mask (sm) and default gateway (gw) are
defined.
#
global1|/
|ht=ethernet|/
|hd=c:\opt\images|/
|sm=255.255.255.0|/
|gw=192.0.1.0|
#
# The following sample entry describes a BootP client:
bay1|ht=ethernet|ha=0060fd000000|ip=192.0.0.1|hd=c:\ezlan\images|b
f=Baystack470.txt
# Where:
# host name: bay1
# hardware type: Ethernet
# MAC address: 00-60-FD-00-00-00
# IP address: 192.0.0.0
# home directory of boot file: c:\ezlan\images
# ASCII config file: Baystack470.txt
# When ASCII configuration download is configured to perform auto
configuration
# on reset using BootP, the filename must be specified using the
'bf' keyword.
# If the ASCII configuration file is not resident on the BootP
server, the
```

```
# server address can be specified using the 'cs' keyword.
```

Supported keywords

The following keywords are supported in the bootptab file:

- ht -- hardware type
- hd -- home directory
- sm -- subnet mask
- gw -- gateways
- ha -- hardware address
- ip -- host IP address
- bf -- boot file
- cs -- configuration server

IP/BootP configuration retention on downgrade

When downgrading a unit with Release 3.0.3 software and later, the system defaults all configurations, except for the following:

- Stack operation mode
- IP configuration
- BootP mode

Previous releases of Ethernet Switch software retained the Stack Operational Mode only on software downgrade. This change allows a remotely accessed switch to maintain its accessibility after downgrade and does not require the user to re-enter this basic information, which remains unchanged after a downgrade.

Managing System Characteristics

The system allows you to view or configure system information such as:

- Base Unit
- Firmware Revision
- Hardware Deviation

- Hardware Revision
- ISVN
- Last Reset Type
- Local GBIC Type
- MAC Address
- Manufacturing Date
- Operation Mode
- Power Status
- Reset Count
- Serial Number
- Size of Stack
- Software Revision
- sysContact
- sysDescr
- sysLocation
- sysName
- sysObjectID
- sysServices
- sysUpTime

These parameters provide general system information.

System Characteristics Configuration Requirements

The only requirement to configure these system parameters is a connection to the device through the network or the serial port.

System Characteristics User Interface Support

The System Characteristics parameters may be manipulated through all user interfaces. Table 66 indicates whether the user has read (r), read-write (rw), or no access to the parameter through the listed user interface.

Table 66 System Characteristics User Interface Support

Parameter	Default	Menu Interface	CLI	Web	Device Manager
Base Unit	na	r	r	no	r
Firmware Revision	na	r	r	r	r
Hardware Deviation	na	r	r	r	no
Hardware Revision	na	r	r	r	r
ISVN	2	r	r	r	r
Last Reset Type	na	r	r	no	no
Local GBIC / MDA Type	none	r	r	r	r
MAC Address	na	r	r	r	r
Manufacture Date	na	r	r	r	no
Operation Mode	na	r	r	r	r
PoE Module Firmware	na	no	r	r	no
Power Status	primary power	r	r	r	r
Reset Count	1	r	r	no	no
Serial number	na	no	r	r	r
Size of Stack	na	r	r	r	r
Software Revision	na	r	r	r	r
sysContact	blank string	rw	rw	rw	rw

Table 66 System Characteristics User Interface Support

Parameter	Default	Menu Interface	CLI	Web	Device Manager
sysDescr	hw / sw versions	r	r	r	r
sysLocation	blank string	rw	rw	rw	rw
sysName	blank string	rw	rw	rw	rw
sysObjectID	Device OID	r	r	r	no
sysServices	3	r	r	no	no
sysUpTime	na	r	r	r	r

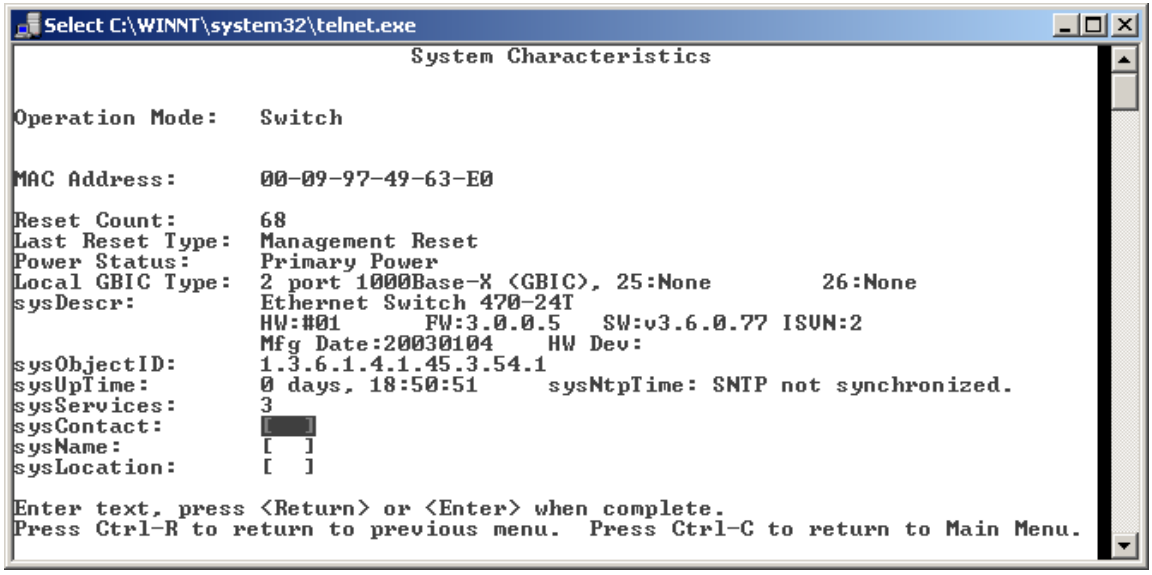
Managing system characteristics using the Console Interface

Use the following procedure to manage the System Characteristics screen using the Console Interface on the Ethernet Switch:

1. Connect to the device through the serial port or through a Telnet connection.
2. After the Nortel logo is displayed, press [Ctrl]-Y to display the Main Menu.

3 Select the System Characteristics from the main menu. Figure 91 displays the Console Interface System Characteristics screen.

Figure 91 Console Interface System Characteristics screen



Configuration Parameters

The fields on the Console Interface System Characteristics are described in Table 67.

Table 67 Fields in the Console Interface system characteristics

Field	Description
Operation Mode	Read-only field that indicates the operation mode of the unit, for example: • When the unit is part of a stack configuration, the (read-only) field indicates the unit is operational in a stack, and lists the current unit number of this switch. • When the unit is *not* part of a stack configuration (operating stand-alone), the read-only field indicates the unit is operating as a switch. When in this operation mode, the Size of Stack and Base Unit fields do not appear.
Size of Stack	This read-only field only appears when the switch is participating in a stack configuration. This field indicates the number of units configured in the stack configuration (1 to 8 units maximum).

Table 67 Fields in the Console Interface system characteristics

Field	Description
Base Unit	This read-only field only appears when the switch is participating in a stack configuration. This field indicates the unit number of the switch that is currently operating as the base unit.
MAC Address	Contains the MAC address of the switch or, when the switch is participating in a stack configuration, the MAC address of the stack configuration.
Reset Count	This read-only field indicates the number of resets since the operational firmware was first loaded on the switch. Default Value 1. Range 0 to 232 -1 (4,294,967,295)
Last Reset Type	This read-only field identifies the last type of reset. Possible values include: ■ Power Cycle ■ Software Download ■ Management Reset ■ Management Factory Reset
Power Status	This read-only field indicates the current power source (primary, RPSU, or both). Possible values include: ■ Primary Power ■ Redundant Power ■ Primary and Redundant Power
Local MDA / GBIC Type	This read-only field indicates the MDA or GBIC type that is configured in this unit.
Inter-Switch Version Number (ISVN)	See the Release Notes for possible restrictions surrounding the ISVN versions required in a stack.
sysDescr	A read-only field that specifies hardware and software versions.
sysObjectID	A read-only field that provides a unique identification of the switch, which contains the vendor's private enterprise number.
sysUpTime	A read-only field that shows the length of time since the last reset. Note that this field is updated when the screen is redisplayed.
sysServices	A read-only field that indicates the switch's physical and data link layer functionality.
sysContact	The name and phone number of the person responsible for the switch. Range: Any ASCII string of up to 56 printable characters.
sysName	A name that uniquely identifies the switch. Range: Any ASCII string of up to 56 printable characters.
sysLocation	The physical location of the switch. Range: Any ASCII string of up to 56 printable.

Troubleshooting

If you face any problems while configuring any of these parameters, follow these procedures:

- Check if have exceeded the number of characters allowed by the user interface.
- Ensure you have only used printable characters in any of the strings.

Usage Guidelines

The various user interfaces allow different lengths for the following SNMP variables: sysDesc, sysLocation, and sysContact.

The following is a list of variable lengths allowed by the various user interfaces:

- CLI allows 126 characters
- Menu Interface allows 56 characters
- Device manager allows 256 characters through the Edit -> Chassis menu
- Device manager allows 32 characters through the Edit -> Chassis -> Base
- Unit Info (or Stack Info) menu
- ACG will only generate strings of 63 characters in length

Not all the information that is available in the sysDescr field on the System Characteristics screen is available on all interfaces.

Table 68 displays the parameters in the SysDescr field that are available in the various interfaces.

Table 68 SysDescr field interface support

Parameter	Menu Interface	CLI	Web Interface	Device Manager
Product Name	•	•	•	•
Hardware revision	•	•	•	•
Firmware revision	•	•	•	•
Software revision	•	•	•	•

Table 68 SysDescr field interface support

Parameter	Menu Interface	CLI	Web Interface	Device Manager
Hardware deviation	•	•	•	
Manufacturing date	•	•	•	

Note: Only Device Manager allows you to retrieve the serial number for all units in a stack.

Software Management

Downloading software

The Ethernet Switch uses non-volatile memory to store the switch software image. The non-volatile memory allows you to update the software image with a newer version without changing the switch hardware. An in-band connection between the switch and the TFTP load host is required to download the software image. The Ethernet Switch supports the following three types of software:

- Runtime Image
- Boot Image (also referred to as the Diagnostic Image and Firmware Image)
- Power-over-Ethernet (PoE) Image

The following section outlines the tools and methods supported by the Ethernet Switch to download different software onto your system.

Software can be downloaded to the switch by the following methods:

- Immediate Download
- Runtime Image
- Boot Image
- Power-over-Ethernet (PoE) Image
- Download if Newer

- Download without resetting
- Runtime Image

Immediate Download

You may use any of the user interfaces to initiate an immediate download of any of the software components onto the system.

Download Image if newer

The system has the ability to download the runtime image only if the image is newer than the version that is currently loaded on the switch. When this feature is enabled, the system checks to see if there is a newer version of software available on the TFTP server whenever it reboots.

Download without resetting

The Download without resetting feature allows you to upgrade the Runtime image or Diagnostic image without resetting the unit.

Note: After downloading the image without resetting, the Web-based management interface is not available until the switch or stack is rebooted.

This feature is only available through the Console Interface or the CLI.

Feature Requirements

To download the software image, you need a properly configured Trivial File Transfer Protocol (TFTP) server in your network, and an IP address for the switch.

Software Management User Interface Support

Table 69 lists the interfaces that support the downloading of software into the Ethernet Switch.

Table 69 Interfaces that support Ethernet Switch software download

Parameter	Menu Interface	CLI	Web Interface	Device Manager	Parameter
Download Runtime Image	blank	rw	rw	rw	rw
Download Boot / Firmware Image	blank	rw	rw	rw	rw
Download PoE Image	blank	none	rw	none	none
Download image if newer	rw	rw	rw	rw	rw
Download image without resetting	rw	none	rw	none	none

Software Management using the Console Interface

The Software Download screen allows you to revise the Ethernet Switch software image located in non-volatile flash memory.

To open the Software Download screen:

1 Choose Software Download (or press f) from the main menu. The Software Download screen appears as depicted in Figure 92.

Caution: Do not interrupt power to the device during the software download process. If the power is interrupted, the firmware image can become corrupted.

Achtung: Unterbrechen Sie die Stromzufuhr zum Gerät nicht, während die Software heruntergeladen wird. Bei Unterbrechung der Stromzufuhr kann das Firmware-Image beschädigt werden.

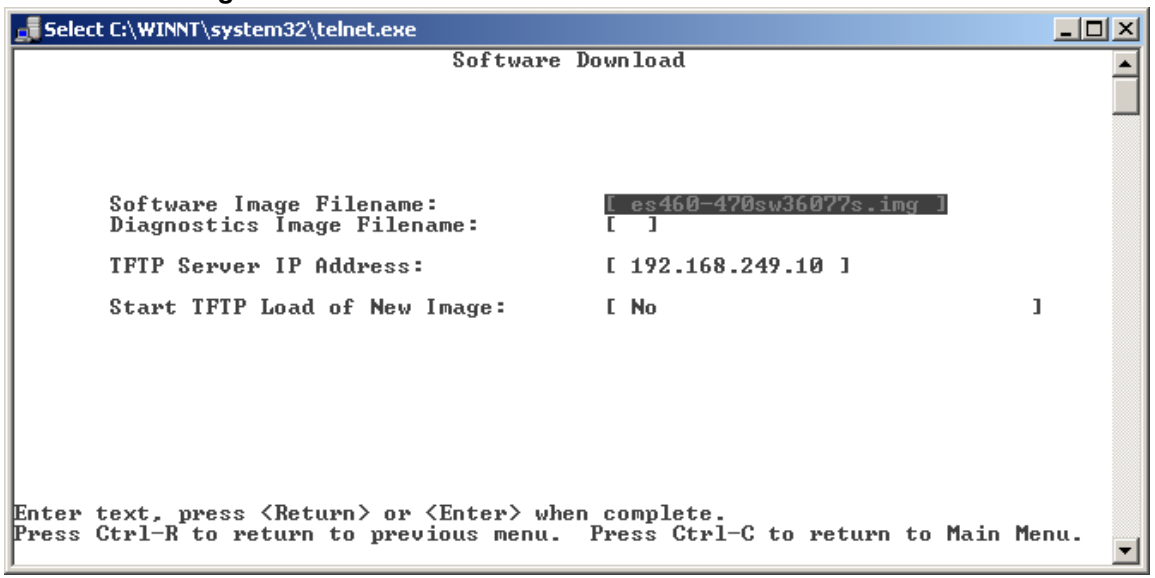
Attention: Ne pas couper l'alimentation de l'appareil pendant le chargement du logiciel. En cas d'interruption, le programme résident peut être endommagé.

Precaución: No interrumpa la alimentación del dispositivo durante el proceso de descarga del software. Si lo hace, puede alterar la imagen de la programación (firmware).

Attenzione: Non interrompere l'alimentazione elettrica al dispositivo durante il processo di scaricamento del software. In caso di interruzione, l'immagine firmware potrebbe danneggiarsi.

注意：ソフトウェアをダウンロードしているとき、ディバイスへの電源を切らないでください。電源を切ると、ファームウェアのイメージを損う恐れがあります。

Figure 92 Console Interface Software Download screen



You can monitor the software download process by observing the LEDs.

2. Enter the name of the file that you wish to download from your TFTP server in the appropriate field. The Console Interface lets you download the runtime image or the firmware image from the server.
3. Enter the IP address of the TFTP server in the TFTP Server IP Address field.
4. Select the appropriate option from the Start TFTP Load of New Image by cycling through the various parameters and pressing enter to initiate the download.
5. The unit reboots after the download.

Note: The Console Interface and CLI both provide the option to download an image file without rebooting.

Note: If your station cannot ping the TFTP server during the downloading process, you may receive the following message:
`Image is Invalid`
The problem is that the TFTP server is not reachable, rather than any problems with the image.

LED Indications during the download process

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Be careful not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

During the download process, the switch is not operational. You can monitor the progress of the download process by observing the LED indications.

Console Interface Software Download Configuration Parameters

The following configuration parameters are available through the Console Interface.

Table 70 describes the configuration parameters available through the Console Interface.

Table 70 Software Download screen fields

Field	Description
Software Image Filename	The Ethernet Switch software image load file name. Default Value Zero-length string Range An ASCII string of up to 30 printable characters
Diagnostics Filename	The Ethernet Switch diagnostics file name. Default Value Zero-length string Range An ASCII string of up to 30 printable characters

Table 70 Software Download screen fields (Continued)

Field	Description	
TFTP Server IP Address	The IP address of your TFTP load host.	
	Default Value	0.0.0.0 (no IP address assigned)
	Range	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Start TFTP Load of New Image	Specifies whether to start the download of the switch software image (default is No). Use the spacebar to toggle the selection to the one you want. Press [Enter] to initiate the software download process.	
	NOTE: The software download process can take up to 60 seconds to complete (or more if the load host path is congested or there is a high volume of network traffic).	
	To ensure that the download process is not interrupted, do not power down the switch for approximately 10 minutes.	
	Default Value	No
	Range	No, Software Image, Diagnostics, Software Image If Newer, Download image without reset, Download diag without reset.

Troubleshooting

If you encounter any problems while downloading software to the switch, take the following steps:

- Check that the Ethernet Switch is logically connected to the TFTP server by pinging the TFTP server.
- Check that the TFTP server is running on the management station.
- Check that the target download file is available on the TFTP server in the correct directory.

Configuration Management

The Configuration Management feature allows you to store and retrieve the configuration parameters of an Ethernet Switch or stack to a TFTP server. This feature supports two different methods for managing the system configuration files:

- Binary configuration file management

- ASCII configuration file management

Managing Binary Configuration Files

The Ethernet Switch stores its configuration information on the system flash in a format that can be easily read by the operating system. When configured in a stack, each Ethernet Switch maintains its own switch parameters. This includes port speed, VLAN attachment and PVID information. All of this data cannot be saved to the Base Unit. The Base Unit stores Trunk information, both MLT and DMLT.

When you upload a backup of the configuration file to a TFTP server, the switch converts the configuration information in flash memory into a single file that can easily be stored on a TFTP server. In the case of a stack of switches, the system concatenates the configuration file from each of the units in the stack and uploads a single aggregate binary configuration file to the TFTP server.

Enable/Disable Autosave

By default, every 60 seconds the Ethernet Switch checks whether a configuration change has occurred, or if a log message has been written to non-volatile storage. If one of these two events has occurred, the system automatically saves its configuration and the non-volatile log to flash. Also, the system automatically saves the configuration file if a system reset command is invoked by the user.

Note: Do not power off the switch within 60 seconds of changing any configuration parameters. Doing so causes loss of changes in the configuration parameters.

You may enable or disable the autosave feature. You may specify that the configuration changes be saved to flash, when the autosave feature is disabled.

Note: You can use the CLI command `copy config nvram` to force a manual save of the configuration when autosave is disabled.

You must use CLI to enable or disable autosave; the default value is enabled. This setting is saved across resetting the unit.

Forcing Immediate Configuration Save

The Ethernet Switch allows you to force an immediate save of the configuration files to non-volatile random access memory (NVRAM). When this feature is used, the system checks to see if any changes have been made to the system configuration since the last configuration save. If a change has been made, the updated configuration file is written to NVRAM.

This feature is only available through the CLI.

Managing Binary Configuration Files

In order to manage binary configuration files, you must have a TFTP server with read / write access to the directory of the TFTP server, in order to upload a binary configuration file.

Managing Binary Configuration Files User Interface Support

You can manage the binary configuration file through any of the following interfaces:

Table 71 lists the various user interfaces supporting the management of binary configuration files.

Table 71 User interface support

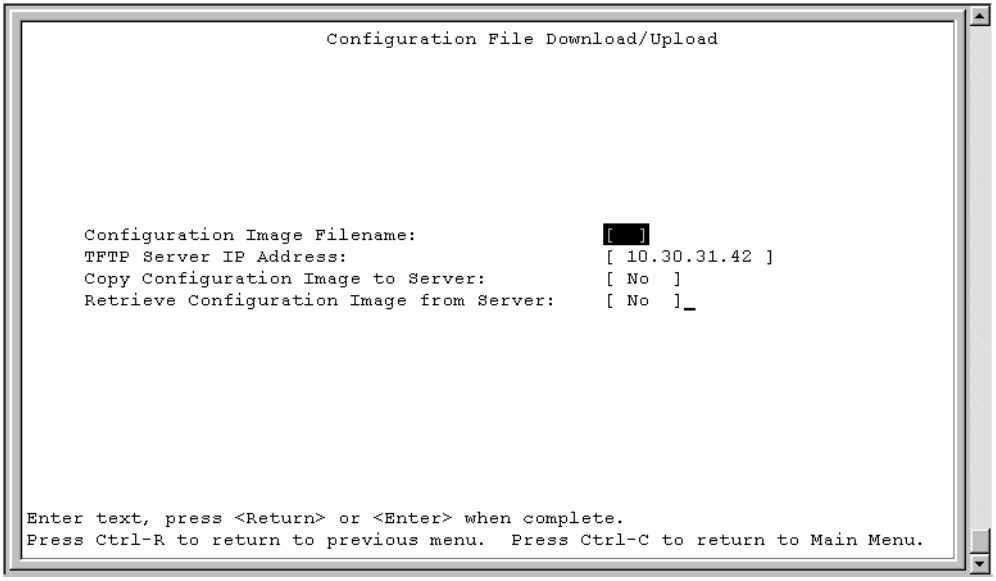
Parameter	Default	Menu Interface	CLI	Web Interface	Device Manager
Backup Binary Configuration	na	rw	rw	rw	rw
Restore Binary Configuration	na	rw	rw	rw	rw
Enable / Disable Autosave	enabled	no	rw	no	no
Force Immediate Configuration Save	na	no	rw	no	no

Binary Configuration File Management Console Interface Support

The Configuration File Menu screen allows you to upload and download the configuration parameters of an Ethernet Switch to a TFTP server.

Figure 93 shows the Configuration File Download/Upload screen for the Console Interface.

Figure 93 Configuration file download/upload screen



These options allow you to store your switch configuration parameters on a TFTP server. You can retrieve the configuration parameters of a stand-alone switch, and use the retrieved parameters to automatically configure a replacement switch. You must set up the file on your TFTP server, and set the filename read-write permission to enabled before you can save the configuration parameters

Table 72 describes the fields on the Console Interface configuration upload/ download screen.

Table 72 Configuration File Download/Upload screen fields

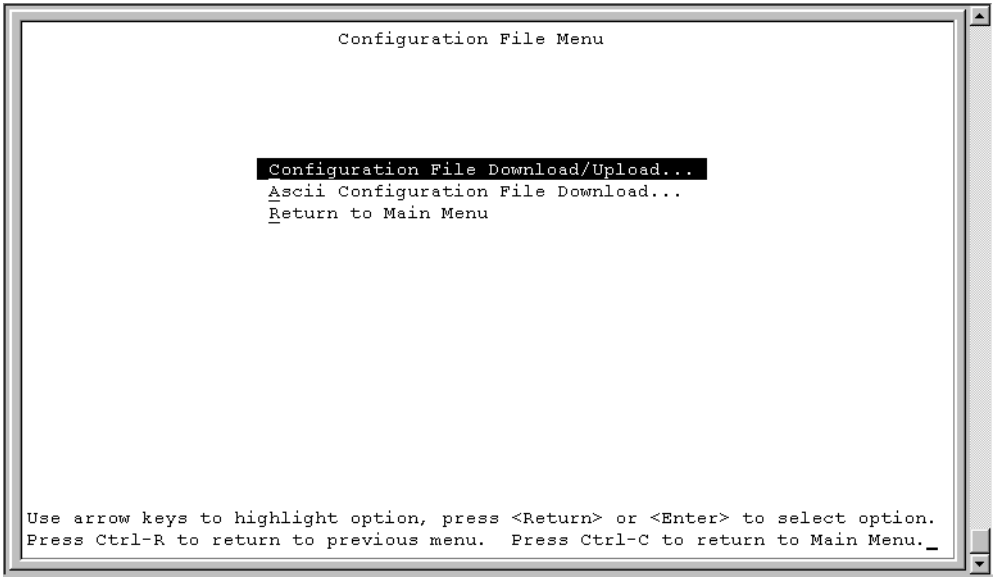
Field	Description
Configuration Image Filename	The file name you have chosen for the configuration file. Choose a meaningful file name that will allow you to identify the file for retrieval when required. The file must already exist on your TFTP server and must be read-write enabled. Default Value Zero-length string Range An ASCII string of up to 30 printable characters
TFTP Server IP Address	The IP address of your TFTP load host. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Copy Configuration Image to Server	Specifies whether to copy the presently configured switch parameters to the specified TFTP server (default is No). Use the spacebar to toggle the selection to Yes. Press [Enter] to initiate the process. Default Value No Range Yes, No
Retrieve Configuration Image from Server	Specifies whether to retrieve the stored switch configuration parameters from the specified TFTP server (default is No). If you choose Yes, the download process begins immediately and, when completed, causes the switch to reset with the new configuration parameters. Use the spacebar to toggle the selection to Yes. Press [Enter] to initiate the process. Default Value No Range Yes, No
Target Unit for Retrieve	Specifies the binary configuration file corresponding to a particular unit number to download to a stand-alone unit. Range 1–8

Creating a Backup Binary Configuration File

Follow this procedure to upload a Binary Configuration using the Console Interface:

1 Choose Configuration File Menu from the main menu. Figure 94 depicts the Configuration file menu.

Figure 94 Configuration file menu



2 Choose Configuration File Download/Upload from the Configuration File Menu.

3 Enter the name of the backup binary configuration file that you are going to create on the TFTP server in the Configuration Image Filename Field.

4 Enter the IP address of the TFTP server in the TFTP Server IP Address Field.

5 Cycle through the options in the Copy Configuration Image to Server field by pressing the space bar; and select Yes.

6 Press the Enter key to activate the upload of the configuration

Restoring a Backup Binary Configuration File

Follow this procedure to restore a backup binary configuration file from a TFTP server:

1 Choose Configuration File Menu from the main menu.

2. Choose Configuration File Download/Upload from the Configuration File Menu.
3. Enter the name of the backup binary configuration file that you are going to retrieve from the TFTP server in the Configuration Image Filename Field.
4. Enter the IP address of the TFTP server in the TFTP Server IP Address Field.
5. If you are retrieving the file for a unit in a stack, cycle through the options in the Target Unit for Retrieval Field, and select the number of the unit whose configuration you wish to retrieve.
6. Cycle through the options in the Retrieve Configuration Image from Server field by pressing the space bar; and select Yes.
7. Press the Enter key to retrieve the configuration file.
8. When you press the Enter key, the software:
   - Contacts the TFTP server
   - If the file is for a unit in a stack, retrieves the configuration file for the entire stack and extracts the target unit's configuration
   - Writes the configuration to flash
   - Resets and performs reconfiguration of the unit

Troubleshooting

If you encounter any problems while downloading the software, take the following steps:

- Check that the Ethernet Switch is logically connected to the TFTP server by pinging the TFTP server.
- Check that the TFTP server is running on the management station.
- If you are downloading a binary configuration file, ensure that the target download file is available on the TFTP server in the correct directory.
- If you are uploading a binary configuration file, ensure that you have read-write privileges on the target server.

Usage Guidelines

- Although most configuration parameters are saved to the configuration file, certain parameters are not saved. The following parameters are not saved in the binary configuration file:
  - -- In-Band Switch IP Address
  - -- In-Band Subnet Mask
  - -- Default Gateway
  - -- Console Read-Only Switch Password
  - -- Console Read-Write Switch Password
  - -- Configuration Image Filename
  - -- TFTP Server IP Address
- The Configuration File feature can be used only to copy stand-alone switch configuration parameters to other stand-alone switches.
- A configuration file obtained from a stand-alone switch can be used only to configure other stand-alone switches that have the same firmware revision and model type as the donor stand-alone switch.
- When configuration changes are written to non-volatile memory, a trap (bsnConfigurationSavedToNvram) is sent to the trap receiver, indicating that a change has occurred to the configuration of the device. This trap also appears as an event in the volatile system log.

Managing ASCII Configuration Files

The Ethernet Switch allows you to manage your system configuration using standard text files. You can create a series of CLI commands and upload them to the Ethernet Switch. Also, by using the ASCII Configuration Generator feature, the switch can display the current configuration as a series of CLI commands.

Configuring the Switch using ASCII Configuration Files

Ethernet Switches can download a user-editable ASCII configuration file from a TFTP server. You can load the ASCII configuration file automatically at boot time or on demand using the management systems (console menus or CLI). Once downloaded, the configuration file automatically configures the switch according to the Command Line Interface (CLI) commands in the file.

This feature allows the flexibility of generating command configuration files that can be use on several switches with minor modifications. Use a text editor to edit the ASCII configuration; the command format is the same as that of the CLI.

ASCII Configuration Generator

The ASCII Configuration Generator (ACG) allows you to display or save the configuration settings of the switch to an external ASCII configuration file consisting of a series of CLI commands. This editable ASCII configuration file can be uploaded to a switch from an external file server.

Note: You must reset the switch to the factory default settings before uploading the ACG-generated ASCII configuration file. Resetting the switch to factory default settings will cause loss of connectivity and loss of the current configuration of the switch.

The ASCII configuration file contains configuration settings for the following network management applications:

- COPS
- Core applications (system information, topology, etc.)
- Custom Banner
- Default Command Interface
- EAPOL
- IP Configuration
- IP Manager
- MAC-Based Security
- Multilink Trunking
- Spanning Tree
- Port configuration
- Port Mirroring
- QoS
- Quality of Service (QoS)
- RMON
- Stack Info
- System Logging

- VLAN configuration
- RMON

The ACG is available only from the Command Line Interface (CLI).

ASCII Configuration File Management

In order to take full advantage of the ASCII Configuration tools, you need to have a TFTP server available on the network and a text editor to customize the text-based configuration files.

ASCII Configuration File Management User Interface Support

Table 73 identifies the support available on the various user interfaces.

Table 73 User interface support for ASCII Configuration file

Parameter	Default	Menu Interface	CLI	Web Interface	Device Manager
ASCII Configuration Filename	blank	rw	rw	no	rw
TFTP Server IP Address	0.0.0.0	rw	rw	rw	rw
Last Manual Configuration Status	Passed	r	r	no	r
Last Auto Configuration Status	Passed	r	r	no	r
Auto Configuration on Reset using local filename	Disabled	rw	rw	no	rw
Auto Configuration on Reset using BootP filename	Disabled	rw	rw	no	rw
Retrieve Configuration File from Server	No	rw	rw	no	rw

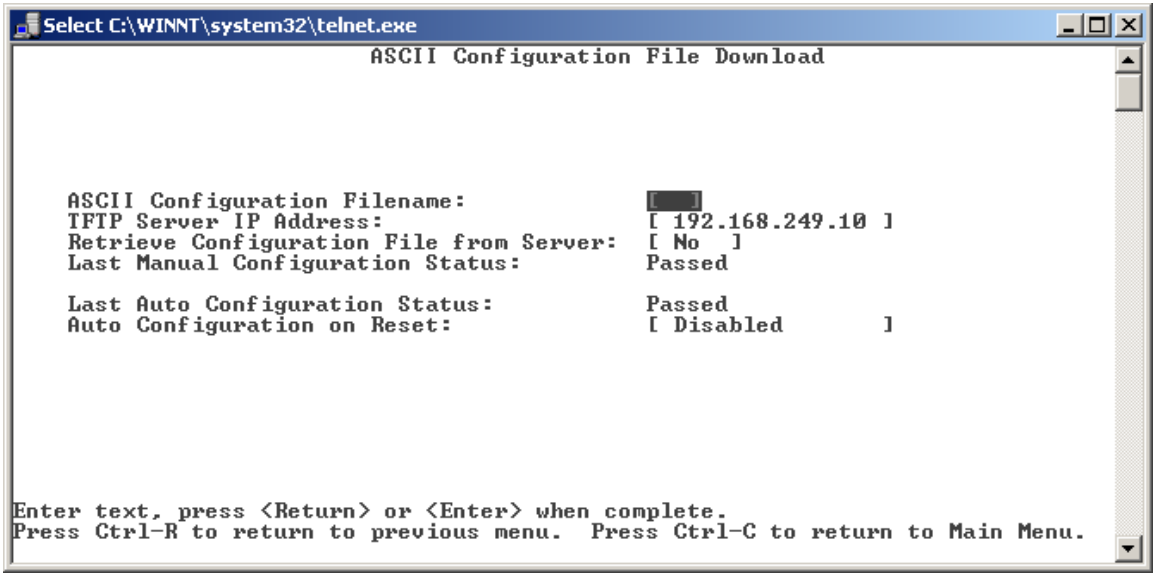
Table 73 User interface support for ASCII Configuration file

Parameter	Default	Menu Interface	CLI	Web Interface	Device Manager
Send ASCII Config file to TFTP Server	No	no	rw	no	rw
Display ASCII Config file on screen	No	no	rw	no	no

Using the Console Interface

The Console Interface enables you to upload and retrieve an ASCII configuration file to and from a TFTP to configure the system. Figure 95 depicts the ASCII configuration file download screen.

Figure 95 ASCII configuration file download screen



ASCII Configuration File Download Console Interface field descriptions

Table 74 on page 279 describes the various fields that appear on the Console Interface ASCII Configuration File Download screen.

Table 74 ASCII Configuration File Download screen fields

Field	Description
ASCII Configuration Filename	Enter the file name you have chosen for the ASCII configuration file. Choose a meaningful file name that will allow you to identify the file for retrieval when required. The file must already exist on your TFTP server and must be read-write enabled. Default Value Zero-length string Range An ASCII string of up to 30 printable characters
TFTP Server IP Address	The IP address of your TFTP load host. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Retrieve Configuration File from Server	Specifies whether to retrieve the stored switch ASCII configuration file from the specified TFTP server (default is No). If you choose Yes, the download process begins immediately and, when completed, causes the switch to be configured according to the CLI commands in the file. Use the spacebar to toggle the selection to Yes. Press [Enter] to initiate the process. Default Value No Range Yes, No
Last Manual Configuration Status	The system displays if the last manual configuration passed or failed. Default Value Passed Range Passed, Failed
Last Auto Configuration Status	The system displays if the last automatic configuration passed or failed. Default Value Passed Range Passed, Failed
Auto Configuration on Reset	Allows you to choose to Disabled, Use Configured, or Use BootP: • Disabled—Auto configuration on reset is disabled. • Use Configured—Use manually configured ASCII configuration filename and TFTP server address for auto configuration on reset. • Use BootP—Retrieve ASCII configuration filename, and optionally server address, using BootP, when BootP is enabled, and perform auto configuration on reset using these parameters. Note: Refer to "Sample bootptab file" on page 253 for a sample BootP configuration file. Default Value Disabled Range Disabled, Use Configured, Use BootP

Retrieving an ASCII Configuration file from the TFTP server

The ASCII Configuration File Download screen allows you to download an ASCII configuration file containing CLI commands from a TFTP server to configure the switch.

1. Choose Configuration File Menu from the main menu
2. Choose ASCII Configuration File Download from the Configuration File Menu to open the ASCII Configuration File Download screen.
3. Enter the name of the file you wish to retrieve from the TFTP server in the ASCII Configuration Filename field.
4. Enter the TFTP Server IP Address in the TFTP Server IP Address field.
5. Cycle through the options in the Retrieve Configuration file from Server field and select Yes.
6. Press the Enter key to initiate the file transfer

Retrieving an ASCII Configuration file from the TFTP server on reset

You can configure the device to retrieve an ASCII configuration file upon system startup. The system will retrieve the filename that is currently configured in flash or it can obtain the name of the target ASCII configuration from the BootP server.

1. Choose Configuration File Menu from the main menu
2. Choose ASCII Configuration File Download from the Configuration File Menu to open the ASCII Configuration File Download screen.
3. Enter the TFTP Server IP Address in the TFTP Server IP Address field.
4. Enter the name of the file you wish to retrieve from the TFTP server in the ASCII Configuration Filename field. If you wish for the system to obtain the filename from the BootP sever, you do not need to fill out this field. You must configure your BootP to supply the filename.
5. Cycle through the options in the Auto Configuration on Reset field and select Use configured if you wish to use the filename entered on the switch. If you wish to have the BootP server provide the filename, select the Use BootP option.
6. Press the Enter key to store the configuration in flash.

7 Reset your switch to verify that the configuration works.

Usage guidelines

- The maximum size for an ASCII configuration file is 100 KBs; larger configuration files must be split into multiple files.

Using SNTP

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 may be overloaded or currently inoperable.

The system retries connecting with the NTP server a maximum of 3 times, with 5 minutes between each retry. If the connection fails after the 3 attempts, the system waits for the next synchronization time (the default is 24 hours) and begins the process again.

Using SNTP provides a real-time timestamp for the software, shown as Greenwich Mean Time (GMT).

If SNTP is enabled (the default value is disabled), the system synchronizes with the configured NTP server at boot-up and at user-configurable periods thereafter (the default sync 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 connecting to the secondary NTP server only if the primary NTP server is unresponsive.

For instructions on configuring SNTP using the CLI, see "Setting time on network elements using Simple Network Time Protocol (SNTP)" on page 400. For instructions on configuring SNTP using Device Manager, see "Working with SNTP" on page 460.

Using DNS to ping and Telnet

Using the DNS client, you can ping or Telnet to a host server or to a host by name.

To use this feature, you must configure at least one domain name server; you may also configure a default domain name. If you configure a default domain name, that name is appended to host names that do not contain a dot. The default domain name and addresses are saved in NVRAM.

The host names for ping and Telnet cannot be longer than 63 alphanumeric characters, and the default DNS domain name cannot be longer than 255 characters.

You can use the CLI to configure the DNS client. For more information, see Chapter 3, “CLI Basics,” on page 153.

Changing HTTP port number

Beginning with Release 3.1 software, you can configure the HTTP port. This feature provides enhanced security and network access.

The default HTTP port typically used to communicate between the Web client and the server is port 80. With this feature, you can change the HTTP port.

You can modify the HTTP port while the switch is running. The HTTP port value is saved in NVRAM, and is saved across reboots of the switch.

Configuring with CLI

You configure the HTTP port number using the following CLI commands:

- show http-port command
- http-port command
- default http-port

For details on these CLI commands, see *Configuring and Managing Security* (217104-A).

Diagnosing and correcting problems

Before you perform the problem-solving steps in this section, cycle the power to the switch (disconnect and then reconnect the AC power cord); then verify that the switch follows the normal power-up sequence.

Warning: To avoid bodily injury from hazardous electrical current, never remove the top cover of the device. There are no user-serviceable components inside.

Warnung: Um Verletzungsgefahr durch einen elektrischen Stromschlag auszuschließen, nehmen Sie niemals die obere Abdeckung vom Gerät ab. Im Geräteinnern befinden sich keine Komponenten, die vom Benutzer gewartet werden können.

Avertissement: Pour éviter tout risque d'électrocution, ne jamais retirer le capot de l'appareil. Cet appareil ne contient aucune pièce accessible par l'utilisateur.

Avertencia: A fin de evitar daños personales por corrientes eléctricas peligrosas, no desmonte nunca la cubierta superior de este dispositivo. Los componentes internos no son reparables por el usuario.

Avviso: Per evitare lesioni fisiche dovute a scariche pericolose di corrente, non rimuovere mai il coperchio superiore del dispositivo. I componenti interni non possono essere manipolati dall'utente.

警告：危険な電流から身体を保護するために、ディバイスの上部カバーを決して取り外さないでください。内部には、ユーザが扱うコンポーネントはありません。

Normal power-up sequence

In a normal power-up sequence, the LEDs appear as follows:

1. After power is applied to the switch, the Pwr (Power) LED turns on within 5 seconds.
2. The switch initiates a self-test, during which the port LEDs display various patterns to indicate the progress of the self-test.
3. Upon successful completion of the self-test (within 10 seconds after power is applied), the Status LED turns on.
4. The remaining port LEDs indicate their operational status, as described in Table 75.

Table 75 Corrective actions

Symptom	Probable cause	Corrective action
All LEDs are off.	The switch is not receiving AC power. The fans are not operating or the airflow is blocked, causing the unit to overheat.	Verify that the AC power cord is fastened securely at both ends and that power is available at the AC power outlet. Verify that there is sufficient space for adequate airflow on both sides of the switch.
		Note: Operating temperature for the switch must not exceed 40°C (104°F). Do not place the switch in areas where it can be exposed to direct sunlight or near warm air exhausts or heaters.
The Activity LED for a connected port is off or does not blink (and you have reason to believe that traffic is present).	The switch is experiencing a port connection problem. The switch's link partner is not autonegotiating properly.	See "Port connection problems "" next.
The Status LED is off.	A fatal error was detected by the self-test.	Cycle the power to the switch (disconnect and then reconnect the AC power cord). If the problem persists, replace the switch.
The Status LED is blinking.	A nonfatal error occurred during the self-test.	Cycle the power to the switch (disconnect and then reconnect the AC power cord). If the problem persists, contact the Nortel Technical Solutions Center.

Port connection problems

You can usually trace port connection problems to either a poor cable connection or an improper connection of the port cables at either end of the link. To remedy these types of problems, make sure that the cable connections are secure and that the cables connect to the correct ports at both ends of the link.

Port connection problems are also traceable to the autonegotiation mode or the port interface.

Autonegotiation modes

Port connection problems can occur when a port (or station) is connected to another port (or station) that is not operating in a compatible mode (for example, connecting a full-duplex port on one station to a half-duplex port on another station).

Note: You cannot *enable* autonegotiation using GBIC ports.

The Ethernet Switch negotiates port speeds according to the IEEE 802.3u autonegotiating standard. The switch adjusts (autonegotiates) its port speed and duplex mode to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode as follows:

- If the connected station uses a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiating standard, the switch cannot negotiate a compatible mode for correct operation.
- If the Autonegotiation feature is not present or not enabled at the connected station, the switch may not be able to determine the correct duplex modes.

In both situations, the switch autosenses the speed of the connected station and, by default, reverts to half-duplex mode. If the connected station is operating in full-duplex mode, it cannot communicate with the switch.

To correct the mode mismatch problem

1 Use the Port Configuration screen to disable autonegotiation for the suspect port (see "Port Configuration screen" on page 142).

2 Manually set the Speed/Duplex field to match the speed/duplex mode of the connected station.

You may have to try several settings before you find the correct speed/duplex mode of the connected station.

If the problem persists

1 Disable the Autonegotiation feature at the connected station.

2 Manually set the speed/duplex mode of the connected station to the same speed/duplex mode you manually set for the switch port.

Note: Nortel recommends that you manually set the switch port to the desired speed/duplex mode when you connect to any of the following Nortel products:

- Ethernet Switch 450 product family
- Ethernet Switch 410 product family

Chapter 7
Ethernet Port Management

This chapter discusses the following topics:

Autosensing and Autonegotiation

The Ethernet Switches 460 and 470 are autosensing and autonegotiating devices:

- The term *autosense* refers to a port's ability to *sense* the speed of an attached device.
- The term *autonegotiation* refers to a standardized protocol (IEEE 802.3u) that exists between two IEEE 802.3u-capable devices. Autonegotiation allows the switch to select the best of both 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 802.3u autonegotiation standard. In this case, because the switch cannot sense the duplex mode of the attached device, the switch reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the Ethernet Switches, the ports negotiate down from 100 Mbps speed and full-duplex mode, until the attached device acknowledges a supported speed and duplex mode.

Note: Autonegotiation is enabled by default on the front panel 10/100BASE-TX ports.

Custom Autonegotiation Advertisements

Custom Autonegotiation Advertisements (CANA) allows you to customize the capabilities that you advertise. For example, if a port is capable of 10/100/1000 full duplex operation, the port can be configured to only advertise 10 half-duplex capabilities.

CANA allows you to control the capabilities that are advertised by the Ethernet Switches as part of the autonegotiation process. In the current software releases, autonegotiation can either be enabled or disabled.

When autonegotiation is disabled, the hardware is configured for a single (fixed) speed and duplex value. When autonegotiation is enabled, the advertisement made by the product is a constant value based upon all speed and duplex modes supported by the hardware.

When autonegotiating, the switch selects the highest common operating mode supported between the switch and its link partner.

In certain situations, it is useful to autonegotiate a specific speed and duplex value. In these situations, the switch can allow for attachment at an operating mode other than its highest supported value.

For example, if the switch advertises only a 100 Mbps full-duplex capability on a specific link, then the link goes active only if the neighboring device is also capable of autonegotiating a 100 Mbps full-duplex capability. This prevents mismatched speed/duplex modes if customers disable autonegotiation on the neighboring device.

CANA is available through the Command Line Interface (CLI) (see "Enabling Custom Autonegotiation Advertisements (CANA)" on page 428) and the Device Manager (JDM) (see "Interface tab for a single port" on page 468).

Note: The CANA feature is available only for built-in 10/100 Ethernet ports.

When custom autonegotiation advertisements is in use on a port, autonegotiation is displayed as custom in the Console Interface and Web-based management interface.

Copper GBIC support

A new full-sized GBIC is supported. This GBIC supports 1000BaseT and works only on Ethernet Switch 470 units. For more information, see "GBIC compatibility matrix" on page 289.

GBIC compatibility matrix

Table 76 lists the Gigabit Interface Converters (GBIC) supported by Release 3.6 software.

Table 76 GBIC compatibility matrix

GBIC	Standard or SFP	Order number	Comment
1000Base-T Copper	Standard (RJ-45 connector)	AA1419042	Ethernet Switch 470 Only
1000Base-SX	Standard (SC connector)	AA1419001	
1000Base-LX	Standard (SC connector)	AA1419002	
1000Base-XD	Standard (SC connector)	AA1419003	Extended distance 50km
1000Base-ZX	Standard (SC connector)	AA1419004	Extended distance 70km

Table 76 GBIC compatibility matrix (Continued)

GBIC	Standard or SFP	Order number	Comment
1000BaseWDM	Standard (SC connector)	From AA1419017 to AA1419024	1470nm-1610nm (in 20nm intervals)
1000Base-SX	SFP (LC connector)	AA1419013	
1000Base-SX	SFP (MT-RJ connector)	AA1419014	
1000Base-LX	SFP (LC connector)	AA1419015	
1000Base-CWDM (40km)	SFP (LC connector)	From AA1419025 to AA1419032	1470nm - 1610nm (in 20nm intervals)
1000Base-CWDM (70km)	SFP (LC connector)	From AA1419033 to AA1419040	1470nm - 1610nm (in 20nm intervals)

Single Fiber Fault Detection (SFFD)

When a partial fiber break occurs, data is lost on one side of a link. Single Fiber Fault Detection (SFFD) detects this error condition, and causes the port that is losing data to go down. This stops the loss of data. The Single Fiber Fault Detection feature is enabled on a port-by-port basis for Ethernet Switches 470-24T and 470-48T GBIC ports. At present, you can access this feature through the CLI. Single Fiber Fault Detection (SFFD) has the following requirements and limitations:

- SFFD must be implemented on both sides of a link. For example: Passport 8600 and Ethernet Switch 470.
- SFFD must be enabled on a per-port basis.
- By default, SFFD is disabled on all ports.
- SFFD takes about 50 seconds to detect a fault.
- Once a link is repaired, the link recovers automatically.

Flow control

Flow Control allows you to control traffic and avoid congestion on the GBIC port. Flow Control field cannot be configured unless you set the Autonegotiation field value to Disabled. The default Value is Disabled and the range is Disabled, Symmetric, Asymmetric.

For more information see the High Speed Flow Control Configuration screen in the *System Configuration Guide* (217105-A).

Far End Fault Indication (FEFI)

When a fiber optic transmission link to a remote device fails, the remote device indicates the failure, and the port is disabled. To use FEFI, you must enable autonegotiation on the port.

Chapter 8
Stacking

Ethernet Switches 460 and 470 can be stacked up to eight units high. The stacks can consist of a mix of Ethernet Switches 460-24T-PWR, Ethernet Switches 470-24T, and Ethernet Switches 470-48T. No other switch types are supported in the stack.

Note: The Hybrid stack mode is not supported in Release 3.6 software. All stacks must contain only Ethernet Switches 460-24T-PWR, Ethernet Switches 470-24T, and Ethernet Switches 470-48T.

This section discusses the following topics:

Stacking

Release 3.6 does not support interleaving switch types within the stack.

Note: All switches in a stack must have the same version of software installed before joining a stack. For Release 3.6 software, all Ethernet Switch 470 and Ethernet Switch 460 units must be running Release 3.6 software. You can have a maximum of eight units in a stack.

You must use either the Console Interface (CI) menus or the CLI to configure the IP addresses for each unit within a stack. You need an IP address to use the Web-based management system or Java Device Manager (JDM). Subsequently, you can change the IP address configuration from the Web management or JDM, but you will lose access until you restart the Web or JDM with the new IP address.

Contiguous units

In a stack, the same types of switches must be stacked contiguously, and in the following order:

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

Any one of the switches in the stack can function as a base unit in a stack; however, if an Ethernet Switch 470-48T is in the stack, it must be the base unit.

Base unit for a stack

In order of preference, one of the following switches can function as a base unit in a stack:

- If an Ethernet Switch 470-48T unit is in the stack, it must be the base unit.
- Otherwise, if an Ethernet Switch 470-24T unit is in the stack, it must be the base unit.
- If no Ethernet Switch 470 units are in the stack, the Ethernet Switch 460-24T PWR can be the base unit.

When stacking the switches, keep in mind the base unit restrictions. Also remember to plan which unit becomes the temporary base unit in the event of a base unit failure.

Basic stacking configuration

For a stack to operate correctly, you must perform the following steps:

1. Power down all the units.
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 the *base* position.
4. Ensure all cascade modules are properly seated.
5. Ensure all the cascade cables are properly connected and screwed into the unit.
6. Power up the stack.

Stack Operational Mode

The Stack Operational Mode screen, as depicted in Figure 96 on page 296, displays the current configuration mode for the stack configuration.

When the stack is reset on the Ethernet Switch 460-24T, the operational mode settings do not revert to the default settings.

For the Ethernet Switch 470-24T, the stack must be reset for changes to the stack operation mode to take effect.

When the stack is reset on the Ethernet Switch 470-48T, the operational mode settings revert to the default settings.

Figure 96 Stacking operational mode

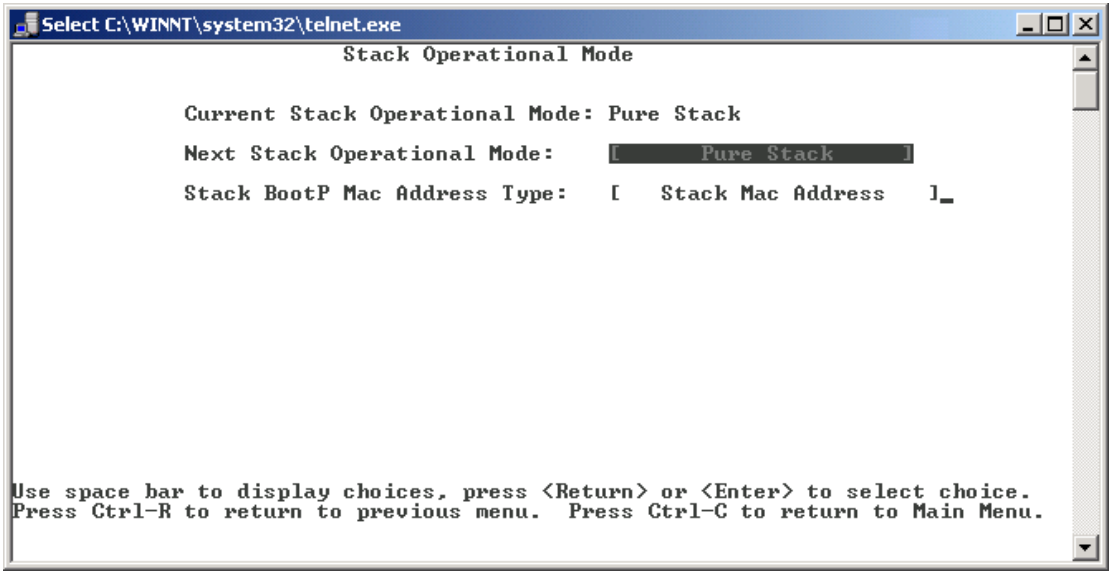


Table 77 describes the Stack Operational Mode screen fields.

Table 77 Stack Operational Mode screen fields

Field	Description
Current Stack Operational Mode	A read-only field that indicates the current mode of your stack. DefaultPure Stack RangePure Stack. In the current software release, this is the only supported stack mode. (Hybrid Stack mode is not supported in the current release.)
Stack BootP Mac Address Type	Allows you to set the location for the BootP MAC address. (The Base Unit Mac Address option is available *only* with Ethernet Switch 470 Stack options.) DefaultStack Mac Address RangeStack Mac Address, Base Unit Mac Address

Merging a switch into a stack

Nortel recommends that you start up the switch you are going to add to the stack initially in a stand-alone mode and perform preliminary IP configuration tasks before you add it to an existing stack.

Adding a new unit does not change the designated base unit. If you want to change the designated base unit when you add a new unit to the stack, you must change the base unit manually:

1. Turn off power to all units in the stack by unplugging the power cords from each unit.
   a. On the unit that was the base unit, use the Unit Select switch to deselect it as the base unit.
   b. On the unit that you want to be the new base unit, use the Unit Select switch to select it as the base unit.
   c. Redo all the cabling so that all the units will work as one stack.
2. Power up the newly joined units by plugging in the power cords.

It can take a few minutes for the entire stack to display on the console. All units display as their new numbers within the newly formed stack.

Joining stacks

You can join two stacks without renumbering units in either stacks.

Note: You cannot join Ethernet Switches 460 and 470 with other switch types. For example, you cannot join an Ethernet Switch 460 stack with an Ethernet Switch 450 stack.

To join two existing stacks:

1. Designate one stack as the one to join the other stack.
2. Reset the stack that will join the other stack to factory defaults.

3 Turn off power to all units in the stack that will join the other stack by unplugging the power cords from each unit.

   a On the unit that was the base unit for this stack, use the Unit Select switch to deselect it as the base unit.

   b Redo all the cabling so that all the units will work as one stack.

4 Power-up the newly joined units by plugging in the power cords.

It can take a few minutes for the entire stack to display on the console. All units display as their new numbers within the newly formed stack.

Automatic failover

The automatic failover is a temporary safeguard only. When you lose the base unit of a stack, one of the other units in the stack takes over as the base unit. If the stack as a whole loses power or is reset, the temporary base unit does not power up as the base unit when the power is restored.

For this reason, always explicitly reassign the temporary base unit to act as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced. When a failure of the base unit is discovered, set the Unit Select switch on the temporary base unit to Base.

Note: If you do not reassign the temporary base unit as the new base unit and the temporary base unit fails, the next unit in the stack becomes the new temporary base unit. This process can continue until there are only two units left in the stack configuration.

Note: Software download is not available when the temporary base unit is active.

Upgrading software in a stack

As a result of the stacking software compatibility requirements, all units in the stack must run the same software release.

Note: Hybrid stacking is not supported in Release 3.6 software. If you upgrade a Release 3.5 software Hybrid stack to Release 3.6 software, the stack configuration is lost. If this occurs, you can successfully downgrade to 3.5 to retain the stack integrity; however, only the stack IP address is saved.

Using the base unit, you can download the software to all units in the stack. To download, or upgrade, software in a stack:

1 Download the operational software image.

2 Download the diagnostics image.

Note: Once you begin the upgrading process, do not interrupt power to the stack.

Unit Replacement in a stack

There are two means of replacing a unit in a stack, as follows:

- "Manual Unit Replacement"
- "Auto Unit Replacement" on page 307

Manual Unit Replacement

The Unit Replacement feature allows you to retrieve the configuration of a single unit from the configuration file of a stack.

If a unit in a stack fails, this feature enables you to prepare a replacement unit for insertion in the stack. You can retrieve the configuration file of the failed unit while the replacement unit is in stand-alone mode. Once the configuration file of the failed unit is retrieved, the replacement unit can be added to the stack.

You do not have to reboot the stack after the replacement unit is added to the stack.

System Requirements

In order to use the Unit Replacement feature, you must ensure that you have the following items:

- Recent Binary Configuration File
- TFTP Server
- Switch identically configured to the failed unit

Interface Support

Table 78 describes the interfaces supported by the Unit Replacement feature.

Table 78 Interface supported by the Unit Replacement feature

Parameter	Default	Menu Interface	CLI	Web Interface	Device Manager
Download unit configuration file from stack configuration file	none	rw	rw	rw	rw

Using Unit Replacement

The unit replacement feature requires you to complete three separate and distinct tasks:

1 Back up the configuration of the stack before a unit failure occurs. Once a unit in the stack fails, you cannot retrieve the configuration of the device. Ensure that your network recovery plan includes having a current binary

configuration file available on a TFTP server. The procedure to back up your configuration file is outlined earlier in this chapter.

2 Configure a stand-alone unit as a replacement for the failed unit. With the exception of the hardware revision level of the device, the replacement unit must be an exact replica of the failed unit. It must be configured with the same MDA, software revision, firmware revision, and GBICs as the failed unit.

3 Insert the replacement unit into the stack.

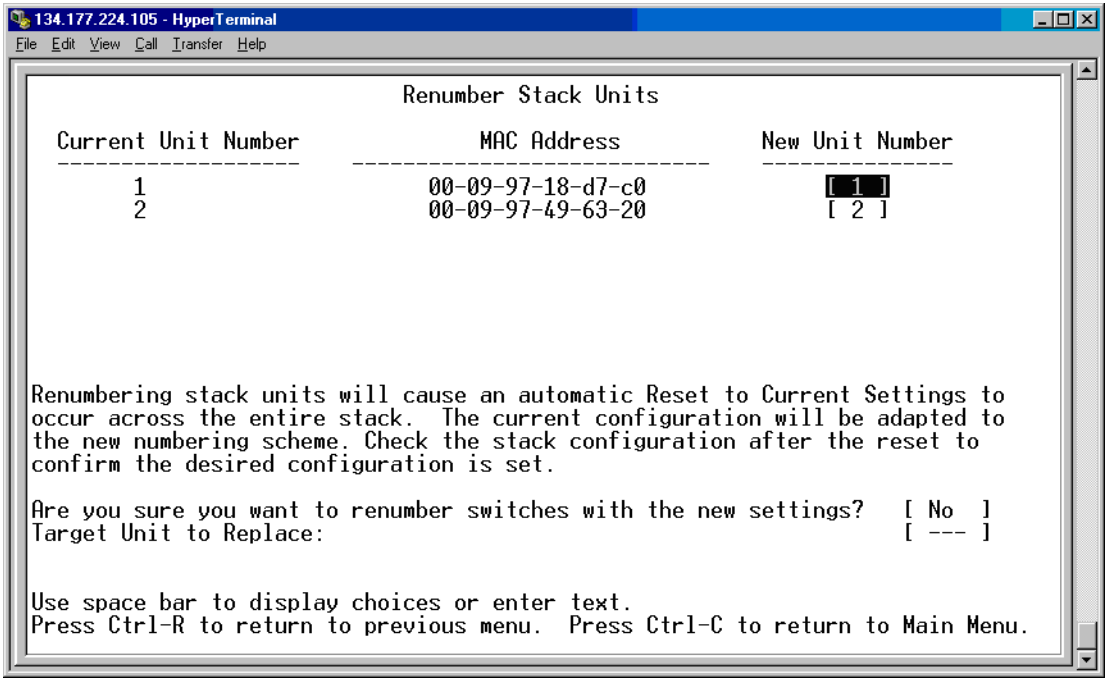
Preparing the stack for the replacement unit

Follow this procedure to prepare the stack for the new unit:

1 Remove failed unit from the stack.

2 Remove the failed unit entry from the stack by going to the Main Menu and selecting the Renumber Stack Units option. Figure 97 displays the Renumbering stack units screen.

Figure 97 Renumbering stack units



3. Highlight the field Target Unit to Replace.
4. Cycle through the options by pressing the space bar.
5. Press the Enter key when the number of the unit you wish to replace is displayed.
6. Insert the new unit into the stack by reconnecting all cables and adding power to the switch.
7. The new unit joins the stack and displays as if it were the old unit without resetting the stack.

Usage guidelines

When using the Unit Replacement Feature:

- You must have an existing binary configuration file prior to using this feature. If you do not have an existing binary file, you have no source from which to recover the configuration of the failed unit.
- You cannot specify a target unit number unless that unit is present in the configuration file.
- The replacement unit resets following download of the failed unit configuration file.
- The Unit Replacement feature supports downloading of the failed unit configuration file only to a stand-alone unit.

Inserting or replacing units in a stack

This section provides you with the procedural steps required to successfully replace a failed unit in a stack configuration, while preserving configuration information. You must perform the following four steps:

- Prepare the new replacement unit for insertion into the stack.
- Insert the replacement unit into the stack.
- Download the configuration to the stack.
- Recable the networking ports on the replacement unit.

When you prepare your replacement unit for insertion into a stack, the replacement unit must have the identical configuration of the unit that it is replacing in order to work properly in the stack. The following steps ensure that the unit integrates successfully into the stack:

Replacing a failed base unit

1. Ensure that the software and firmware versions on the replacement unit match the software and firmware versions of the unit that was removed from the stack. This step assumes that you did not upgrade the software on the stack after the failed unit was removed.
2. Ensure that the hardware configuration of the replacement unit is the same as that of the failed unit. This means that you must move the MDAs, GBIC, and other modules from the failed unit to the replacement unit.
3. Set the configuration of the replacement unit to the default values to ensure that no legacy configuration is present on the device to hinder the integration of the replacement unit into the stack.
4. Ensure that the Stack Operational Mode is set correctly on the replacement unit. Failure to do so causes the replacement unit to be unable to join the stack.
5. Ensure that the Base Unit Selector Switch is not activated on the replacement unit. You do not want the replacement unit to immediately take over the role of the base unit when it is inserted into the stack. If the replacement unit assumes base unit responsibilities, it overwrites the existing configuration with the configuration in its memory (which was previously defaulted).
6. On the stack with the failed unit, place the Base Unit Selector Switch on the temporary base unit in the base unit position. This ensures that the temporary base unit remains the base unit throughout the unit replacement process. At the end of this process, you will receive instruction on how make the replacement unit the new base unit.

Replacing a failed non-base unit

1. Ensure that the software and firmware versions on the replacement unit matches the software and firmware versions of the unit that was removed from the stack. This step assumes that you did not upgrade the software on the stack after the failed unit was removed.

2 Ensure that the hardware configuration of the replacement unit is the same as that of the failed unit. This means that you must move the MDAs, GBIC, and other modules from the failed unit to the replacement unit.

3 Set the replacement unit configuration to default values to ensure that no legacy configuration is present on the device to hinder the integration of the replacement unit into the stack.

After you complete these steps, your device is now ready to be inserted into the stack at the location previously occupied by the failed unit.

Inserting the replacement unit into the stack

1 Insert the replacement unit into the space previously occupied by the failed unit. Ensure that all physical mounting devices, screws, and rack mounts are secure.

2 Attach the stacking cables to the back of the unit. Do not cable any network connections at this time.

3 Apply power to the device.

4 Ensure that the unit number of the replacement unit is the same as that of the failed unit.

Downloading the configuration to the stack

Once the replacement unit is physically integrated into the stack and is powered on, download the configuration from a TFTP (Trivial File Transfer Protocol) server to the entire stack. The binary configuration file for a stack contains information about each unit in the stack. The configuration information for each unit is associated with the unit by the unit number. When the configuration file is downloaded, it overwrites the configuration of each unit, including the replacement unit, and reboots the stack.

This procedure makes two assumptions: that you have a TFTP server and know how to use it, and that you have a binary stack configuration file that was created before the unit failed.

1 Save your existing configuration, but do not overwrite any existing configuration files. This is insurance in case your configuration file is corrupt or fails to load onto the stack.

2 Download your pre-failure configuration file to the stack.

The stack reboots automatically when the configuration file downloads.

Note: This process uses the binary configuration file to apply the configuration of the settings from the failed unit to the replacement unit. You can also restore the unit configuration by uploading an ASCII configuration file to the unit. ASCII configuration upload does not initiate an automatic reboot of the stack. (See "Configuration Management" on page 268 for details.)

Recabling the network connections

1 Verify the configuration of the replacement unit. Ensure that the Spanning Tree Protocol (STP), Multilink Trunking (MLT), and other settings are correct. For example, you can check the following MLT settings:

- Trunk members have the same PVID.
- Trunk members are on the same VLANs.
- Trunk members have the same tagging.
- Trunk members filter tagged frames the same way.
- Trunk members filter untagged frames the same way.
- Trunk members do rate limiting the same way.
- Trunk members have the same spanning tree mode of operation.
- Trunk members have identical IGMP participation. Static router ports and mode of operation must agree on all trunk ports.

2 Recable all networking connections.

3 If the failed unit had a switch IP address configured, then configure the replacement unit to match the previous configuration.

Replacing a failed base unit

You can make the replacement unit the base unit if the failed unit was the system base unit. To do so, follow this procedure:

1 Set the Base Unit Selector Switch on the replacement unit to the base unit position.

2 Set the Base Unit Selector Switch on all other units in the stack to the non-base unit position.

3 Reset the stack to activate the new base unit.

Troubleshooting hints

If you encounter problems with the unit replacement or with a newly installed stack configuration, start troubleshooting by verifying the following items:

- Ensure that the TFTP server is accessible to the Ethernet Switch.
- Ensure that the configuration file contains the configuration of the target unit.
- Ensure that the replacement unit is configured identically to the failed unit. It must be the same model number with the same MDA configuration.
- Ensure that one switch is designated as the base unit.
- Ensure that all other units in the stack have the Base Unit Selector Switch set to Off.
- Ensure that all units in the stack are running Release 3.6 software.

When the stack is powered up, ensure that the Cas Up and Cas Dwn (cascade) and Base LEDs are green (steady, not blinking).

Configuring Unit Replacement using the CLI

You can replace a unit in the stack using the following commands:

- "Copy tftp config unit command"
- "stack replace unit command" on page 307

Copy tftp config unit command

The `copy tftp config unit` command downloads the configuration of the unit you wish to replace, to a replacement unit. Use this command in stand-alone mode. The syntax for the `copy tftp config unit` command is:

```
copy tftp config unit <unit #>
```

The `copy tftp config unit` command is in the privExec command mode.

Table 79 describes the parameters and variables for the `copy tftp config unit` command.

Table 79 `copy tftp config unit` command parameters and variables

Parameters and variables	Description
`<unit #>`	Enter the number of the unit you want to replace.

stack replace unit command

The `stack replace unit` command prepares the stack to receive the replacement unit. Use this command in stack mode. The syntax for the `stack replace unit` command is:

```
stack replace unit <1-8>
```

The `stack replace unit` command is in the privExec command mode.

Table 80 describes the parameters and variables for the `stack replace unit` command.

Table 80 `stack replace unit` command parameters and variables

Parameters and variables	Description
`<1-8>`	Enter the number of the replacement unit.

Auto Unit Replacement

This section contains information on the following topics:

AUR Overview

The Auto Unit Replacement (AUR) feature allows users to replace a unit from a stack, while retaining the configuration of the unit. This feature requires the stack power to be on during the unit replacement.

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

Other information related to this feature:

- The new unit must have the same hardware configuration as the old, including the same number of ports. If the user adds a new unit with a different hardware configuration, the previous configuration of the new unit is lost. It is overwritten with the restored configuration from the stack.
- This feature can be disabled/enabled at any time using the CLI. The default mode is ENABLE.
- Customer log messages are provided.

Note: The AUR feature cannot be enabled for a stand-alone switch. As a result, AUR cannot function properly if you remove one unit from a stack of only two switches. In this case, the CFG image of the removed unit is not retained.

AUR function

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

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

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

Refer to the following sections for additional details on the AUR functions:

- "CFG Mirror Image process"
- "Restoring a CFG image" on page 314
- "Synchronizing the CFG mirror images with CFG images" on page 315

CFG Mirror Image process

Specific events trigger the CFG mirror image process. Refer to the following sections for details on each trigger:

- "Power Cycle"
- "Adding a unit" on page 311
- "Removing an NBU" on page 311
- "Removing a BU" on page 312

Power Cycle

After a power cycle, the system mirrors all the CFG images in a stack.

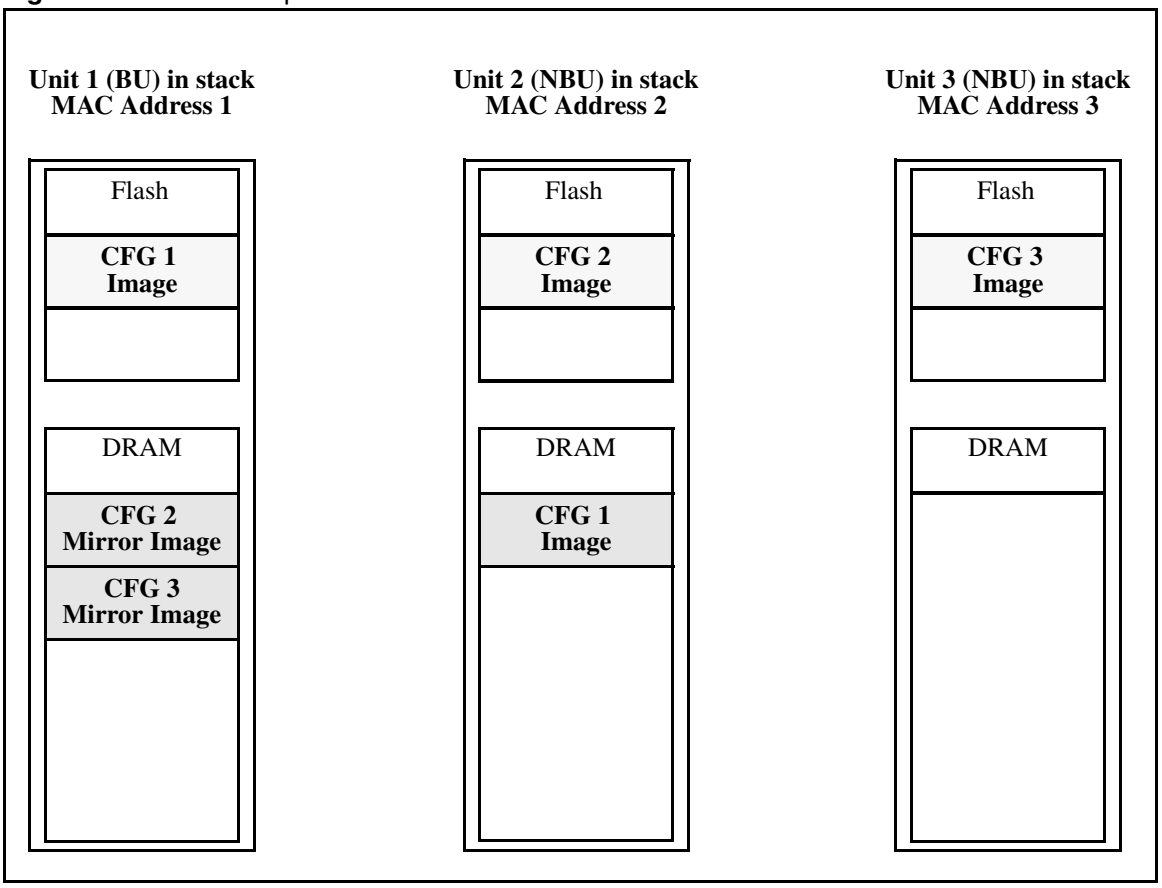
Note: After a reboot, the system requires between 5 and 10 minutes to mirror the CFG images from all units in the stack. When the process has completed successfully, the system displays the following log message: `All units mirrored for the first time`. This message indicates that you can safely begin replacing units.

Figure 98 on page 310 illustrates the CFG mirror images in a three-unit stack after the stack is powered on. Unit 1 is the Based Unit (BU) and all other units are Non-Based Units (NBU).

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

- All three mirror images (CFG 1, CFG 2, and CFG 3) are active.
- Unit 2 is the Associated Unit of the CFG 2 mirror image.
- The Mac Address 2 is the Associated Mac Address (AMA) of the CFG 2 mirror image.

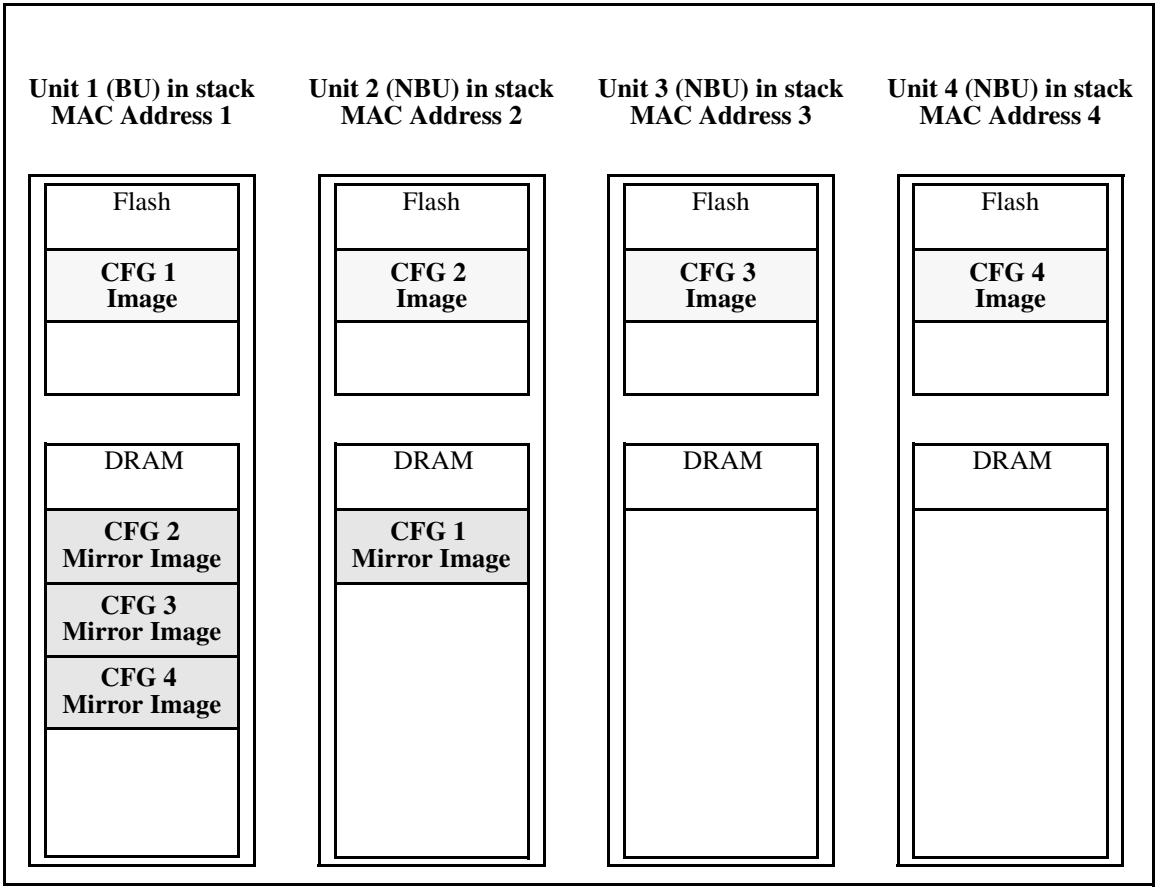
Figure 98 CFG mirror process in stack



Adding a unit

In a stack that has no INACTIVE CFG mirror images, adding a new unit causes the CFG image of the new unit to be mirrored in the stack. For example, in Figure 99, after adding unit 4 to the stack, the CFG 4 mirror image is created in the BU (unit 1).

Figure 99 CFG mirror images in the stack after adding unit 4



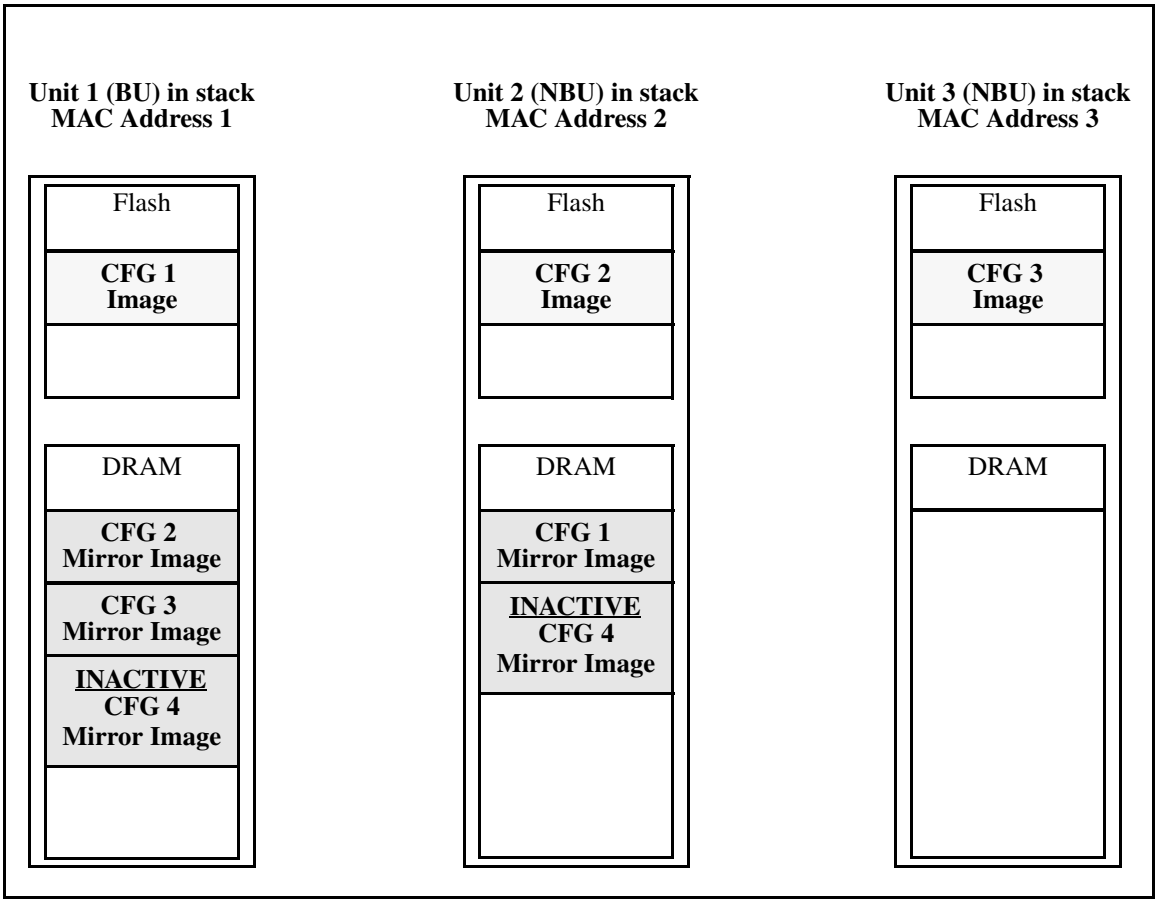
Removing an NBU

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

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

For example, after removing unit 4 from the stack shown in Figure 99 on page 311, the CFG 4 mirror image becomes INACTIVE (see Figure 100). Another copy of the INACTIVE CFG 4 mirror image is also created in unit 2.

Figure 100 CFG mirror images after removing unit 4

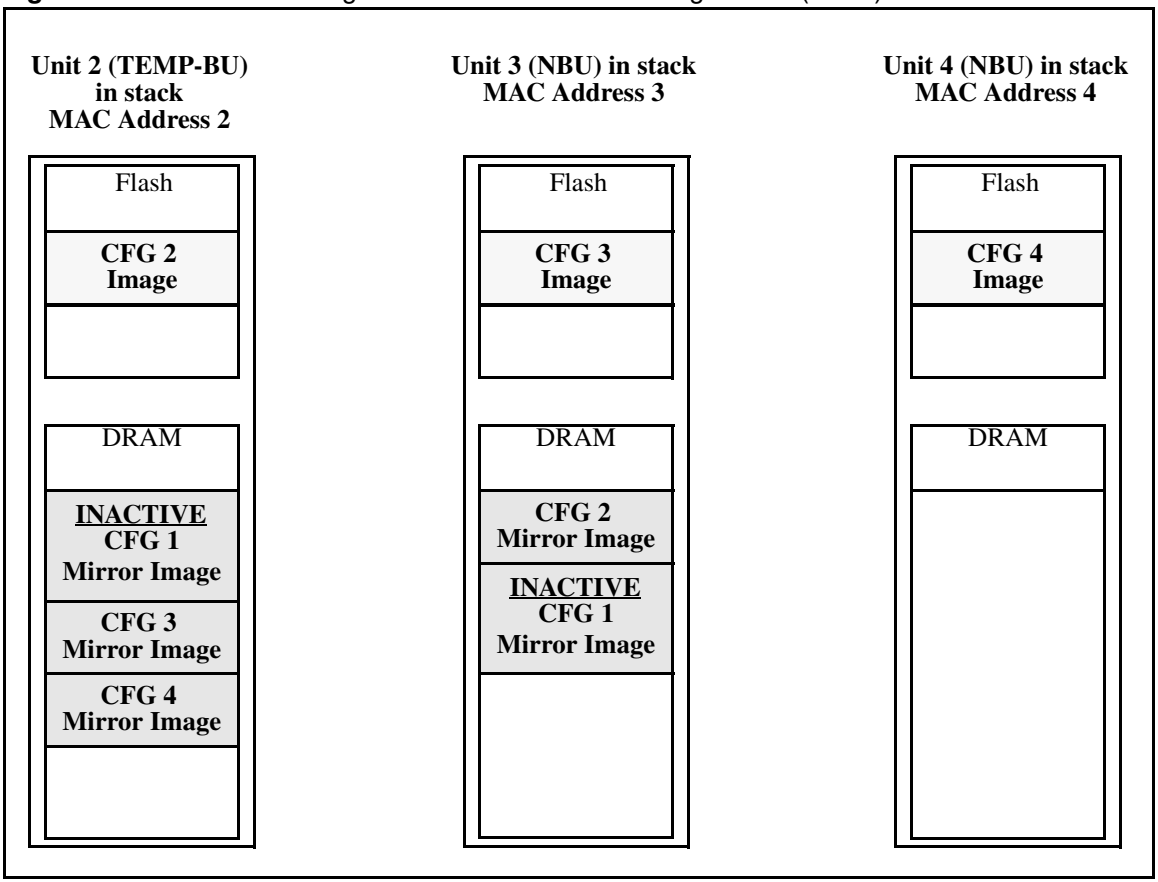


Removing a BU

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

After removing the BU from the stack shown in Figure 99 on page 311, the TEMP-BU (unit 2) must mirror all the CFG images in the stack (see Figure 101). The feature also ensures that the stack always has two copies of an INACTIVE CFG mirror image.

Figure 101 CFG mirror images in the stack after removing the BU (unit 1)



As shown in Figure 101:

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

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

Restoring a CFG image

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

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

- The AUR feature is enabled.
- There is at least one INACTIVE CFG mirror image in the stack.
- The MAC Address of the new unit is different from all the AMA of the INACTIVE CFG mirror images in the stack.

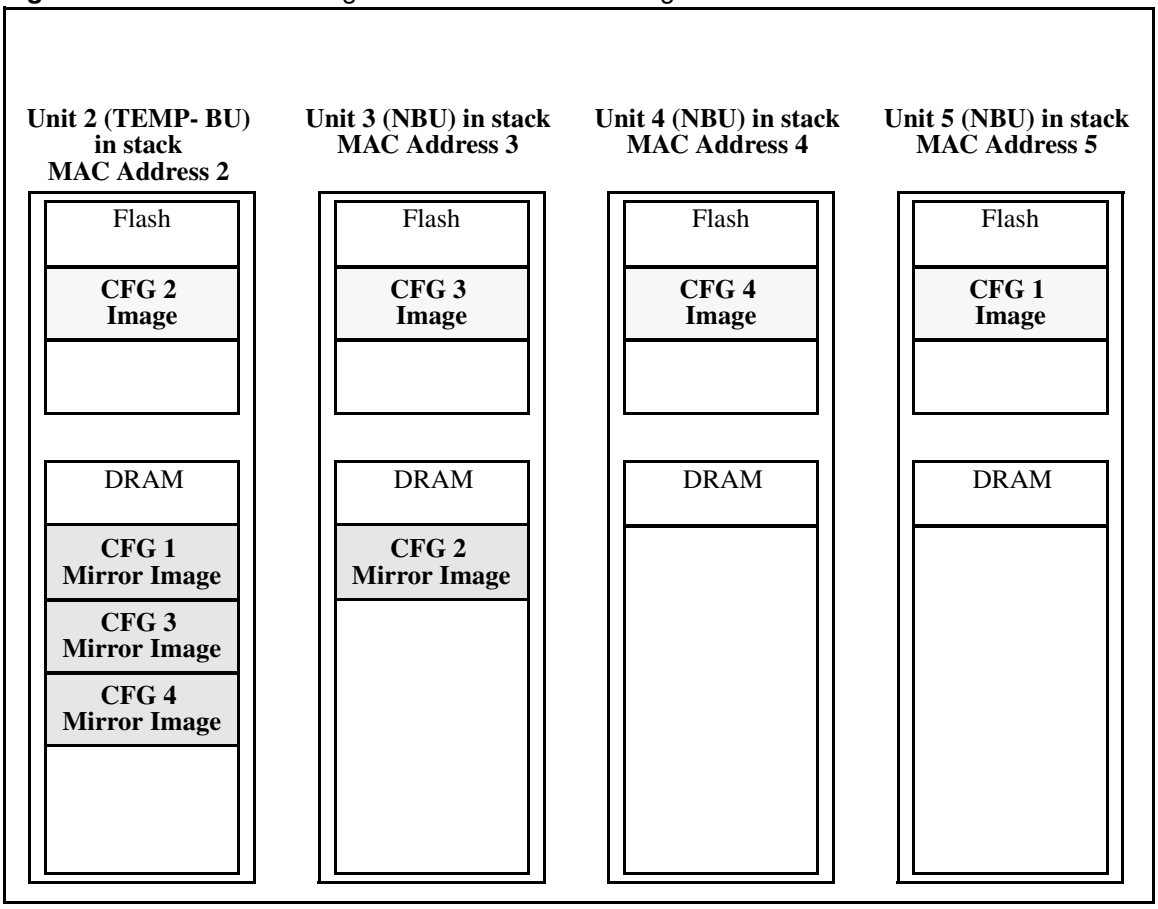
Once the a new unit is added to a stack, the image restore process consists of the following steps:

1. If there is more than one INACTIVE CFG mirror image in the stack, the last one to become INACTIVE is selected for restoring (last out, first in).
2. The INACTIVE CFG mirror image in the stack is sent to the new unit. The INACTIVE CFG mirror image become ACTIVE.
3. The new unit saves the received CFG image to its flash.
4. The new unit resets itself.

For example, if a unit 5 (MAC Address 5) is added to the stack shown in Figure 101 on page 313, the following occurs (see Figure 102 on page 315):

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

Figure 102 CFG mirror images in the stack after adding unit 5



Synchronizing the CFG mirror images with CFG images

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

Configuring Auto Unit Replacement using the CLI

You can configure the Auto Unit Replacement (AUR) feature with the following CLI commands:

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 `show stack auto-unit-replacement` 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 config 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 config 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 config mode.

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

Configuring Auto Unit Replacement using Device Manager

You can also enable or disable Auto Unit Replacement using Device Manager, under the System tab (Edit > Chassis > System). See "System tab" on page 444 for details.

Chapter 9
Power over Ethernet for the Ethernet Switch 460

The Ethernet Switch 460-24T-PWR provides IEEE 802.3af-compliant power over the front-panel RJ-45 ports. The switch provides power discovery, power management, and statistics on power use on a per port and per switch basis. You can use the Ethernet Switch 460-24T-PWR to provide power to network appliances, such as IP telephones, wireless access points, and video devices.

You configure the Power over Ethernet (PoE) parameters using the Command Line Interface (CLI), the Web-based management system, or Device Manager (JDM).

This chapter contains the following topics:

Diagnosing and correcting PoE problems

This section discusses some common problems in using the PoE features of the Ethernet Switch 460-24T-PWR. This section discusses the following topics:

Status codes on PoE ports

You may see an error displayed for a port running PoE. If these errors appear, they are in the port status section of the PoE displays in the CLI and the Web-based management system. The following are the messages that display and their explanations:

- Detecting—port detecting IP device requesting power
- Delivering power—port delivering requested power to device
- Disabled—port power state disabled
- Invalid PD—port detecting device that is not valid to request power
- Deny low priority—power disabled from port because of port setting and demands on power budget
- Overload—power disabled from port because port is overloaded
- Test—port in testing mode, which is set using SNMP
- Error—an unspecified error condition

External power source

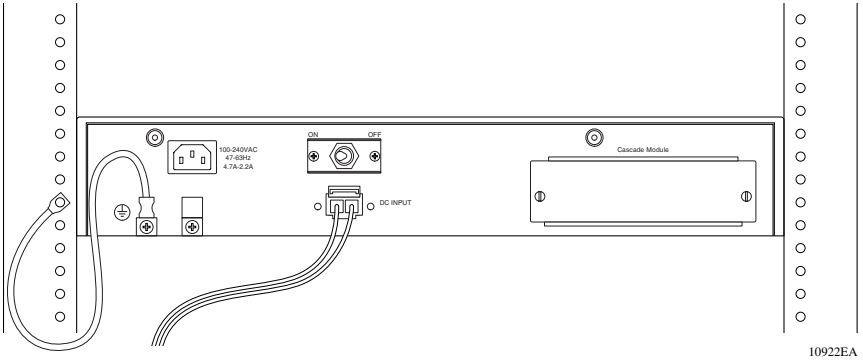
To connect the external power source, perform the following steps:

1. Plug the cord from the Ethernet Switch 460-24T-PWR into the wall outlet.
2. Ensure that the DC ON/OFF switch on the back of the Ethernet Switch 460-24T-PWR is in the OFF position.
3. Using the 2-pin connector, plug the external power source into the DC connector receptacle on the back of the Ethernet Switch 460-24T-PWR.
4. Attach the ground lug to a grounding point.
5. Turn the DC ON/OFF switch on the back of the switch to the ON position.

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

Figure 103 shows an external power source connected to the back of the Ethernet Switch 460-24T-PWR. Note that the grounding wire is connected to the rack and the DC ON/OFF switch is in the ON position.

Figure 103 External power source connected to back of the Ethernet Switch 460-24T-PWR



Whatever the physical power sources you use, you can configure the Ethernet Switch 460-24T-PWR power as *one* of the following:

- power sharing
- uninterruptible power supply (UPS)
- redundant power supply unit (RPSU)

Once you have correctly attached an external power source, ensure that your configuration is set for the correct one. Also, check the DC ON/OFF switch on the back of the Ethernet Switch 460-24T-PWR to ensure that it is in the ON position. Finally, check your configuration to ensure that you have chosen the correct DC source type and DC source configuration you want.

Configuring PoE switch parameters using the CLI

You configure power parameters for each Ethernet Switch 460-24T-PWR using the CLI. You can configure the DC power source, the power pairs, and the power usage with this management system. This section covers the following topics:

- "poe poe-dc-source-type command" on page 322
- "poe poe-dc-source-conf command" on page 323

poe poe-dc-source-type command

The `poe poe-dc-source-type` command allows you to set the type of external DC power source you are using with the switch. The syntax for the `poe poe-dc-source-type` command is:

```
poe poe-dc-source-type [unit <1-8>] {RPS10|nes}
```

The `poe poe-dc-source-type` command is in the config mode.

Table 81 describes the parameters and variables for the `poe poe-dc-source-type` command.

Table 81 `poe poe-dc-source-type` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number that you want to configure for an external power source. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the `#` alone, you will get an error.
`RPS10|nes`	Sets the type of external DC power source you are using: • `RPS10`—sets the external DC power source as the Ethernet Switch Power Supply Unit 10 • `nes`—sets the external DC power source as the Intergy* Network Energy Source (NES) from Invensys Energy Systems Note: The default setting is `RPS10`. You set this parameter whether or not you are physically attached to an external power source.

poe poe-dc-source-conf command

The `poe poe-dc-source-conf` command allows you to configure the type of power sharing you want to use on the Ethernet Switch 460-24T-PWR. The syntax for the `poe poe-dc-source-conf` command is:

```
poe poe-dc-source-conf [unit <1-8>] {powersharing|rpsu|ups}
```

The `poe poe-dc-source-conf` command is in the config mode.

Table 82 describes the parameters and variables for the `poe poe-dc-source-conf` command.

Table 82 `poe poe-dc-source-conf` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to configure the power-sharing option. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the `#` alone, you will get an error.
`powersharing|rpsu|ups`	Sets the type of powersharing for the Ethernet Switch 460-24T-PWR: • `powersharing` • `rpsu` • `ups` Note: The default setting is `powersharing`. You set this parameter whether or not you are physically attached to an external power source.

poe poe-pd-detect-type command

The `poe poe-pd-detect-type` command sets the method the Ethernet Switch 460-24T-PWR uses to detect the power devices connected to the front ports. The syntax for the `poe poe-pd-detect-type` command is:

```
poe poe-pd-detect-type [unit <1-8>]
{802dot3af|802dot3af_and_legacy}
```

The `poe poe-pd-detect-type` command is in the config mode.

Note: You must ensure that this setting is the correct one for the IP appliance you use with the switch. Please note this setting applies to the entire switch, not port-by-port. So, you must ensure that this setting is configured correctly for *all* the IP appliances on a specified switch.

Table 83 describes the parameters and variables for the `poe poe-pd-detect-type` command.

Table 83 `poe poe-pd-detect-type` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to configure the power option detection. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the `#` alone, you will get an error.
`802dot3af|802dot3af_and_legacy`	Sets the detection method the switch use to detect power needs of devices connected to front ports: • `802dot3af` • `802dot3af_and_legacy` Note: The default setting is 802dot3af. Ensure that the power detection method you choose for the Ethernet Switch 460-24T-PWR matches that used by the IP devices you are powering.

poe poe-power-pairs command

The `poe poe-power-pairs` command sets the RJ-45 connector pins on the front port that you use to deliver power to the device. The syntax for the `poe poe-power-pairs` command is:

`poe poe-power-pairs [unit <1-8>] {spare|signal}`

The `poe poe-power-pairs` command is in the config mode.

Note: You must ensure that this setting is the correct one for the IP appliance you use with the switch. Please note this setting applies to the entire switch, not port-by-port. So, you must ensure that this setting is configured correctly for *all* the IP appliances you on a specified switch.

Table 84 describes the parameters and variables for the `poe poe-power-pairs` command.

Table 84 `poe poe-power-pairs` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to configure the power pairs. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you will get an error.
`spare|signal`	Sets the type of external DC power source you are using: • `spare`—sets power-carrying pins to the spare set • `signal`—sets power-carrying pins to the signal set The default value is spare. Refer to "Features" on page 46 for complete information on power pairs. Note: Ensure that the power pair you choose for the Ethernet Switch 460-24T-PWR matches the power pair used by the IP devices you are powering. Each unit uses the same power pairs; you cannot configure this on each port.

poe poe-power-usage-threshold command

The `poe poe-power-usage-threshold` command allows you to set a percentage usage threshold above which the system sends a trap for each Ethernet Switch 460-24T-PWR. The syntax for the `poe poe-power-usage-threshold` command is:

```
poe poe-power-usage-threshold [unit <1-8>] <1-99>
```

The `poe poe-power-usage-threshold` command is in the config mode.

Table 85 describes the parameters and variables for the `poe poe-power-usage-threshold` command.

Table 85 `poe poe-power-usage-threshold` command parameters

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to configure the trap generation. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the `#` alone, you receive an error.
<1-99>	Enter the percentage of total available power you want the switch to use prior to sending a trap. Note: The default setting is 80%.

poe poe-trap command

The `poe poe-trap` command enables the traps for the PoE functions on the Ethernet Switch 460-24T-PWR. The syntax for the `poe poe-trap` command is:

```
poe poe-trap [unit <1-8>]
```

The `poe poe-trap` command is in the config mode.

Table 86 describes the parameters and variables for the `poe poe-trap` command.

Table 86 `poe poe-trap` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to enable traps. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the `#` alone, you receive an error.

no poe-trap command

The `no poe-trap` command disables the traps for the PoE functions on the Ethernet Switch 460-24T-PWR. The syntax for the `no poe-trap` command is:

```
no poe-trap [unit <1-8>]
```

The `no poe-trap` command is in the config mode.

Table 87 describes the parameters and variables for the `no poe-trap` command.

Table 87 `no poe-trap` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to disable traps. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the `#` alone, you receive an error.

Configuring PoE port parameters using the CLI

You can configure power parameters for each port on the Ethernet Switch 460-24T PWR using the CLI. You enable the power and set the power limit and power priority on each port. This section covers the following topics:

no poe-shutdown command

The `no poe-shutdown` command enables power to the port. The syntax for the `no poe-shutdown` command is:

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

The `no poe-shutdown` command is in the config-if mode.

Table 88 describes the parameters and variables for the `no poe-shutdown` command.

Table 88 `no poe-shutdown` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the port numbers on which you want to enable power. The default value is enabled. Note: If you omit this parameter, the system uses the port entered with the `interface FastEthernet` command.

poe poe-shutdown command

The `poe poe-shutdown` command disables power to the port. The syntax for the `poe poe-shutdown` command is:

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

The `poe poe-shutdown` command is in the config-if mode.

Table 89 describes the parameters and variables for the `poe poe-shutdown` command.

Table 89 `poe poe-shutdown` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the port numbers on which you want to disable power. The default value is enabled. Note: If you omit this parameter, the system uses the port entered with the `interface FastEthernet` command.

poe poe-priority command

The `poe poe-priority` command allows you to set the power priority for each port to low, high, or critical. The system uses the port power priority settings to distribute power to the ports depending on the available power budget. The syntax for the `poe poe-priority` command is:

```
poe poe-priority [port <portlist>] {low|high|critical}
```

The `poe poe-priority` command is in the config-if mode.

Table 90 describes the parameters and variables for the `poe poe-priority` command.

Table 90 `poe poe-priority` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the port numbers on which you want to disable power. Note: If you omit this parameter, the system uses the port entered with the `interface FastEthernet` command.
`low|high|critical`	Sets the port priority as: • `low` • `high` • `critical` Note: The default setting is low. When two ports have the same priority and one must be shut down, the port with the higher port number is shut down first.

poe poe-limit command

The `poe poe-limit` command sets the maximum power allowed to a port. The syntax for the `poe poe-limit` command is:

```
poe poe-limit [port <portlist>] <3-16>
```

The `poe poe-limit` command is in the config-if mode.

Table 91 describes the parameters and variables for the `poe poe-limit` command.

Table 91 `poe poe-limit` command parameters and variables

Parameters and variables	Description
<3-16>	Enter the maximum number of watts you want to allow to the specified port. The range is 3W to 16W; the default value is 16W.
`ports`	Enter the port number you want to disable power on. Note: If you omit this parameter, the system uses the port entered with the `interface FastEthernet` command.

Displaying PoE configuration using the CLI

You display the status for the PoE configuration on the Ethernet Switch 460-24T-PWR using the following CLI commands:

- "show poe-main-status command"
- "show poe-port-status command" on page 333
- "show poe-power-measurement command" on page 334

show poe-main-status command

The `show poe-main-status` command displays the current PoE configuration of the Ethernet Switch 460-24T-PWR, and per port PoE settings. The syntax for the `show poe-main-status` command is:

```
show poe-main-status [unit <1-8>]
```

The `show poe-main-status` command is in the exec command mode.

Table 92 describes the parameters and variables for the `show poe-main-status` command.

Table 92 `show poe-main-status` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Enter the unit number for which you want to display the power statistics. Note: If you omit this parameter and you are working from the console port, this command sets your connected unit. If you omit this parameter and you are working through Telnet, this command sets the base unit. To specify a unit, you must enter `unit #`. If you enter the # alone, you receive an error.

Figure 104 on page 332 displays sample output from the `show poe-main-status` command.

Figure 104 `show poe-main-status` command output

```
460-24T-PWR>show poe-main-status
PoE Main Status - Unit# 1
-------------------------------------------------
Available DTE Power         : 200 Watts
DTE Power Status            : Normal
DTE Power Consumption       : 0 Watts
DTE Power Usage Threshold   : 80 %
Power Pairs                 : Spare
Traps Control Status        : Enable
PD Detect Type              : 802.3af
Power Source Present        : AC Only
DC Source Type              : RPS 10
DC Source Configuration     : Power Sharing
```

Note: The Power Source Present listing displays the current power source for the switch: AC Only, DC Only, or AC and DC.

show poe-port-status command

The `show poe-port-status` command displays the status, power status, power limit, and port priority of each port. The syntax for the `show poe-port-status` command is:

`show poe-port-status [port <portlist>]`

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

The DTE Power Status displays error messages if the port is not providing power. The following messages can appear:

- Detecting—port detecting IP device requesting power
- Delivering power—port delivering requested power to device
- Invalid PD—port detecting device that is not valid to request power
- Deny low priority—power disabled from port because of port setting and demands on power budget
- Overload—power disabled from port because port is overloaded
- Test—port in testing mode
- Error—none of the other conditions apply

Table 93 describes the parameters and variables for the `show poe-port-status` command.

Table 93 `show poe-port-status` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to display the status. Note: If you omit this parameter, the system displays all ports.

Figure 105 on page 334 displays sample output from the `show poe-port-status` command.

Figure 105 `show poe-port-status` command output

```
460-24T-PWR>show poe-port-status
            Admin      Current              Limit
Unit/Port   Status     Status               (Watts)  Priority
---------   -------    -----------------    -------  --------
1/1         Enable     Detecting            16       Low
1/2         Enable     Detecting            16       Low
1/3         Enable     Detecting            16       Low
1/4         Enable     Detecting            16       Low
1/5         Enable     Detecting            16       Low
1/6         Enable     Detecting            16       Low
1/7         Enable     Detecting            16       Low
1/8         Enable     Detecting            16       Low
1/9         Enable     Detecting            16       Low
1/10        Enable     Detecting            16       Low
1/11        Enable     Detecting            16       Low
1/12        Enable     Detecting            16       Low
1/13        Enable     Detecting            16       Low
1/14        Enable     Detecting            16       Low
1/15        Enable     Detecting            16       Low
1/16        Enable     Detecting            16       Low
1/17        Enable     Detecting            16       Low
1/18        Enable     Detecting            16       Low
1/19        Enable     Detecting            16       Low
1/20        Enable     Detecting            16       Low
1/21        Enable     Detecting            16       Low
1/22        Enable     Detecting            16       Low
1/23        Enable     Detecting            16       Low
1/24        Enable     Detecting            16       Low
--More--
```

show poe-power-measurement command

The `show poe-power-measurement` command displays the voltage, current and power values for each powered device connected to each port. The syntax for the `show poe-power-measurement` command is:

`show poe-power-measurement [port <`*`portlist`*`>]`

The `show poe-power-measurement` command is in the exec command mode.

Table 94 shows the variables and parameters for the `show poe-power-measurement` command.

Table 94 show poe-power-measurement command parameters

Parameters and variables	Description
`port <portlist>`	Enter the ports for which you want to display the power measurements. Note: If you omit this parameter, the system displays all ports.

Figure 106 displays sample output from the `show poe-power-measurement` command.

Figure 106 `show poe-power-measurement` command output

```
460-24T-PWR>show poe-power-measurement
Unit/Port   Volt(V)   Current(mA)    Power(Watt)
---------   -------   -----------    ---------------
1/1         0.0       0              0.000
1/2         0.0       0              0.000
1/3         0.0       0              0.000
1/4         0.0       0              0.000
1/5         0.0       0              0.000
1/6         0.0       0              0.000
1/7         0.0       0              0.000
1/8         0.0       0              0.000
1/9         0.0       0              0.000
-More--
```

Configuring PoE using Web-based management

You can display and configure Power over Ethernet (PoE) parameters using the Web-based management system.

- "Displaying and configuring power management for the switch" on page 336
- "Displaying and configuring power management for the ports" on page 338

Displaying and configuring power management for the switch

To display and configure power settings for the entire switch:

1 From the main menu, choose Configuration > Power Management > Global Power Mgmt.

The Global Power Management page opens (Figure 107).

Figure 107 Global Power Management page

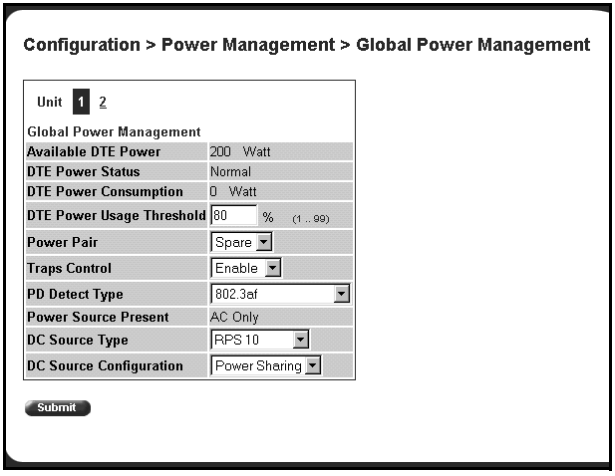


Table 43 describes the items on the Global Power Management page.

Table 43 Global Power Management page items

Item	Description
Available DTE Power	Displays the amount of power available to powered devices from the switch. Depending on the power sources you use and the power configuration you enable, you see one of the following values: • 75 Watt • 200 Watt • 235 Watt • 370 Watt
DTE Power Status	Displays the status of the PoE feature. It displays: • Normal—all power functioning correctly • Error—PoE failed

Table 43 Global Power Management page items (Continued)

Item	Description
DTE Power Consumption	Displays total power use on all devices currently drawing power.
DTE Power Usage Threshold	Enter the percentage of total power consumption on the switch necessary to trigger a trap. The default value is 80%.
Power Pair	Choose the power pair (of the RJ-45 pin connectors) you want to supply the power: • spare • signal The default value is spare. Note: Ensure that the power pair you choose for the Ethernet Switch matches the power pair used by the IP devices you are powering. Each unit uses the same power pairs; you cannot configure power pairs on each port.
Traps Control	Choose to enable or disable trap from agent.
PD Detect Type	Choose the type of power detection you want for the switch: • 802.3af • 802.3af and legacy The default is 802.3af. Note: Ensure that the power detection method you choose for the Ethernet Switch matches that used by the IP devices you are powering.
Power Source Present	This display-only field displays the current power supply for the switch: • AC Only—using only the internal power source of the switch • DC Only—using only an optional external DC power source for the switch • AC and DC—using the internal power source and an optional external DC power source for the switch

Table 43 Global Power Management page items (Continued)

Item	Description
DC Source Type	Choose the optional external power source you are using: • RPS 10—Ethernet Switch Power Supply Unit 10 • NES—Intergy* Network Energy Source (NES) from Invensys Energy Systems The default value is RPS 10. Note: You set this parameter whether or not you are physically attached to an external power source.
DC Source Configuration	Choose the DC configuration you are using: • Power Sharing • UPS • RPSU The default value is Power Sharing. Note: You set this parameter whether or not you are physically attached to an external power source.

2 Type the information, or make a selection from the list.

3 Click Submit.

Displaying and configuring power management for the ports

To configure power management settings for each port:

1 From the main menu, choose Configuration > Power Management > Port Property.

The Port Property page opens (Figure 108 on page 339).

Figure 108 Port Property page

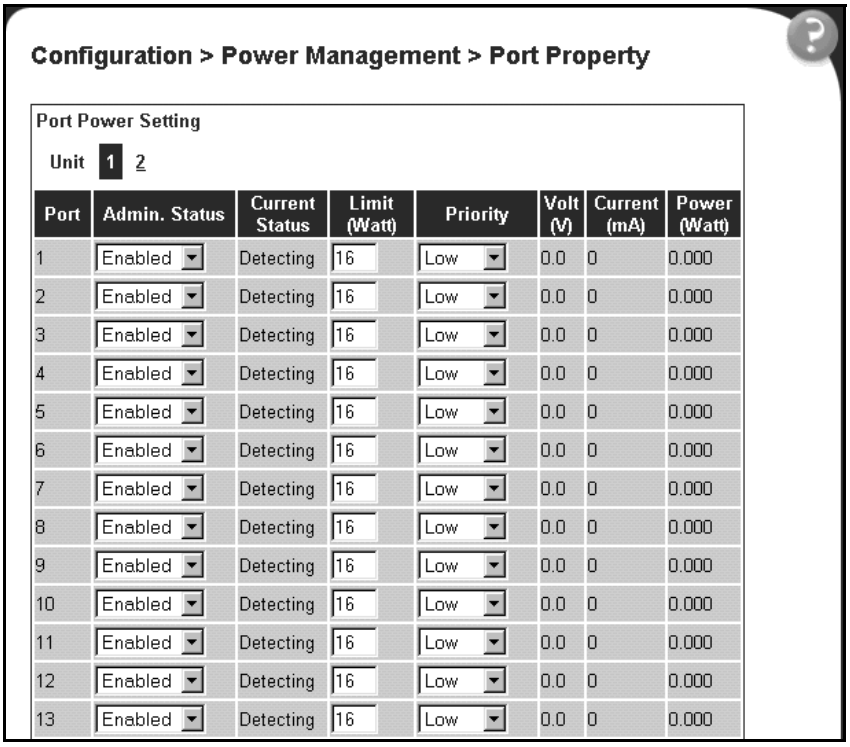


Table 44 describes the items on the Port Property page.

Table 44 Port Property page items

Item	Description
Admin. Status	Choose to enable or disable power on selected port. The default value is Enabled.
Current Status	Displays the current status of the port: • Detecting—port detecting IP device requesting power • Delivering power—port delivering requested power to device • Disabled—port power state disabled • Invalid PD—port detecting device that is not a valid power device to request power • Deny low priority—power disabled from port because of port setting and demands on power budget (available DTE power exceeded). • Overload—power disabled from port because port overloaded • Test—port in testing mode, which is set using SNMP • Error—none of the other conditions apply
Limit (Watt)	Sets the maximum amount of power supplied to that port. The range is 3W to 20W. The default value is 16W.
Priority	Priority is used to determine which port(s) will be shut down when the total power of the Ethernet Switch 460-24T-PWR exceeds the power budget for that switch (or available DTE power). The lower priority ports are shut down in favor of higher priority ports. The range is low, high, and critical. The default value is low. Note: When two ports have the same priority and one must be shut down, the port with the higher port number is shut down first.
Volt (V)	Displays the measured voltage supplied by the port.
Current (mA)	Displays the measured current supplied by the port.
Power (Watt)	Displays the measured power supplied by the port.

2 Type the information, or make a selection from the list.

3 Click Submit.

Editing and viewing switch PoE configurations using Device Manager

Note: You must view and edit the switch-wide PoE parameters for each Ethernet Switch 460-24T-PWR one by one. If you select more than one unit, you cannot view or edit the PoE power parameters; the PoE tab and DC source tabs do not appear.

You can use Device Manager to view and edit the Power over Ethernet (PoE) parameters that apply to the whole switch. You can also use Device Manager to set PoE parameters on individual ports.

One PoE-related tab that is not described in this section is the Power Supply tab. This tab is accessible through the Chassis dialog box, and it displays the status of the internal power supply (see "Power Supply tab" on page 453).

The following sections provide a description of the PoE tabs, and details about each item on the tab:

- "PoE tab for a single unit" on page 342
- "DC Source tab for a single unit" on page 344
- "Device Manager display for PoE ports" on page 347
- "PoE tab for a single port" on page 348
- "PoE tab for multiple ports" on page 350

PoE tab for a single unit

To set the power usage threshold, the power pairs you want to use, and the power detection method you want to use, select a *single* unit.

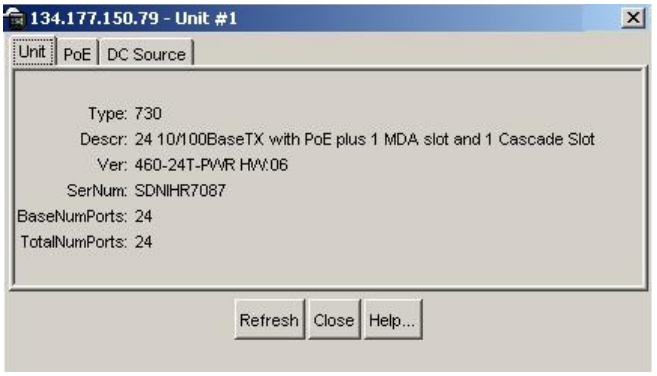
Note: You can view and set these parameters only by selecting a *single* unit. If you select more than one unit, you do not see the PoE tab and you cannot set any of the PoE parameters.

To open the PoE tab for a *single* unit:

1. Select a *single* unit.
2. From the shortcut menu, choose Edit > Unit.

   The Unit dialog box opens with the Unit tab displayed (Figure 109).

Figure 109 Edit Unit dialog box—Unit tab for a single unit



3. Click the PoE tab.

   The PoE tab opens (Figure 110 on page 343).

Figure 110 Edit Unit dialog box—PoE tab for a single unit

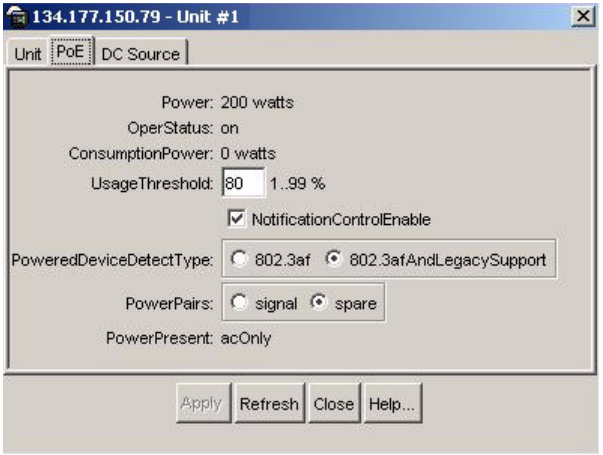


Table 45 describes the PoE tab items for a single unit.

Table 45 PoE tab items for a single unit

Item	Description
Power	Displays the total power available to the switch.
OperStatus	Displays the power state of the switch: • on • off • faulty
Consumption Power	Displays the power being used by the switch.
UsageThreshold	Allows you to set a percentage of the total power usage of the switch above which the system sends a trap. Note: You must enable the traps (refer to NotificationControlEnable, below) to receive a power usage trap.
Notification ControlEnable	Allows you to enable or disable sending traps if the switch power usage exceeds the percentage set in the UsageThreshold field.

Table 45 PoE tab items for a single unit

Item	Description
PowerPairs	Allows you to set the RJ-45 pin pairs that the switch uses to send power to the ports on the switch: • signal • spare Note: The default setting is spare. Ensure that this setting matches the setting for the power pairs on the powered devices you use on this switch.
PowerDetection Method	Allows 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: • 802.3af • 802.3af and legacy Note: The default setting is 802.3af. Ensure that this setting matches the setting for the detection method used by the powered devices on this switch.
PowerPresent	This read-only field displays the current power supply for the switch: acOnly—only the internal power source of the switch dcOnly—only an optional external DC power source for the switch ac and cd—the internal power source and an optional external DC power source for the switch

DC Source tab for a single unit

Note: You can view and set DC source parameters only by selecting a *single* unit. If you select more than one unit, you do not see the PoE tab or the DC Source tab, and you cannot set any of the PoE parameters. The Power Supply under Edit > Chassis also provides information on the DC source type, or redundant power supply (refer to "Power Supply tab" on page 453).

The DC Source tab displays the presence or absence of an optional external power source, either the Ethernet Switch Power Supply Unit 10 or the Intergy* Network Energy Source (NES) from Invensys Energy Systems. Additionally, you configure the DC source type and the DC source configuration using this dialog box.

Note: You *always* configure the DC source type and the DC source configuration whether or not you use an optional external DC power source.

To open the DC Source tab for a *single* unit:

1. Select a *single* unit.
2. From the shortcut menu, choose Edit > Unit.

   The Unit dialog box opens with the Unit tab displayed (Figure 109 on page 342).

3. Click the DC Source tab.

   The DC Source tab opens (Figure 111).

Figure 111 Edit Unit dialog box—DC Source tab for a single unit

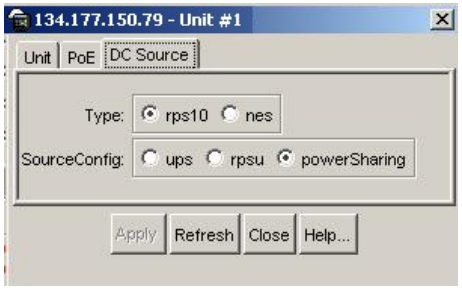


Table 46 describes the DC Source tab fields for a single unit.

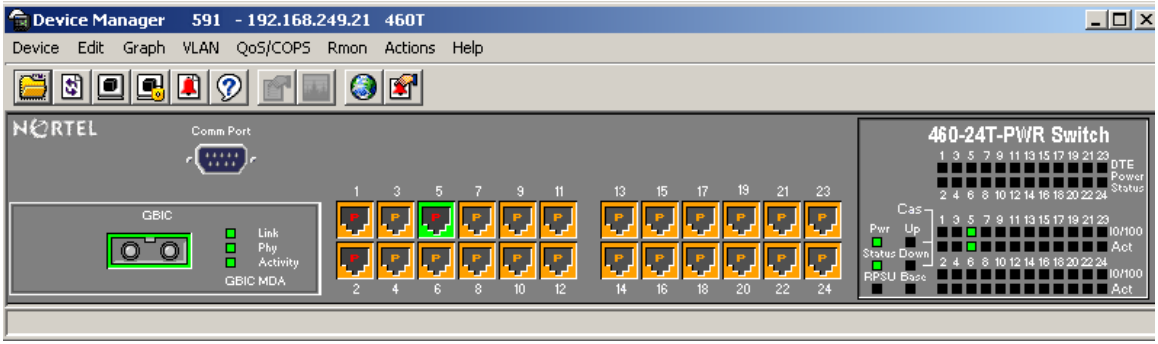
Table 46 DC Source tab fields for a single unit

Field	Description
Type	Allows you to configure the type of external power source the switch is using: • RPS 10—Ethernet Switch Power Supply Unit 10 • nes—NES unit Note: The default setting is RPS 10. You configure this field whether or not you are physically using an external power source. You must configure the DC source type under all circumstances.
SourceConfig	Allows you to configure the DC source configuration: • ups • rpsu • powerSharing Note: The default setting is powerSharing. You configure this field whether or not you are physically using an external power source.You must specify the DC source configuration under all circumstances.

Device Manager display for PoE ports

The Device Manager displays PoE ports differently than non-PoE port (see Figure 112).

Figure 112 460-24T-PWR with PoE ports



The port coloring scheme for the data aspect is the same for PoE ports as for all other ports. The difference for the PoE ports is the addition of the power aspect (colored p).

Table 47 shows the status assigned to each color.

Table 47 Port power color codes

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

Note: The coloring scheme for data aspect and the power aspect are independent of each other. With this GUI enhancement, you can view the initial status for both data and power aspect for the port.

PoE tab for a single port

The PoE tab allows you to configure PoE power settings for a single port.

To view the PoE tab:

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

   The Port dialog box for a single port opens (Figure 164 on page 469) with the Interface tab displayed.
3. Click the PoE tab.

The PoE tab opens (Figure 113).

Figure 113 Edit Port dialog box — PoE tab

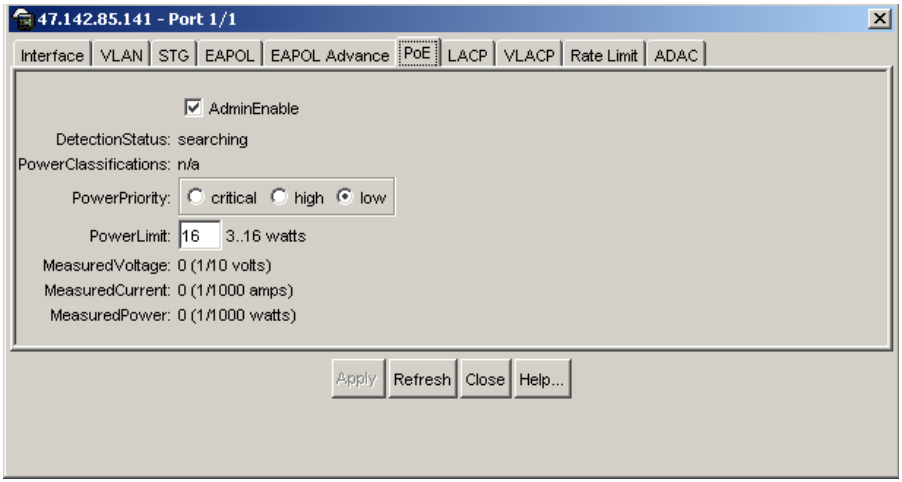


Table 48 describes the PoE tab items.

Table 48 PoE tab items for a single port

Item	Description
AdminEnable	Allows you to enable or disable PoE on this port. By default, PoE is enabled.
Detection Status	Displays the operational status of the power-device detecting mode on the specified port: • 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 • denyLowPrioriy—port disabled by management system to supply power to higher-priority ports • test—detecting device in test mode Note: Nortel recommends against using the test operational status.

Table 48 PoE tab items for a single port (Continued)

Item	Description
PowerClassifications	Not applicable for this release.
PowerPriority	Allows you to set the power priority for the specified port to: • critical • high • low
PowerLimit	DTE Power limit per port, in watts.
MeasuredVoltage	Measured port voltage, in 1/10 volts. When the port is not supplying power, the value is 0.
MeasuredCurrent	Measured port current, in 1/1000 amps.
MeasuredPower	Measured port power, in 1/1000 watts. This value cannot exceed 1000 times the current value of the PowerLimit field.

PoE tab for multiple ports

When you select multiple ports, the PoE tab shows the PoE settings for the selected ports.

To view or edit the PoE tab for multiple ports:

1 Select the ports that you want to edit.

[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for multiple ports (Figure 166 on page 474) opens with the Interface tab displayed.

3 Click the PoE tab.

The PoE tab opens (Figure 114 on page 351).

Figure 114 PoE tab for multiple ports

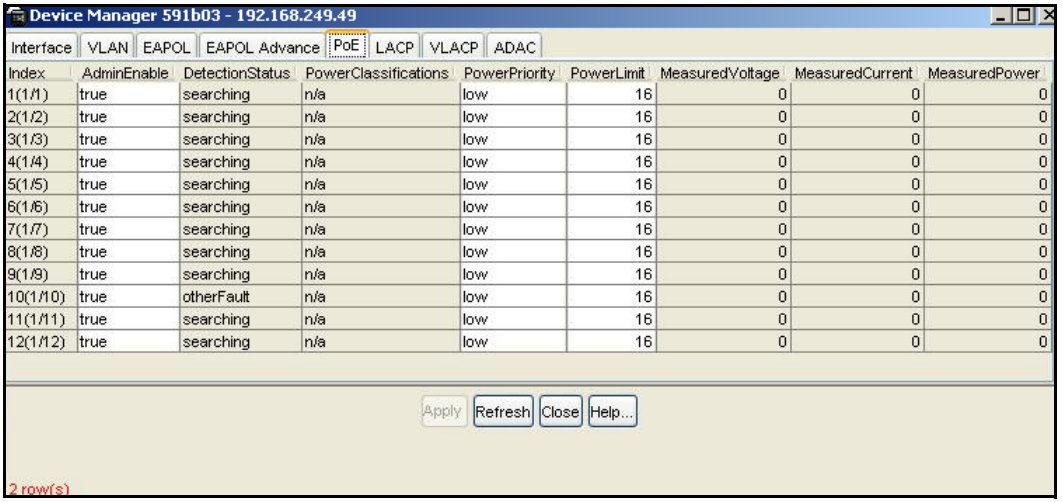


Table 49 describes the PoE tab fields for multiple ports.

Table 49 PoE tab fields for multiple ports

Field	Description
Index	Displays the unique value assigned to each interface.
AdminEnable	Allows you to enable or disable PoE on this port. By default, PoE is enabled.

Table 49 PoE tab fields for multiple ports (Continued)

Field	Description
Detection Status	Displays the operational status of the power-device detecting mode on the specified port: • 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 • denyLowPrioriy—port disabled by management system to supply power to higher-priority ports • test—detecting device in test mode Note: Nortel recommends against using the test operational status.
PowerClassifications	Not applicable for this release.
PowerPriority	Allows you to set the power priority for the specified port to: • critical • high • low
PowerLimit	DTE Power limit per port, in watts.
MeasuredVoltage	Measured port voltage, in 1/10 volts. When the port is not supplying power, the value is 0.
MeasuredCurrent	Measured port current, in 1/1000 amps.
MeasuredPower	Measured port power, in 1/1000 watts. This value cannot exceed 1000 times the current value of the PowerLimit field.

Chapter 10
System configuration using the CLI

In the switch, the Command Line Interface (CLI) commands allow you to display and modify the switch configuration while the switch is operating.

This chapter includes information about the system configuration, such as Configuring the switch IP address, downloading and uploading your software, and customizing your system. This chapter covers the following topics:

- "Enabling Autotopology" on page 409

Setting the default management system

The `cmd-interface` command allows you to set the default management interface when you use the console port or Telnet.

The syntax for the `cmd-interface` command is:

```
cmd-interface [cli|menu]
```

The `cmd-interface` command is in the privExec command mode.

Configuring the switch IP address, subnet mask, and default gateway

IP notation

You enter IP addresses and subnet masks in one of the following two ways in the CLI. You can always enter an IP address in dotted decimal notation (XXX.XXX.XXX.XXX), specifying both the IP address and the subnet mask in dotted-decimal notation.

Assigning and clearing IP addresses

Using the CLI, you can assign IP addresses and gateway addresses, clear these addresses, and view configured IP addresses. This section covers these topics:

- "ip address command"
- "no ip address command" on page 355
- "ip default-gateway command" on page 356
- "no ip default-gateway command" on page 357
- "show ip command" on page 357

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 [switch|stack|unit] <XXX.XXX.XXX.XXX> [netmask <XXX.XXX.XXX.XXX>]`

The `ip address` command is in the config command mode.

If you do not enter either the stack or switch parameter, the system automatically modifies the stack IP address when in stack mode, and modifies the switch IP address when in stand-alone mode.

Table 50 describes the parameters and variables for the `ip address` command.

Table 50 ip address command parameters and variables

Parameters and variables	Description
`switch|stack|unit`	Sets the switch, stack, or other unit IP address and netmask.
XXX.XXX.XXX.XXX	Enter IP address in dotted decimal notation; netmask is optional.
`netmask`	Sets the IP subnet mask for the switch or stack.

Note: When you change the IP address or subnet mask, you can lose connection to Telnet and the Web-based management interface.

no ip address command

The `no ip address` command clears the IP address and subnet mask. This command sets the IP address and subnet mask for a switch to all zeros (0). The syntax for the `no ip address` command is:

`no ip address {switch|stack|unit}`

The `no ip address` command is in the config command mode.

Table 51 describes the parameters and variables for the `no ip address` command.

Table 51 `no` ip address command parameters and variables

Parameters and variables	Description
`switch|stack|unit`	Zeros out the IP address and subnet mask for the switch, stack, or other unit in the stack.

Note: When you change the IP address or subnet mask, you may lose connection to Telnet and the Web. You also disable any new Telnet connection, and you must connect to the serial console port to configure a new IP address.

ip default-gateway command

The `ip default-gateway` command sets the IP default gateway address for a switch or a stack to use. The syntax for the `ip default-gateway` command is:

`ip default-gateway <XXX.XXX.XXX.XXX>`

The `ip default-gateway` command is in the config command mode.

Table 52 describes the parameters and variables for the `ip default-gateway` command.

Table 52 ip default-gateway command parameters and variables

Parameters and variables	Description
XXX.XXX.XXX.XXX	Enter the dotted-decimal IP address of the default IP gateway.

Note: When you change the IP gateway, you may lose connection to Telnet and the Web.

no ip default-gateway command

The `no ip default-gateway` command sets the IP default gateway address to zeros (0). The syntax for the `no ip default-gateway` command is:

```
no ip default-gateway
```

The `no ip default-gateway` command is in the config command mode.

The `no ip default-gateway` command has no parameters or variables.

Note: When you change the IP gateway address, you may lose connection to Telnet and the Web. You also may disable any new Telnet connection be required to connect to the serial console port to configure a new IP gateway address.

show ip command

The `show ip` command displays the IP configurations, specifically BootP mode, stack address, switch address, subnet mask, and gateway address. This command displays the parameters for what is configured, what is in use, and the last BootP. The syntax for the `show ip` command is:

```
show ip [bootp] [default-gateway] [address [switch|stack]]
```

The `show ip` command is in the exec command mode. If you do not enter any parameters, this command displays all the IP-related configuration information.

Table 53 describes the parameters and variables for the `show ip` command.

Table 53 `show ip` command parameters and variables

Parameters and variables	Description
`bootp`	Displays BootP-related IP information.
`default-gateway`	Displays the IP address of the default gateway.
`address`	Displays the current IP address.
`switch|stack`	Specifies current IP address of the switch or stack.

Figure 115 displays a sample output of the `show ip` command.

Figure 115 `show ip` command output

```
470_24T#show ip
BootP Mode: BootP Disabled

                     Configured        In Use         Last BootP
                    --------------- --------------- ---------------
Stack IP Address:   10.20.30.41     10.20.30.41     0.0.0.0
Switch IP Address:  10.30.31.200                    0.0.0.0
Subnet Mask:        255.255.255.0   255.255.255.0   0.0.0.0
Default Gateway:    10.20.30.1      10.20.30.1      0.0.0.0
```

Assigning and clearing IP addresses for specific units

You can assign IP addresses for a specific units within a stack. This section covers these topics:

- "ip address unit command"
- "no ip address unit command" on page 359
- "default ip address unit command" on page 360

ip address unit command

The `ip address unit` command sets the IP address and subnet mask for a specific stand-alone unit or a specific unit in a 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 in the config command mode.

Table 54 describes the parameters and variables for the `ip address unit` command.

Table 54 ip address `unit` command parameters and variables

Parameters and variables	Description
<1-8>	Sets the unit you are assigning an IP address.
A.B.C.D	Enter IP address in dotted decimal notation.

Note: When you change the IP address or subnet mask, you may lose connection to Telnet and the Web.

no ip address unit command

The `no ip address unit` command sets the IP address for the specified unit to all 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 in the config command mode.

Table 55 describes the parameters and variables for the `no ip address unit` command.

Table 55 no ip address `unit` command parameters and variables

Parameters and variables	Description
<1-8>	Zeros out the IP address for the specified unit.

Note: When you change the IP address or subnet mask, you may lose connection to Telnet and the Web. You also disable any new Telnet connection, and you must connect to the serial console port to configure a new IP address.

default ip address unit command

The `default ip address unit` command sets the IP address for the specified unit 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 in the config command mode.

Table 56 describes the parameters and variables for the `default ip address unit` command.

Table 56 default ip address `unit` command parameters and variables

Parameters and variables	Description
`unit <1-8>`	Zeros out the IP address for the specified unit.

Note: When you change the IP gateway, you may lose connection to Telnet and the Web.

show stack-info command

The `show stack-info` command displays the current stack information, which includes unit numbers, cascade attachments, and software version for all units. The syntax for the `show stack-info` command is:

`show stack-info`

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

The `show stack-info` command has no parameters or variables.

Figure 116 on page 361 displays sample output from the `show stack-info` command.

Figure 116 `show stack-info` command output

```
470-24T#show stack-info
Unit# Switch Model      MDA Model  GBIC Port   GBIC Port   Cascade  SW Version
                                                            Module
----- ---------------- ---------- ---------- ---------- ------- ----------
1     470-24T                     (25) None   (26) None   400-ST1   v3.6.0.77
```

Refer to "Stacking" on page 293 for more information on stack operation.

Renumber unit command

The `renumber unit` command changes the unit number of each switch. The syntax for the `renumber unit` command is:

`renumber unit`

The `renumber unit` command is in the config command mode.

The `renumber unit` command has no parameters or variables.

Note: This command does not take effect until you reset the stack.

Pinging the switch

You can ping from Ethernet Switches 460 and 470. This ability greatly enhances the ease of network management. The ping command tests the network connection to another network device. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device. The local IP address must be set before issuing the ping command.

For more information on the CLI commands, see "ping command" on page 363.

Using DNS to ping and Telnet

Using the DNS client, you can ping or Telnet to a host server or to a host by name. To use this feature, you must configure at least one domain name server; you can also configure a default domain name. If you configure a default domain name, that name is appended to hostnames that do not contain a dot. The default domain name and addresses are saved in NVRAM.

The hostnames for ping and Telnet cannot be longer than 63 alphanumeric characters, and the default DNS domain name cannot be longer than 255 characters. This section covers these commands:

show ip dns command

The `show ip dns` command displays the DNS domain name, as well as any configured DNS servers. The syntax for the `show ip dns` command is:

```
show ip dns
```

The `show ip dns` command is in the exec command mode.

The `show ip dns` command has no parameters or variables.

Figure 117 on page 363 displays sample output from the `show ip dns` command.

Figure 117 `show ip dns` command output

```
470-48T#show ip dns
DNS Default Domain name: us.nortel.com
DNS Servers
- - - - - - -
47.82.2.10
0.0.0.0
0.0.0.0
470-48T#
```

ping command

The `ping` command tests the network connection to another network device. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device. The local IP address must be set before issuing the `ping` command.

You can ping a host using either its IP address or hostname.

The syntax for the `ping` command is:

```
ping <A.B.C.D or Hostname>
```

The `ping` command is in the exec command mode.

Table 57 describes the parameters and variables for the `ping` command.

Table 57 ping command parameters and variables

Parameters and variables	Description
<A.B.C.D or Hostname>	Specify: • the IP address of the target device in dotted-decimal notation • the hostname of the device to ping (The hostname can be a simple name, such as fred; in this case the DNS domain name, if set, is appended. Or the hostname can be a full hostname, such as fred.ca.nortel.com.)

If the device receives the packet, it sends a ping reply. When the switch receives the reply, it displays a message indicating that the specified IP address is alive. If no reply is received, a message indicates that the address is not responding.

Figure 118 displays sample `ping` responses.

Figure 118 `ping` command responses

```
470_48T#ping 10.10.40.29
Host is reachable
```

There is no default value for this command.

ip name-server command

The `ip name-server` command adds one or more DNS servers' IP addresses. The syntax for the `ip name-server` command is:

```
ip name-server <A.B.C.D>
```

The `ip name-server` command is in the config command mode.

Note: You can add up to 3 servers; adding one at a time.

Table 58 describes the parameters and variables for the `ip name-server` command.

Table 58 ip name-server command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of a DNS server.

The default value is 0.0.0.0.

no ip name-server command

The `no ip name-server` command removes one or more DNS servers' IP addresses. The syntax for the `no ip name-server` command is:

```
no ip name-server <A.B.C.D>
```

The `no ip name-server` command is in the config command mode.

Table 59 describes the parameters and variables for the `no ip name-server` command.

Table 59 no ip name-server command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of a DNS server.

The default value is 0.0.0.0.

ip domain-name command

The `ip domain-name` command sets the system's DNS domain name. The syntax for the `ip domain-name` command is:

```
ip domain-name [<LINE>]
```

The `ip domain-name` command is in the config command mode.

Table 60 describes the parameters and variables for the `ip domain-name` command.

Table 60 ip domain-name command parameters and variables

Parameters and variables	Description
<LINE>	Enter a DNS domain name.

The default value for this command is an empty string.

no ip domain-name command

The `no ip domain-name` command clears the system's DNS domain name (sets it to an empty string). The syntax for the `no ip domain-name` command is:

```
no ip domain-name
```

The `no ip domain-name` command is in the config command mode.

The `no ip domain-name` command has no parameters or variables.

default ip domain-name command

The `default ip domain-name` command clears the system's DNS domain name (set it to an empty string). The syntax for the `default ip domain-name` command is:

```
default ip domain-name
```

The `default ip domain-name` command is in the config command mode.

The `default ip domain-name` command has no parameters or variables.

Configuring the switch with a BootP/Dynamic IP Configuration

The Ethernet Switches 460 and 470 have 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 BootP requests from an Ethernet Switch. 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).

IP/BootP configuration retention on downgrade

When downgrading a unit with Release 3.0.3 software and later, the system defaults all configurations, except for the following:

- Stack operation mode
- IP configuration
- BootP mode

Previous releases of Ethernet Switch software retained the Stack Operational Mode only on software downgrade. This change allows a remotely accessed switch to maintain its accessibility after downgrade and does not require the user to re-enter this basic information, which remains unchanged after a downgrade.

Configuration Management

The Configuration File Menu screen allows you to upload and download the configuration parameters of an Ethernet Switch to a TFTP server. You can also download an ASCII configuration file from a TFTP server.

Binary upload and binary download

The Configuration File upload/download are of two types:

- Binary config file upload/download
- ASCII config file upload/download

These options allow you to store your switch configuration parameters on a TFTP server. You can retrieve the configuration parameters of a stand-alone switch, and use the retrieved parameters to automatically configure a replacement switch. You must set up the file on your TFTP server and set the filename read-write permission to enabled before you can save the configuration parameters.

Automatically loading an ASCII configuration file

This section discusses how to download a configuration file when the system boots. You use standard CLI commands to modify the configuration file you want to download. This section covers these commands:

- "configure-network command"
- "show config-network command" on page 369

configure-network command

The `configure-network` command allows you to load and execute a script immediately and to configure parameters to automatically download a configuration file when you reboot the switch or stack. The syntax for the `configure-network` command is:

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

The `configure-network` command is in the exec mode.

Note: When you enter the `configure-network` command with no parameters, the system prompts you for the script file name and TFTP server address and then downloads the script.

Table 61 describes the parameters and variables for the `configure-network` command.

Table 61 configure-network command parameters and variables

Parameters and variables	Description
`load-on-boot {disable| use-bootp| use-config}`	Specifies the settings for automatically loading a configuration file when the system boots: • `disable`—disables the automatic loading of config file • `use-boot`—specifies using the BootP file as the automatically loaded config file • `use-config`—specifies using the ASCII configuration file as the automatically loaded config file Note: If you omit this parameter, the system immediately downloads and runs the ASCII config file.
`filename <WORD>`	Specifies the file name. Note: If you omit this parameter and do not specify BootP, the system uses the configured file name.
`address <XXX.XXX.XXX.XXX>`	Specifies the TFTP server from which to load the file. Enter the IP address in dotted-decimal notation. Note: If you omit this parameter and do not specify BootP, the system uses the configured address.

Note: When you specify the file name or address, these parameters are changed at the next reboot, even if you do not specify load-on-boot.

show config-network command

The `show config-network` command displays information regarding the automatic loading of the configuration file, including the current status of this feature, the file name, the TFTP server address, and the status of the previous automatic configuration command. The syntax for the `show config-network` command is:

```
show config-network
```

The `show config-network` command is in the privExec mode.

The `show config-network` command has no parameters or variables.

The output for the `show config-network` command is shown in Figure 119,

Figure 119 `show config-network` command

```
470-24T(config)#show config-network
Auto-Load Configuration On Boot:  Disabled
Configuration Filename:
TFTP Server IP Address:  192.168.100.15
Last Auto Configuration Status:  Passed
```

ASCII Configuration Generator (ACG)

The ACG application allows you to save a switch's provisioning information to an external file and download this information to a switch from an external file server.

Note: The external file server must support TFTP.

You can use ACG to:

- Display the current configuration on the CLI.
- Store the current configuration in an external file.
- Load configuration from an external file
- Load configuration at boot time

This section covers the ACG commands available and includes:

- "show running-config" on page 371
- "copy running-config" on page 372
- "configure network" on page 372
- "configure network load-on-boot" on page 375

show running-config

The `show running-config` command displays the current switch configuration information. The syntax for the `show running-config` command is:

```
show running-config
```

The `show running-config` command is in the privExec command mode.

Note: The `show running-config` command is available, but its use is restricted, when a user has read-only access.

The `show running-config` command has no parameters or variables.

Figure 120 displays a sample output of the `show running-config` command.

Figure 120 `show running-config` command output

```
470-24T#show running-config
enable
config t
mac-address-table aging-time 300
autotopology
snmp-server authentication-trap enable
snmp-server contact "SysAdmin"
snmp-server name "470"
snmp-server location "Lab"
snmp-server community "public" ro
snmp-server community "private" rw
--More--
```

copy running-config

The `copy running-config` command copies the current switch configuration as an ASCII file on the TFTP server. The syntax for the `copy running-config` command is:

```
copy running-config tftp [address <A.B.C.D>] filename <WORD>
```

Note: The `copy config` command will copy a binary configuration file to the TFTP server. To store the configuration as an ASCII file, you must use the `copy running-config` command.

The `copy running-config` command is in the privExec command mode.

Table 62 describes the parameters and variables for the `copy running-config` command.

Table 62 copy running-config command parameters and variables

Parameters and variables	Description
address <A.B.C.D>	Specifies the TFTP server IP address; enter in dotted-decimal notation.
filename <WORD>	Specifies the name of the existing ASCII configuration file on the TFTP server. This file must be read-write enabled.

Figure 121 displays a sample output of the `copy running-config` command.

Figure 121 `copy running-config` command output

```
470-24T#copy running-config tftp address 134.177.118.56
filename config.txt
%Contacting TFTP host: 134.177.118.56.
%ACG Configuration file successfully written.
470-24T#
```

configure network

The `configure network` command loads configuration from an external file on to the switch. The syntax for the `configure network` command is:

```
configure network [address <A.B.C.D>] [filename <WORD>]
```

The `configure network` command is in the PrivExec mode, Global configuration mode, and Interface configuration mode.

Table 63 describes the parameters and variables for the `configure network` command.

Table 63 configure network command parameters and variables

Parameters and variables	Description
address <A.B.C.D>	Specifies the TFTP server IP address; enter in dotted-decimal notation.
filename <WORD>	Enter the name of the ASCII configuration file you want to copy from the TFTP server.

Figure 122 on page 374 displays a sample output of the `configure network` command.

Figure 122 `configure network` command output

```
470-24T#configure network address 134.177.118.56 filename config.txt
Downloading Config File [|]
470-24T#enable
Downloaded file successfully, executing . . .
470-24T#config t
Enter configuration commands, one per line.  End with CNTL/Z.
470-24T(config)#mac-address-table aging-time 300
470-24T(config)#autotopology
470-24T(config)#snmp-server authentication-trap enable
470-24T(config)#snmp-server contact "HCS lab"
470-24T(config)#snmp-server community "public" ro
470-24T(config)#snmp-server community "private" rw
470-24T(config)#ip bootp server disable
470-24T(config)#ip default-gateway 134.177.150.1
470-24T(config)#ip address 134.177.150.79
470-24T(config)#ip address netmask 255.255.255.0
470-24T(config)#no auto-pvid
% AutoPVID already disabled.
470-24T(config)#vlan mgmt 1
470-24T(config)#vlan name 1 "VLAN #1"
470-24T(config)#vlan members remove 1 ALL
470-24T(config)#vlan members 1 ALL
470-24T(config)#vlan members 2 1-12
470-24T(config)#$ed-frame disable filter-untagged-frame disable priority
0
470-24T(config)#$ enable proxy enable robust-value 2 query-interval 125
470-24T(config)#$ enable proxy enable robust-value 2 query-interval 125
470-24T(config)#vlan mgmt 1
470-24T(config)#spanning-tree priority 8000
470-24T(config)#spanning-tree hello-time 2
470-24T(config)#spanning-tree max-age 20
470-24T(config)#spanning-tree forward-time 15
470-24T(config)#interface FastEthernet ALL
470-24T(config-if)#spanning-tree port 1-24 learning normal
470-24T(config-if)#exit
470-24T(config)#no mlt
470-24T(config)#mlt 1 name "Trunk #1"
470-24T(config)#mlt 2 name "Trunk #2"
470-24T(config)#mlt 3 name "Trunk #3"
470-24T(config)#mlt 4 name "Trunk #4"
470-24T(config)#mlt 5 name "Trunk #5"
470-24T(config)#mlt 6 name "Trunk #6"
470-24T(config)#interface FastEthernet ALL
470-24T(config-if)#no shutdown port 1-24
470-24T(config-if)#snmp trap link-status port 1-24 enable
470-24T(config-if)#speed port 1-24 auto
470-24T(config-if)#duplex port 1-24 auto
470-24T(config-if)#exit
```

configure network load-on-boot

The `configure network load-on-boot` command is used to configure the switch to automatically download a configuration file when you reboot the switch. The syntax for the `configure network load-on-boot` command is:

```
configure network load-on-boot {disable|use-bootp|
use-config} [address <A.B.C.D>] filename <WORD>
```

The `configure network load-on-boot` command is in the PrivExec mode, Global configuration mode, and Interface configuration mode.

Table 64 describes the parameters and variables for the `configure network load-on-boot` command.

Table 64 configure network load-on-boot command parameters

Parameters and variables	Description
{disable | use-bootp| use-config}	Specifies the settings for automatically loading a configuration file when the system boots: • disable—disables the automatic loading of the configuration file • use-bootp—specifies using the BootP file as the automatically loaded configuration file • use-config—specifies using the ASCII configuration file as the automatically loaded configuration file
address <A.B.C.D>	Specifies the TFTP server IP address; enter in dotted-decimal notation.
filename <WORD>	Enter the name of the ASCII configuration file you want to copy from the TFTP server.

Figure 123 displays a sample output of the `configure network load-on-boot` command.

Figure 123 `configure network load-on-boot` command output

```
470-24T#configure network load-on-boot use-config address
134.177.118.56 filename config.txt
470-24T#
```

Downloading and uploading your software

You can download the switch software image that is located in non-volatile flash memory. To download the switch software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the Ethernet Switch must have an IP address. To learn how to configure the switch IP address, refer to "Assigning and clearing IP addresses" on page 354.

Caution: Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

You also download the Power over Ethernet (PoE) image using the CLI.

This section covers the following topics:

download command

The `download` command upgrades the software for the switch. You can upgrade the software image, the diagnostics image, and/or the PoE image. If you upgrade to a stack configuration, the entire stack is upgraded, and the new image is loaded onto every unit of the stack.

Note: The default downloading process without this command, is that the unit resets after downloading.

The syntax for the `download` command is:

```
download [address <ip>] {image <image-name>|image-if-newer
<image-name>|diag <filename>}[no-reset]
```

The `download` command is in the privExec command mode.

Table 65 describes the parameters and variables for the `download` command.

Table 65 download command parameters and variables

Parameters and variables	Description
address <ip>	Specifies the TFTP server you want to use. Note: If this parameter is omitted, the system goes to the server specified by the `tftp-server` command.
image <image-name>	Enter the name of the software image you want to download.
image-if-newer <image-name>	Enter the name of the software image you want to download if newer than the current running image.
diag <filename>	Enter the name of the diagnostics image you want to download.
no-reset	Download the specified software without resetting the unit.

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Do not attempt any switch configurations or otherwise interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

When the download process is complete, the switch automatically resets (unless you specify no-reset) and the new software image initiates a self-test. The system returns a message after successfully downloading a new image. Figure 124 displays a sample output of the download command.

Figure 124 download message

```
Download Image [/]
Saving Image [-]
Finishing Upgrading Image
```

You can monitor the progress of the download process by observing the LED indications.

Observing LED indications

Note: When you upgrade the software in a stack, all the BU LEDs on all switch units can light or blink. Disregard these lights.

Table 66 describes the LED indications during the software download process for the Ethernet Switch 470-24T.

Table 66 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs ports 1 to 24:** The LEDs blink in succession from both ends and criss-cross at the center of the switch.
2	The switch erases the flash memory.	**100 Mb/s LEDs ports 1 and 24 stay lit**.
3	The switch programs the new software image into the flash memory.	**Same as phase 1**.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Table 67 describes the LED indications during the software download process for the Ethernet Switch 460-24T-PWR.

Table 67 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs (ports 18 to 24 only):** The LEDs begin to turn on in succession beginning with port 24, which indicates the progress of the download process. When LEDs 18 to 24 are all on, the switch has received the new software image successfully.
2	The switch erases the flash memory.	**100 Mb/s port status LEDs (ports 1 to 12 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that various sectors of the switches flash memory are being erased. When LEDs 1 to 12 are all on, the switches flash memory has been erased.

Table 67 LED Indications during the software download process

Phase	Description	LED Indications
3	The switch programs the new software image into the flash memory.	**100 Mb/s port status LEDs (ports 1 to 8 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that the new software image is being programmed into the switches flash memory. When LEDs 1 to 8 are all on, the new software image has been programmed successfully into the switches flash memory.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Table 68 describes the LED indications during the software download process for the Ethernet Switch 470-48T.

Table 68 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs ports 1 to 48:** The LEDs blink in succession from both ends and criss-cross at the center of the switch.
2	The switch erases the flash memory.	**100 Mb/s LEDs ports 1 and 48 stay lit**.
3	The switch programs the new software image into the flash memory.	**Same as phase 1**.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Upgrading software in an Ethernet Switch stack

With Ethernet Switch software, you must download software for the stack using the base unit.

Any one of the switches in the stack can function as a base unit in a stack; however, if an Ethernet Switch 470-48T is in the stack, it must be the base unit. Otherwise, if an Ethernet Switch 470-24T unit is in the stack, it must be the base unit. If neither an Ethernet Switch 470-48T nor an Ethernet Switch 470-24T is in the stack, then an Ethernet Switch 460-24T-PWR can be the base unit.

Note: The Hybrid stack mode is not supported in Release 3.6 software. All stacks must contain only Ethernet Switches 460-24T-PWR, Ethernet Switches 470-24T, and Ethernet Switches 470-48T.

To download, or upgrade, software in an Ethernet Switch stack:

1. Enter `download [address <ip>] image` **`<3.6_image.img>`**.

   The system resets and opens to the Nortel banner.

2. Enter `download [address <ip>] diag` **`<3.6_diags.bin>`**.

   The system resets and opens to the Nortel banner.

Customizing your system

You can customize your system using the following CLI commands. This section covers:

Setting the terminal

You can view the terminal settings, set them to default settings, or customize the terminal settings. This section covers:

show terminal command

The `show terminal` command displays the current serial port information, which includes connection speed, as well as the terminal width and length in number of characters. The syntax for the `show terminal` command is:

```
show terminal
```

The `show terminal` command is in the exec command mode.

The `show terminal` command has no parameters or variables.

Figure 125 displays the output from the `show terminal` command.

Figure 125 `show terminal` command output

```
470-24T#show terminal
Terminal speed: 9600
Terminal width: 79
Terminal length: 23
```

default terminal command

The `default terminal` command configures default settings for the terminal. These settings are transmit and receive speeds, terminal length, and terminal width. The syntax for the `default terminal` command is:

```
default terminal {speed|width|length}
```

The `default terminal` command is in the exec mode.

Table 69 describes the parameters and variables for the `default terminal` command.

Table 69 default terminal command parameters and variables

Parameters and variables	Description
`speed|width|length`	Sets the defaults • `speed`—transmit and receive baud rates for the terminal; default is 9600 baud • `width`—width of the terminal display; default is 79 characters • `length`—Length of the terminal display; default is 24 characters

terminal command

The `terminal command` configures the settings for the terminal. 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
<1-132>|width <1-132>
```

The `terminal command` is in the exec mode.

Table 70 describes the parameters and variables for the `terminal` command.

Table 70 terminal command parameters and variables

Parameters and variables	Description
`speed {2400|4800|9600|19200|38400}`	Sets the transmit and receive baud rates for the terminal. You can set the speed at one of the five options shown; default is 9600.
`length`	Sets the length of the terminal display in characters; default is 24.
`width`	Sets the width of the terminal display in characters; default is 79.

show cli command

The `show cli` command displays the current CLI settings. The syntax for the `show cli` command is:

```
show cli [info|password]
```

The `show cli` command is in the exec command mode.

Table 71 describes the parameters and variables for the `show cli` command.

Table 71 show cli command parameters and variables

Parameters and variables	Description
`info`	Displays general CLI settings.
`password`	Displays CLI usernames and passwords.

Figure 126 displays the output from the `show cli` command.

Figure 126 `show cli` command output

```
470-24T#show cli info
Inactivity Timeout:  15 minute(s)
Login Timeout:  1 minute(s)
Login Retries:  3
More:
Screen Lines:
470-24T#show cli password
          Switch
Access Login     Password
------ --------- ------------------
RWA    RWA       secure
RW     RW        secure
RO     RO        user

           Stack
Access Login     Password
------ --------- ------------------
RWA    RWA       secure
RW     RW        secure
RO     RO        user
```

Displaying system information

The `show sys-info` command displays the current system characteristics, which includes HW rev, FW rev, date of manufacture (DOM), and Hardware deviation number. The syntax for the `show sys-info` command is:

```
show sys-info
```

The `show sys-info` command is in the privExec command mode.

The `show sys-info` command has no parameters or variables.

Figure 127 on page 385 and Figure 128 on page 386 displays sample output from the `show sys-info` command.

Figure 127 `show sys-info` command output

```
460_24T_PWR#show sys-info
Operation Mode:         Switch
MAC Address:            00-09-97-29-1F-00
Reset Count:            1
Last Reset Type:        Software Download
Power Status:           Primary Power
Autotopology:           Enabled
Current Switch Mode:    L2
Next Boot Switch Mode:  L2
Local MDA Type:         None
PoE Module FW:          7013.2
sysDescr:               Ethernet Switch 460 - 24T - PWR
                        HW:00       FW:3.0.0.5   SW:v3.6.0.0
ISVN:2
                        Mfg Date:20021102    HW Dev:
Serial #:               SDNIHR007B
sysObjectID:            1.3.6.1.4.1.45.3.49.1
sysUpTime:              12 days, 07:04:49
sysNtpTime:             SNTP not synchronized.
sysServices:            3
sysContact:
sysName:
sysLocation:
460_24T_PWR#show sys-info
```

Figure 128 `show sys-info` command output

```
470-48T#show sys-info
Operation Mode:          Switch
MAC Address:             00-04-38-D5-9F-C0
Reset Count:             1
Last Reset Type:         Software Download
Power Status:            Primary Power
Autotopology:            Enabled
Current Switch Mode:     L2
Next Boot Switch Mode:   L2
GBIC Port 47:            None
GBIC Port 48:            None
sysDescr:                Ethernet Switch 470 - 48T
                         HW:#0D      FW:3.0.0.5    SW:v3.6.0.0
ISVN:2
                         Mfg Date:20020717    HW Dev:
Serial #:                ACC1000CP
sysObjectID:             1.3.6.1.4.1.45.3.46.1
sysUpTime:               12 days, 08:43:00
sysNtpTime:              SNTP not synchronized.
sysServices:             3
sysContact:
sysName:
sysLocation:
470-48T#
```

To change the system contact, name, or location, refer to the `snmp-server` command.

Setting boot parameters

You can reboot the switch or stack and configure BootP. The topics covered in this section are:

boot command

The `boot` command performs a soft-boot of the switch. The syntax for the `boot` command is:

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

The `boot` command is in the privExec command mode.

Table 72 describes the parameters and variables for the `boot` command.

Table 72 boot command parameters and variables

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

Note: When you reset to factory defaults, the switch retains the last reset count, and reason for last reset; these parameters are not changed to factory defaults.

ip bootp server command

The `ip bootp server` command configures BootP on the current instance of the switch or server. You use this command if you want 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 {last|needed|disable|always}
```

The `ip bootp server` command is in the config command mode.

Table 73 describes the parameters and variables for the `ip bootp server` command.

Table 73 ip bootp server command parameters and variables

Parameters and variables	Description
last|needed|disable|always	Specifies when to use BootP: • always—Always use BootP • disable—never use BootP • last—use BootP or the last known address • needed—use BootP only when needed NOTE: The default value is to use BootP when needed.

stack bootp-mac-addr-type command

The `stack bootp-mac-addr-type` command allows you to choose which MAC address is used for BootP operation when running in a stack. The syntax for the `stack bootp-mac-address-type` command is:

```
stack bootp-mac-addr-type {base-unit|stack}
```

The `stack bootp-mac-addr-type` command is in the config command mode.

Table 74 describes the parameters and variables for the `stack boot-mac-addr-type` command.

Table 74 stack boot-mac-addr-type command parameters and variables

Parameters and variables	Description
`base-unit|stack`	Specifies location of BootP MAC address: • `base-unit`—use the base unit MAC address for BootP • `stack`—use the stack MAC address for BootP

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 in the config command mode.

The `no ip bootp server` command has no parameters or variables.

default ip bootp server command

The `default ip bootp server` command disables the BootP server. The syntax for the `default ip bootp server` command is:

```
default ip bootp server
```

The `default ip bootp server` command is in the config command mode.

The `default ip bootp server` command has no parameters or variables.

Setting TFTP parameters

You can display the IP address of the TFTP server, assign an IP address you want to use for a TFTP server, copy a configuration file to the TFTP server, or copy a configuration file from the TFTP server to the switch to use to configure the switch. This section covers:

show tftp-server command

The `show tftp-server` command displays the IP address of the server used for all TFTP-related transfers. The syntax for the `show tftp-server` command is:

```
show tftp-server
```

The `show tftp-server` command is in the privExec command mode.

The `show tftp-server` command has no parameters or variables.

Figure 129 displays a sample output of the `show tftp-server command`.

Figure 129 `show tftp-server` command output

```
470-24T#show tftp-server
TFTP Server IP address : 192.168.100.15
```

tftp-server command

The `tftp-server` command assigns the address for the switch to use for TFTP services. The syntax for the `tftp-server` command is:

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

The `tftp-server` command is in the config command mode.

Table 75 describes the parameters and variables for the `tftp-server` command.

Table 75 tftp-server command parameters and variables

Parameters and variables	Description
XXX.XXX.XXX.XXX	Enter the dotted-decimal IP address of the server you want to use for TFTP services.

no tftp-server command

The `no tftp-server` command clears the TFTP server IP address to `0.0.0.0`. The syntax of the `no tftp-server` command is:

```
no tftp-server
```

The `no tftp-server` command is in the config command mode.

The `no tftp-server` command has no parameters or variables.

copy config tftp command

The `copy config tftp` command copies the current configuration file onto the TFTP server. The syntax for the `copy config tftp` command is:

```
copy config tftp [address <XXX.XXX.XXX.XXX>] filename <WORD>
```

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

Table 76 describes the parameters and variables for the `copy config tftp` command.

Table 76 copy config tftp command parameters and variables

Parameters and variables	Description
`[address <XXX.XXX.XXX.XXX>]`	Specifies the TFTP server IP address; enter in dotted-decimal notation.
`filename <WORD>`	Specifies that you want to copy the configuration file onto the TFTP server. Enter the name you want the configuration file to have on the TFTP server.

Customizing the opening banner

You can customize the opening banner that appears when you either connect to the switch console port, or Telnet to the switch. You can customize the word NORTEL, written in asterisks, when the screen is opened the first time. You cannot customize the portion that displays “Enter Ctrl-Y to begin” (Figure 130 on page 392).

Figure 130 Portion of opening banner you *cannot* customize

```
Enter Ctrl-Y to begin.

  ************************************************************
  * Ethernet Switch 470 - 24T                                *
  * Nortel                                                   *
  * Copyright (c) 1996-2005, All Rights Reserved             *
  * BoSS 3.6                                                 *
  * Ver:  HW:#0A      FW:3.0.0.4   SW:v3.6.0.0 ISVN:2        *
  ************************************************************
```

The banner cannot exceed 11215 bytes, or 15 rows x 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.

You must create the custom banner one line at a time using the Command Line Interface (CLI). Additionally, you can download the customer banner using the ASCII configuration file.

The following topics describe the CLI commands you use to customize the display banner:

- "show banner command"
- "banner command for displaying banner" on page 393
- "banner command for creating banner" on page 394
- "no banner command" on page 394

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 in the privExec command mode.

Table 77 describes the parameters and variables for the `show banner` command.

Table 77 `show banner` command parameters and variables

Parameters and variables	Description
`static|custom`	Displays which banner is currently set to display • `static` • `custom`

Figure 131 displays a sample output of the `show banner` command.

Figure 131 `show banner` command output

```
470-24T#show banner
Current banner setting: CUSTOM
```

banner command for displaying banner

The `banner` command for displaying banner specifies the banner displayed at startup; either static or custom. The syntax for the `banner` command for displaying banner is:

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

The `banner` command for displaying banner is in privExec command mode.

Table 78 describes the parameters and variables for the `banner` command.

Table 78 `banner` command for displaying banner parameters and variables

Parameters and variables	Description
`static|custom`	Sets the display banner as: • `static` • `custom`

banner command for creating banner

The `banner` command for creating banner allows you to create a custom banner. The syntax for the `banner` command for creating banner is:

`banner <line number> <text>`

The `banner` command for creating banner is in the privExec command mode.

Table 79 describes the parameters and variables for the `banner` command.

Table 79 `banner` command for creating banner parameters and variables

Parameters and variables	Description
<line number>	Enter the banner line number you are setting. The range is 1 to 15.
<text>	Enter the character string you want to display. The range is 1 to 80.

no banner command

The `no banner` command allows you to clear all lines of a previously stored custom banner. The syntax for the `no banner` command is:

`no banner`

The `no banner` command is in the privExec command mode.

Displaying the ARP table

The `show arp-table` command displays the Address Resolution Protocol (ARP) table of the device. The syntax for the `show arp-table` command is:

`show arp-table`

The `show arp-table` command is in the exec command mode.

The `show arp-table` command has no parameters or variables.

Figure 132 displays a sample output of the `show arp-table` command.

Figure 132 `show arp-table` command output

```
470-24T#show arp-table
Port IP Address      MAC Address
---- --------------- -----------------
24   10.30.40.1      00:00:A2:0B:3D:45
```

Displaying interfaces

You can view the status of all interfaces on the switch, including MultiLink Trunk membership, link status, autonegotiation, and speed.

show interfaces command

The `show interfaces` command displays the current configuration and status of all interfaces. The syntax for the `show interfaces` command is:

`show interfaces [names] [<portlist>]`

The `show interfaces` command is in the exec command mode.

Table 80 describes the parameters and variables for the `show interfaces` command.

Table 80 show interfaces command parameters and variables

Parameters and variables	Description
`names` `<portlist>`	Displays the interface names; enter specific ports if you want to see only those.

Figure 133 on page 396 displays a sample output of the `show interfaces names` command.

Figure 133 `show interfaces names` command output

```
470-24T>show interfaces names 1-3
Port Name
---- ----------------------------------------------------------------
1     LabBldg4
2     Testing
3     Floor1Bldg2
```

Figure 134 displays a sample output of the `show interfaces` command without the names variable.

Figure 134 `show interfaces` command output

```
470-24T#show interfaces
               Status                        Auto                          Flow
Port Trunk Admin   Oper Link LinkTrap Negotiation Speed    Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
1          Enable  Down Down Enabled  Enabled
2          Enable  Down Down Enabled  Enabled
3          Enable  Down Down Enabled  Enabled
4          Enable  Down Down Enabled  Enabled
5          Enable  Down Down Enabled  Enabled
6          Enable  Down Down Enabled  Enabled
7          Enable  Down Down Enabled  Enabled
8          Enable  Down Down Enabled  Enabled
9          Enable  Down Down Enabled  Enabled
10         Enable  Down Down Enabled  Enabled
11         Enable  Down Down Enabled  Enabled
12         Enable  Down Down Enabled  Enabled
13         Enable  Down Down Enabled  Enabled
14         Enable  Up   Up   Enabled  Enabled     10M
15         Enable  Down Down Enabled  Enabled
16         Enable  Down Down Enabled  Enabled
17         Enable  Down Down Enabled  Enabled
18         Enable  Down Down Enabled  Enabled
19         Enable  Down Down Enabled  Enabled
--More--
```

show cmd-interface command

The `show cmd-interface` command displays the current default interface. The syntax for the `show cmd-interface` command is:

```
show cmd-interface
```

Figure 135 displays a sample output of the `show cmd-interface` command.

Figure 135 `show cmd-interface` command output

```
-- --------------------------------------------------------------------
460_24T_PWR#show cmd-interface
Default interface: Menu
460_24T_PWR#
```

Displaying unit uptime

You can display the uptime for each unit in a stack. Unit stack uptime collects the stack uptime for each unit in a stack and reports this information when requested. This allows you to determine how long each unit has been connected to the stack. You must use the Command Line Interface (CLI) commands system to display the unit uptimes.

The `show stack-info uptime` command displays the uptime for all units in the stack.

The syntax for the `show stack-info uptime` command is:

```
show stack-info uptime
```

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

The `show stack-info uptime` command has no parameters or variables.

Figure 136 on page 398 displays sample output from the `show stack-info uptime` command.

Figure 136 `show stack-info uptime` command output

```
470_24T#show stack-info uptime
Unit# Switch Model     Unit UpTime
----- ---------------- --------------------
1          470-24T 4 days, 21:38:46
2          470-24T 4 days, 21:38:46
3          470-24T 4 days, 21:38:46
4          470-24T 4 days, 21:38:46
5          470-24T 4 days, 21:38:44
6          470-24T 4 days, 21:38:46
```

Enabling and disabling autosave

You can enable or disable the autosave feature of your unit. Autosave automatically saves your configuration information across reboots. This section covers these commands:

- "show autosave command"
- "autosave enable command" on page 399
- "no autosave enable command" on page 399
- "default autosave enable command" on page 399

Note: You can use the CLI command `copy config nvram` to force a manual save of the configuration when autosave is disabled.

show autosave command

The `show autosave` command displays the status of the autosave feature, either enabled or disabled. The syntax for the `show autosave` command is:

```
show autosave
```

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

The `show autosave` command has no parameters or variables.

Figure 137 displays sample output from the `show autosave` command.

Figure 137 `show autosave` command output

```
470-48T#show autosave
Auto Save:  Enabled
```

autosave enable command

The `autosave enable` command enables the autosave feature. The syntax for the `autosave enable` command is:

```
autosave enable
```

The `autosave enable` command is in the config command mode.

The `autosave enable` command has no parameters or variables.

no autosave enable command

The `no autosave enable` command disables the autosave feature. The syntax for the `no autosave enable` command is:

```
no autosave enable
```

The `no autosave enable` command is in the config command mode.

The `no autosave enable` command has no parameters or variables.

default autosave enable command

The `default autosave enable` command defaults the autosave feature to the default value of enabled. The syntax for the `default autosave enable` command is:

```
default autosave enable
```

The `default autosave enable` command is in the config command mode.

The `default autosave enable` command has no parameters or variables.

Setting time on network elements using Simple Network Time Protocol (SNTP)

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.

You use the CLI to configure the SNTP feature, ensuring that you complete the following steps:

1. Set the primary and secondary NTP server.
2. Enable SNTP.
3. Display the UTC time.

Optionally, to ensure the synchronization happens immediately, force a synchronization.

Note: If you have trouble using this feature, try various NTP servers. Some NTP servers can be either overloaded or currently inoperable.

- “show sntp command” on page 401
- “show sys-info command” on page 401
- “sntp enable command” on page 402
- “no sntp enable command” on page 403
- “sntp server primary address command” on page 403
- “sntp server secondary address command” on page 404
- “no sntp server command” on page 404
- “sntp sync-now command” on page 405
- “sntp sync-interval command” on page 405

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 in the privExec command mode.

The `show sntp` command has no parameters or variables.

Figure 138 displays sample output from the `show sntp` command.

Figure 138 `show sntp` command output

```
470-48T#show sntp
SNTP Status:                    Enabled
Primary server address:         47.82.2.10
Secondary server address:       47.81.2.10
Sync interval:                  24 hours
Last sync source:               47.82.2.10
Primary server sync failures:   0
Secondary server sync failures: 0
Last sync time:                 2003-10-27 19:32:17 GMT
Next sync time:                 2003-10-28 19:32:17 GMT
Current time:                   2003-10-27 19:47:35 GMT
```

show sys-info command

The `show sys-info` command displays the current system characteristics.

Note: You must have SNTP enabled and configured to display GMT time.

The syntax for the `show sys-info` command is:

```
show sys-info
```

The `show sys-info` command is in the privExec command mode.

The `show sys-info` command has no parameters or variables.

Figure 139 displays sample output from the `show sys-info` command.

Figure 139 `show sys-info` command output

```
470-48T#show sys-info
Operation Mode:         Switch
MAC Address:            00-04-38-D5-9F-C0
Reset Count:            1
Last Reset Type:        Software Download
Power Status:           Primary Power
Autotopology:           Enabled
Current Switch Mode:    L2
Next Boot Switch Mode:  L2
GBIC Port 47:           None
GBIC Port 48:           None
sysDescr:               Ethernet Switch 470 - 48T
                        HW:#0D      FW:3.0.0.5    SW:v3.6.0.0
ISVN:2
                        Mfg Date:20020717    HW Dev:
Serial #:               ACC1000CP
sysObjectID:            1.3.6.1.4.1.45.3.46.1
sysUpTime:              12 days, 08:43:00
sysNtpTime:             SNTP not synchronized.
sysServices:            3
sysContact:
sysName:
sysLocation:
470-48T#
```

sntp enable command

Note: The default setting for SNTP is disabled.

The `sntp enable` command enables SNTP. The syntax for the `sntp enable` command is:

```
sntp enable
```

The `sntp enable` command is in the config command mode.

The `sntp enable` command has no parameters or variables.

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 in the config command mode.

The `no sntp enable` command has no parameters or variables.

sntp server primary address command

The `sntp server primary address` command specifies the IP addresses of the primary NTP server. The syntax for the `sntp server primary address` command is:

```
sntp server primary address <A.B.C.D>
```

The `sntp server primary address` command is in the config command mode.

Table 81 describes the parameters and variables for the `sntp server primary address` command.

Table 81 `sntp server primary address` command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of the primary NTP server.

The default is 0.0.0.0.

sntp server secondary address command

The `sntp server secondary address` command specifies the IP addresses of the secondary NTP server. The syntax for the `sntp server secondary address` command is:

```
sntp server secondary address <A.B.C.D>
```

The `sntp server secondary address` command is in the config command mode.

Table 82 describes the parameters and variables for the `sntp server secondary address` command.

Table 82 `sntp server secondary address` command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of the secondary NTP server.

The default is 0.0.0.0.

no sntp server command

The `no sntp server` command clears the NTP server IP addresses. The syntax for the `no sntp server` command is:

```
no sntp server <primary|secondary>
```

The `no sntp server` command is in the config command mode.

Table 83 describes the parameters and variables for the `no sntp server` command.

Table 83 `no sntp server` command parameters and variables

Parameters and variables	Description
<primary|secondary>	Enter the NTP server you want to clear: • primary—clears the IP address for the primary NTP server • secondary—clears the IP address for the secondary NTP server

sntp sync-now command

The `sntp sync-now` command forces a manual synchronization with the NTP server.

Note: You must have SNTP enabled before this command can take effect.

The syntax for the `sntp sync-now` command is:

```
sntp sync-now
```

The `sntp sync-now` command is in the config command mode.

The `no sntp sync-now` command has no parameters or variables.

sntp sync-interval command

The `sntp sync-interval` command specifies recurring synchronization with the 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 in the config command mode.

Table 84 describes the parameters and variables for the `sntp sync-interval` command.

Table 84 `sntp sync-interval` command parameters and variables

Parameters and variables	Description
<0-168>	Enter the number of hours you want for periodic synchronization with the NTP server. NOTE: 0 is boot-time only, and 168 is once a week; the default value is 24 hours.

Enabling traffic separation

You can separate traffic on the network so that IP packets are forwarded to a predefined CDN port using the traffic separation mode. Enabling this feature also ensures that both control and data PPoE packets are forwarded to a predefined ISP port.

To enable traffic separation, use the following command:

```
config switch mode <l2|traffic-separation>
```

The `config switch mode` command is in the privExec command mode.

Table 85 describes the parameters and variables for the `config switch mode` command.

Table 85 `config switch mode` command parameters and variables

Parameters and values	Description
`<l2|traffic-separation>`	Enter traffic-separation to enable the traffic separation feature.

Default traffic-separation restrict

This command sets the mode for traffic separation restrict to Layer3 restriction, The user is not allowed to create new L3 policies. This command is similar to the `traffic-separation restrict` command.

This command can be executed in the Global Configuration mode and there are no parameters associated with this command.

No traffic-separation restrict

This command sets the mode for traffic separation restrict, to no restriction. The user is allowed to create all types of L3 policies.There are no restrictions on creation of policies.

This command can be executed in the Global Configuration mode and has no associated parameters.

show traffic-separation

This command displays the current traffic separation settings, including the traffic separation restrict mode. Figure 140 shows the output of this command.

Figure 140 `show traffic restriction` command output

```
Traffic Separation:  Enabled
CDN Port Number:  47
ISP Port Number:    48
Policy Config Restriction Mode:  L3
```

Saving the configuration to NVRAM

You can save your configuration parameters to Non-Volatile RAM (NVRAM) using the CLI. This section covers the following topic:

- "copy config nvram" on page 408

copy config nvram

The `copy config nvram` copies the current configuration to NVRAM. The syntax for the `copy config nvram` command is:

```
copy config nvram
```

The `copy config nvram` command is in the privExec command mode.

The `copy config nvram` command has no parameters or variables.

Note: The system automatically issues the `copy config nvram` command periodically.

Trap notification when configuration changes are saved to NVRAM

When configuration changes are written to non-volatile memory, a trap (bsnConfigurationSavedToNvram) is sent to the trap receiver indicating that a change has occurred to the configuration of the device. This trap will also appear as an event in the volatile system log.

For each stand-alone and stack configuration, you must configure a trap destination. Use the following CLI commands:

```
snmp-server community trap notify-view snmpv1Objs command

snmp-server host <a.b.c.d> v1 trap command
```

Enabling Autotopology

This section includes information about enabling autotopology on the switch.

You can enable the Optivity* Autotopology* protocol using the CLI. Refer to the www.nortel.com/support URL for information on Autotopology. (The product family for Optivity and Autotopology is Data and Internet.) This section covers the following commands:

autotopology command

The `autotopology` command enables the Autotopology protocol. The syntax for the `autotopology` command is:

```
autotopology
```

The `autotopology` command is in the config command mode.

The `autotopology` command has no parameters or variables.

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 in the config command mode.

The `no autotopology` command has no parameters or variables.

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 in the config command mode.

The `default autotopology` command has no parameters or variables.

show autotopology settings

The `show autotopology settings` command displays information on the Autotopology configuration. The syntax for the `show autotopology settings` command is:

```
show autotopology settings
```

The `show autotopology settings` command is in the privExec mode.

The `show autotopology settings` command has no parameters or variables. Figure 141 on page 411 displays a sample output of the `show autotopology settings` command.

Figure 141 `show autotopology settings` command output

```
470-24T#show autotopology settings
Autotopology:  Enabled
Last NMM Table Change:  4578
Maximum NMM Table Entries:  100
Current NMM Table Entries:  1
```

show autotopology nmm-table

The `show autotopology nmm-table` command displays information about the 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 in the privExec mode.

The `show autotopology nmm-table` command has no parameters or variables.

Figure 142 displays a sample output of the `show autotopology nmm-table` command.

Figure 142 `show autotopology nmm-table` command output

```
470-48T#show autotopology nmm-table
LSlot                                                                    RSlot
LPort IP Addr          Seg ID  MAC Addr     Chassis Type     BT LS   CS   RPort
----- --------------- -------- ------------ ---------------- -- --- ---- ---
 0/ 0 134.177.150.80  0x000000 000438D59FC1     470-24T      12 Yes HTBT    NA
 1/ 1 134.177.150.6   0x000108 000F6A7DC121     470-48T      12 Yes HTBT   1/ 8
 1/ 1 134.177.150.79  0x000101 000997291F01     460-24T-PWR  12 Yes HTBT
1/ 1
470-48T#
```

Chapter 11
Ethernet port management using the CLI

This chapter describes how to enable a port, name a port, enable rate limit and display the status for the Power over Ethernet (PoE) configuration. This chapter covers the following topics:

Refer to the "Power over Ethernet for the Ethernet Switch 460" on page 319 for more information on the PoE feature.

Note: For information on downloading the PoE image, refer to "download command" on page 376.

Enabling or disabling a port

You can enable or disable a port using the CLI. This section covers the following commands:

shutdown port command

The `shutdown port` command disables the port. The syntax for the `shutdown port` command is:

`shutdown [port <portlist>]`

The `shutdown port` command is in the config-if command mode.

Table 86 describes the parameters and variables for the `shutdown port` command.

Table 86 `shutdown port` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to shut down or disable. Enter the port numbers you want to disable. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

no shutdown command

The `no shutdown` command enables the port. The syntax for the `no shutdown` command is:

`no shutdown [port <portlist>]`

The `no shutdown` command is in the config-if command mode.

Table 87 describes the parameters and variables for the `no shutdown` command.

Table 87 `no shutdown` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to enable. Enter the port numbers you want to enable. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Naming ports

You can name a port using the CLI. This section covers the following commands:

- "name command"
- "no name command" on page 416
- "default name command" on page 416

name command

The `name` command allows you to name ports or to change the name. The syntax for the `name` command is:

```
name [port <portlist>] <LINE>
```

The `name` command is in the config-if command mode.

Table 88 describes the parameters and variables for the `name` command.

Table 88 `name` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to name. Note: If you omit this parameter, the system uses the port number you specified in the `interface` command.
`<LINE>`	Enter up to 26 alphanumeric characters.

no name command

The `no name` command clears the port names; it resets the field to an empty string. The syntax for the `no name` command is:

```
no name [port <portlist>]
```

The `no name` command is in the config-if command mode.

Table 89 describes the parameters and variables for the `no name` command.

Table 89 `no name` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to clear of names. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

default name command

The `default name` command clears the port names; it resets the field to an empty string. The syntax for the `default name` command is:

```
default name [port <portlist>]
```

The `default name` command is in the config-if command mode.

Table 90 describes the parameters and variables for the `default name` command.

Table 90 `default name` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to clear of names. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Setting port speed

You can set the speed and duplex mode for a port. This section covers:

- "speed command"
- "default speed command" on page 418
- "duplex command" on page 419
- "default duplex command" on page 420

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 in the config-if command mode.

Note: You cannot *enable* autonegotiation on fiber optic ports.

Table 91 describes the parameters and variables for the `speed` command.

Table 91 `speed` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to configure the speed. Enter the port numbers you want to configure. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.
`10|100|1000|auto`	Sets speed to: • `10`—10 Mb/s • `100`—100 Mb/s • `1000`—1000 Mb/s or 1 GB/s • `auto`—autonegotiation

Note: 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 in the config-if command mode.

Table 92 describes the parameters and variables for the `default speed` command.

Table 92 `default speed` command parameters and variables

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 specified with the `interface` 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 in the config-if command mode.

Note: You cannot *enable* autonegotiation on fiber optic ports.

Table 93 describes the parameters and variables for the `duplex` command.

Table 93 `duplex` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port number to configure the duplex mode. Enter the port number you want to configure, or `all` to configure all ports simultaneously. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.
`full|half|auto`	Sets duplex to: • `full`—full-duplex mode • `half`—half-duplex mode • `auto`—autonegotiation

Note: 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 in the config-if command mode.

Table 94 describes the parameters and variables for the `default duplex` command.

Table 94 `default duplex` command parameters and variables

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, or `all` to configure all ports simultaneously. The default value is autonegotiation. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Note: You cannot *enable* autonegotiation on fiber optic ports.

Enabling flow control

If you use a Gigabit Interface Connector (GBIC) with the switch, you control traffic on this port using the `flowcontrol` command. This section covers the following commands:

- "flowcontrol command"
- "no flowcontrol command" on page 422
- "default flowcontrol command" on page 423

flowcontrol command

The `flowcontrol` command is used only on Gigabit Interface Connector 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 in the config-if mode.

Table 95 describes the parameters and variables for the `flowcontrol` command.

Table 95 `flowcontrol` command parameters and variables

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 port number specified with the `interface` command.
`asymmetric|symmetric|auto|disable`	Sets the mode for flow control: • `asymmetric`—enables the local port to perform flow control on the remote port • `symmetric`—enables the local port to perform flow control • `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 in the config-if mode.

Table 96 describes the parameters and variables for the `no flowcontrol` command.

Table 96 `no flowcontrol` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable flow control. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

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 in the config-if mode.

Table 97 describes the parameters and variables for the `default flowcontrol` command.

Table 97 `default flowcontrol` command parameters and variables

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 specified with the `interface` command.

Enabling rate limiting

You can limit the percentage of multicast traffic, or broadcast traffic, or both using the CLI.

This section covers:

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 in the privExec command mode.

The `show rate-limit` command has no parameters or variables.

Figure 143 on page 425 displays sample output from the `show rate-limit` command.

Figure 143 `show rate-limit` command output

```
470-24T #show rate-limit
Port  Packet Type  Limit  Last 5 Minutes  Last Hour  Last 24 Hours
----  -----------  -----  --------------  ---------  -------------
1     Both         None          0.0%         0.0%         0.0%
2     Both         None          0.0%         0.0%         0.0%
3     Both         None          0.0%         0.0%         0.0%
4     Both         None          0.0%         0.0%         0.0%
5     Both         None          0.0%         0.0%         0.0%
6     Both         None          0.0%         0.0%         0.0%
7     Both         None          0.0%         0.0%         0.0%
8     Both         None          0.0%         0.0%         0.0%
9     Both         None          0.0%         0.0%         0.0%
10    Both         None          0.0%         0.0%         0.0%
11    Both         None          0.0%         0.0%         0.0%
12    Both         None          0.0%         0.0%         0.0%
13    Both         None          0.0%         0.0%         0.0%
14    Both         None         80.6%        66.6%        69.6%
15    Both         None          0.0%         0.0%         0.0%
16    Both         None          0.0%         0.0%         0.0%
17    Both         None          0.0%         0.0%         0.0%
18    Both         None          0.0%         0.0%         0.0%
19    Both         None          0.0%         0.0%         0.0%
20    Both         None          0.0%         0.0%         0.0%
--More--
```

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 in the config-if command mode.

Table 98 on page 426 describes the parameters and variables for the `rate-limit` command.

Table 98 `rate-limit` command parameters and variables

Parameters and values	Description
`port <portlist>`	Specifies the port numbers to configure for rate limiting. Enter the port numbers you want to configure. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.
`multicast <pct>| broadcast <pct>|both <pct>`	Applies rate limiting to the type of traffic. Enter an integer between 1 and 10 to set the rate limiting percentage: • `multicast`—applies rate limiting to multicast packets • `broadcast`—applies rate limiting to broadcast packets • `both`—applies rate limiting to both multicast and broadcast packets

no rate-limit command

The `no rate-limit` command disables rate limiting on the port. The syntax for the `no rate-limit` command is:

`no rate-limit [port <portlist>]`

The `no rate-limit` command is in the config-if command mode.

Table 99 describes the parameters and variables for the `no rate-limit` command.

Table 99 `no rate-limit` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable from rate limiting. Enter the port numbers you want to disable. Note: If you omit this parameter, the system uses the port number you specified in the `interface` command.

default rate-limit command

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

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

The `default rate-limit` command is in the config-if command mode.

Table 100 describes the parameters and variables for the `default rate-limit` command.

Table 100 `default rate-limit` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to reset rate limiting to factory default. Enter the port numbers on which you want to set rate limiting to default. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Enabling Custom Autonegotiation Advertisements (CANA)

You can control the capabilities that are advertised by the Ethernet Switch as part of the autonegotiation process using the Custom Autonegotiation Advertisements (CANA) feature. When autonegotiation is disabled, the hardware is configured for a single (fixed) speed and duplex value. When autonegotiation is enabled, the advertisement made by the switch is a constant value, based upon all speed and duplex modes supported by the hardware. When autonegotiating, the switch selects the highest common operating mode supported between it and its link partner.

This section covers:

show auto-negotiation-advertisements command

The `show auto-negotiation-advertisements` command displays the current autonegotiation advertisements. The syntax for the `show auto-negotiation-advertisements` command is:

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

The `show auto-negotiation-advertisements` command is in the userExec command mode.

Table 101 describes the parameters and variables for the `show auto-negotiation-advertisements` command.

Table 101 `show auto-negotiation-advertisements` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want the current autonegotiation advertisements displayed.

Figure 144 displays sample output from the `show auto-negotiation-advertisements` command.

Figure 144 `show auto-negotiation-advertisements` command output

```
460_24T_PWR#show auto-negotiation-advertisements port 4,8,10
Port Autonegotiation Advertised Capabilities
-----------------------------------------------------
4    10Full 10Half 100Full 100Half
8    10Full 10Half 100Full 100Half
10   10Full 10Half 100Full 100Half
```

show auto-negotiation-capabilities command

The `show auto-negotiation-capabilities` command displays the hardware advertisement capabilities for the switch. The syntax for the `show auto-negotiation-capabilities` command is:

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

The `show auto-negotiation-capabilities` command is in the userExec command mode.

Table 102 describes the parameters and variables for the `show auto-negotiation-capabilities` command.

Table 102 `show auto-negotiation-capabilities` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want the autonegotiation capabilities displayed.

Figure 145 displays sample output from the `show auto-negotiation-capabilities` command.

Figure 145 `show auto-negotiation-capabilities` command output

```
460_24T_PWR#show auto-negotiation-capabilities port 5,6,10
Port Autonegotiation Capabilities
---- ------------------------------------------------------------------
5    10Full 10Half 100Full 100Half
6    10Full 10Half 100Full 100Half
10   10Full 10Half 100Full 100Half
460_24T_PWR#
```

auto-negotiation-advertisements command

The `auto-negotiation-advertisements` command configures advertisements for the switch. The syntax for the `auto-negotiation-advertisements` command is:

```
auto-negotiation-advertisements [port <portlist>] [10-full]
[10-half] [100-full] [100-half] [1000-full] [1000-half]
[asymm-pause-frame] [pause-frame]
```

The `auto-negotiation-advertisements` command is in the interface configuration command mode.

Table 103 describes the parameters and variables for the `auto-negotiation-advertisements` command.

Table 103 `auto-negotiation-advertisements` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want to configure advertisements.
`[10-full] [10-half] [100-full] [100-half] [1000-full] [1000-half] [asymm-pause-frame] [pause-frame]`	These are speed-duplex-pause settings. Any combination of these settings is allowed, but parameters must be given in the order shown.

no auto-negotiation-advertisements command

The `no auto-negotiation-advertisements` command clears all advertisements for the switch. This command is used for testing. The syntax for the `no auto-negotiation-advertisements` command is:

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

Note: The use of this command affects traffic and brings down the link.

The `no auto-negotiation-advertisements` command is in the interface configuration command mode.

Table 104 describes the parameters and variables for the `no auto-negotiation-advertisements` command.

Table 104 `no auto-negotiation-advertisements` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want to clear all advertisements.

default auto-negotiation-advertisements command

The `default auto-negotiation-advertisements` command sets default advertisements for the switch. The syntax for the `default auto-negotiation-advertisements` command is:

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

The `default auto-negotiation-advertisements` command is in the interface configuration command mode.

Table 105 describes the parameters and variables for the `default auto-negotiation-advertisements` command.

Table 105 `default auto-negotiation-advertisements` command

Parameters and values	Description
`port <portlist>`	Enter ports for which you want to set default advertisements.

Configuring FEFI

When a fiber optic transmission link to a remote device fails, the remote device indicates the failure and the port is disabled. To use Far End Fault Indication (FEFI), the user must enable autonegotiation on the port.

Configuring SFFD

When a partial fiber break occurs, data is lost on one side of a link. Single Fiber Fault Detection (SFFD) detects this error condition, and causes the port that is losing data to go down. This stops the loss of data.

The Single Fiber Fault Detection feature is enabled on a port-by-port basis for the Ethernet Switch GBIC ports. At present, you can access this feature through the CLI.

Single Fiber Fault Detection (SFFD) has the following requirements and limitations:

- SFFD must be implemented on both sides of a link. For example: Passport 8600 and Ethernet Switch 470-24T.
- SFFD must be enabled on a per-port basis.
- By default, SFFD is disabled on all ports.
- SFFD takes about 50 seconds to detect a fault.
- Once a link is repaired, the link recovers automatically.

This section lists the CLI commands that are used on the Ethernet Switch products to support the SFFD feature:

- "show sffd command"
- "sffd enable command" on page 434
- "no sffd enable command" on page 435
- "default sffd enable command" on page 435

show sffd command

The `show sffd` command displays the SFFD configuration information for all ports with the SFFD feature. The display also indicates whether the SFFD feature is enabled or disabled. The syntax of the `show sffd` command is:

```
show sffd
```

The `show sffd` command is in all command modes.

The `show sffd` command has no parameters or variables.

Figure 146 on page 434 displays the `show sffd` command output.

Figure 146 `show sffd` command output

```
 470-48T#show sffd
Port  SFFD Mode
----  ---------
47     Disabled
470-48T#
```

sffd enable command

The `sffd enable` command enables the SFFD feature on specified ports, and is available only in the CLI. The syntax of the `sffd enable` command is:

`sffd [port <portlist>] enable`

The `sffd enable` command is in the config-if command mode.

Table 106 describes the parameters and variables for the `sffd enable` command.

Table 106 `sffd enable` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to enable the SFFD feature. The portlist can be separated by commas or dashes. For example: 2/16, 3/16, or 2/26 - 2/27. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Figure 147 on page 435 displays sample output from the `sffd enable` command.

Figure 147 `sffd enable` command output

```
470-48T(config-if)#sffd enable
470-48T(config-if)#show sffd
Port  SFFD Mode
----  ---------
47     Enabled
470-48T(config-if)#
```

no sffd enable command

The `no sffd enable` command disables the SFFD feature on specified ports, and is available only in the CLI. The syntax of the `no sffd enable` command is:

`no sffd [port <portlist>] enable`

The `no sffd enable` command is in the config-if command mode.

Table 107 describes the parameters and variables for the `no sffd enable` command.

Table 107 `no sffd enable` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to disable the SFFD feature. The portlist can be separated by commas or dashes. For example: 2/16, 3/16, or 2/26 - 2/27. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

default sffd enable command

The `default sffd enable` command changes the SFFD feature on specified ports to the factory default setting. The factory default setting is disabled. The syntax of the `default sffd enable` command is:

`default sffd [port <portlist>] enable`

The `default sffd enable` command is in the config-if command mode.

Table 108 describes the parameters and variables for the `default sffd enable` command.

Table 108 `default sffd enable` command parameters and variables

Parameters and variables	Description
`port <portlist>`	Specifies the port numbers to change the SFFD feature to the factory default of disabled. The portlist can be separated by commas or dashes. For example: 2/16, 3/16, or 2/26 - 2/27. Note: If you omit this parameter, the system uses the port number specified with the `interface` command.

Chapter 12
Configuring the switch using Device Manager

This chapter describes how you can use Device Manager to configure your switch.

This chapter contains the following topics:

Viewing Unit information

You can view unit information by using the Unit dialog box.

To open the Unit dialog box:

1 Select the unit by clicking in the Device View area of the switch.

2 From the Device Manager main menu, choose Edit > Unit.

The Unit dialog box (Figure 148) opens with the unit tab displayed.

Figure 148 Unit dialog box

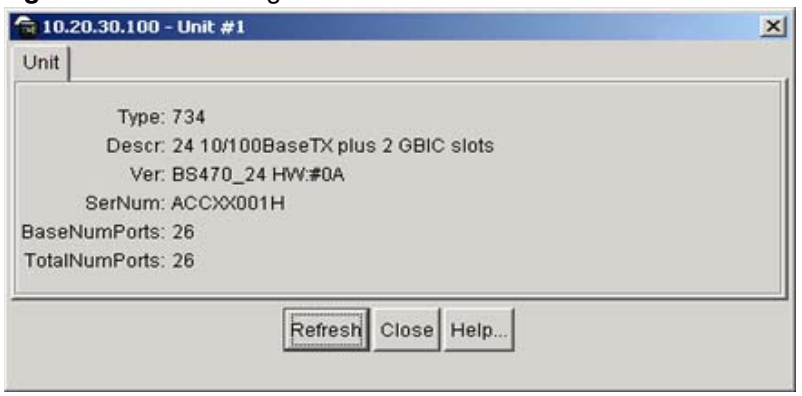


Table 109 describes the Unit tab items.

Table 109 Unit tab items

Item	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.

Unit dialog box for multiple units

When you select multiple units simultaneously, the Unit tab displays information about the switches you are using.

To open the Unit tab for multiple units:

1 Select the units you want to edit.

Press [Ctrl] + left click the units you want to view. A yellow outline appears around the selected units.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Unit.
- Double-click on the selected units.
- On the toolbar, click Edit.

The Unit dialog box opens with the Unit tab for multiple units displayed (Figure 149).

Figure 149 Edit Unit dialog box—Unit tab for multiple units

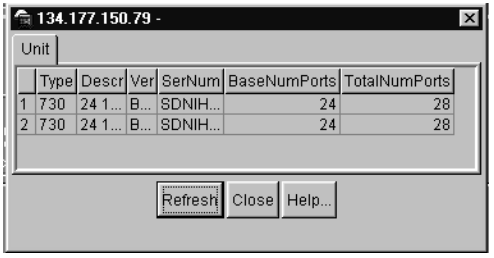


Table 110 describes the Unit tab items for multiple units.

Table 110 Unit tab items for multiple units

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.

Viewing switch IP information

You can view the switch IP information using the IP dialog box. This section describes the tabs available under the IP dialog box, and includes the following topics:

- "Globals tab"
- "Addresses tab" on page 441
- "ARP tab" on page 442

Globals tab

To open the Globals tab:

➨ From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens (Figure 150 on page 441) with the Globals tab displayed.

Figure 150 Globals tab

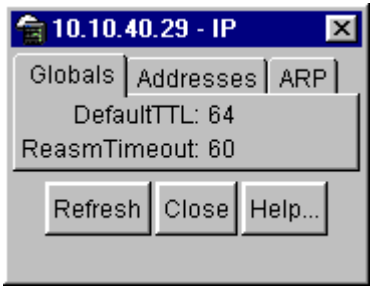


Table 111 describes the Globals tab items.

Table 111 Globals tab items

Item and MIB association	Description
DefaultTTL	Default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol. Default value is 16.
ReasmTimeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity. Default value is 5.

Addresses tab

The Addresses tab shows the IP address information for the device.

To open the Addresses tab:

1 From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens with the Globals tab displayed (Figure 150).

2 Click the Addresses tab.

The Addresses tab opens (Figure 151 on page 442).

Figure 151 Edit IP dialog box — IP Address tab

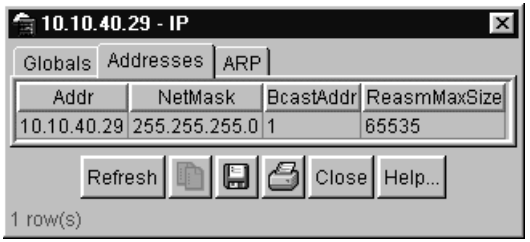


Table 112 describes the IP Address tab items.

Table 112 IP Addresses tab items

Item	Description
Addr	The device IP address.
NetMask	The subnet mask address.
BcastAddr	The IP broadcast address used.
ReasmMaxSize	The size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface.

ARP tab

The Address Resolution Protocol (ARP) tab shows the MAC addresses and the associated IP addresses for the switch.

To open the ARP tab:

1 From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens with the Globals tab displayed (Figure 150 on page 441).

2 Click the ARP tab.

The ARP tab opens (Figure 152 on page 443).

Figure 152 Edit IP dialog box — ARP tab

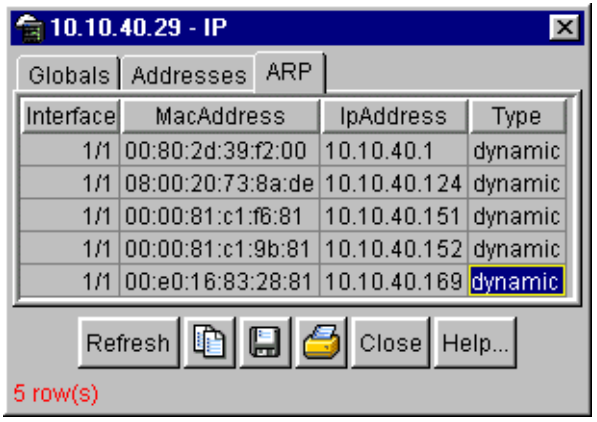


Table 113 describes the ARP tab items.

Table 113 ARP tab items

Item	Description
Interface	The device unit number.
MacAddress	The unique hardware address of the device.
IpAddress	The Internet Protocol address of the device used to represent a point of attachment in a TCP/IP internetwork.
Type	The type of mapping.

Editing the chassis configuration

You can edit a chassis configuration from the Edit Chassis dialog box (Figure 153 on page 445).

To open the Chassis dialog box:

1. Select the chassis.
2. Do *one* of the following:
   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Chassis.

- On the toolbar, click Edit.

The following sections provide a description of the tabs in the Edit > Chassis dialog box and details about each item on the tab:

- "System tab"
- "Base Unit Info tab" on page 447
- "Stack Info tab" on page 449
- "Agent tab" on page 452
- "Power Supply tab" on page 453
- "Fan tab" on page 454

System tab

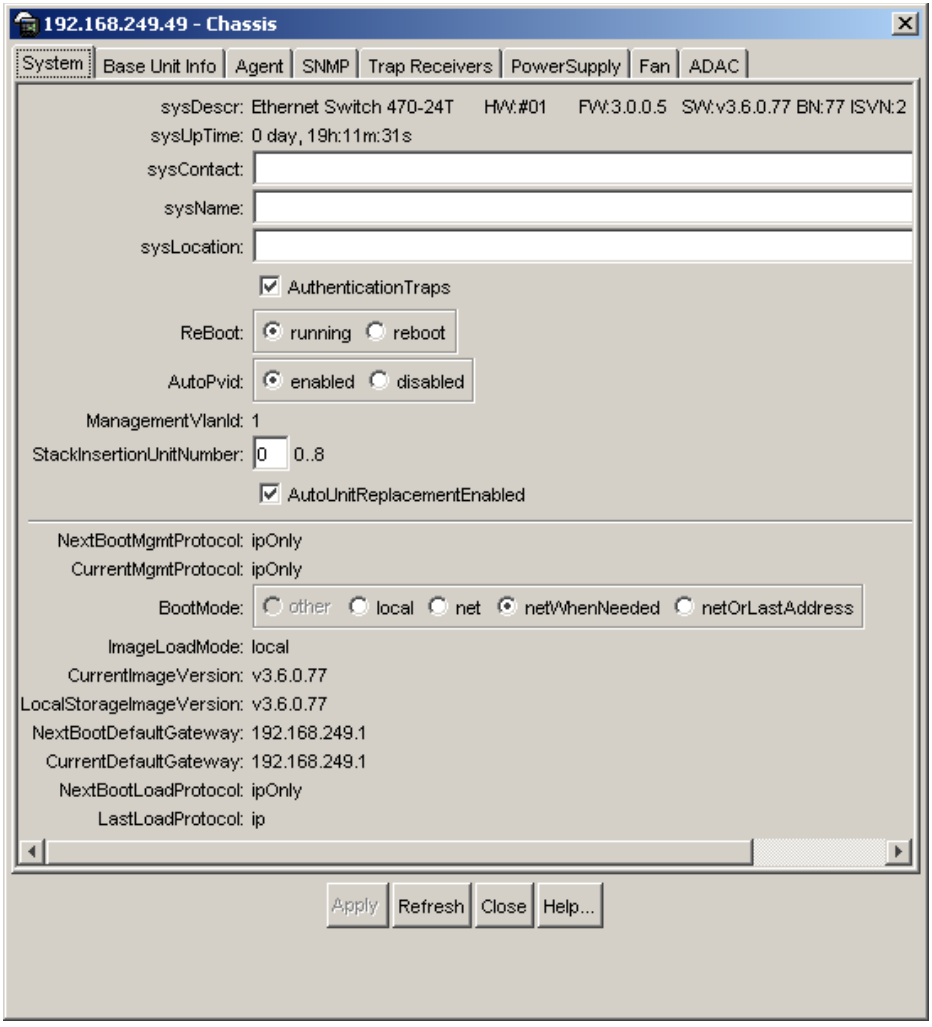
Use the System tab to specify, among other things, tracking information for a device and device descriptions.

To open the System tab:

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

   The Chassis dialog box opens with the System tab displayed (Figure 153 on page 445).

Figure 153 Edit Chassis dialog box — System tab



Note: The chassis keeps track of the elapsed time and calculates the time and date using the system clock of the Device Manager machine as a reference.

Table 114 describes the System tab items.

Table 114 System tab items

Item	Description
sysDescr	A description of the device.
sysUpTime	The time since the system was last booted.
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	Click enable or disable. When you select enabled, SNMP traps are sent to trap receivers for all SNMP access authentication. When you select disabled, no traps are received. To view traps, click the Trap toolbar button. 
Reboot	Action object to reboot the agent. Reset — initiates a hardware reset. The agent does best efforts 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.
AutoPvid	Click enabled or disabled. When you select enabled, Port VLAN ID (PVID) is automatically assigned.
ManagementVlanId	The current management VLAN ID.
StackInsertionUnitNumber	The unit number assigned to the switch when it is inserted into a stack.
AutoUnitReplacementEnabled	Enables or disables the Auto Unit Replacement feature. (See “Auto Unit Replacement” on page 307.)
StackInsertionNumber	Number of switches used to form the stack.
NextBootMgmtProtocol	The transport protocol(s) to use after the next boot of the agent.
CurrentMgmtProtocol	The current transport protocol(s) that the agent supports.

Table 114 System tab items (Continued)

Item	Description
BootMode	The source from which to load the initial protocol configuration information to boot the switch the next time: • local (from the switch) • net (use BootP over the network) • netWhenNeeded (use BootP only when needed) • netOrLastAddress (use BootP or the last known address)
ImageLoadMode	The source from which to load the agent image at the next boot.
CurrentImageVersion	The version number of the agent image that is currently used on the switch.
LocalStorageImageVersion	The version number of the agent image that is stored in flash memory on the switch.
NextBootDefaultGateway	The IP address of the default gateway for the agent to use after the next time the switch is booted.
CurrentDefaultGateway	The IP address of the default gateway that is currently in use.
NextBootLoadProtocol	The transport protocol to be used by the agent to load the configuration information and the image at the next boot.
LastLoadProtocol	The transport protocol last used to load the image and configuration information on the switch.

Base Unit Info tab

The Base Unit Info tab provides read-only information about the operating status of the hardware and allows you to enable or reset the switch, as well as to enter information on the switch's location.

To open the Base Unit Info tab:

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

   The Chassis dialog box opens with the System tab displayed (Figure 153 on page 445).

3. Click the Base Unit Info tab.

The Base Unit Info tab opens (Figure 154).

Note: In a stack environment, if the base unit number does not begin with the number one, the information does not display. Use the Console Interface and the Web-based management interface to change your base unit number.

Figure 154 Edit Chassis dialog box — Base Unit Info tab

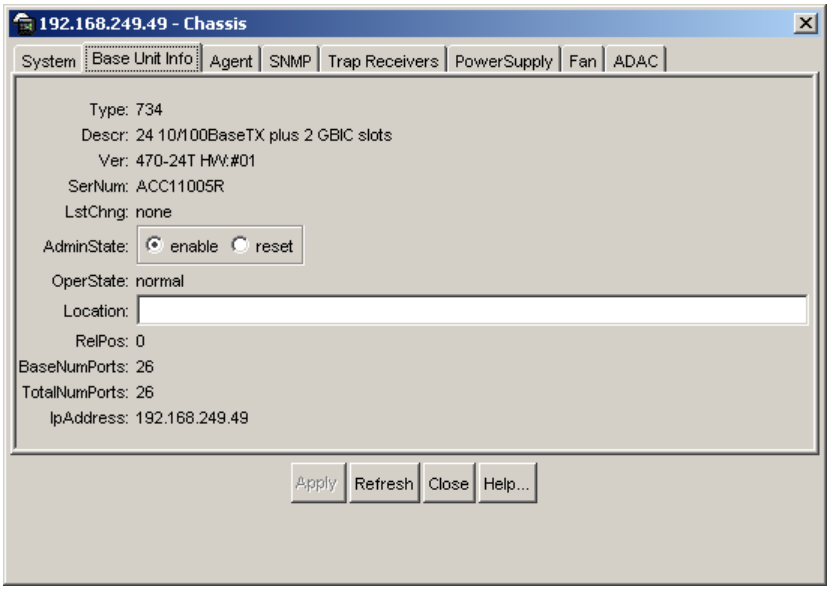


Table 115 describes the Base Unit Info tab items.

Table 115 Base Unit Info tab items

Item	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.

Table 115 Base Unit Info tab items (Continued)

Item	Description
LstChng	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
AdminState	Administrative state of the switch. Select either `enable` or `reset`. Note: In a stack configuration, `Reset` only resets the base unit.
OperState	The operational state of the switch.
Location	Type the physical location of the switch.
RelPos	The relative position of the switch.
BaseNumPorts	The number of base ports of the switch.
TotalNumPorts	The number of ports of the switch.
IpAddress	The base unit IP address.

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. This tab also allows you to enable or disable switch, as well as to enter information on the switch's location. This tab is enabled for a stack of switches.

To open the Stack Info tab:

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

   The Chassis dialog box opens with the System tab displayed (Figure 153 on page 445).

3. Click the Stack Info tab.

   The Stack Info tab opens (Figure 155 on page 450).

Figure 155 Edit Chassis dialog box — Stack Info tab

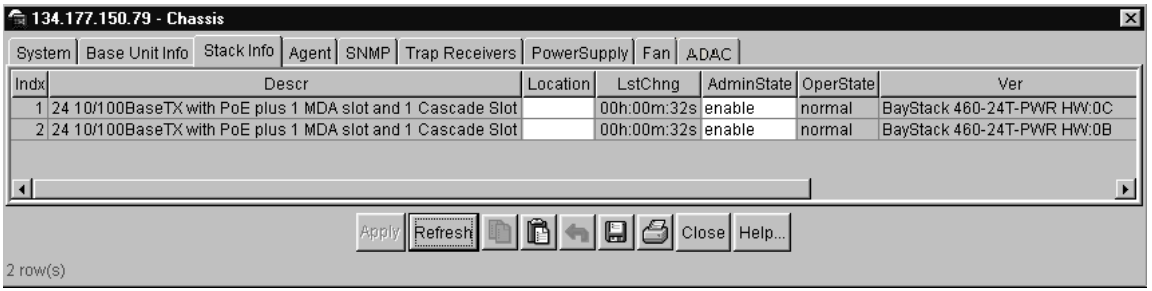


Table 116 describes the Stack Info tab fields.

Table 116 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 object is applicable only to components that can be found in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in Board or Unit group, the value is a zero length string. 2. If this object is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value will default to the value of the object s5ChasComSerNum.
LstChng	The value of sysUpTime when it was detected that the component/ sub-component was added to the chassis. If this has not occurred since the cold/warm start of the agent, then the value is zero.

Table 116 Stack Info tab fields (Continued)

Field	Description
AdminState	The state of the component or subcomponent. The values that are read-only are: • other — currently in some other state • notAvail — actual value is not available The possible values that can be read and written are: 1.disable—disables operation 2.enable—enables operation 3.reset—resets component 4.test—starts self test of component, with the result to be normal, warning, nonFatalErr, or fatalErr in object s5ChasComOperState The allowable (and meaningful) values are determined by the component type.
OperState	The current operational state of the component. The possible values are: • 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 The allowable (and meaningful) values are determined by the component type.
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.

Agent tab

The Agent tab provides information about the addresses that the agent software uses to identify the switch.

To open the Agent tab:

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

   The Chassis dialog box opens (Figure 153 on page 445) with the System tab displayed.

3. Click the Agent tab.

   The Agent tab opens (Figure 156).

Figure 156 Edit Chassis dialog box — Agent tab

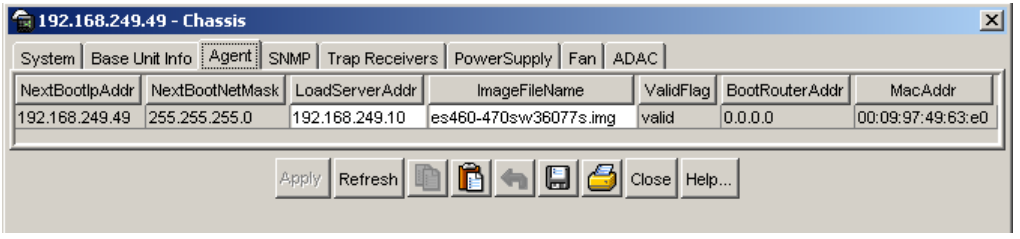


Table 117 describes the Agent tab fields.

Table 117 Agent tab fields

Item	Description
NextBootpAddr	The IP address of the BootP server to be used the next time the switch is booted. This is a read-only field.
NextBootNetMask	The subnet mask to be used the next time the switch is booted; read. This is a read-only field
LoadServerAddr	The IP address of the server from which the device loads the image file.
ImageFileName	The name of the image file.
ValidFlag	Indicates if the configuration and/or image file(s) were downloaded from this interface and if the file names have not been changed. This is a read-only field

Table 117 Agent tab fields (Continued)

Item	Description
BootRouterAddr	The IP address of the boot router for the configuration file and/or the image file. This is a read-only field
MacAddr	The switch's MAC address. This is a read-only field

Power Supply tab

The Power Supply tab provides read-only information about the operating status of the power supplies to the switch. Refer to "Editing and viewing switch PoE configurations using Device Manager" on page 341 for more information on the Power over Ethernet (PoE) external DC power source.

To open the PowerSupply tab:

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

   The Chassis dialog box opens (Figure 153 on page 445) with the System tab displayed.

3. Click the PowerSupply tab.

   The PowerSupply tab opens (Figure 157).

Figure 157 Edit Chassis dialog box — Power Supply tab

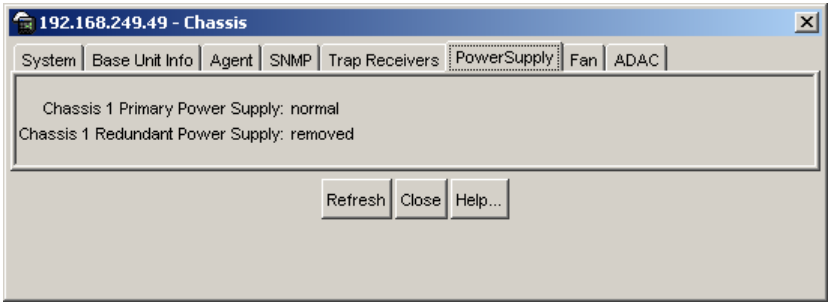


Table 118 describes the Power Supply tab fields.

Table 118 Power Supply tab fields

Field	Description
Desc	The power supply type: • Primary Power Supply—This is the internal power source for the switch. • Redundant Power Supply—This is the external power source, or DC source, for the switch. (Refer to DC Source tab for a single unit for more information on the external power source.)
OperStat	The operational state of the power supply. Possible values include: • other: Some other state. • notAvail: State not available. • removed: Component was removed. • disabled: Operation disabled. • normal: State is in normal operation. • resetInProg: There is a reset in progress. • testing: System is doing a self test. • warning: System is operating at a warning level. • nonFatalErr: System is operating at error level. • fatalErr: A fatal error stopped operation. • notConfig: A module needs to be configured. The allowable values are determined by the component type.

Fan tab

The Fan tab provides read-only information about the operating status of the switch fans.

To open the Fan tab:

1 From the menu bar, choose Edit > Chassis.

The Chassis dialog box opens (Figure 153 on page 445) with the System tab displayed.

2 Click the Fan tab.

The Fan tab opens (Figure 158 on page 455).

Figure 158 Edit Chassis dialog box — Fan tab

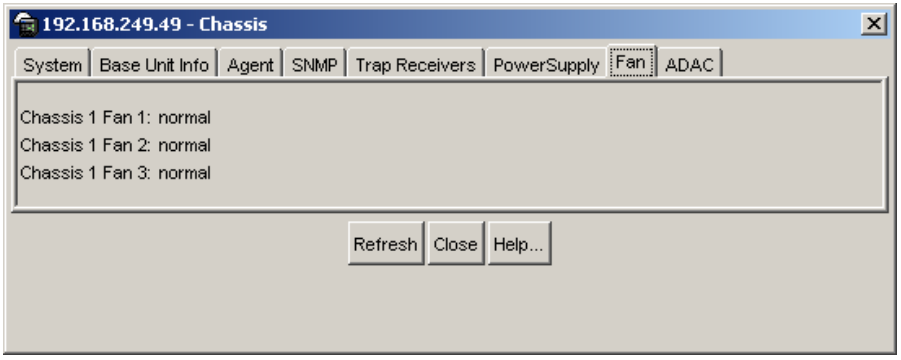


Table 119 describes the Fan tab fields.

Table 119 Fan tab fields

Field	Description
Desc	The fan type.
OperStat	The operational state of the fan. Values include: • other: Some other state. • notAvail: This state is not available. • removed: Fan was removed. • disabled: Fan is disabled. • normal: Fan is operating in normal operation. • resetInProg: A reset of the fan is in progress. • testing: Fan is doing a self-test. • warning: Fan is operating at a warning level. • nonFatalErr: Fan is operating at error level. • fatalErr: An error stopped the fan operation. • notConfig: Fan must be configured. The allowable values are determined by the component type.

Working with configuration files

Use the FileSystem dialog box to view information and upload or download the configuration and image files.

The following sections describe how to use the:

- "FileSystem dialog box"
- "ASCII Config File dialog box" on page 458

FileSystem dialog box

To open the Edit FileSystem dialog box:

➨ From the Device Manager main menu, choose Edit > File System.

The FileSystem dialog box opens with the Config/Image/Diag file tab displayed (Figure 159).

Update only one item at a time. Click Apply after each change.

Figure 159 Edit FileSystem dialog box—Config/Image/Diag file tab

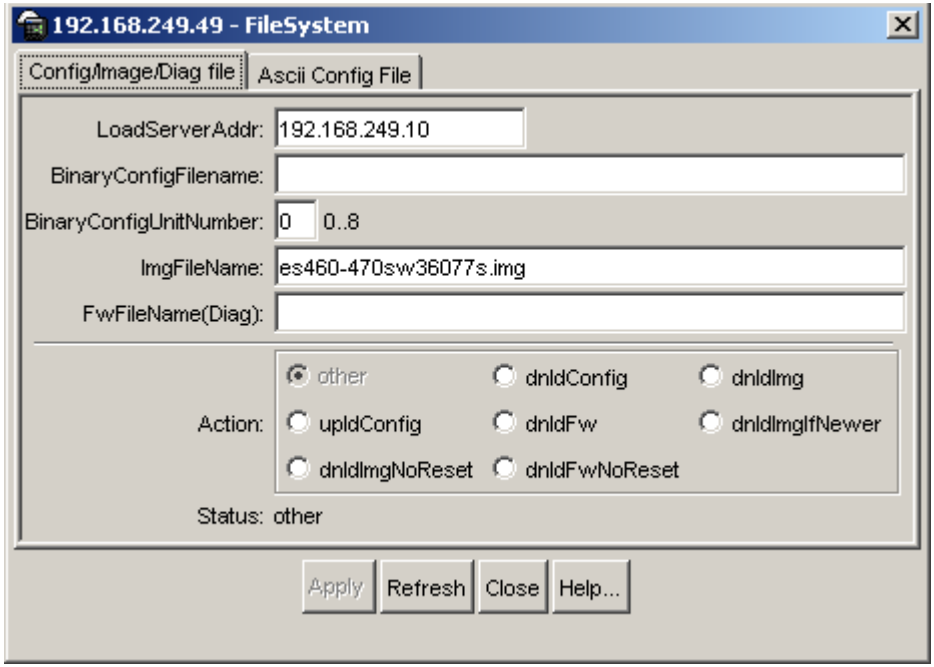


Table 120 describes the FileSystem dialog box items.

Table 120 FileSystem dialog box items

Item	Description
LoadServerAddr	The IP address of the load server for the configuration file and/or the image file. If not used, then the value is 0.0.0.0.
ConfigFileName	Name of the configuration file currently associated with the interface. When not used, the value is a zero length string.
BinaryConfigUnitNumber	This field specifies the unit number in the Binary Configuration file from where information is extracted and used to configure the stand-alone unit. The extraction of the Binary Configuration file information is required when the switch is operating in a stand-alone mode and the Binary Configuration file was created in a stack mode.
ImageFileName	Name of the image file(s) currently associated with the interface. When the object is not used, the value is a zero length string.
FwFileName(Diag)	Name of the diagnostics file currently associated with the interface. When the object is not used, the value is a zero length string.

Table 120 FileSystem dialog box items (Continued)

Item	Description
Action	Allows you to select whether to download or upload a binary config file, image file, or diagnostics file, download the image only if it is newer than the image stored on local NV storage, or download without resetting. In read operation, if there is no action taken since the boot up, it returns with a value of other. Otherwise, it returns the latest action, such as: • other • dnldConfig • dnldImg • upldConfig • dnldFw • dnldImgIfNewer • dnldImgNoReset • dnldFwNoReset The config file contains the current MIB object values of the device.
Status	This object is used to get the status of the latest action as shown by s5AgInfoFileAction. The values that can be read are: • other — if no action taken since the boot up • inProgress — the operation is in progress • success — the operation succeeds. • fail — the operation failed.

ASCII Config File dialog box

To select the ASCII config file download options:

1 From the Device Manager menu bar, choose Edit > File System.

The FileSystem dialog box opens with the Config/Image/Diag file tab displayed.

2 Click the Ascii Config File tab.

The Ascii Config File tab opens (Figure 160 on page 459).

Figure 160 Edit File System dialog box—Ascii Config File tab

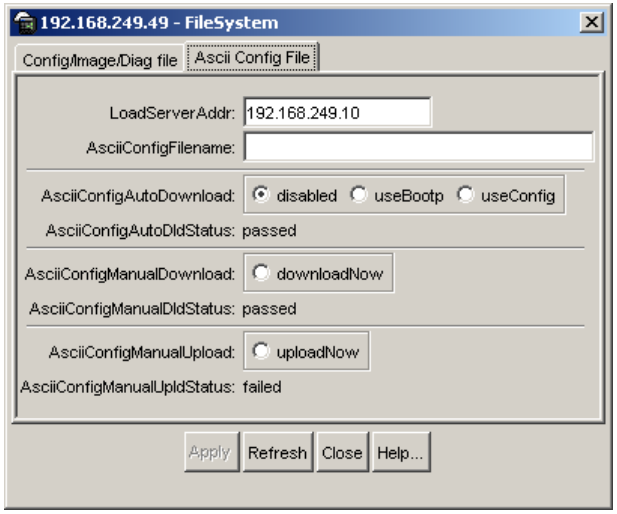


Table 121 describes the Ascii Config File tab fields.

Table 121 Ascii Config File tab fields

Field	Description
LoadServerAddr	Set the server address.
AsciiConfigFilename	Set the ASCII config filename.
AsciiConfigAutoDownload	The current ASCII config file download setting, which can be one of the following: • disabled • useBootp • useConfig If set to disabled, the device will not automatically download the ASCII config file.
AsciiConfigAutoDldStatus	Displays the status of the automatic ASCII config file download. The values that can be read are: • passed—successfully downloaded. • inProgress — the operation is in progress • fail — the operation failed.
AsciiConfigManualDownload	Allows you to download the ASCII configuration file immediately.

Table 121 Ascii Config File tab fields (Continued)

Field	Description
AsciiConfigManualDownload Status	Displays the progress of the immediate downloading of the ASCII configuration file: • passed • InProgress • failed
AsciiConfigManualUpload	Allows you to upload the ASCII configuration file immediately.
AsciiConfigManualUpload Status	Displays the progress of the immediate uploading of the ASCII configuration file: • passed • InProgress • failed

Working with SNTP

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.

The system retries connecting with the NTP server a maximum of 3 times, with 5 minutes between each retry. If the connection fails after the 3 attempts, the system waits for the next synchronization time (the default is 24 hours) and begins the process again.

Using SNTP provides a real-time timestamp for the software, shown as Greenwich Mean Time (GMT). If SNTP is enabled (the default value is disabled), the system synchronizes with the configured NTP server at boot-up and at user-configurable periods thereafter (the default sync 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.

SNTP

The SNTP dialog box contains the parameters for Simple Network Time Protocol (SNTP).

To open the SNTP dialog box:

➨ From the Main Menu, choose Edit > SNTP.

The SNTP dialog box opens (Figure 161 on page 461).

Figure 161 Simple Network Time Protocol dialog box

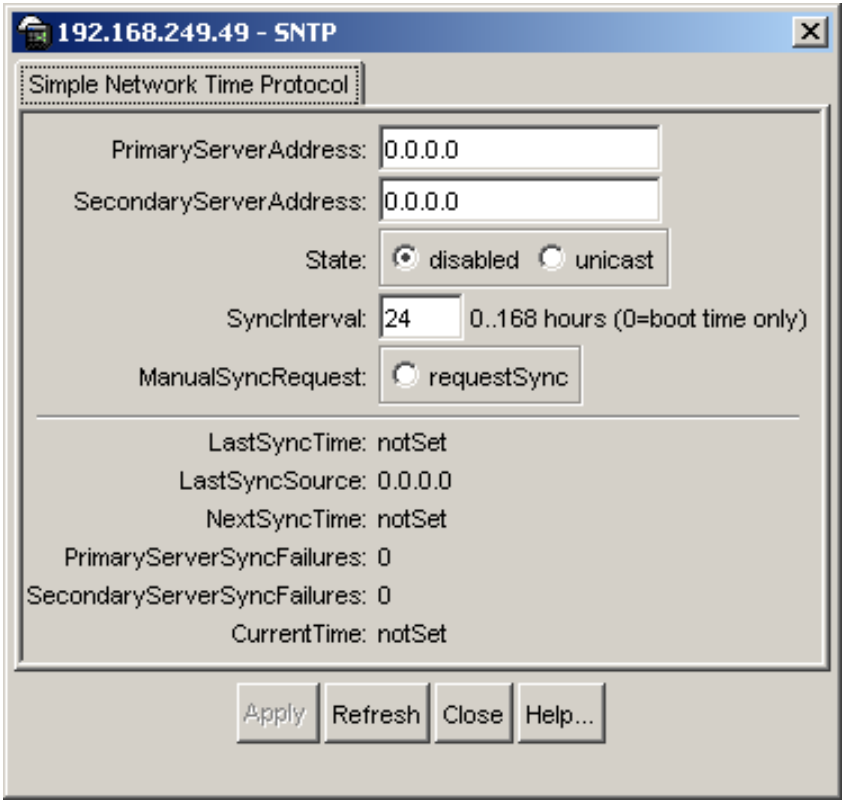


Table 122 describes the SNTP tab fields.

Table 122 SNTP dialog box fields

Field	Description
PrimaryServer Address	The IP address of the primary SNTP server.
SecondaryServer Address	The IP address of the secondary SNTP server.
State	Controls whether the device uses the Simple Network Time Protocol (SNTP), to synchronize the device clock to the Coordinated Universal Time (UTC). If the value is disabled, the device does not synchronize its clock using SNTP. If the value is unicast, the device synchronizes shortly after boot time when network access becomes available, and periodically thereafter.
SynchInterval	Controls the frequency, in hours, that the device attempts to synchronize with the NTP servers
ManualSynchRequest	Specifies that the device immediately attempts to synchronize with the NTP servers.
LastSynchTime	Specifies the Coordinated Universal Time (UTC) when the device last synchronized with an NTP server.
LastSynchSource	Specifies the IP source address of the NTP server with which this device last synchronized.
NextSynchTime	Specifies the Coordinated Universal Time (UTC) at which the next synchronization is scheduled.
PrimaryServer SynchFailures	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.
SecondaryServer SynchFailures	Specifies the number of times the switch failed to synchronize with the secondary server address.
CurrentTime	Specifies the current Coordinated Universal Time (UTC) of the switch.

Viewing topology information using Device Manager

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

- "Topology tab"
- "Topology Table tab" on page 464

Topology tab

To view topology information:

➡ From the Device Manager menu bar, select Edit > Diagnostics.

The Diagnostics dialog box opens with the Topology tab displayed (Figure 162).

Figure 162 Diagnostics dialog box — Topology tab

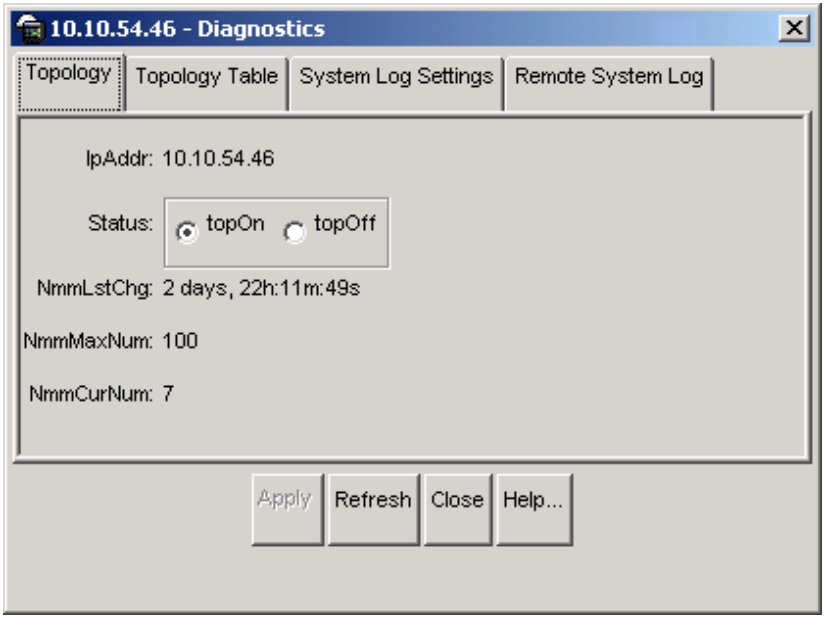


Table 123 describes the Topology tab items.

Table 123 Topology tab items

Items	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:

1 From the Device Manager menu bar, choose Edit > Diagnostics.

The Diagnostics dialog box opens with the Topology tab displayed (Figure 162 on page 463).

2 Click the Topology Table tab.

The Topology Table tab opens (Figure 163 on page 465).

Figure 163 Diagnostics dialog box — Topology Table tab

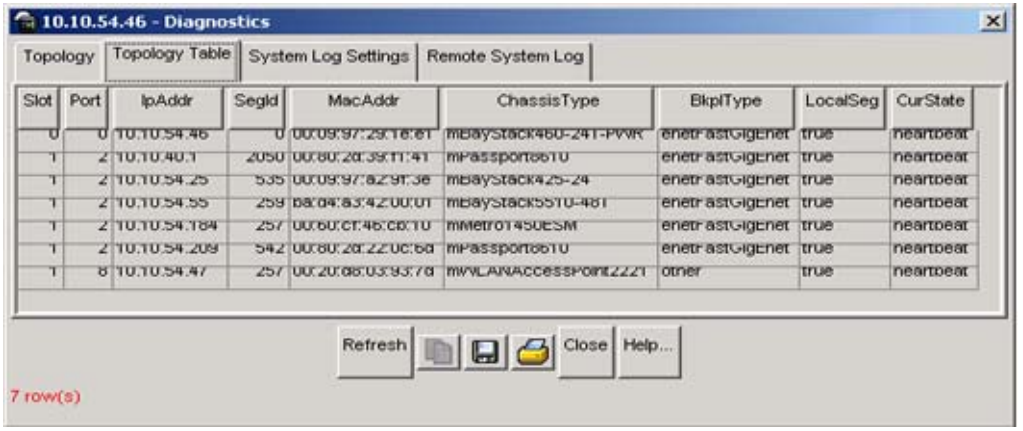


Table 124 describes the Topology Table tab fields.

Table 124 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: • topChanged —Topology information has recently changed. • heartbeat —Topology information is unchanged. • new — The sending agent is in a new state.

Chapter 13
Configuring ports using Device Manager

This chapter describes how you use Device Manager to configure ports on Ethernet Switches 460 and 470.

The windows displayed when you configure a single port have a different appearance than those displayed when you configure multiple ports. However, the options available for configuring either a single port or multiple ports are similar.

See the following sections for more information about configuring and graphing ports:

- "Viewing and editing a single port configuration"
- "Viewing and editing multiple port configurations" on page 473

Viewing and editing a single port configuration

To view or edit the configuration of a single port, double-click on the port.

To view or edit the configuration of a single or multiple ports:

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

Note: When you edit a single port, tabs that are not applicable are not available for you to select.

When you edit multiple ports, some tabs are not available, and some tabs are available even though the options are not applicable. When the option does not apply for a given port, NoSuchObject is displayed.

The following sections provide a description of the tabs in the Edit Port dialog box, and details about each field on the tab.

Interface tab for a single port

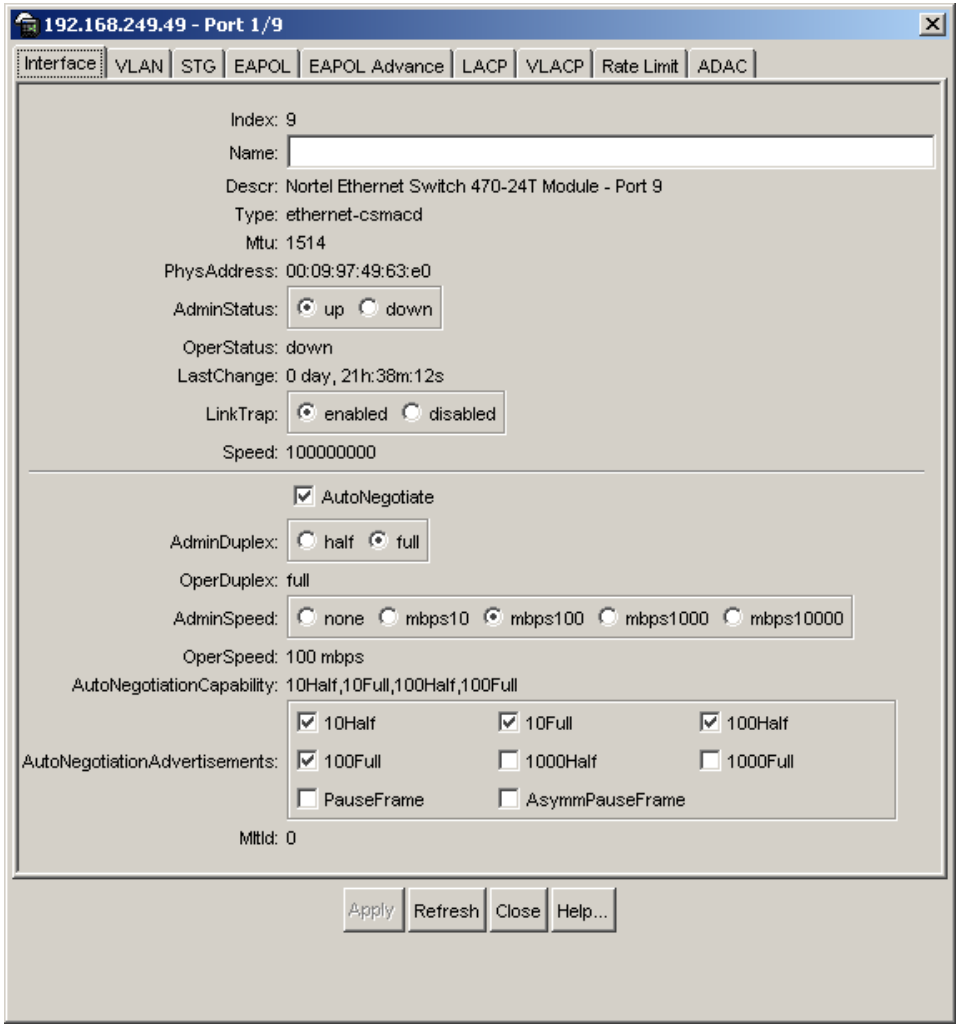
The Interface tab shows the basic configuration and status of a single port.

To view the Interface tab:

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

   The Port dialog box for a single port opens (Figure 164 on page 469) with the Interface tab displayed.

Figure 164 Edit Port dialog box — Interface tab



Note: 10/100BASE-TX ports may not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question.

Check the Nortel web site (www.nortel.com/support) for the latest compatibility information.

Table 125 describes the Interface tab items for a single port.

Table 125 Interface tab items for a single port

Field	Description
Index	A unique value assigned to each interface. The value ranges between 12 and 255.
Name	Allows you to enter a name for the port. This name is shown in the Port Tooltip window.
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	The current administrative state of the interface, which can be one of the following: • up • down 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.

Table 125 Interface tab items for a single port (Continued)

Field	Description
OperStatus	The current operational state of the interface, which can be one of the following: • up • down • testing If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
LinkTrap	Enables and disables the link up/down traps.
Speed	The current speed of the port.
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's speed.
OperSpeed	The current operating speed of the port.
AutoNegotiationCapability	Displays the current autonegotiation advertisements capability. (See "Custom Autonegotiation Advertisements" on page 288.)
AutoNegotiationAdvertisements	Sets the autonegotiation advertisements. Any combination of speed-duplex settings is allowed from among those displayed in the AutoNegotiationCapability field.
MltId	The Multilink Trunk to which the port is assigned (if any).

Rate Limit tab for a single port

The Rate Limit tab shows the Rate Limit configuration and status for a single port.

To view the Rate Limit tab:

1 Select the port you want to edit.

2 Do one of the following:

- Double-click on the selected port
- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit button.

The Port dialog box for a single port opens (Figure 164 on page 469) with the Interface tab displayed.

3 Click the Rate Limit tab.

The Rate Limit tab displays (Figure 165).

Figure 165 Edit Port dialog box — Rate Limit tab

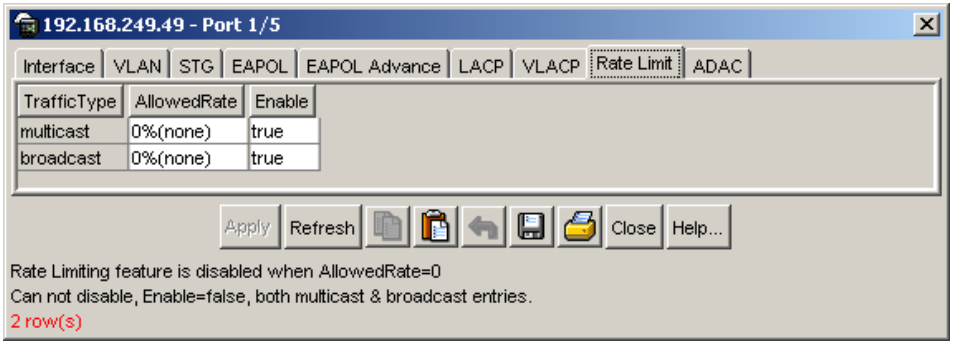


Table 126 describes the Rate Limit tab items for a single port.

Table 126 Rate Limit tab items for a single port

Field	Description
TrafficType	Specifies the two types of traffic that can be set with rate limiting, broadcast and multicast.
AllowedRate	Sets the rate limiting percentage. Available options are 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).

Viewing and editing multiple port configurations

To view or edit the configurations of multiple ports:

1 Select the ports you want to edit.

Press [Ctrl] + left click the ports you want to view or configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- Double-click on the selected port.
- On the toolbar, click Edit.

Note: When you edit multiple ports, some tabs are not available, and some tabs are available even though the options are not applicable. When the option does not apply for a given port, NoSuchObject is displayed.

Interface tab for multiple ports

The Interface tab shows the basic configuration and status of the selected ports.

To view or edit the Interface tab for multiple ports:

1 Select the ports that you want to edit.

[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for multiple ports opens with the Interface tab (Figure 166) displayed.

Figure 166 Port dialog box — Port Interface tab

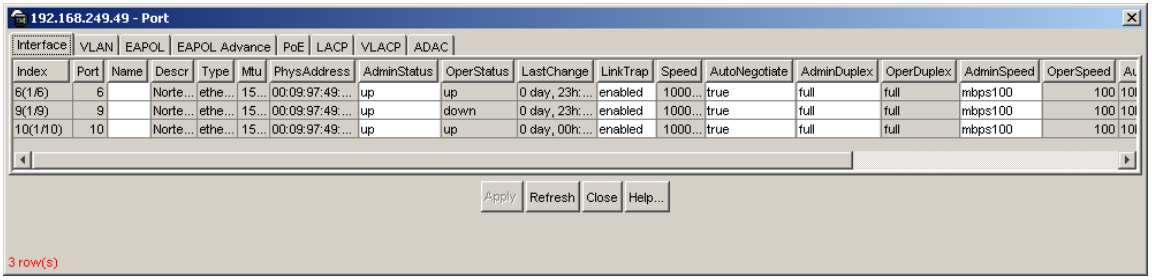


Table 127 describes the Port Interface tab fields.

Table 127 Port Interface tab fields for multiple ports

Field	Description
Index	A unique value assigned to each interface.
Port	Number of unit and port number.
Name	Allows you to enter a character string to name the port.
Descr	Type of switch and number of ports.
Type	Media type for this interface.

Table 127 Port Interface tab fields for multiple ports (Continued)

Field	Description
Mtu	Size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	MAC address assigned to a particular interface.
AdminStatus	Set administrative state of the interface from the pull-down menu, which can be one of the following: • up • down 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.
OperStatus	Current operational state of the interface, which can be one of the following: • up • down • testing If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	Value of 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	Enables and disables the link up/down traps.
Speed	The estimated bandwidth of the interface in bits per second (bps). For interfaces that do not vary in bandwidth or have no way to estimate the bandwidth, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reported by the object, then the object displays its maximum value (4,294,967,295). For a sub-layer that has no concept of bandwidth, the object should be zero.
AutoNegotiate	Set autonegotiation on the port from the pull-down menu.
AdminDuplex	Set the administrative duplex mode of the port from the pull-down menu (half or full).
OperDuplex	Indicate current duplex value of the port.
AdminSpeed	Set the speed of a port: none, mbps10, and mbps100, mbps1000. Note: The system returns an error if you attempt to set ports 1 to 24 for 1000 Mbps.

Table 127 Port Interface tab fields for multiple ports (Continued)

Field	Description
OperSpeed	The current operating speed of the port.
MltId	The MultiLink Trunk to which the port is assigned (if any).
AutoNegotiation Capability	Displays the current autonegotiation advertisements capability. (See "Custom Autonegotiation Advertisements" on page 288.)
AutoNegotiation Advertisements	Sets the autonegotiation advertisements. Any combination of speed-duplex settings is allowed from among those displayed in the AutoNegotiationCapability field.
IsPortShared	Specifies whether a port is shared. Multiple ports that are logically represented as a single port are shared. Only one shared port can be active at a time.
PortActiveComponent	Specifies the physical port components that are active for a shared port.

Chapter 14
Administering the switch using Web-based management

The administrative options available to you using Web-based management are:

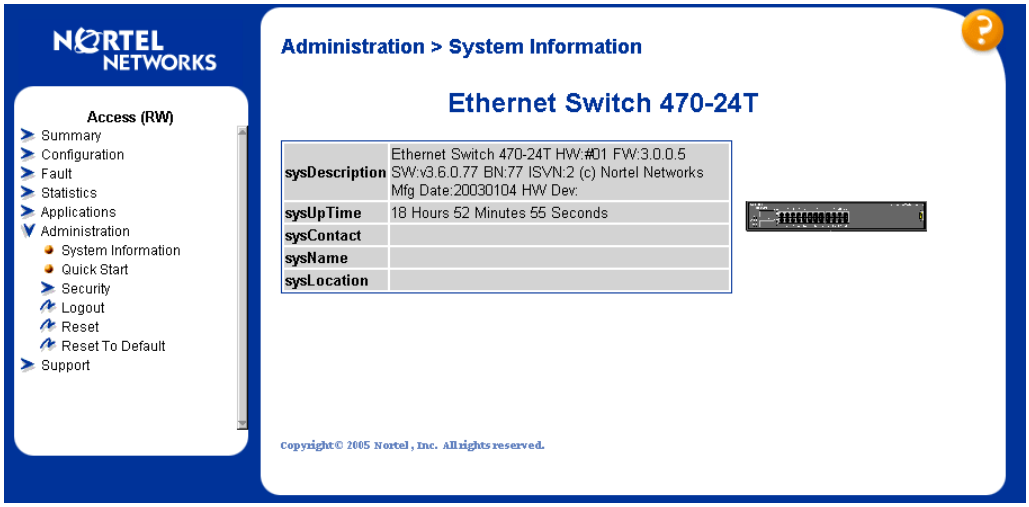
Note: Starting with Release 3.6 software, Secure Socket Layer (SSL) is available to provide security for the Web-based management system. It allows access to the Web-based management using a secure https session. The user must enable SSL for the browser through the Command Line Interface (CLI).

For more information on SSL Web-based management, refer to *Configuring and Managing Security* (217104-A).

Viewing general information

The viewing general information page, as shown in Figure 167, contains an image of the switch or an image of your entire stack configuration, information about the host device (or stack), and, if provided, the contact person or manager for the switch. The System Information page is also the Web-based management interface home page.

Figure 167 General Information.



Viewing system information

To view system information:

➡ From the main menu, choose Administration > System Information.

The System Information page opens (Figure 168)

Note: You create or modify existing system information parameters on the System page.

Figure 168 System Information home page on Ethernet Switch 470-24T

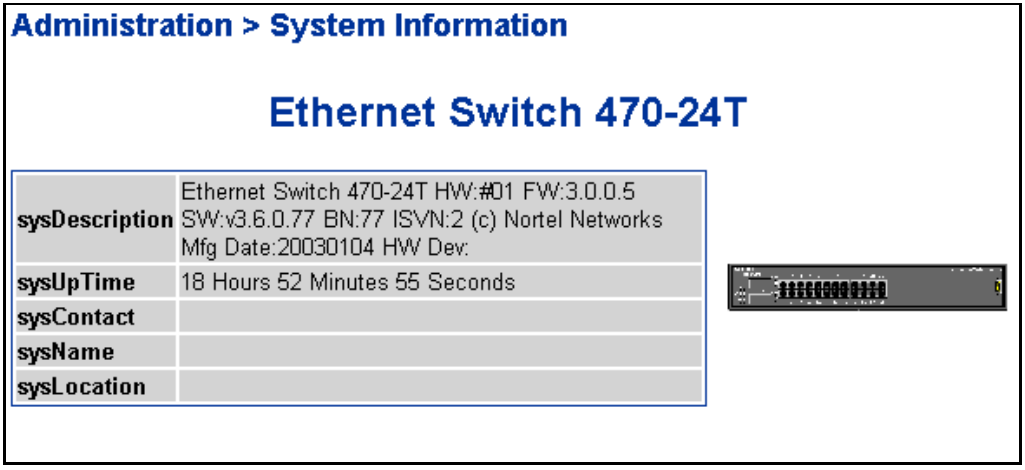


Table 128 describes the items on the System Information page.

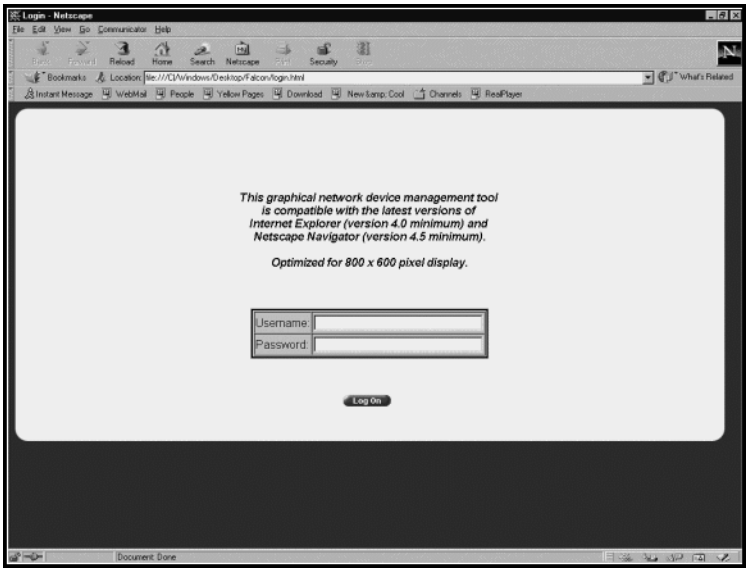
Table 128 System information page

Item	Range	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 re-initialized. Note: This field is updated only when the screen is redisplayed.
System Name	0..255	A a character string used to create a name to identify the switch, for example Finance Group.
System Location	0..255	A character string used to create a name for the switch location, for example, First Floor.
System Contact	0..255	A character string used to specify the name of a person to contact about switch operation, for example, mcarlson@company.com Note: To operate correctly with the Web interface, the system contact should be an e-mail address.

Logging on to the management interface

Once switch and stack passwords and RADIUS authentication settings are integrated into the Web-based management user interface, anyone who attempts to use the application is presented with a log on page (Figure 169).

Figure 169 Web-based management interface log on page



To log on to the Web-based management interface:

1 In the Username text box, type **RO** for read-only access, or **RW** for read-write access.

Note: RW and RO must be entered in uppercase.

2 In the Password text box, type your password.

3 Click Log On.

The System Information home page opens (see Figure 168 on page 479).

With Web-based management access enabled, the switch can support up to four concurrent Web-based management users. Two predefined user levels are available, and each user level has a corresponding username and password.

Table 129 shows the predefined user levels available and the access levels within the Web-based management user interface.

Table 129 User levels and access levels

User level	Username for each level	Password for each user level	Access Level
Read-only	RO	user	Read only
Read-write	RW	secure	Full read-write access

Resetting the switch

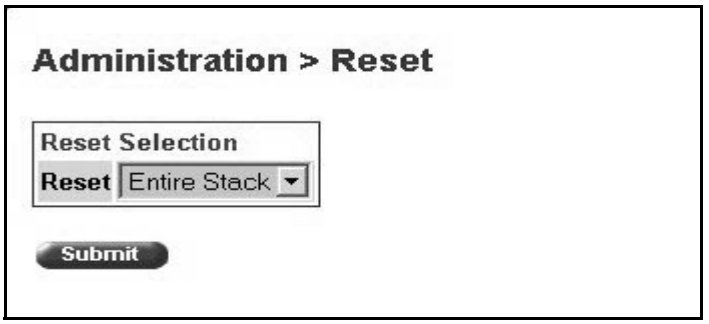
You can reset a stand-alone switch, a specific unit in a stack configuration, or an entire stack without erasing any configured switch parameters. While resetting, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

To reset the switch without making changes (since your last Submit request):

1 From the main menu, choose Administration > Reset.

The Reset page opens (Figure 170).

Figure 170 Reset page



2 From the list, choose to reset the switch or the entire stack.

3 Click Submit.

Note: When you are working on a single (non-stacked) switch, the system returns the message:
`Are you sure your want to reset the switch?`
Click OK, and the switch resets.

Note: If you have not configured system password security, a reset returns you to the home page, as shown in Figure 86 on page 232. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 169 on page 481.

Resetting the switch to system defaults

You can reset a stand-alone switch, a specific unit in a stack configuration, or an entire stack to system defaults. This replaces all configured switch parameters with the factory default values.

Caution: If you choose to reset to default settings, all configured settings are replaced with factory default settings when you click Submit (Stack Operational Mode is not reset to factory default). Resetting to default settings also causes loss of connection to the web until a new IP address is assigned. For more information on factory default settings, see Appendix A, "Default Settings," on page 517.

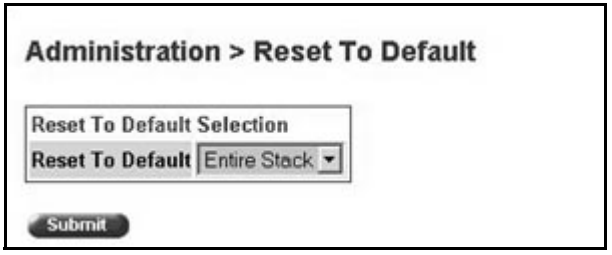
During the reset process, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

To reset the switch to system defaults:

1 From the main menu, choose Administration > Reset to Default.

The Reset to Default page opens (Figure 171).

Figure 171 Reset to Default page



2 From the list, choose to reset the switch only to system defaults, or the entire stack.

3 Click Submit.

Note: When you are working on a single (nonstacked) switch, the system returns the message:

```
Are you sure your want to reset the switch?
```

When you press OK, the switch resets.

Note: If you have not configured system password security, a reset returns you to the home page, as shown in Figure 86 on page 232. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 169 on page 481.

Logging out of the management interface

To log out of the Web-based management interface:

1. From the main menu, choose Administration > Logout.

   A message appears prompting you to confirm your request.

2. Do one of the following:

   - Click OK to log out of the Web-based management interface.
   - Click Cancel to return to the Web-based management interface home page.

Viewing summary information

The summary information options are:

- "Viewing stack information" on page 487
- "Viewing summary switch information" on page 489
- "Changing stack numbering" on page 491
- "Identifying unit numbers" on page 493

Viewing stack information

You can use Web-based management to view a summary of your stack framework, including the current version of the running software and the IP address of the Web-based management interface.

Note: The Web-based management user interface automatically detects the operational mode of your system. If the system is in stand-alone mode, the Stack Information page is not an option listed in the menu.

To view stack information:

1 From the main menu, choose Summary > Stack Information.

The Stack Information page opens (see Figure 172).

Figure 172 Stack Information page

Summary > Stack Information

Stack Information	
System Description	Ethernet Switch 470 - 48T HW:#01 FW:3.0.0.5 SW:v3.6.0.77
Software Version	v3.6.0.77
MAC Address	00-09-97-18-D7-DF
IP Address	134.177.224.105
Manufacturing Date Code	08222002
Serial #	ACC1002PQ
Operational State	Normal

Stack Inventory

Unit	Description	MDA	GBIC Port	GBIC Port	Software Version	Operational State
1	Ethernet Switch 470 - 48T 48 10/100BaseTX plus 2 Overlapped GBIC slots		(47) None	(48) None	v3.5.0.38	Normal
2	Ethernet Switch 470 -24T 2410/100BaseTX plus 2 GBIC slots		(25) None	(26) None	v3.5.0.38	Normal

Table 130 describes the fields on the Stack Information and Stack Inventory sections of the Stack Information page.

Table 130 Stack Information page 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 #	The serial number of the base unit.
	Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured
Stack Inventory	Unit	The unit number assigned to the device by the network manager. For more information on stack numbering, see "Changing stack numbering" on page 491.
	Description	The description of the device or its subcomponent.
	MDA	Not applicable
	GBIC Port	The shared GBIC port adapter connected to port 25/47 of the switch.
	GBIC Port	The shared GBIC port adapter connected to port 26/48 of the switch.
	Software Version	The current running software version.
	Operational State	The current operational state of the stack. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.

2 In the upper-left corner of the Stack Information page, click the number of the device you want to view.

The Stack Information page is updated with information about the selected switch.

Viewing summary switch information

You can view summary information about the switch, for example, the unit number and its corresponding physical description and serial number.

To view summary switch information:

1 From the main menu, choose Summary > Switch Information.

The Switch Information page opens (Figure 173).

Figure 173 Switch Information page

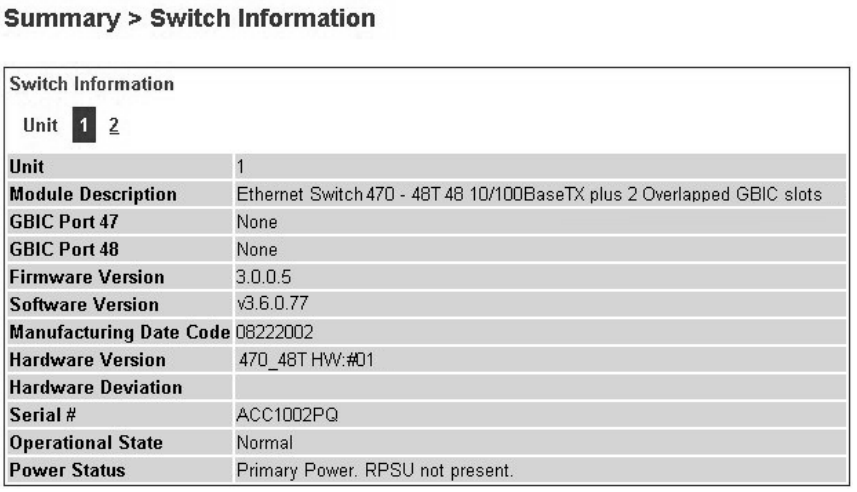


Table 131 describes the fields on the Switch Information page.

Table 131 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.
Module Description	The factory set description of the switch.
GBIC Port 25/47	The factory set description of the GBIC shared port 25/47. For additional hardware information on installed GBICs, click the GBIC hyperlink.
GBIC Port 26/48	The factory set description of the GBIC shared port 26/48. For additional hardware information on installed GBICs, click the GBIC hyperlink.
Software Version	The version of the running software.
Manufacturing Date Code	The date of manufacture of the board in ASCII format.
Serial Number	The serial number of the 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 the upper-left corner of the Switch Information page, click the number of the device you want to view.

The Switch Information page is updated with information about the selected switch.

Note: Firmware version, hardware version and hardware deviation are shown when system is in the stack mode, but not shown in stand-alone mode.

Changing stack numbering

If your system is set to “stack” operational mode, you can view existing stack numbering information and renumber the devices in your stack framework.

Note: The unit number does not affect the base unit designation.

To view or renumber devices within the stack framework:

1 From the main menu, choose Summary > Stack Numbering.

The Stack Numbering Setting page opens (Figure 174).

Figure 174 Stack Numbering Setting page

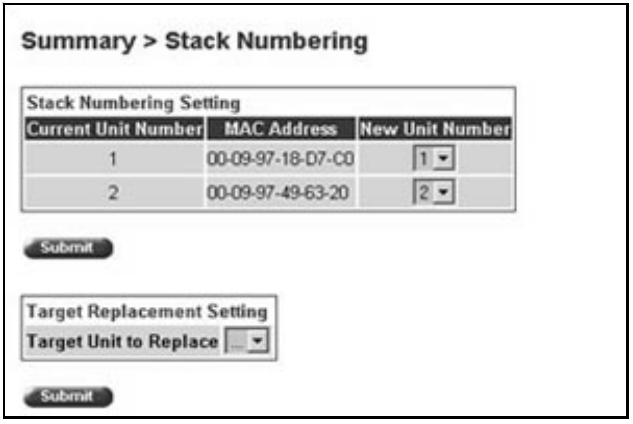


Table 132 describes the fields on the Stack Numbering Setting page.

Table 132 Stack Numbering Setting page fields

Item	Range	Description
Current Unit Number	1..8	Unit number previously assigned to the Ethernet Switch. The entries in this column are displayed in order of their current physical cabling with respect to the base unit, and can show nonconsecutive unit numbering if one or more units were previously moved or modified. The entries can also 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 Ethernet Switch. Note: If you leave the field blank, the system automatically selects the next available number.

2 Choose the new number to assign to your switch.

3 Click Submit.

A message opens prompting you to confirm your request.

4 Do one of the following:

- Click OK to renumber the stack.
- Click Cancel to return to the Stack Numbering page without making changes.

Identifying unit numbers

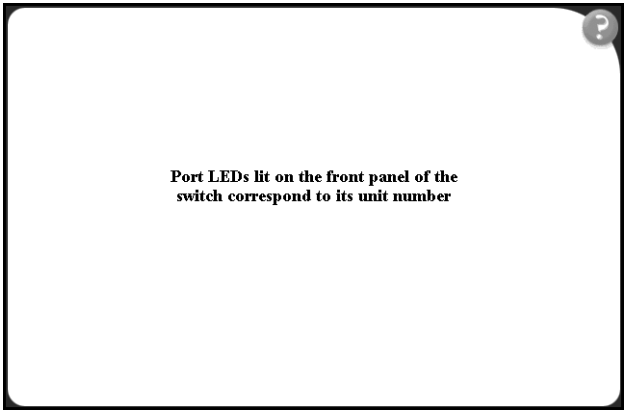
You can identify the unit numbers of the switches participating in a stack configuration by viewing the LEDs on the front panel of each switch.

To identify unit numbers in your configuration:

1 From the main menu, choose Summary > Identify Unit Numbers.

The Identify Unit Numbers page opens (Figure 175).

Figure 175 Identify Unit Numbers page



2 To continue viewing summary information or to start the configuration process, choose another option from the main menu.

Chapter 15
Configuring the switch using Web-based management

The switch configuration options available to you are:

Configuring BootP, IP, and gateway settings

You can configure the BootP mode settings, create and modify your in-band stack and in-band switch IP addresses and in-band subnet mask parameters, and configure the IP address of your default gateway. You can also configure IP addresses for individual units in a stack.

Note: Settings take effect immediately after you click Submit.

To configure BootP, IP, and gateway settings:

1 From the main menu, choose Configuration > IP.

The IP page opens (see Figure 176 for the display for a single unit and Figure 177 on page 497 for the display in a stack).

Figure 176 IP page for a single unit

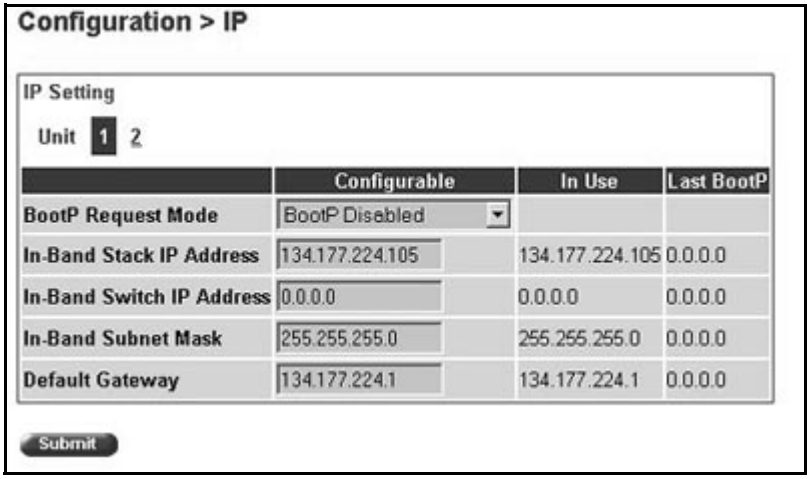
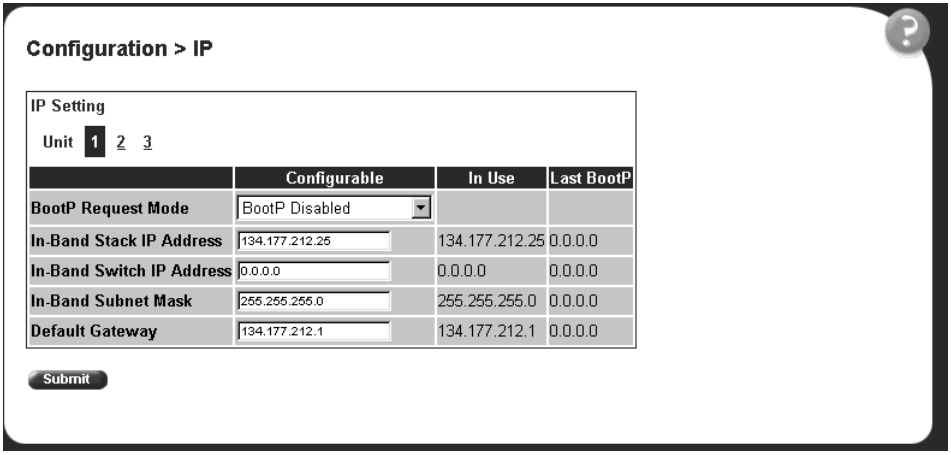


Figure 177 IP page for a stack



Note: To change the IP information for a specific unit in a stack, choose that unit, and enter the desired IP information into the In-Band Switch IP address field.

Table 133 describes the items on the IP page.

Table 133 IP page items

Section	Item	Range	Description
Boot Mode Setting	BootP Request Mode	BootP When Needed	Choose this mode for the switch to send a BootP request when the IP address stored in non-volatile memory is the same as the factory default value. If this IP address differs from the factory default value, the switch uses the stored network parameters. If the switch cannot find a BootP server, it attempts to search for the BootP server five more times. If the switch fails to connect with the BootP server sets the BootP request mode to the default factory settings.
		BootP Always	Choose this mode for the switch to ignore any stored network parameters, and send a BootP request every time the switch boots. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to boot normally.
		BootP Disabled	Choose this mode for the switch to use the IP configuration parameters stored in non-volatile memory each time the switch boots. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.
		BootP or Last Address	Choose this mode to inform the switch, at each startup, to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its non-volatile memory. Note: Valid parameters obtained in using BootP always replace current information stored in the non-volatile memory.
		Note: Whenever the switch is broadcasting BootP requests, the BootP process times out if a reply is not received within (approximately) 7 minutes. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to any of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.	
IP Setting	In-Band Stack IP Address	XXX.XXX.XXX.XXX	Type a new stack IP address in the appropriate format.

Table 133 IP page items

Section	Item	Range	Description
	In-Band Switch IP Address	XXX.XXX.XXX.XXX	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. This field is based on the class of the IP address entered in the In-Band IP Address field.
	In-Band Subnet Mast	XXX.XXX.XXX.XXX	Type a new subnet mask in the appropriate format.
	In-Use		The column header for the read-only fields in this screen. The data displayed in this column represents data that is currently in use.
	Last BootP		The column header for the read-only fields in this screen. The read-only data displayed in this column represents data obtained from the last BootP reply received.
Gateway Setting	Default Gateway	XXX.XXX.XXX.XXX	Type an IP address for the default gateway in the appropriate format.

2 Specify the required information in the text boxes, or select from list box.

3 Click Submit.

Modifying system settings

You can create or modify the system name, system location, and network manager contact information.

Note: The configurable parameters on the System page are displayed in a read only-format on the Web-based management user interface System Information home page (see Figure 86 on page 232).

To configure system settings:

1 From the main menu, choose Configuration > System.

The System page opens (Figure 178).

Figure 178 System page

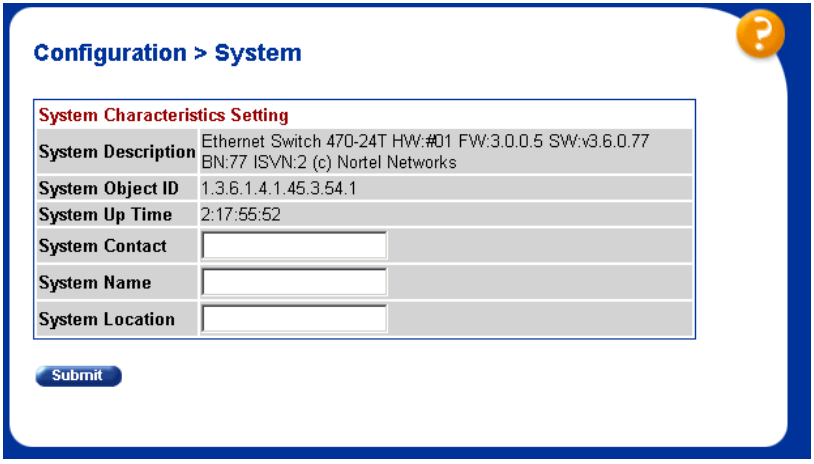


Table 134 describes the items on the System page.

Table 134 System page elements

Item	Range	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 re-initialized. Note: This field is updated only when the screen is redisplayed.
System Contact	0..255	A character string used to specify the name of a person to contact about switch operation, for example, mcarlson@company.com Note: To operate correctly with the Web interface, the system contact should be an e-mail address.
System Name	0..255	A a character string used to create a name to identify the switch, for example Finance Group.
System Location	0..255	A character string used to create a name for the switch location, for example, First Floor.

2 Specify the required information in the text boxes.

3 Click Submit.

Configuring port autonegotiation, speed, duplex, status, and alias

You can configure a specific switch port or all switch ports to autonegotiate for the highest available speed of the connected station or you can set the speed for selected switch ports. Autonegotiation is not supported on fiber optic ports.

You can name each port, or assign an alias to it, using 27 alphanumeric characters.

To configure a switch port's alias, status, autonegotiation and speed/duplex:

1 From the main menu, choose Configuration > Port Management.

The Port Management page opens (Figure 179).

Figure 179 Port Management page

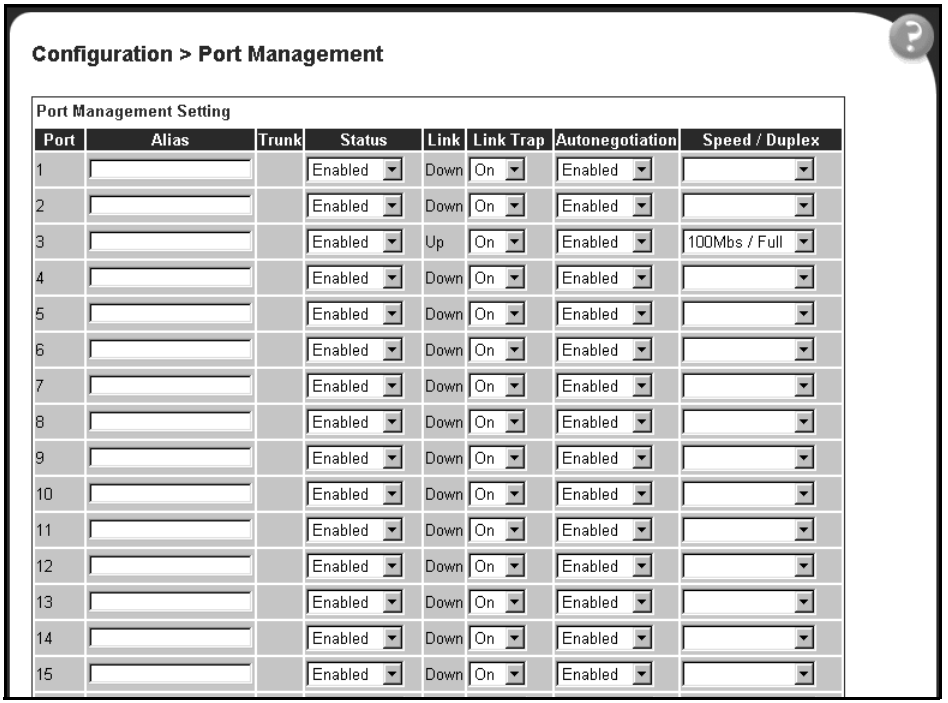


Table 135 describes the items on the Port Management page.

Table 135 Port Management page items

Item	Range	Description
Port		The switch port number of the corresponding row. To select the switch row, click the check box to the right. The values that you set in each switch row affect all switch ports and, when the switch is part of a stack, the values that set in the stack row affect all ports in the entire stack (except the GBIC ports or fiber optic ports when installed). For information on setting high speed flow control, see "Configuring high speed flow control" on page 505.
Alias	27 alphanumeric characters	Displays the name, or alias, you assigned the port. To assign a name or to change the name, enter up to 26 alphanumeric characters.
Trunk		The trunk group that the switch port belongs to as specified in the Trunk Member fields on the MultiLink Trunk page. For more information, see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A).
Status	(1) Enabled (2) Disabled	Choose to enable or disable the port. You can also use this field to control access to any switch port. The default setting is Enabled.
Link		The current link state of the corresponding port as follows: • Up: The port is connected and operational • Down: The port is not connected or is not operational.
Link/Trap	(1) On (2) Off	Choose to control whether link up/down traps are sent to the configured trap sink from the switch. The default setting is On.

Table 135 Port Management page items

Item	Range	Description
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. Choosing to enable autonegotiation sets the corresponding port speed to match the best service provided by the connected station, up to 100Mb/s in full-duplex mode. **NOTE**: This field is disabled for all fiber optic ports. Use the High Speed Flow Control Configuration screen (next) to set autonegotiation for all gigabit ports. The default setting is Enabled.
Speed / Duplex	(1) 10Mbs / Half (2) 10Mbs / Full (3) 100Mbs / Half (4) 100Mbs / Full (5) 1000Mbs / Full	Choose the Ethernet speed you want the port to support. **NOTE**: Fiber optic ports can only be set to 100 Mb/s/ Half or 100 Mb/s/Full. Use the High Speed Flow Control Configuration screen (next) to set autonegotiation for all gigabit ports. The default setting is 100Mbs/Half when autonegotiation is disabled and 1000 Mb/s full-duplex for gigabit ports only.

2 In the upper-left hand corner, click the unit number of the Ethernet Switch to manage.

The page is updated with the information for the selected switch.

3 In the port row of your choice, select from the lists.

4 Click Submit.

Configuring high speed flow control

You can use this screen to set switch port parameters, and set autonegotiation for all gigabit ports.

To configure high speed flow control:

1 From the main menu, choose Configuration > High Speed Flow Control.

The High Speed Flow Control page opens (Figure 180).

Figure 180 High Speed Flow Control page

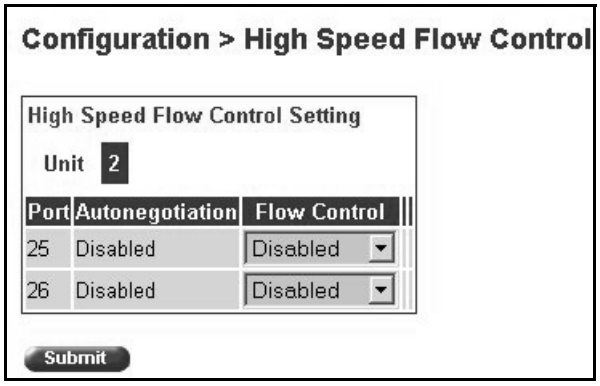


Table 136 describes the items on the High Speed Flow Control page.

Table 136 High Speed Flow Control page items

Item	Range	Description
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. **NOTE**: This field is disabled for all fiber optic ports. When enabled, the port advertises support for flow control autonegotiation.
Flow Control	(1) Enabled (2) Symmetric (3) Asymmetric	Choose your flow control preference to control traffic and avoid congestion on the GBIC port.

Table 136 High Speed Flow Control page items

Item	Range	Description
Preferred Phy	(1) Left (2) Right	Choose the preferred physical port. The port not selected automatically reverts to a backup physical port.
Active Phy		The current operating physical port. The physical port options are left or right.

2. In the upper-left hand corner, click on the unit number of the GBIC to configure.
3. Select from the lists.
4. Click Submit.

Downloading switch images

You can download the Ethernet Switch software image that is located in non-volatile flash memory. To download the software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the switch must have an IP address. To learn how to configure the switch IP address, refer to "Configuring BootP, IP, and gateway settings" on page 496.

Caution: Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

To download a switch image:

1 From the main menu, choose Configuration > Software Download.

The Software Download page opens (Figure 181).

Figure 181 Software Download page

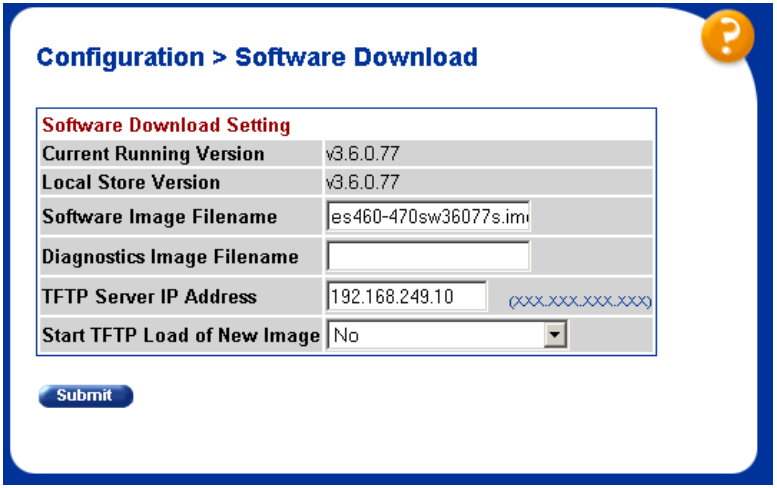


Table 137 describes the items on the Software Download page.

Table 137 Software Download page items

Item	Range	Description
Current Running Version		The version of the current running software.
Local Store Version		The local version of the software in the flash memory.
Software Image Filename	1..30	Type the software image load filename.
Diagnostics Filename	1..30	Type the diagnostics filename.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of your TFTP load host.
Start TFTP Load of New Image	(1) No (2) Software Image (3) Diagnostics (4) Software Image If Newer	Choose the software image to load.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Take care not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

When the download process is complete, the switch automatically resets and the new software image initiates a self-test.

Storing and retrieving a switch configuration file from a TFTP server

You can store switch configuration parameters on a Trivial File Transfer Protocol (TFTP) server. You can retrieve the configuration parameters of a switch and use the retrieved parameters to automatically configure a replacement switch.

To store a switch configuration, you must set up the file on your TFTP server and set the filename read-write permission to enabled.

To download the switch configuration file, a properly configured TFTP server must be present in your network, and the Ethernet Switch must have an IP address. To learn how to configure the switch or stack IP address, refer to "Configuring BootP, IP, and gateway settings" on page 496.

To store or retrieve a switch configuration file:

1 From the main menu, choose Configuration > Configuration File.

The Configuration File Download/Upload page opens (Figure 182).

Figure 182 Configuration File Download/Upload page

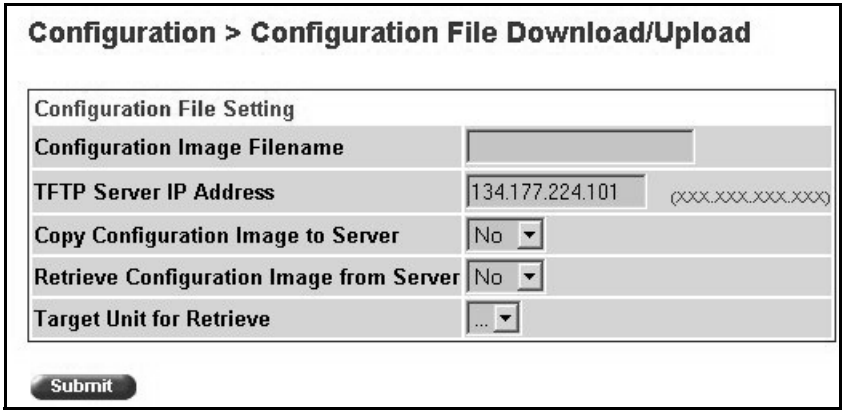


Table 138 describes the items on the Configuration File page.

Table 138 Configuration File page items

Item	Range	Description
Configuration Image Filename	1..32	Type the configuration file name.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of the TFTP load host.
Copy Configuration Image to Server	(1) Yes (2) No	Choose whether or not to copy the configuration image to the server.
Retrieve Configuration Image from Server	(1) Yes (2) No	Choose whether or not to retrieve the configuration image from a server. If you choose Yes, the download process begins immediately and, when completed, causes the switch or stack to reset with the new configuration parameters.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Table 139 describes the requirements for storing or retrieving configuration parameters on a TFTP server.

Table 139 Requirements for storing or retrieving configuration parameters on a TFTP server

Requirements
• The Configuration File feature can be used only to copy *stand-alone switch configuration parameters to other stand-alone switches* or to copy *stack configuration parameters to other stack configurations*. For example, you cannot duplicate the configuration parameters of a unit in a *stack* configuration and use it to configure a *stand-alone* switch.
• A configuration file obtained from a stand-alone switch can only be used to configure other stand-alone switches with the same firmware revision and model type as the donor stand-alone switch.
• A configuration file obtained from a stack unit can be used only to configure other stacks that have the same number of switches, firmware version, model types, and physical IDs as the stack the donor stack unit resides in.
• Reconfigured stacks are configured according to the unit order number of the donor unit. For example, the configuration file parameters from a donor unit with physical ID *x* are used to reconfigure the unit with physical ID *x*.
• The configuration file also duplicates any settings that exist for any GBIC that is installed in the donor switch. If you use the configuration file to configure another switch that has the same GBIC model installed, the configuration file settings will also apply to and override the existing GBIC settings.

Table 140 describes the parameters that are not saved to the configuration file.

Table 140 Parameters not saved to the configuration file

These parameters are not saved:	**Used in this screen:**	**See page:**
In-Band Stack IP Address	IP Configuration/Setup	496
In-Band Switch IP Address		
In-Band Subnet Mask		
Default Gateway		
Configuration Image Filename	Configuration File Download/Upload	509
TFTP Server IP Address		
Console Read-Only Switch Password	Console/Comm Port Configuration	512
Console Read-Write Switch Password		
Console Read-Only Stack Password		
Console Read-Write Stack Password		

Configuring port communication speed

You can view the current console/communication port settings and configure the console port baud rate to match the baud rate of the console terminal.

To view current console/communication port settings and configure console port speed:

1 From the main menu, choose Configuration > Console/Comm Port.

The Console/Communication Port page opens (Figure 183).

Figure 183 Console/Communication Port page

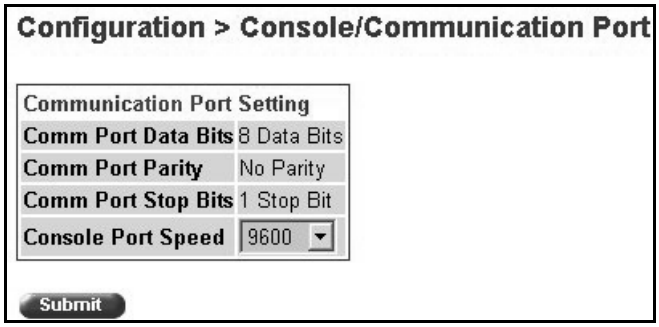


Table 141 describes the items on the Console/Communication Port page.

Table 141 Console/Communication Port Setting page items

Item	Range	Description
Comm Port Data Bits		The current console communication port data bit setting.
Comm Port Parity		The current console communication port parity setting.
Comm Port Stop Bits		The current console communication port stop bit setting.
Console Port Speed	2400 4800 9600 19200 38400	Choose the console port speed baud rate. Note: The default setting is 9600.
		Caution: If you choose a baud rate that does not match your console terminal baud rate, you will lose communication with the configuration interface when you click Submit.

2 Select from the list.

3 Click Submit.

Configuring rate limiting

You can view the current forwarding rate of broadcast and multicast packets, and configure the Ethernet Switches 460 and 470 to limit the forwarding rate of broadcast and multicast packets on each interface. When you configure rate limiting, you set the percentage of port bandwidth allowed for a packet type. When the threshold is exceeded, additional packets are discarded.

Note: If a port is configured for rate limiting, and it is a MultiLink trunk member, all trunk member ports implement rate limiting. If the port becomes disabled, all trunk members become disabled.

To configure rate limiting:

1 From the main menu, choose Application > Rate Limiting.

The Rate Limiting page opens (Figure 184).

Figure 184 Rate Limiting page

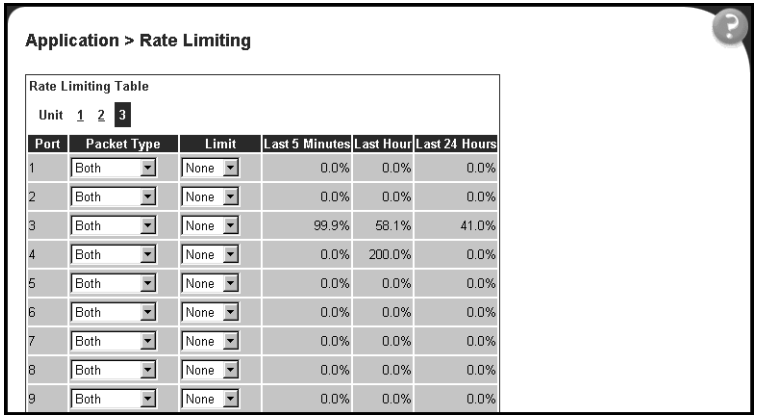


Table 142 describes the items on the Rate Limiting page.

Table 142 Rate Limiting page items

Item	Range	Description
Port	1..26	The selected unit's port number. The normal port range is 1 to 48.
Packet Type	(1) Multicast (2) Broadcast (3) Both	Choose the packet type to view on the table. The default setting is Both.
Limit	None, 1-10%	Choose the percentage, if any, of bandwidth allowed for forwarding the packet type specified in the Packet Type field. When the threshold is exceeded, any additional packets are discarded. Note: Rate limiting is disabled if this field is set to none. This allows you to select and view the percentage of specific packet types present in the network, without inadvertently limiting the forwarding rate. The default setting is None.
Last 5 Minutes	0..100%	The percentage of packets received by the port in the last five minutes. This field provides a running average of network activity and is updated every 15 seconds.
Last Hour	0..100%	The percentage of packets received by the port in the last hour. This field provides a running average of network activity and is updated every five minutes.
Last 24 Hours	0..100%	The percentage of packets received by the port in the last 24 hours. This field provides a running average of network activity and is updated every hour.
		Note: The Last 5 Minutes, Last Hour, and Last 24 Hours fields indicate the receiving port's view of network activity regardless of the rate limiting setting.
		Note: When the volume of broadcast and multicast packets is high, placing severe strain on the network (often referred to as a "storm"), you can set the forwarding rate of those packet types to *not exceed* a specified percentage of the total available bandwidth.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

3 Type information in the text boxes, or select from a list.

4 Click Submit.

Note: To avoid broadcast storms (when the volume of a particular packet type is extreme, placing severe strain on the network), set the forwarding rate of the packet type to not exceed a lower percentage of the total available bandwidth.

Appendix A
Default Settings

Table 143 lists the factory default settings for the Ethernet Switch 470 according to the Console Interface (CI) screens and fields for the settings.

Table 143 Factory default Ethernet Switch 470 settings

Field	Default setting	Refer to the following:
Unit	1	"IP configuration screen" on page 243
BootP Request Mode	BootP When Needed	
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	SNMP Configuration screen (see *Configuring and Managing Security* (217104-A))
Read-Write Community String	private	
Trap IP Address	0.0.0.0 (no IP address assigned)	
Community String	Zero-length string	
Authentication Trap	Enabled	
Link Up/Down Trap	Enabled	
sysContact	Zero-length string	"Console Interface System Characteristics screen" on page 259
sysName	Zero-length string	
sysLocation	Zero-length string	

Table 143 Factory default Ethernet Switch 470 settings (Continued)

Field	Default setting	Refer to the following:
Aging Time	300 seconds	"MAC Address Table screen" (see *Configuring and Managing Security* (217104-A))
Find an Address	00-00-00-00-00-00 (no MAC address assigned)	
Port Mirroring Address A:	00-00-00-00-00-00 (no MAC address assigned)	
Port Mirroring Address B:	00-00-00-00-00-00 (no MAC address assigned)	
MAC Address Security	Disabled	"MAC Address Security Configuration Menu screen" (see *Configuring and Managing Security* (217104-A))
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	MAC Address Security Port Configuration screen (see *Configuring and Managing Security* (217104-A))
Security	Disabled	
Port List	blank field	MAC Address Security Port Lists screens (see *Configuring and Managing Security* (217104-A))
Find an Address	blank field	MAC Address Security Table screens (see *Configuring and Managing Security* (217104-A))
MAC Address	- - - - - - (no address assigned)	
Allowed Source	- (blank field)	
MAC-SA based VLAN	The least active MAC-SA based VLAN is displayed.	MAC Address Configuration for MAC-SA-Based VLAN screen (see *Configuring and Managing Security* (217104-A))
Display/Create MAC Address	00-00-00-00-00-00	

Table 143 Factory default Ethernet Switch 470 settings (Continued)

Field	Default setting	Refer to the following:
Create VLAN	1	VLAN Configuration screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A))
Delete VLAN	blank field	
VLAN Name	VLAN # (*VLAN number*)	
Management VLAN	Yes, VLAN #1	
IVL/SVL	IVL	
VLAN Type	Port-based	
Protocol ID (PID)	None	
User-Defined PID	0x0000	
VLAN State	Inactive	
Subnet Addr	0.0.0.0.	
Subnet Mask	0.0.0.0.	
Port Membership	U (all ports assigned as untagged members of VLAN 1)	
Unit	1	VLAN Port Configuration screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A))
Port	1	
Filter Tagged Frames	No	
Filter Untagged Frames	No	
Filter Unregistered Frames	No	
Port Name	Unit 1, Port 1	
PVID	1	
Port Priority	0	
Tagging	Untagged Access	
AutoPVID	Disabled	

Table 143 Factory default Ethernet Switch 470 settings (Continued)

Field	Default setting	Refer to the following:
Unit	1	VLAN Display by Port screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A))
Port	1	
PVID	1 (read only)	
Port Name	Unit 1, Port 1 (read only)	
Unit	1	"Port Configuration screen" on page 142
Status	Enabled (for all ports)	"Rate Limiting Configuration screen" on page 148
Autonegotiation	Enabled (for all ports)	
Speed/Duplex	100Mbs/Half (when Autonegotiation is Disabled)	
Trunk	1 to 6 (depending on configuration status)	MultiLink Trunk Configuration Menu screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A))
Trunk Members (Unit/Port)	Blank field	
STP Learning	Normal	
Trunk Mode	Basic	
Trunk Status	Disabled	
Trunk Name	Trunk #1 to Trunk #6	
Traffic Type	Rx and Tx	MultiLink Trunk Utilization screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A))

Table 143 Factory default Ethernet Switch 470 settings (Continued)

Field	Default setting	Refer to the following:
Monitoring Mode	Disabled	Port Mirroring Configuration screen (see *System Monitoring Guide* (217107-A))
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)	
Packet Type	Both	"Rate Limiting Configuration screen" on page 148
Limit	None	
VLAN	1	IGMP Configuration screen (see *Configuring IP Multicast Routing Protocols* (217459-A))
Snooping	Enabled	
Proxy	Enabled	
Robust Value	2	
Query Time	125 seconds	
Set Router Ports	Version 1	
Static Router Ports	- (for all ports)	
Unit	1	Port statistics screen (see *System Monitoring Guide* (217107-A))
Port	1	
Console Port Speed	9600 Baud	"Configuring the Console Port" on page 116
Console Switch Password	Not Required	
Console Stack Password	Not Required	
Console Read-Only Switch Password	user	
Console Read-Write Switch Password	secure	
Console Read-Only Stack Password	user	
Console Read-Write Stack Password	secure	

Table 143 Factory default Ethernet Switch 470 settings (Continued)

Field	Default setting	Refer to the following:
Group	1	Spanning Tree Group Configuration screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A))
Bridge Priority	8000	
Bridge Hello Time	2 seconds	
Bridge Maximum Age Time	20 seconds	
Bridge Forward Delay	15 seconds	
Add VLAN Membership	1	
Tagged BPDU on tagged port	• STP Group 1—No • Other STP Groups—Yes	
STP Group State	• STP Group 1—Active • Other STP Groups—InActive	
VID used for tagged BPDU	4001-4008 for STGs 1-16, respectively	
STP Group	1	Spanning Tree Port Configuration screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A))
Participation	Normal Learning	
Priority	128	
Path Cost	10 or 100	
STP Group	1	Spanning Tree Switch Settings screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A))
STP Group	1	Spanning Tree VLAN Membership screen (see *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A))

Table 143 Factory default Ethernet Switch 470 settings (Continued)

Field	Default setting	Refer to the following:
TELNET Access	Enabled	TELNET/SNMP/Web Access Configuration screen (see *Configuring and Managing Security* (217104-A))
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 nine 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 nine fields: 255.255.255.255 (any address is allowed)	
Image Filename	Zero-length string	"Software Management" on page 262
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	"Configuration file download/upload screen" on page 271
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Copy Configuration Image to Server	No	
Retrieve Configuration Image from Server	No	
ASCII Configuration Filename	Zero-length string	"ASCII configuration file download screen" on page 278
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Retrieve Configuration file from Server	No	
Last Manual Configuration Status	Passed	
Last Auto Configuration Status	Passed	
Auto Configuration on Reset	Disabled	

Table 144 lists the additional factory default settings for the Ethernet Switch 460-24T-PWR.

Table 144 Factory default Ethernet Switch 460-24T-PWR settings

Field	Default setting	Refer to the following:
Port Power Admin. Status	Enabled	Chapter 9, “Power over Ethernet for the Ethernet Switch 460,” on page 319
Power Usage Threshold	80%	
Power Pair	Spare	
Power Traps Control	Enabled	
Port Power Limit	Power Level = 16W Resolution = 1W Range = 3W to 20W	
Port Power Priority	Low	
Device Power Detection Mode	802.3af	
DC Source Type	Ethernet Switch Power Supply Unit 10	
DC Source Configuration	Power-sharing	

Appendix B
CLI Command List

This appendix provides the complete Command Line Interface (CLI) command list in alphabetical order, with associated references for further explanations.

Note: The information in this list is presented for reference only and is not to be considered an exact representation.

Table 145 CLI command list

Command	See:
`adac [enable] [op-mode <untagged-frames-basic | untagged-frames-advanced| tagged-frames>] [traps enable] [voice-vlan <1-4094>] [uplink-port <slot/port>] [call-server-port <slot/port>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`adac port <port-list> enable`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`auto-negotiation-advertisements [port <portlist>] [10-full] [10-half] [100-full] [100-half] [1000-full] [1000-half] [asymm-pause-frame] [pause-frame]`	page 430
`auto-pvid`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`autotopology`	page 409
`boot [default] [unit <unitno>]`	page 387
`clear logging [nv]`	*System Monitoring Guide* (217107-A)

Table 145 CLI command list (Continued)

Command	See:
clear-stats [port<*portlist*>]	*System Monitoring Guide* (217107-A)
cli-password {switch|stack} {ro|rw} <*WORD*> <*WORD*> cli-password {switch|stack} {serial|telnet} {none|local|radius}	*Configuring and Managing Security* (217104-A)
config radius auth-info-attr-value <*value*>	*Configuring IP Multicast Routing Protocols* (217459-A)
config radius mcast-addr-attr-value <*value*>	*Configuring IP Multicast Routing Protocols* (217459-A)
config switch mode <l2|traffic-separation>	page 406
configure {terminal|network}	page 166
configure network [load-on-boot {disable|use-bootp|use-config}] configure network [filename <*WORD*>] configure network [address <*XXX.XXX.XXX.XXX*>]	page 372
configure network [address <A.B.C.D>] [filename <WORD>]	page 372
configure network load-on-boot {disable|use-bootp| use-config} [address <A.B.C.D>] filename <WORD>	page 375
cops retry	*Configuring Quality of Service, and IP Filtering* (217106-A)
cops server	*Configuring Quality of Service, and IP Filtering* (217106-A)
copy config nvram	page 408
copy config tftp [address <*XXX.XXX.XXX.XXX*>] filename <*WORD*>	page 391
copy running-config tftp [address <A.B.C.D>] filename <WORD>	page 372
copy tftp config [address <*XXX.XXX.XXX.XXX*>] filename <*WORD*>	page 391
copy tftp config unit <unit #>	page 391
default adac [enable] [op-mode] [traps enable] [voice-vlan] [uplink-port] [call-server-port]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
`default adac [port <port-list>] enable`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`default auto-negotiation-advertisements [port <portlist>]`	page 432
`default autotopology`	page 410
`default cops retry`	*Configuring Quality of Service, and IP Filtering* (217106-A)
`default cops server`	*Configuring Quality of Service, and IP Filtering* (217106-A)
`default duplex [port <portlist>]`	page 420
`default eapol guest-vlan`	*Configuring and Managing Security* (217104-A)
`default eapol multihost enable`	*Configuring and Managing Security* (217104-A)
`default eapol multihost eap-mac-max`	*Configuring and Managing Security* (217104-A)
`default flowcontrol [port <portlist>]`	page 423
`default ip address unit <1-8>`	page 360
`default ip bootp server`	page 389
`default lacp aggregation [port <portlist>] enable`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`default lacp mode [port <portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`default lacp priority [port <portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`default lacp timeout-time [port <portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`default lacp system-priority`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`default logging`	*System Monitoring Guide* (217107-A)

Table 145 CLI command list (Continued)

Command	See:
`default logging remote level`	*System Monitoring Guide* (217107-A)
`default mac-address-table aging-time`	*Configuring and Managing Security* (217104-A)
`default name [port <portlist>]`	page 416
`default rate-limit [port <portlist>]`	page 427
`default set logging`	*System Monitoring Guide* (217107-A)
`default snmp trap link-status [port <portlist>]`	*Configuring and Managing Security* (217104-A)
`default snmp-server authentication-trap`	*Configuring and Managing Security* (217104-A)
`default snmp-server community [ro|rw]`	*Configuring and Managing Security* (217104-A)
`default snmp-server contact`	*Configuring and Managing Security* (217104-A)
`default snmp-server host`	*Configuring and Managing Security* (217104-A)
`default snmp-server location <text>`	*Configuring and Managing Security* (217104-A)
`default snmp-server name <text>`	*Configuring and Managing Security* (217104-A)
`default snmp trap link-status [port <portlist>]`	*Configuring and Managing Security* (217104-A)
`default spanning-tree [stp <1-16>] [forward-time] [hello-time] [max-age] [priority] [tagged-bpdu]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`default spanning-tree [port <portlist>] [stp <1-16>] [learning] [cost] [priority]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`default spanning-tree vlan <vlan-id>` (used with PVST+)	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`default speed [port <portlist>]`	page 418
`default ssh [dsa-auth|dsa-key|max-sessions|pass-auth|port|timeout]`	*Configuring and Managing Security* (217104-A)

Table 145 CLI command list (Continued)

Command	See:
`default stack auto-unit-replacement enable`	page 317
`default telnet-access`	*Configuring and Managing Security* (217104-A)
`default terminal {speed|length|width}`	page 381
`default vlan igmp {<1-4094> | unknown-mcast-no-flood}`	*Configuring IP Multicast Routing Protocols* (217459-A)
`default vlan mgmt <1-4094>`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`disable`	page 167
`download [address <ip>] {image <image-name> | image-if-newer <image name> | diag <filename>} [no-reset]`	page 376
`duplex [port <portlist>] {full|half|auto}`	page 419
`eapol [{enable|disable}] [port <portlist>] [init] [status authorized|unauthorized|auto] [traffic-control in-out|in] [re-authentication enable|disable] [re-authentication-interval <num>] [re-authenticate] [quiet-interval <num>] [transmit-interval <num>] [supplicant-timeout <num>] [server-timeout <num>] [max-request <num>]`	*Configuring and Managing Security* (217104-A)
`eapol guest-vlan <portlist> vid <1-4094>`	*Configuring and Managing Security* (217104-A)
`eapol multihost <port> enable [eap-mac-max <1-32>]`	
`eapol user-based-policies enable`	*Configuring and Managing Security* (217104-A)
`enable`	page 166
`end`	page 168
`exit`	page 168
`flowcontrol [port <portlist>] {asymmetric|symmetrid|auto|disable}`	page 421
`help`	page 161

Table 145 CLI command list (Continued)

Command	See:
help commands [mode {current | exec | privExec | config | ifconfig}]	page 162
help modes	page 164
interface FastEthernet {<*portlist*>}	page 167
ip address[stack|switch] <*XXX.XXX.XXX.XXX*> [netmask <*XXX.XXX.XXX.XXX*>]	page 355
ip address unit <*1-8*> A.B.C.D	page 358
ip bootp server {last|needed|disable|always}	page 387
ip default-gateway <*XXX.XXX.XXX.XXX*>	page 356
ipmgr {telnet|snmp|http} {[source-ip <1-50> <*XXX.XXX.XXX.XXX*>] [mask <*XXX.XXX.XXX.XXX*>]}	*Configuring and Managing Security* (217104-A)
lacp aggregation [port <portlist>] enable	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
lacp key [port <portlist>] <1-4095>	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
lacp mode [port <portlist>] {off | passive | active}	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
lacp priority [port <portlist>] <0-255>	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
lacp system-priority [0-65535]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
lacp timeout-time [port <portlist>] {short | long}	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
logging remote address <A.B.C.D>	*System Monitoring Guide* (217107-A)
logging remote level {critical|informational|serious}	*System Monitoring Guide* (217107-A)
logout	page 166
mac-address-table aging-time <*time*>	*Configuring and Managing Security* (217104-A)

Table 145 CLI command list (Continued)

Command	See:
`mac-security [disable|enable] [filtering {enable|disable}] [intrusion-detect {enable|disable|forever}] [intrusion-timer <1-65535>] [learning-ports <portlist>] [learning {enable|disable}] [snmp-lock {enable|disable}] [snmp-trap {enable|disable}]`	*Configuring and Managing Security* (217104-A)
`mac-security auto-learning <portlist> [enable | disable] [max-addrs <1-25>]`	*Configuring and Managing Security* (217104-A)
`mac-security auto-learning aging time <0-65535>`	*Configuring and Managing Security* (217104-A)
`mac-security [port <portlist>] {disable|enable|learning}`	*Configuring and Managing Security* (217104-A)
`mac-security mac-address-table address <H.H.H.> {port <portlist>|security-list <1-32>}`	*Configuring and Managing Security* (217104-A)
`mac-security security-list <1-32>` `mac-security security-list <portlist>`	*Configuring and Managing Security* (217104-A)
`mac-security mac-da-filter`	*Configuring and Managing Security* (217104-A)
`mlt <id> [name <trunkname>] [enable|disable] [member <portlist>] [learning {disable | fast | normal} ]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`mlt spanning-tree <1-6> [stp <stp id>, ALL>] [learning {disable|normal|fast}]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`name [port <portlist>] <LINE>`	page 415
`no adac [enable] [traps enable] [voice-vlan] [uplink-port] [call-server-port]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`no adac port <port-list> enable`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`no auto-negotiation-advertisements [port <portlist>]`	page 431
`no auto-pvid`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`no autotopology`	page 409

Table 145 CLI command list (Continued)

Command	See:
no cops server	*Configuring Quality of Service, and IP Filtering* (217106-A)
no eapol guest-vlan <*portlist*>	*Configuring and Managing Security* (217104-A)
no eapol multihost enable	*Configuring and Managing Security* (217104-A)
no flowcontrol [port <*portlist*>]	page 422
no ip address {stack|switch}	page 355
no ip address unit <*1-8*>	page 359
no ip bootp server	page 389
no ip default-gateway	page 357
no ipmgr {telnet|snmp|http}	*Configuring and Managing Security* (217104-A)
no ipmgr {source IP [<*1-50*>]}	*Configuring and Managing Security* (217104-A)
no lacp aggregation [port <portlist>] enable	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
no logging remote address	*System Monitoring Guide* (217107-A)
no logging remote level	*System Monitoring Guide* (217107-A)
no mac-security	*Configuring and Managing Security* (217104-A)
no mac-security mac-address-table {address <*H.H.H*>| port <*portlist*>|security-list <*1-32*>]	*Configuring and Managing Security* (217104-A)
no mac-security security-list <*1-32*>	*Configuring and Managing Security* (217104-A)
no mlt [<*id*>]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
no name [port <*portlist*>]	page 416
no password security	*Configuring and Managing Security* (217104-A)

Table 145 CLI command list (Continued)

Command	See:
`no port-mirroring`	*System Monitoring Guide* (217107-A)
`no radius-server`	*Configuring and Managing Security* (217104-A)
`no rate-limit [port <portlist>]`	page 426
`no remote logging enable`	*System Monitoring Guide* (217107-A)
`no rmon alarm [1...65535]`	*System Monitoring Guide* (217107-A)
`no rmon event [1...65535]`	*System Monitoring Guide* (217107-A)
`no rmon history [1...65535]`	*System Monitoring Guide* (217107-A)
`no rmon stats [1...65535]`	*System Monitoring Guide* (217107-A)
`no set logging`	*System Monitoring Guide* (217107-A)
`no shutdown [port <portlist>]`	page 414
`no snmp server [authentication-trap|community [ro|rw] contact|host [<host-ip> <community-string>] [location|name]`	*Configuring and Managing Security* (217104-A)
`no snmp trap link-status [port <portlist>]`	*Configuring and Managing Security* (217104-A)
`no sntp enable`	page 403
`no sntp server <primary|secondary>`	page 404
`no ssh [dsa-auth|dsa-key|pass-auth]`	*Configuring and Managing Security* (217104-A)
`no ssh secure`	*Configuring and Managing Security* (217104-A)
`no ssl`	*Configuring and Managing Security* (217104-A)
`no spanning-tree [port <portlist>] [stp <1-16>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`no spanning-tree vlan <vlan-id>` (used with PVST+)	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
no stack auto-unit-replacement enable	page 317
no telnet-access [source-ip [<*1-50*>]]	*Configuring and Managing Security* (217104-A)
no tftp-server	page 391
no vlacp enable	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
no vlacp macaddress	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
no vlan <*1-4094*> no vlan mac-address <*1-4094*> address <*H.H.H.*>	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
no web-server	*Configuring and Managing Security* (217104-A)
password aging-time day <aging-value>	*Configuring and Managing Security* (217104-A)
password security	*Configuring and Managing Security* (217104-A)
ping <*XXX.XXX.XXX.XXX*>	page 363
poe poe-dc-source-conf [unit <*1-8*>] {powersharing|rpsu|ups}	page 323
poe poe-dc-source-type [unit <*1-8*>] {RPS10|nes}>	page 322
poe poe-pd-detect-type [unit <*1-8*>] {802dot3af|802dot3af_and_legacy}	page 324
poe poe-limit [unit <*1-8*>] <*3-16*>	page 330
poe poe-power-pairs [unit <*1-8*>] {spare|signal}	page 325
poe poe-power-usage-threshold [unit <*1-8*>] <*1-99*>	page 326
poe poe-priority [port <*portlist*>] {low|high|critical}	page 329
poe poe-shutdown [port <*portlist*>]	page 328
poe poe-trap [unit <*1-8*>]	page 326

Table 145 CLI command list (Continued)

Command	See:
port-mirroring mode disable port-mirroring mode Xrx monitor-port <*portlist*> mirror-port X <*portlist*> port-mirroring mode XrxOrXtx monitor-port <*portlist*> mirror-port X <*portlist*> mirror-port-Y <*portlist*> port-mirroring mode XrxOrYtx monitor-port <*portlist*> mirror-port X <*portlist*> mirror-port-Y <*portlist*> port-mirroring mode XrxYtx monitor-port <*portlist*> mirror-port X <*portlist*> mirror-port-Y <*portlist*> port-mirroring mode XrxYtxOrYrxXtx monitor-port <*portlist*> mirror-port X <*portlist*> mirror-port-Y <*portlist*> port-mirroring mode Asrc monitor-port <*portlist*> mirror-MAC-A <*macaddr*> port-mirroring mode Adst monitor-port <*portlist*> mirror-MAC-A <*macaddr*> port-mirroring mode AsrcOrAdst monitor-port <*portlist*> mirror-MAC-A <*macaddr*> port-mirroring mode AsrcBdst monitor-port <*portlist*> mirror-MAC-A <*macaddr*> mirror-MAC-B <*macaddr*> port-mirroring mode AsrcBdstOrBsrcAdst monitor-port <*portlist*> mirror-MAC-A <*macaddr*> mirror-MAC-B <*macaddr*>	*System Monitoring Guide* (217107-A)
qos action <*actid*> name <*actname*> qos action <*actid*> drop-action {enable|disable} qos action <*actid*> update-dscsp <*dscp*> qos action <*actid*> update-1p {<*ieee1p*>|default|use-egress-map} qos action <*actid*> set-drop-prec {loss-sensitive|not-loss-sensitive|default|use-egress-map}	*Configuring Quality of Service, and IP Filtering* (217106-A)

Table 145 CLI command list (Continued)

Command	See:
qos egressmap	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos if-assign	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos if-assign-list	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos if-assign-list name <*tag*> {add|del} [portlist <*portlist*>]	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos if-assign name <*tag*> {add|del} [port <*portlist*>]	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos if-group	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos if-group name <*tag*> {create <*ifclass*>|delete}	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos ingressmap	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos ingressmap 1p <*ieee1p*> ds <*dscp*>	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos ip-filter <*fid*> {create src-ip <*src-ip-info*>} qos ip-filter <*fid*> {create dst-ip <*dst-ip-info*>} qos ip-filter <*fid*> {create ds-field <*dscp*>} qos ip-filter <*fid*> {create protocol <*protocoltype*>} qos ip-filter <*fid*> {create src-port <*port*>} qos ip-filter <*fid*> {create dst-port <*port*>} qos ip-filter <*fid*> {delete}	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos ip-filter-set <*fgid*> {create set <*setid*> [name <*setname*>] filter-id <*fid*> filter-prec <*prec*>} qos ip-filter-set <*fgid*> {delete}	*Configuring Quality of Service, and IP Filtering* (217106-A)

Table 145 CLI command list (Continued)

Command	See:
qos l2-filter <*fid*> {create ethertype <*etype*>} qos l2-filter <*fid*> {create vlan <*vidlist*>} qos l2-filter <*fid*> {create vlantag <*vtag*>} qos l2-filter <*fid*> {create priority<ieee1p-seq>} qos l2-filter <*fid*> {create dsfield <*dscp*>} qos l2-filter <*fid*> {create protocol <*protocoltype*>} qos l2-filter <*fid*> {create src-port <*min*> src-port <*max*>} qos l2-filter <*fid*> {create dst-port <*min*> dst-port <*max*>} qos l2-filter <*fid*> {delete}	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos l2-filter-set <*fgid*> {create set <*setid*> [name <*setname*>] filter-id <*fid*> filter-prec <*prec*>} qos l2-filter-set <*fgid*> {delete}	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos meter <*metid*> {create [name <*metname*>] committed-rate <*rate*> max-burst-rate <*burstrate*> [max-burst-duration <*burstdur*>] |delete}	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos policy	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos queue-set	*Configuring Quality of Service, and IP Filtering* (217106-A)
qos shaper	*Configuring Quality of Service, and IP Filtering* (217106-A)
qosagent class-restrictions	*Configuring Quality of Service, and IP Filtering* (217106-A)
qosagent packet-reordering	*Configuring Quality of Service, and IP Filtering* (217106-A)
qosagent police-statistics {enable|disable}	*Configuring Quality of Service, and IP Filtering* (217106-A)
qosagent reset-default	*Configuring Quality of Service, and IP Filtering* (217106-A)
qosagent server-control	*Configuring Quality of Service, and IP Filtering* (217106-A)

Table 145 CLI command list (Continued)

Command	See:
radius-server host <*address*> [secondary-host <*address*>] port <*num*> key <*string*> timeout <*1-60*>	*Configuring and Managing Security* (217104-A)
rate-limit [port <*portlist*>] {multicast <*pct*>|broadcast <*pct*>|both <*pct*>}	page 425
remote logging enable	*System Monitoring Guide* (217107-A)
renumber unit	page 361
rmon alarm <*1-65535*> <*WORD*> <*1-2147483647*> [absolute|delta] rising-threshold <*-2147483647-2147483648*> [<*1-65535*>] falling-threshold <*-2147483647-2147483648*> [<*1-65535*>] [owner <*LINE*>]	*System Monitoring Guide* (217107-A)
rmon event <*1-65535*> [log] [trap] [description <*LINE*>] [owner <*LINE*>]	*System Monitoring Guide* (217107-A)
rmon history <*1-65535*> <*LINE*> <*1-65535*> <*1-3600*> [owner <*LINE*>]	*System Monitoring Guide* (217107-A)
rmon stats <*1-65535*> <*LINE*> [owner <*LINE*>]	*System Monitoring Guide* (217107-A)
set logging [enable|disable] [level critical|serious|informational] [nv-level critical|serious|informational|none]	*System Monitoring Guide* (217107-A)
show adac	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
show adac interface <interface-type> <slot/port>	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
show arp-table command	page 394
show audit log [asccfg | serial | ssh | telnet]	*Configuring and Managing Security* (217104-A)
show auto-negotiation-advertisements [port <portlist>]	page 428
show auto-negotiation-capabilities [port <portlist>]	page 429
show autotopology settings	page 410

Table 145 CLI command list (Continued)

Command	See:
`show autotopology nmm-table`	page 411
`show config-network`	page 369
`show cops`	*Configuring Quality of Service, and IP Filtering* (217106-A)
`show cops retry`	*Configuring Quality of Service, and IP Filtering* (217106-A)
`show cops server`	*Configuring Quality of Service, and IP Filtering* (217106-A)
`show cops stats`	*Configuring Quality of Service, and IP Filtering* (217106-A)
`show eapol`	*Configuring and Managing Security* (217104-A)
`show interfaces [names] [<portlist>]`	page 395
`show interfaces gbic-info <portlist>`	page 178
`show ip [bootp] [default-gateway] [address [stack|switch]]`	page 357
`show ipmgr`	*Configuring and Managing Security* (217104-A)
`show lacp debug member [portlist]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show lacp port [<portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show lacp stats [port <portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show lacp system`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

`show logging [critical]`
`show logging [serious]`
`show logging [informational]`
	System Monitoring Guide (217107-A)

`show mac-address-table [aging-time]` `show mac-address-table [vid <1-4094>] [address <H.H.H.>]`	*Configuring and Managing Security* (217104-A)

Table 145 CLI command list (Continued)

Command	See:
`show mac-security {config|mac-address-table [addr <macaddr>]|port|security-lists}`	*Configuring and Managing Security* (217104-A)
`show mac-security mac-da-filter`	*Configuring and Managing Security* (217104-A)
`show mlt [utilization <1-6>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show password aging-time day`	*Configuring and Managing Security* (217104-A)
`show poe-main-status [unit <1-8>]`	page 331
`show poe-port-status [ports <portlist>]`	page 333
`show poe-power-measurement [ports <portlist>]`	page 334
`show port-mirroring`	*System Monitoring Guide* (217107-A)
`show port-statistics [port <portlist>]`	*System Monitoring Guide* (217107-A)

`show qos if-assign-list`
`show qos interface-assignments`
`show qos interface-groups`
`show qos egressmap`
`show qos ingressmap`
`show qos ip-filters`
`show qos ip-filter-sets`
`show qos l2-filters`
`show qos l2-filter-sets`
`show qos actions`
`show qos meters`
`show qos shapers`
`show qos policies`
`show qos queue-sets`
`show qos queue-set-assignments`
`show qos agent`
`show qos statistics`
	Configuring Quality of Service, and IP Filtering (217106-A)

`show radius-server`	*Configuring and Managing Security* (217104-A)

Table 145 CLI command list (Continued)

Command	See:
`show rate-limit`	page 424
`show rmon alarm`	*System Monitoring Guide* (217107-A)
`show rmon event`	*System Monitoring Guide* (217107-A)
`show rmon history`	*System Monitoring Guide* (217107-A)
`show rmon stats`	*System Monitoring Guide* (217107-A)
`show running-config`	page 371
`show sntp`	page 401
`show spanning-tree {stp <1-16>] {config|port}`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree rstp info`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree rstp statistics`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree rstp status`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree rstp port info`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree rstp port statistics`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree rstp port status`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree mstp info`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree mstp region`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
`show spanning-tree mstp statist`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree mstp statu`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree mstp port info [<portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree mstp port statistics [<portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree mstp msti info <1 - 15>`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree mstp msti statistics <1-15>`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree mstp msti port info <1-15> [<portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree mstp msti port statistics <1-15> [<portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree config vlan` *<vlan-id>* `(used with PVST+)`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree op-mode`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show spanning-tree port vlan` *<vlan-id>* [*<port-list>*] `(used with PVST+)`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show ssh global`	*Configuring and Managing Security* (217104-A)
`show ssh session`	*Configuring and Managing Security* (217104-A)
`show ssh download-auth-key`	*Configuring and Managing Security* (217104-A)

Table 145 CLI command list (Continued)

Command	See:
`show ssl`	*Configuring and Managing Security* (217104-A)
`show ssl certificate`	*Configuring and Managing Security* (217104-A)
`show stack auto-unit-replacement`	page 316
`show-stack-info`	page 175
`show stack-oper-mode`	page 307
`show sys-info`	page 173
`show system verbose`	page 176
`show tech`	page 178
`show telnet-access`	*Configuring and Managing Security* (217104-A)
`show terminal`	page 381
`show tftp-server`	page 390
`show vlacp`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show vlacp interface <slot/port>`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show vlan igmp <1-4094> | unknown-mcast-no-flood`	*Configuring IP Multicast Routing Protocols* (217459-A)
`show vlan interface info [<portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show vlan interface vids [<portlist>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show vlan mac-address <1-4094> [<H.H.H.>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`show vlan multicast membership <1-4094>`	*Configuring IP Multicast Routing Protocols* (217459-A)
`shutdown`	page 168
`shutdown [port <portlist>]`	page 414

Table 145 CLI command list (Continued)

Command	See:
snmp trap link-status [port <*portlist*>]	*Configuring and Managing Security* (217104-A)
snmp-server {{enable|disable}|authentication-trap|community <community-string> [ro|rw] contact <*text*>|host <*host-ip*> <*community-string*>| location <*text*> | name <*text*>}	*Configuring and Managing Security* (217104-A)
snmp trap link-status [port <*portlist*>]	*Configuring and Managing Security* (217104-A)
sntp enable	page 402
sntp server primary address <A.B.C.D>	page 403
sntp server secondary address <A.B.C.D>	page 404
sntp sync-interval <0-168>	page 405
sntp sync-now	page 405
spanning-tree [stp <*1-16*>] [forward-time <*4-30*>] [hello-time <*1-10*>] [max-age <*6-40*>] [priority <*0000|1000|2000|...|F000*>] [tagged-bpdu {enable|disable}] [tagged-bpdu-vid <*1-4094*>] [multicast-address <*H.H.H.*>]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning- tree mstp [max-hop <600 - 4000>] [max-instance <1 - 65>] [forward-time <4 - 30>] [hello-time <1 - 10>] * not available in software [max-age <6 - 40>] [pathcost-type { bits16 | bits32 }] [priority { 0000 | 10000 | 20000 | … | F0000 }] [tx-holdcount <1 - 10>] [version { stp-compatible | rstp| mstp }]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
spanning- tree mstp [port <portlist>] [cost <1 - 200000000>] [edge-port { false | true }] [hello-time <1 - 10>] [learning { disable | enable }] [p2p { auto | force-false | force-true }] [priority { 00 | 10 | … | F0 }] [protocol-migration { false | true }]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning- tree mstp region [config-id-sel <0 - 255>] [region-name <1 - 32 chars>] [region-version <0 - 65535>]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning- tree mstp msti<1-15>[forward-time <4 - 30>] * not available in software [hello-time <1 - 10>] * not available in software [max-hop <600 - 4000>] * not available in software [priority { 0000 | 1000 | … | F000 }] [add-vlan <vid>] [remove-vlan <vid>]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning- tree mstp msti <1-15> [port <portlist>] [cost <1 - 200000000>] [learning { disable | enable }] [priority { 00 | 10 | … | F0 }]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning-tree op-mode *<pvst | stpg | rstp | mstp>*	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning-tree [port <portlist>] [stp <*1-16*>] [learning {disable|normal|fast}] [cost <*1-65535*>] [priority <*00|10|20|...|F0*>]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning-tree [stp <*1-16*>] [forward-time <*4-30*>] [hello-time <*1-10*>] [max-age <*6-40*>] [priority <*0-65535*>] [tagged-bpdu {enable|disable}] [tagged-bpdu-vid <*1-4094*>]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
spanning-tree [port <*portlist*>] [stp <*1-16*>] [learning {disable|normal|fast}] [cost <*1-65535*>] [priority <*0-255*>]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning- tree rstp [forward-time <4 - 30>] [hello-time <1 - 10>] [max-age <6 - 40>] [pathcost-type { bits16 | bits32 }] [priority { 0000 | 10000 | 20000 | … | F0000 }] [tx-holdcount <1 - 10>] [version { stp-compatible | rstp }]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning- tree rstp [port <portlist>] [cost <1 - 200000000>] [edge-port { false | true }] [learning { disable | enable }] [p2p { auto | force-false | force-true }] [priority { 00 | 10 | … | F0 }] [protocol-migration { false | true }]	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning-tree [stp <*1-16*>] remove-vlan <*1-4094*>	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning-tree stp <*2-16*> create	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning-tree stp <*2-16*> delete	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning-tree stp <*2-16*> disable	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
spanning-tree stp <*2-16*> enable	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
`spanning-tree vlan <vlan-id>` [enable] [forward-time <*4-30secs*>] [hello-time <*1-10secs*>] [max-age <*6-40secs*>] [priority <*value*>] `(used with PVST+)`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`spanning-tree vlan` *<vlan-id>* [port *<port-list>*] [cost *<cost>*] [learning *<disable / normal / fast>*] [priority *<value>*] `(used with PVST+)`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`speed [port <portlist>] {10|100|1000|auto}`	page 417
`ssh`	*Configuring and Managing Security* (217104-A)
`ssh download-auth-key [address <XXX.XXX.XXX.XXX>] [key-name <file>]`	*Configuring and Managing Security* (217104-A)
`ssh dsa-auth`	*Configuring and Managing Security* (217104-A)
`ssh dsa-key [<512-1024>]`	*Configuring and Managing Security* (217104-A)
`ssh max-sessions <0-2>`	*Configuring and Managing Security* (217104-A)
`ssh pass-auth`	*Configuring and Managing Security* (217104-A)
`ssh port <1-65535>`	*Configuring and Managing Security* (217104-A)
`ssh secure`	*Configuring and Managing Security* (217104-A)
`ssh timeout <1-120>`	*Configuring and Managing Security* (217104-A)
`ssl`	*Configuring and Managing Security* (217104-A)
`ssl certificate`	*Configuring and Managing Security* (217104-A)
`ssl reset`	*Configuring and Managing Security* (217104-A)
`stack auto-unit-replacement enable`	page 316
`stack bootp-mac-addr-type {base-unit|stack}`	page 388
`stack replace unit <1-8>`	page 307

Table 145 CLI command list (Continued)

Command	See:
`telnet-access [enable|disable] [login-timeout <1-10>] [retry <1-100>] [inactive-timeout <0-60>] [logging {none|access|failures|all}] [source-ip <1-50> <XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]]`	*Configuring and Managing Security* (217104-A)
`terminal {2400|4800|9600|19200|38400} | length <1-132> | width <1-132>`	page 382
`tftp-server <XXX.XXX.XXX.XXX>`	page 390
`vlacp enable`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`vlacp macaddress <macaddress>`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`vlacp <port-type> <slot/port> [enable | disable] [timeout <long/short>] [fast-periodic-time <integer>] [slow-periodic-time <integer>] [timeout-scale <integer> ] [funcmac-addr <mac>] [ethertype <integer>]`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
vlan create <*1-4094*> type macsa vlan create <*1-4094*> type port vlan create <*1-4094*> type protocol-ApltkEther2Snap vlan create <*1-4094*> type protocol-decEther2 vlan create <*1-4094*> type protocol-decOtherEther2 vlan create <*1-4094*> type protocol-ipEther2 vlan create <*1-4094*> type protocol-ipv6Ether2 vlan create <*1-4094*> type protocol-ipx802.2 vlan create <*1-4094*> type protocol-ipx802.3 vlan create <*1-4094*> type protocol-ipxEther2 vlan create <*1-4094*> type protocol-ipxSnap vlan create <*1-4094*> type protocol-Netbios vlan create <*1-4094*> type protocol-RarpEther2 vlan create <*1-4094*> type protocol-sna802.2 vlan create <*1-4094*> type protocol-snaEther2 vlan create <*1-4094*> type protocol-Userdef <4096-65534> vlan create <*1-4094*> type protocol-vinesEther2 vlan create <*1-4094*> type protocol-xnsEther2	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
vlan create <*1-4094*> name <*line*> type macsa vlan create <*1-4094*> name <*line*> type port vlan create <*1-4094*> name <*line*> type protocol-ApltkEther2Snap vlan create <*1-4094*> name <*line*> type protocol-decEther2 vlan create <*1-4094*> name <*line*> type protocol-decOtherEther2 vlan create <*1-4094*> name <*line*> type protocol-ipEther2 vlan create <*1-4094*> name <*line*> type protocol-ipv6Ether2 vlan create <*1-4094*> name <*line*> type protocol-ipx802.2 vlan create <*1-4094*> name <*line*> type protocol-ipx802.3 vlan create <*1-4094*> name <*line*> type protocol-ipxEther2 vlan create <*1-4094*> name <*line*> type protocol-ipxSnap vlan create <*1-4094*> name <*line*> type protocol-Netbios vlan create <*1-4094*> name <*line*> type protocol-RarpEther2 vlan create <*1-4094*> name <*line*> type protocol-sna802.2 vlan create <*1-4094*> name <*line*> type protocol-snaEther2 vlan create <*1-4094*> name <*line*> type protocol-Userdef <*1-4094*> vlan create <*1-4094*> name <*line*> type protocol-vinesEther2 vlan create <*1-4094*> name <*line*> type protocol-xnsEther2	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
vlan create <*1-4094*> type macsa learning IVL vlan create <*1-4094*> type port learning IVL vlan create <*1-4094*> type protocol-ApltkEther2Snap learning IVL vlan create <*1-4094*> type protocol-decEther2 learning IVL vlan create <*1-4094*> type protocol-decOtherEther2 learning IVL vlan create <*1-4094*> type protocol-ipEther2 learning IVL vlan create <*1-4094*> type protocol-ipv6Ether2 learning IVL vlan create <*1-4094*> type protocol-ipx802.2 learning IVL vlan create <*1-4094*> type protocol-ipx802.3 learning IVL vlan create <*1-4094*> type protocol-ipxEther2 learning IVL vlan create <*1-4094*> type protocol-ipxSnap learning IVL vlan create <*1-4094*> type protocol-Netbios learning IVL vlan create <*1-4094*> type protocol-RarpEther2 learning IVL vlan create <*1-4094*> type protocol-sna802.2 learning IVL vlan create <*1-4094*> type protocol-snaEther2 learning IVL vlan create <*1-4094*> type protocol-Userdef <*4096-65534*> learning IVL vlan create <*1-4094*> type protocol-vinesEther2 learning IVL vlan create <*1-4094*> type protocol-xnsEther2 learning IVL	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
vlan create <*1-4094*> type macsa learning SVL vlan create <*1-4094*> type port learning SVL vlan create <*1-4094*> type protocol-ApltkEther2Snap learning SVL vlan create <*1-4094*> type protocol-decEther2 learning SVL vlan create <*1-4094*> type protocol-decOtherEther2 learning SVL vlan create <*1-4094*> type protocol-ipEther2 learning SVL vlan create <*1-4094*> type protocol-ipv6Ether2 learning SVL vlan create <*1-4094*> type protocol-ipx802.2 learning SVL vlan create <*1-4094*> type protocol-ipx802.3 learning SVL vlan create <*1-4094*> type protocol-ipxEther2 learning SVL vlan create <*1-4094*> type protocol-ipxSnap learning SVL vlan create <*1-4094*> type protocol-Netbios learning SVL vlan create <*1-4094*> type protocol-RarpEther2 learning SVL vlan create <*1-4094*> type protocol-sna802.2 learning SVL vlan create <*1-4094*> type protocol-snaEther2 learning SVL vlan create <*1-4094*> type protocol-Userdef <*4096-65534*> learning SVL vlan create <*1-4094*> type protocol-vinesEther2 learning SVL vlan create <*1-4094*> type protocol-xnsEther2 learning SVL	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:
vlan create <*1-4094*> name <*line*> type macsa learning IVL vlan create <*1-4094*> name <*line*> type port learning IVL vlan create <*1-4094*> name <*line*> type protocol-ApltkEther2Snap learning IVL vlan create <*1-4094*> name <*line*> type protocol-decEther2 learning IVL vlan create <*1-4094*> name <*line*> type protocol-decOtherEther2 learning IVL vlan create <*1-4094*> name <*line*> type protocol-ipEther2 learning IVL vlan create <*1-4094*> name <*line*> type protocol-ipv6Ether2 learning IVL vlan create <*1-4094*> name <*line*> type protocol-ipx802.2 learning IVL vlan create <*1-4094*> name <*line*> type protocol-ipx802.3 learning IVL vlan create <*1-4094*> name <*line*> type protocol-ipxEther2 learning IVL vlan create <*1-4094*> name <*line*> type protocol-ipxSnap learning IVL vlan create <1-4094> name <*line*> type protocol-Netbios learning IVL vlan create <*1-4094*> name <*line*> type protocol-RarpEther2 learning IVL vlan create <*1-4094*> name <*line*> type protocol-sna802.2 learning IVL vlan create <*1-4094*> name <*line*> type protocol-snaEther2 learning IVL vlan create <1-4094> name <*line*> type protocol-Userdef <4096-65534> learning IVL vlan create <*1-4094*> name <*line*> type protocol-vinesEther2 learning IVL vlan create <*1-4094*> name <*line*> type protocol-xnsEther2 learning IVL	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:

`vlan create <1-4094> name <line> type macsa learning SVL`
`vlan create <1-4094> name <line> type port learning SVL`
`vlan create <1-4094> name <line> type protocol-ApltkEther2Snap learning SVL`
`vlan create <1-4094> name <line> type protocol-decEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-decOtherEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipv6Ether2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipx802.2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipx802.3 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipxEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-ipxSnap learning SVL`
`vlan create <1-4094> name <line> type protocol-Netbios learning SVL`
`vlan create <1-4094> name <line> type protocol-RarpEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-sna802.2 learning SVL`
`vlan create <1-4094> name <line> type protocol-snaEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-Userdef <1-4094> learning SVL`
`vlan create <1-4094> name <line> type protocol-vinesEther2 learning SVL`
`vlan create <1-4094> name <line> type protocol-xnsEther2 learning SVL`
	Configuring VLANs, Spanning Tree, and MultiLink Trunking (217460-A)

`vlan delete <1-4094>`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

Table 145 CLI command list (Continued)

Command	See:

`vlan igmp <1-4094> [snooping {enable|disable}] [proxy {enable|disable}]`
`[robust-value <value>] [query-interval <time>] [v1-members <portlist>]`
`[v2-members <portlist>] [unknown-mcast-no-flood {enable|disable }]`
	Configuring IP Multicast Routing Protocols (217459-A)

`vlan mac-address <1-4094> address <H.H.H.>`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

`vlan members <1-4094> <portlist>`
`vlan members add <1-4094> <portlist>`
`vlan members remove <1-4094> <portlist>`
	Configuring VLANs, Spanning Tree, and MultiLink Trunking (217460-A)

`vlan mgmt <1-4094>`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
`vlan name <1-4094> <line>`	*Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)

`vlan ports [<portlist>] [tagging {enable|disable}]`
`[pvid <1-4094>] [filter-tagged-frame {enable|disable}]`
`[filter-untagged-frame {enable|disable}]`
`[filter-unregistered-frames {enable|disable}]`
`[priority <0-7>] [name <line>]`
	Configuring VLANs, Spanning Tree, and MultiLink Trunking (217460-A)

`web-server {enable|disable}`	*Configuring and Managing Security* (217104-A)

Appendix C
Technical specifications

This appendix provides technical specifications for the Ethernet Switch 460-24T-PWR, the Ethernet Switch 470-24T, and the Ethernet Switch 470-48T.

Environmental

Table 146 lists environmental specifications.

Table 146 Environmental specifications

Parameter	Operating specification	Storage specification
Temperature	0° to 40°C (32° to 104°F)	-25° to 70°C (-13° to 158°F)
Humidity	85% maximum relative humidity, noncondensing	95% maximum relative humidity, noncondensing
Altitude	3024 m (10,000 ft)	3024 m (10,000 ft)

Electrical

Table 147 lists power electrical parameters for the Ethernet Switch 460-24T-PWR, Ethernet Switch 470-24T, and Ethernet Switch 470-48T.

Table 147 Electrical parameters

Parameter	Ethernet Switch 460-24T-PWR	Ethernet Switch 470-24T and Ethernet Switch 470-48T
Input Voltage	100 to 240 VAC @ 47 to 63 Hz	100 to 240 VAC @ 47 to 63 Hz
Input Power Consumption	400 W maximum	90 W maximum
Input Volt Amperes Rating	440 VA maximum	2000 VA maximum

Table 147 Electrical parameters (Continued)

Parameter	Ethernet Switch 460-24T-PWR	Ethernet Switch 470-24T and Ethernet Switch 470-48T
Input current	4.5 A @ 100 VAC 2.5 A @ 240 VAC	1.5 A @ 100 VAC 0.75 A @ 240 VAC
Maximum thermal output	500 BTU/hr	324 BTU/hr

Power specifications

AC power specifications

	Ethernet Switch 460-24T-PWR	Ethernet Switch 470-24T and Ethernet Switch 470-48T
Input current:	4.5 to 2.25 A	1.5 to 0.75 A
Input voltage (rms):	100 to 240 VAC at 47 to 63 Hz	100 to 240 VAC at 47 to 63 Hz
Input power consumption:	400 W	90 W
Thermal rating:	500 BTU/hr maximum	324 BTU/hr maximum

DC power specifications (applies to Ethernet Switch 460-24T-PWR only)

The DC power specifications vary depending on configuration and if you are interoperating with an optional external power source (Ethernet Switch Power Supply Unit 10 or the NES unit).

Internal power source (no PoE power):	335 BTU/hr maximum
Internal power source (200W PoE power):	500 BTU/hr maximum
External power source (200W PoE power):	430 BTU/hr maximum
Internal and external power source (370W PoE power):	650 BTU/hr maximum

Ethernet Switch Power Supply Unit 10 (applies to Ethernet Switch 460-24T-PWR only)

Input current:	4.2 A maximum
Input voltage:	-48 VDC

NES unit (applies to Ethernet Switch 460-24T-PWR only)

Input current:	8 A maximum
Input voltage:	-54 VDC

Physical dimensions

Table 148 lists physical dimensions.

Table 148 Physical dimensions

Parameter	Ethernet Switch 460-24T-PWR	Ethernet Switch 470-24T Ethernet Switch 470-48T
Height	7.04 cm (2.77 in.)	4.32 cm (1.70 in.)
Width	43.82 cm (17.25 in.)	43.82 cm (17.25 in.)
Depth	38.35 cm (15.1 in)	35.31 cm (13.9 in)
Weight	5.8 kg (12.76 lb.)	6.7 kg (14.7 lb.)

Performance specifications

Table 149 lists performance specifications.

Table 149 Performance specifications

Parameter	Specifications
Frame Forward Rate (64-byte packets)	Up to 3.2 million packets per second (pps) maximum, learned unicast traffic
Port Forwarding/Filtering Performance (64-byte packets)	• For 10 Mb/s: 14,880 pps maximum • For 100 Mb/s: 148,810 pps maximum
Address Database Size	16,000 entries at line rate (32,000 entries without flooding)
Addressing	48-bit MAC address
Frame Length	64 to 1518 bytes (IEEE 802.1Q Untagged) 64 to 1522 bytes (IEEE 802.1Q Tagged)

Data rate

The data rate is 10 Mb/s Manchester encoded or 100 Mb/s 4B/5B encoded.

Interface options

The Ethernet Switch 460-24T-PWR has 10BASE-T/100BASE-TX switch ports with RJ-45 (8-pin modular) connectors for MDA-X interfaces.

The Ethernet Switch 470-24T and Ethernet Switch 470-48T have 10BASE-T/100BASE-TX switch ports with RJ-45 (8-pin modular) connectors for GBICs.

Refer to *Installing Media Dependent Adapters (MDAs)* and *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* for information on the interface connectors on available uplink modules.

Regulatory Certifications

The following certifications were completed to the latest Standard in effect at the time of release. Additional National Certifications may be applicable and are available through Nortel or their representative in specific countries.

Safety Regulatory Certifications

The safety regulatory certifications follow:

- IEC60950 International Safety; CB Report/Certificate
- All Member National Differences applied
- UL 60950 United States Safety Licensed
- CSA 22.2, No. 60950 Canada Safety Licensed
- EN 60950 German/European Union Safety Licensed
- NOM-019 Mexico Safety Licensed
- Electromagnetic Compliance Certifications:

Electromagnetic Compliance Certifications

The Ethernet Switch 460-24T-PWR, Ethernet Switch 470-24T, and Ethernet Switch 470-48T meet the following electromagnetic compliance certifications:

- CISPR22/CISPR24, Class A, International EMC Certification
- EN55022/EN55024, Class A, European Union EMC Certification
  Including additional testing of EN 61000-3-2 and EN 61000-3-3
- FCC CFR47, Part 15 Class A, United States EMC Certification
- ICES-003, Class A, Canada EMC Certification
- AS/NZ 3548, Class A, Australia/New Zealand EMC Certification
- VCCI, Class A, Japan EMC Certification

Declaration of Conformity

The Declaration of Conformity for the Ethernet Switch 460-24T-PWR, Ethernet Switch 470-24T, and Ethernet Switch 470-48T complies with ISO/IEC Guide 22 and EN45014. The declaration identifies the product models, the Nortel Networks name and address, and the specifications recognized by the European community.

As stated in the Declaration of Conformity, the Ethernet Switch 460-24T-PWR, Ethernet Switch 470-24T, and Ethernet Switch 470-48T comply with the provisions of Council Directives
89/336/EEC and 73/23/EEC.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W