Nortel Ethernet Routing Switch 8300

Upgrades — Software Release 4.1

Release: 4.1
Document Revision: 04.03

www.nortel.com

NN46200-400 318769-G Rev 03

Nortel Ethernet Routing Switch 8300
Release: 4.1
Publication: NN46200-400
Document status: Standard
Document release date: 30 June 2008

Printed in Canada, China, and the United States of America

ATTENTION

For information about the regulatory and safety precautions, read "Regulatory Messages and Safety Precautions" in this guide.

For information about the software license, read "Software license" in this guide.

Contents

Regulatory Information and Safety Precautions

Read the information in this section to learn about regulatory conformities and compliances.

International Regulatory Statements of Conformity

This is to certify that the Nortel 8300 Series chassis and components installed within the chassis 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 (8300 Series chassis and installed components) does 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 (8300 Series chassis) 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 8300 Series chassis and components installed within the chassis are shielded against the generation of radio interference in accordance with the application of Council Directive 2004/108/EC. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

CAUTION
This device is a Class A product. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users are required to take appropriate measures necessary to correct the interference at their own expense.

EN 55 024 Statement

This is to certify that the Nortel 8300 Series chassis is shielded against the susceptibility to radio interference in accordance with the application of Council Directive 2004/108/EC. Conformity is declared by the application of EN 55 024 (CISPR 24).

EN 300386 Statement

The Ethernet Routing Switch 8300 Series chassis complies with the requirements of EN 300386 V1.3.3 for emissions and for immunity for a Class A device intended for use in either Telecommunications centre or locations other than telecommunications centres given the performance criteria as specified by the manufacturer.

EC Declaration of Conformity

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

European Union and European Free Trade Association (EFTA) Notice

CE All products labeled with the CE marking comply with R&TTE Directive (1999/5/EEC) which includes the Electromagnetic Compliance (EMC) Directive (2004/108/EC) and the Low Voltage Directive (2006/95/EC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (ENs). The equivalent international standards are listed in parenthesis.

- EN 55022 (CISPR 22)–Electromagnetic Interference
- EN 55024 (IEC 61000-4-2, -3, -4, -5, -6, -8, -11)–Electromagnetic Immunity
- EN 61000-3-2 (IEC 610000-3-2)–Power Line Harmonics
- EN 61000-3-3 (IEC 610000-3-3)–Power Line Flicker

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。

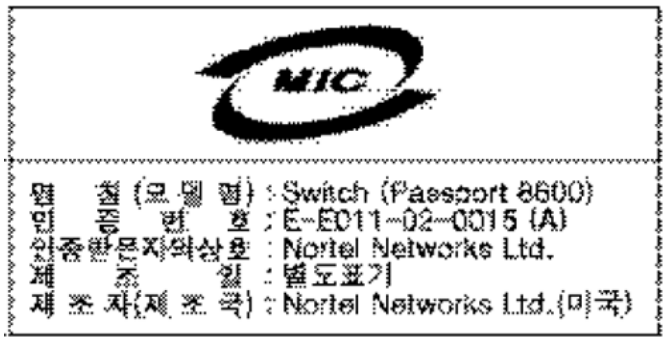
BSMI Statement for 8310, and 8306 Chassis (Taiwan only)

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 8310, and 8306 chassis (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.



National Safety Statements of Compliance

CE Marking Statement (Europe only)

EN 60 950 Statement

This is to certify that the Nortel 8300 Series chassis and components installed within the chassis 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. Some components installed within the 8300 Series chassis may use a nickel-metal hydride (NiMH) and/or lithium-ion battery. The NiMH and lithium-ion batteries are long-life batteries, and it is very possible that you will never need to replace them. However, should you need to replace them, refer to the individual component manual for directions on replacement and disposal of the battery.

NOM Statement 8310 and 8306 Chassis (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:	(8306 and 8310 Chassis only) 8301AC: 100 to 240 VAC 16A 47 to 60 Hz per power supply 8301AC: 200 to 240 VAC 12 A 47 to 60 Hz per power supply single supply, single supply + one redundant supply, two supplies, or two supplies + one redundant supply configurations 8302AC: 100 to 240 VAC 12A 47 to 60 Hz per power supply 8302AC: 200 to 240 VAC 10A 47 to 60 Hz per power supply single supply, single supply + one redundant supply, two supplies, or two supplies + one redundant supply configurations 8005DIDC: 40 to 75 VDC, 48.75 to 32.5 A single supply, single supply + one redundant supply, two supplies, or two supplies + one redundant supply configurations 8005DC: 48 to 60 VDC, 42 to 34 A single supply, single supply + one redundant supply, two supplies, or two supplies + one redundant supply configurations

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:	(8306 and 8310 Chassis)
	8301AC:100 to 240 VAC 16A 47 to 60 Hz por fuente de poder
	8301AC: 200 to 240 VAC 12 A 47 to 60 Hz por fuente de poder una fuente, una fuente + configuraciones de una fuente redundante, dos fuentes o dos + configuraciones de una fuente redundante
	8302AC:100 to 240 VAC 12A 47 to 60 Hz por fuente de poder
	8302AC: 200 to 240 VAC 10 A 47 to 60 Hz por fuente de poder una fuente, una fuente + configuraciones de una fuente redundante, dos fuentes o dos + configuraciones de una fuente redundante
	8005DIDC: 40 to 75 VDC, 48.75 to 32.5 A una fuente, una fuente + configuraciones de una fuente redundante, dos fuentes o dos + configuraciones de una fuente redundante
	8005DC: 48 to 60 VDC, 42 to 34 A una fuente, una fuente + configuraciones de una fuente redundante, dos fuentes o dos + configuraciones de una fuente redundante

Denan Statement (Japan/Nippon only)

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

- 接続ケーブル、電源コード、ACアダプタなどの部品は、必ず製品に同梱されております添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となることがあります。
- 同梱されております付属の電源コードを他の機器には使用しないでください。上記注意事項を守らないと、死亡や大怪我など人身事故の原因となることがあります。

Safety Messages

This section describes the different precautionary notices used in this document. This section also contains precautionary notices that you must read for safe operation of the Nortel Ethernet Routing Switch 8300.

Notices

Notice paragraphs alert you about issues that require your attention. The following sections describe the types of notices. For a list of safety messages used in this guide and their translations, see "Translations of safety messages".

Attention Notice

ATTENTION
An attention notice provides important information regarding the installation and operation of Nortel products.

Caution ESD Notice

CAUTION
ESD
ESD notices provide information about how to avoid discharge of static electricity and subsequent damage to Nortel products.

CAUTION
ESD (décharge électrostatique)
La mention ESD fournit des informations sur les moyens de prévenir une décharge électrostatique et d'éviter d'endommager les produits Nortel.

CAUTION
ACHTUNG ESD
ESD-Hinweise bieten Information dazu, wie man die Entladung von statischer Elektrizität und Folgeschäden an Nortel-Produkten verhindert.

CAUTION
PRECAUCIÓN ESD (Descarga electrostática)
El aviso de ESD brinda información acerca de cómo evitar una descarga de electricidad estática y el daño posterior a los productos Nortel.

CAUTION
CUIDADO ESD
Os avisos do ESD oferecem informações sobre como evitar descarga de eletricidade estática e os conseqüentes danos aos produtos da Nortel.

CAUTION
ATTENZIONE ESD
Le indicazioni ESD forniscono informazioni per evitare scariche di elettricità statica e i danni correlati per i prodotti Nortel.

Caution Notice

CAUTION
Caution notices provide information about how to avoid possible service disruption or damage to Nortel products.

CAUTION
ATTENTION
La mention Attention fournit des informations sur les moyens de prévenir une perturbation possible du service et d'éviter d'endommager les produits Nortel.

CAUTION
ACHTUNG
Achtungshinweise bieten Informationen dazu, wie man mögliche Dienstunterbrechungen oder Schäden an Nortel-Produkten verhindert.

CAUTION
PRECAUCIÓN
Los avisos de Precaución brindan información acerca de cómo evitar posibles interrupciones del servicio o el daño a los productos Nortel.

CAUTION
CUIDADO
Os avisos de cuidado oferecem informações sobre como evitar possíveis interrupções do serviço ou danos aos produtos da Nortel.

CAUTION
ATTENZIONE
Le indicazioni di attenzione forniscono informazioni per evitare possibili interruzioni del servizio o danni ai prodotti Nortel.

Warning Notice

WARNING
Warning notices provide information about how to avoid personal injury when working with Nortel products.

WARNING
AVERTISSEMENT
La mention Avertissement fournit des informations sur les moyens de prévenir les risques de blessure lors de la manipulation de produits Nortel.

WARNING
WARNUNG
Warnhinweise bieten Informationen dazu, wie man Personenschäden bei der Arbeit mit Nortel-Produkten verhindert.

WARNING
ADVERTENCIA
Los avisos de Advertencia brindan información acerca de cómo prevenir las lesiones a personas al trabajar con productos Nortel.

WARNING
AVISO
Os avisos oferecem informações sobre como evitar ferimentos ao trabalhar com os produtos da Nortel.

WARNING
AVVISO
Le indicazioni di avviso forniscono informazioni per evitare danni alle persone durante l'utilizzo dei prodotti Nortel.

Danger High Voltage Notice

DANGER
Danger—High Voltage notices provide information about how to avoid a situation or condition that can cause serious personal injury or death from high voltage or electric shock.

DANGER
La mention Danger—Tension élevée fournit des informations sur les moyens de prévenir une situation ou une condition qui pourrait entraîner un risque de blessure grave ou mortelle à la suite d'une tension élevée ou d'un choc électrique.

DANGER
GEFAHR
Hinweise mit Vorsicht – Hochspannung" bieten Informationen dazu, wie man Situationen oder Umstände verhindert, die zu schweren Personenschäden oder Tod durch Hochspannung oder Stromschlag führen können.

DANGER
PELIGRO
Los avisos de Peligro-Alto voltaje brindan información acerca de cómo evitar una situación o condición que cause graves lesiones a personas o la muerte, a causa de una electrocución o de una descarga de alto voltaje.

DANGER
PERIGO
Avisos de Perigo—Alta Tensão oferecem informações sobre como evitar uma situação ou condição que possa causar graves ferimentos ou morte devido a alta tensão ou choques elétricos.

DANGER
PERICOLO
Le indicazioni Pericolo—Alta tensione forniscono informazioni per evitare situazioni o condizioni che potrebbero causare gravi danni alle persone o il decesso a causa dell'alta tensione o di scosse elettriche.

Danger Notice

DANGER
Danger notices provide information about how to avoid a situation or condition that can cause serious personal injury or death.

DANGER
La mention Danger fournit des informations sur les moyens de prévenir une situation ou une condition qui pourrait entraîner un risque de blessure grave ou mortelle.

DANGER
GEFAHR
Gefahrenhinweise stellen Informationen darüber bereit, wie man Situationen oder Umständen verhindert, die zu schweren Personenschäden oder Tod führen können.

DANGER
PELIGRO
Los avisos de Peligro brindan información acerca de cómo evitar una situación o condición que pueda causar lesiones personales graves o la muerte.

DANGER
PERIGO
Avisos de perigo oferecem informações sobre como evitar uma situação ou condição que possa causar graves ferimentos ou morte.

DANGER
PERICOLO
Le indicazioni di pericolo forniscono informazioni per evitare situazioni o condizioni che potrebbero causare gravi danni alle persone o il decesso.

Software license

This section contains the Nortel Networks software license.

Nortel Networks Inc. software license agreement

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

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

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms

of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

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

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

1. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer

software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

2. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
3. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
6. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

New in this release

The following sections detail what's new in *Nortel Ethernet Routing Switch 8300 Upgrades, NN46200-400* for Release 4.1.

Features

See the following sections for information about feature changes:

Advanced and Premier licenses

For Release 4.1, both Advanced and Premier (new for this release) licenses are available. For information about licenses and upgrade, see "Feature licensing" (page 26).

Other changes

See the following sections for information about changes that are not feature-related.

Files required for upgrade

Information about the files required for upgrade is updated. For more information about the required files for upgrade, see "New software files" (page 27) .

8393SF/CPU memory upgrade

Information about upgrading the 8393SF/CPU to 256 MB is added to "8393SF/CPU memory upgrade" (page 33).

Hot swapping modules

All procedures about hot swapping modules and replacing a single CPU module in a single-CPU chassis are now included in this document. These procedures are removed from *Nortel Ethernet Routing Switch 8300 Installation — Modules, NN46200-305*. The module installation and removal procedures remain in NN46200-305.

Document changes

This document is modified to meet Nortel Customer Documentation Standards. For more information about these standards, see *Nortel Ethernet Routing Switch 8300 Documentation Roadmap, NN46200-101*.

Introduction

This guide provides instructions for upgrading the Ethernet Routing Switch 8300 to Release 4.1.

Navigation

Ethernet Routing Switch 8300 upgrade fundamentals

Use this section to aid you in upgrading the Ethernet Routing Switch 8300. Review the considerations and concepts in this section before you upgrade the Ethernet Routing Switch 8300.

Upgrade the chassis and module software to take advantage of all the latest Ethernet Routing Switch 8300 features and improvements. This document describes how to upgrade the software for the Ethernet Routing Switch 8300 SF/CPU.

For more information about how to use the command line interface (CLI), the Nortel Networks command line interface (NNCLI), and Device Manager, see *Nortel Ethernet Routing Switch 8300 User Interface Fundamentals, NN46200-103*.

Navigation

Feature licensing

For Release 4.1 and later, you require the Advanced Routing license to use the following features:

- Split MultiLink Trunking (SMLT)
- Routed Split MultiLink Trunking (RSMLT)
- Simple Loop Prevention Protocol (SLPP)
- Open Shortest Path First (OSPF)
- Equal Cost Multipath Protocol (ECMP)
- Virtual Router Redundancy Protocol (VRRP)
- Protocol Independent Multicast – Sparse Mode (PIM-SM)
- Virtual Link Aggregation Protocol (VLACP)
- Deep Pattern Match Filtering (DPF)

For Release 4.1 and later, you require a Premier Routing license to use Virtual Routing and Forwarding, Lite version (VRF-Lite). The Premier Routing license includes all Advanced License features.

With Software Release 4.1, route policies are part of the Basic license, and no longer part of the Advanced license.

For Release 4.1.0.0, VLACP and SLPP functions require an Advanced License. These features are both being moved under the Basic License. To find support for either or both of these features without requiring an Advanced License, users must move to 4.1.1.0 code. 4.1.0.0 code will only support these features via an Advanced License. Advanced Licenses will NOT be supplied to customers running 4.1.0.0 code to get support for these features.

If you plan to use Release 4.1 software (only available via a product maintenance contract or new software purchase), you can use any prior license to maintain all licensed features associated with the license level you purchased: Advanced or Premier. You will have access to any new features associated with that license level for the 4.1 Release. If you need features now offered within Release 4.1 that are not associated with your current license level, contact your local Nortel sales or Nortel partner sales teams.

Under some circumstances, you may require a new license; it depends on the version of the license file you are currently using. If you are running a pre-4.1 Release, you can use the show license command to check your version number. If the version number has a nonzero value, you will require a new Advanced or Premier license in order to properly function with Release 4.1. Note that the show license command in Release 4.1

no longer shows a version number field. If you have any issues running any licensed feature, before you contact Technical Support, first obtain an updated license. If this does not resolve the issue, then contact Technical Support.

For information about the licenses, including how to install them, see *Nortel Ethernet Routing Switch 8300 Administration, NN46200-604*.

After you obtain the required license file and load the file to flash, PCMCIA, or TFTP, specify the path of the software license file using boot configuration commands. You can change the default license file name (license.dat) to another file name for convenience (for example, thirdflr.dat). For the appropriate configuration commands, see "Configuring boot sources" (page 71) (CLI) and "Configuring boot sources" (page 83) (NNCLI).

When the system starts up, it looks for the license file specified in the boot.cfg file. If none is found, or the load fails, the system tries to load the default license file instead. The default (base) license file is /flash/license.dat.

The Ethernet Routing Switch 8300 cannot run more than one license file at any one time. You need only one valid license file for the chassis (which could be the default/base license file), regardless of the modules installed.

The Ethernet Routing Switch 8300 lets you define a primary, secondary, and tertiary path for the license file, similar to configuration and system image files. This protects against system flash failures. For example, the primary path may point to /flash, the secondary to /PCMCIA and the tertiary to a network path.

New software files

To upgrade the Ethernet Routing Switch 8300, depending on the modules present in the chassis and your operating system, you require some or all of the files listed in the following table.

From the Nortel Technical Support Web site, you can download each file separately, or you can download all files at once using the tar file.

Table 1
Software files

Module or file type	Description	File name	Size in bytes
Software tar file	Tar file of all software files	v4.1.0.tar.gz	
Ethernet Routing Switch images			

Table 1
Software files (cont'd.)

Module or file type	Description	File name	Size in bytes
Boot monitor image	Required SF/CPU firmware for the Ethernet Routing Switch 8300	p83b4100.img	1.0 MB
Runtime image	Required Ethernet Routing Switch 8300 image	p83a4100.img	8.5 MB
Runtime image for I/O modules	Runtime image required for I/O modules	p83r4100.dld	2.2 MB
Pre-boot monitor image	This pre-boot image file is only required to be loaded when upgrading from software release 2.0.0.1 and the pre-boot image version is below Release 3.7.	p83f4100.img	230 786
Software license	Needed for licensed features.	license.dat	variable
MIB (zip file)	Zip file containing MIBs. This compressed .mib file contains a file named "manifest", which contains a list of the MIBs supported by the switch, including the private MIBs.	p83a4100.mib.zip p83a4100.mib (private MIB)	542 KB 3.3 MB
MD5 checksum file	Required for integrity check; contains Message Digest 5 (MD5) checksums for all files	p83a4100.md5	745

Table 1
Software files (cont'd.)

Module or file type	Description	File name	Size in bytes
AES/SNMPv3 image	Encryption module required for SNMPv3 Advanced Encryption Standard (AES) and DES support	p83c4100.aes; only available from www.nortel.com/support	26 KB
3DES	Encryption module required for Secure Shell (SSH) Triple Data Encryption Standard (3DES) support	p83c4100.img; only available from www.nortel.com/support	51 MB
Device Manager images			
Solaris for SPARC image	Required for Device Manager for Solaris	jdm_6130_solaris_ sparc.sh	
Microsoft Windows image	Required for Device Manager for Windows	jdm_6130.exe	
Linux image	Required for Device Manager for Linux	jdm_6130_linux.sh	

For a complete list of files that you require to upgrade, their sizes, and any last-minute upgrade procedure changes, see the release notes or ReadMe files that accompany your software release. You can download these documents from the Nortel Technical Support Web site: www.nortel.com/support.

Upgrade requirements

Nortel does not support different software versions, for example, Releases 4.0.x and 3.1.0.x, on the Master and Secondary SF/CPU except during an upgrade process. The Master and Secondary SF/CPU must have the same amount of memory.

ATTENTION
V mode requires the 8394 SF/CPU. V mode is not programmable with an 8393 SF/CPU.

Upgrade prerequisites

CAUTION
Risk of service interruption
If the switch has only one SF/CPU, the upgrade procedure can cause interruption of normal switch operation.

Before you upgrade the Ethernet Routing Switch 8300:

- Read the entire upgrade procedure.
- Back up your runtime configuration and boot configuration for both Master and Secondary SF/CPUs. If the SavetoStandby feature is enabled, you only need to back up the files from the Master.

The configuration file generated with Software Release 4.1 contains options that are not backward-compatible with any pre-4.1 release. Loading a 4.1.0.0 configuration file on any earlier run-time image can generate errors and may cause the image to abort loading the configuration file.

ATTENTION
Before you upgrade, save a copy of the previous release's configuration files.

If the upgrade is unsuccessful, you may need to return to the previous software version. To return to the previous software version, you need the previously saved configuration files (boot.cfg and config.cfg). The upgrade process automatically converts, but does not save, the existing configuration files to a format compatible with the new software release. The new configuration files may not be backward compatible.

Before you run any **copy** command that uses Trivial File Transfer Protocol (TFTP), be aware that if a failure occurs (for example, a TFTP server is not available), the file that you specify in the copy command is deleted. To preserve the original file, rename the file or make a copy of the file on the Personal Computer Memory Card International Association (PCMCIA) card or flash memory before you begin the copy process.

When you install files on the onboard flash memory or PCMCIA card, verify capacity before you download the files.

CAUTION
Loss of access to /pcmcia/boot.cfg
If you use a PCMCIA card manufactured by SanDisk, the Ethernet Routing Switch 8300 might be unable to access the /pcmcia/boot.cfg file during bootup. This limitation is observed only during bootup.

Upgrades from Release 2.0.0.1

Upgrades from Software Release 2.0.0.1 to Release 4.1.0.0 require the pre-boot image file (p83f4000.img). If you have previously booted your 8393 SF/CPU with any p83fxxxx image, it is not necessary to repeat the process. The p83fxxxx image is the same for all releases.

To check if your system has the pre-boot image installed, use the **show sys sw** (CLI) or **show sys software** (NNCLI) command. If the pre-boot monitor software was previously upgraded (and does not require additional updates), then the switch displays the following: Pre-Boot Monitor Software: Rel 3.7

For instructions about installing the pre-boot image, see *Nortel Ethernet Routing Switch 8300 Upgrades — Software Release 4.0, NN46200-400; 318769-F Rev 01*.

Nocheck-sw-version and upgrade considerations

In the Ethernet Routing Switch 8300 software, a **config bootconfig flags nocheck-sw-version <true|false>** command exists. This command is for use for troubleshooting procedures by Nortel Technical Support. If this flag is changed, it can disable all image consistency checks in a dual-SF/CPU system. The default value is false, (that, is the check is enabled).

During redundant SF/CPU upgrade procedures, this flag must be configured to true for successful upgrade. This step is included in the dual SF/CPU upgrade procedures.

Hot swapping modules

When an upgrade includes I/O or SF/CPU module replacement, be aware that the removal of an active module or SF/CPU can cause an undesirable effect on the forwarding plane. After you remove an active SF/CPU module, packets currently traversing that switch fabric can be lost or corrupted. The same is true if you want to replace an active SF/CPU module and the chassis has dual SF/CPUs.

CAUTION

To avoid loss of data in a dual SF/CPU system, you should switchover the active (Master) CPU so that the Secondary SF/CPU becomes active. Then you can disable and remove the old Master.

If only one SF/CPU exists in the chassis, disabling the SF/CPU causes a loss of data. Additionally, the removal and replacement of the SF/CPU in a single-CPU system causes all I/O modules to be reset.

When you remove active devices, all I/O modules are susceptible to corruption, which can cause other I/O modules in the chassis to inadvertently stop receiving or forwarding traffic. If this occurs, a full system reboot is required to restore all services. To remove a module from an active system, you must disable the module before you remove it.

CAUTION
Risk of initialization failure
Do not hot swap or insert modules in an Ethernet Routing Switch 8300 while the switch is booting. If you do, the switch cannot recognize the module, which causes initialization failure.

Before you swap an SF/CPU module, make sure that you save all files you may need later.

When you hot swap the active SF/CPU module in an Ethernet Routing Switch 8300 with dual SF/CPU modules, wait until the new Master is stabilized before you insert the replacement SF/CPU, or any other modules. Wait until the new Master is stabilized before you insert a replacement SF/CPU, the original SF/CPU, or any I/O modules. The new Master is stable when the SF/CPU module displays a login prompt on the console screen. If no console connection is available, wait for at least 30 seconds or until the previous Secondary CPU becomes the new Master, whichever happens first. Then you can insert modules.

Flash memory and PCMCIA card file systems

The files that determine how an Ethernet Routing Switch 8300 boots and operates are in onboard flash memory. You can also download files from an ATA-compatible PCMCIA flash memory card. The flash file system stores executable images and the switch configuration. The p83a4100.img and p83b4100.img files can also be loaded from a TFTP or FTP server.

Each Ethernet Routing Switch 8300 has two onboard flash memory devices: the boot flash memory and the system flash memory.

For all SF/CPUs, the boot flash memory is 2 MB and contains the boot-monitor image file. The boot-monitor image is not directly user accessible. It is updated using a special boot-monitor update mechanism that writes to the area reserved for the boot image. The system flash memory primarily stores run-time images, configuration files, the system log, and other general storage.

The 8393SF/CPU with 256 MB and the 8394SF/CPU have two flash devices. Each flash is accessible; when you issue the **`dir`**, the output shows one device as "/flash" and the other device as "/flash1". You may not see /flash1 until you copy a file to /flash1.

Table 2
SF/CPU flash memory

	128 MB 8393SF/CPU	256 MB 8393SF/CPU	256 MB 8394SF/CPU
Boot flash (not user accessible)	2 MB	2 MB	2 MB
System flash /flash	32 MB	30 MB	30 MB
System flash /flash1	N/A	32 MB	32 MB

Before upgrading to the Ethernet Routing Switch 8300 Release 4.1, ensure you have adequate memory space available on the Ethernet Routing Switch 8300 flash. You need a minimum of 12 MB of free space. Otherwise, you are unable to copy all the relevant files. Use the **dir** command to check for memory availability.

You can use a PCMCIA card for general storage for all file types. The PCMCIA card provides a convenient way of moving files between switches because they are portable. You can use one PCMCIA card to update the configuration and image file on several switches. An Ethernet Routing Switch 8300 accepts an ATA-type, SanDisk-compatible flash memory card.

With the Ethernet Routing Switch 8300 file system, you can use the maximum number of characters for file names such as those used with Microsoft Windows 95, Windows 98, and Windows NT operating systems. The file naming convention for system flash files is /flash/<filename>. The file naming convention for PCMCIA is /pcmcia/<filename>.

To verify file names, you can use the **dir** command in the CLI or, in Device Manager, choose **Edit > File System** and select **Flash Files** or **PCMCIA Files**. You can also use the CLI and Device Manager commands or options to copy files.

The CLI is the default interface when you first power up the Ethernet Routing Switch 8300.

ATTENTION
The NNCLI has four command modes: User EXEC, Privileged EXEC, Global configuration, and Interface configuration, in order of increasing privilege.

8393SF/CPU memory upgrade

Software Release 4.1 requires 256 MB of memory to support some scaled environments. An upgrade from 128 MB to 256 MB of memory is available for the 8393SF/CPU. As well, a new 8393SF/CPU version with 256 MB is available; the 8394SF/CPU has 256 MB of DRAM.

If you have an 8393SF/CPU, you can use one of the three following options:

A chargeable field upgrade from 128 MB of DRAM to 256 MB of DRAM is available for the 8393SF/CPU. To upgrade a 128 MB 8393SF/CPU to 256 MB, contact Nortel Technical Logistics Support (1-800-4NORTEL) and request order number 316811-K. An advanced replacement RMA will be issued for the original 128 MB SF/CPU. The user will be sent an 8393SF/CPU with 256 MB of DRAM to install in their system; the original 128 MB SF/CPU will need to be returned by using the standard RMA process.

As mentioned, a new version of the 8393SF/CPU with 256 MB of DRAM is available. The part number for this module is DS1404118-E5.

You can directly upgrade an Ethernet Routing Switch 8300 system (at Software Release 4.0.x.x or 3x.x.x) that is configured with the 8393SF/CPU and 128 MB of memory to Software Release 4.1 without upgrading to 256 MB of memory if both the following conditions exist:

- the current memory utilization is 80% or lower.

  ATTENTION
  80% utilization is a conservative estimate. Systems as high as 90% utilization can successfully upgrade; however, such systems may not be able to scale (for example, FDB entries), or add additional features or functions. Therefore, Nortel highly recommends that you upgrade high-utilization systems to 256 MB. Because scaling is not always controllable, Nortel cannot guarantee the operation of such systems.

- you make no configuration or feature changes to the system as part of the upgrade to Software Release 4.1

To view current memory utilization, use the **show sys perf** command.

ATTENTION
For the 8393SF/CPU with 128 MB of DRAM, if the memory utilization of a system running 4.1.0.0 software exceeds 95%, a log message is generated as a warning. Under these conditions, Nortel highly recommends that you upgrade the memory to 256 MB to avoid any potentially negative system operations.

For instructions about replacing the SF/CPU module, see:

- “Replacing a SF/CPU module in a single CPU chassis” (page 73), CLI
- “Replacing both SF/CPU modules in a dual CPU chassis” (page 75), CLI
- “Replacing a SF/CPU module in a single CPU chassis” (page 85), NNCLI
- “Replacing both SF/CPU modules in a dual CPU chassis” (page 88), NNCLI

High Secure mode considerations

High Secure (hsecure) mode introduces a protection mechanism to filter certain IP addresses and introduces two restrictions for passwords: 10-character enforcement and password aging time.

When the switch boots in hsecure mode without a previously configured password, you can use a default password to log on. However, you are prompted to change the password. The new password must follow hsecure mode rules. After you enable hsecure and reboot the switch, any user with an invalid-length password is prompted to change their password.

Note the following information about hsecure mode operations:

- When you enable the hsecure flag, after the aging time expires you are asked to change your password. If you do not configure the aging parameter, the aging parameter defaults to 90 days. To change the aging time, use the **`config cli password aging <days>`** CLI command or the **`password aging-time <day>`** NNCLI command.
- For SNMP and FTP, access is denied when a password expires. You must change community strings to a new string made up of more than eight characters before you can access the system.
- You cannot enable the Web server at any time.
- You can now enable the SSH password-authentication feature along with hsecure.

Hsecure is disabled by default. After you enable hsecure, it is applied to all ports.

ATTENTION
Hsecure operations have changed for Release 4.1. For more information, see *Ethernet Routing Switch 8300 Release Notes, NN46200-402.*.

For more information about hsecure, see *Nortel Ethernet Routing Switch 8300 Security, NN46200-605*.

Network security

For additional security-related information, consult important security information for the Ethernet Routing Switch 8300:*Nortel Ethernet Routing Switch 8300 Configuration — Security using CLI and NNCLI, NN46200-503* and *Nortel Ethernet Routing Switch 8300 Configuration — Security using Device Manager, NN46200-508*.

MD5 information

By verifying the MD5 checksum, you can verify that files transferred properly (error-free) to the switch. This command is available from both the boot monitor or run-time CLI.

The **md5** command calculates the MD5 checksum for files on the switch flash memory or PCMCIA card and either shows the output on screen or stores the output in a file that you specify. An MD5 command option compares the calculated MD5 checksums with checksums present in a checksum file on flash memory or PCMCIA card, and shows the compared output on the screen.

The Ethernet Routing Switch 8300 software includes the MD5 file p83a4100.md5, which includes the MD5 checksums of all of the new files.

Transfer your image files to the switch and use the **md5** command to ensure the checksums of the images on the switch are the same as those in the checksum file.

For information about using the **md5** command, see “Verifying the MD5 checksums” (page 79) (CLI) and “Verifying the MD5 checksums” (page 91).

Ethernet Routing Switch 8300 upgrade using the CLI

Upgrade software to add new functionality to your Ethernet Routing Switch. Release 4.1 supports many advanced features, including SMLT, SLPP, PIM-SM, RSMLT, DPF, ECMP, and VLACP. Release 4.1 supports the premier feature Virtual Routing and Forwarding (VRF) Lite.

The upgrade places all routing configurations in VRF 0.

Prerequisites to Ethernet Routing Switch 8300 upgrade

CAUTION
Risk of service interruption
If the switch has only one SF/CPU, the upgrade procedure can cause interruption of normal switch operation.

ATTENTION
All upgrade procedures assume that files use the default names. Use caution in any procedure if the file names are nondefault. Ensure all parameters associated with file names take into consideration the use of nondefault values.

- Read the latest release notes. See *Ethernet Routing Switch 8300 Release Notes — Software Release 4.1, NN46200-401*.
- Read the section “Safety Message Translations” (page 95).
- Read the section “Ethernet Routing Switch 8300 upgrade fundamentals” (page 25).
- You must be able to access the new software from the site www.nortel.com/support. You need a valid user or site ID and password.
- If necessary, schedule a time for the switch to be nonoperational.

Ethernet Routing Switch 8300 upgrade time requirements

The following table lists tasks used to upgrade the Ethernet Routing Switch 8300 software and the estimated time to complete each task. Not all tasks are required for every Ethernet Routing Switch 8300 system; the required tasks depend on the hardware present in the chassis. Upgrade times may vary depending on the software access method, such as TFTP and FTP, number and size of files, and the number of boot sources you configure.

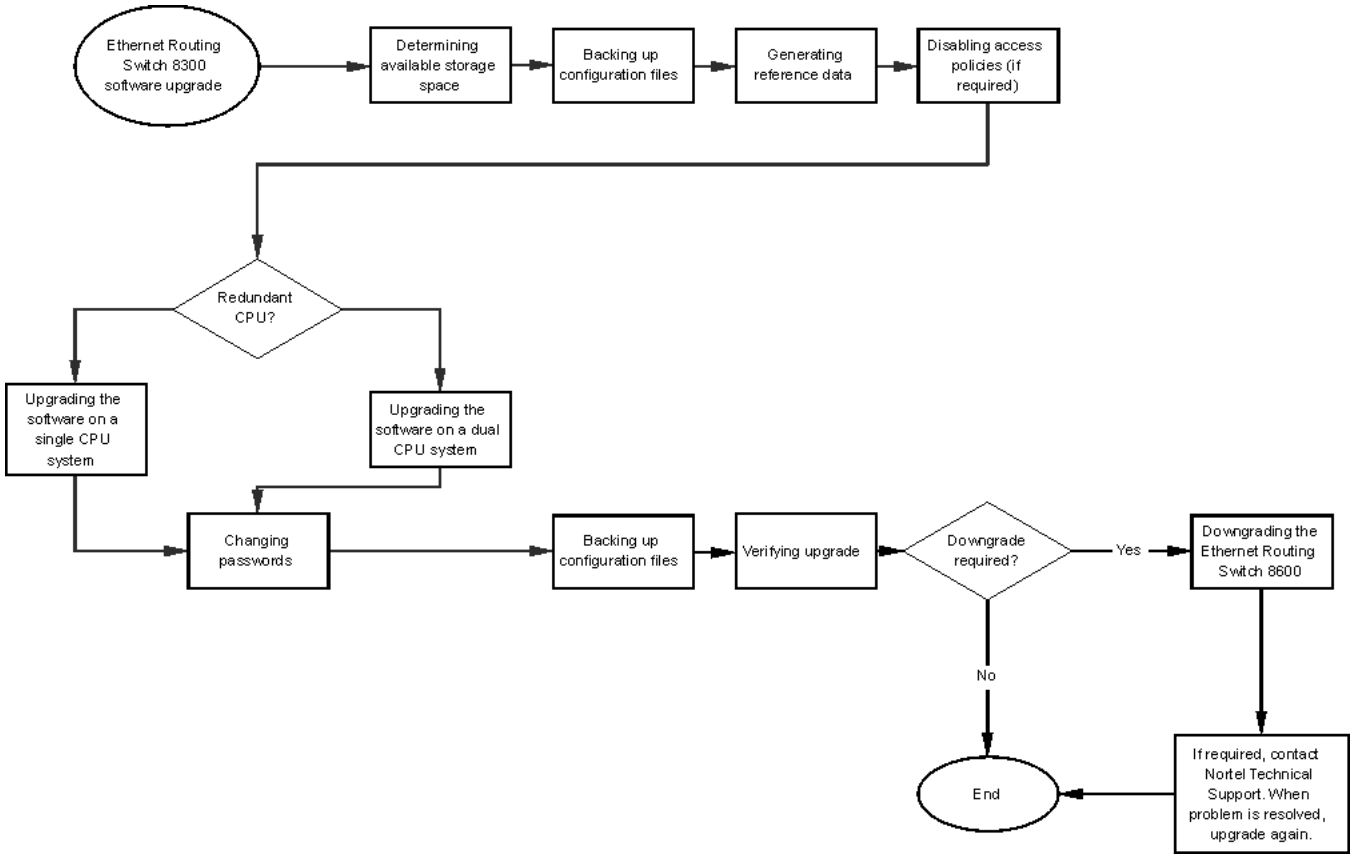
Table 3
Upgrade tasks and times

Task	Application	Estimated time required
Preupgrade tasks	Determining available storage space Backing up files Generating reference data	10–15 minutes
Upgrading Ethernet Routing Switch 8300 software on a single CPU system		30–45 minutes The required time depends on the access methods (CLI or TFTP), which files must be copied, and whether boot sources must be configured.
Upgrading Ethernet Routing Switch 8300 software on a dual CPU system		45–60 minutes The required time depends on the access methods (CLI or TFTP), which files must be copied, and whether boot sources must be configured.
Post-upgrade tasks	Changing passwords Backing up upgraded configuration files Verifying the upgrade	10–15 minutes
Downgrading the Ethernet Routing Switch 8300		Similar to upgrade time

Ethernet Routing Switch 8300 upgrade using the CLI tasks

This task flow shows you the sequence of tasks you perform to upgrade the Ethernet Routing Switch 8300. To link to any procedure, go to “Ethernet Routing Switch 8300 upgrade navigation” (page 39).

Figure 1
Ethernet Routing Switch 8300 upgrade using the CLI tasks



Ethernet Routing Switch 8300 upgrade navigation

Determining available storage space

Determine whether the switch has enough storage space to store the new software.

Procedure steps

Step	Action
1	Use the CLI to enter the following command to view the free space and files in flash memory: **`dir`** The bottom line shows the amount of free space in flash memory and on the PCMCIA card.
2	If you must remove files to make space, use the **`rm`** command: **`rm /flash/<filename>`** **`rm /pcmcia/<filename>`**

ATTENTION
Older load, boot, and configuration files may be required if the upgrade is unsuccessful. Make sure you back up these files to a safe place before you remove them.

--End--

Variable definitions

Use the information in the following table to help you perform this procedure.

Variable	Value
`<filename>`	Species the file by name.

Backing up configuration files

Before you upgrade your switch software, make copies of the configuration files. If an upgrade is unsuccessful, use backup configuration files to return the switch to its previous state.

Prerequisites

- If you are using FTP or TFTP, ensure the switch allows FTP or TFTP access. For more information about FTP and TFTP, see “Enabling FTP and TFTP” (page 71).
- For more details about copying files, see “Copying files” (page 70).

Procedure steps

Step	Action
1	Use the following CLI command to determine the configuration file names: **`show boot choice primary`**
2	Save the configuration files. Assuming the files use the default file names, enter: **`save config`** **`save bootconfig`** **`save config standby config.cfg`** **`save bootconfig standby boot.cfg`** If the SaveToStandby flag is true, you do not need to save the files to the Secondary SF/CPU.
3	Copy the files to a safe place: **`copy /flash/boot.cfg /pcmcia/boot_backup.cfg`** **`copy /flash/config.cfg /pcmcia/config_backup.cfg`** **OR** Copy to a TFTP server: **`copy /flash/config.cfg <tftpipaddress>:config_backup.cfg`** **`copy /flash/boot.cfg <tftpipaddress>:boot_backup.cfg`**
4	Ensure you also back up all other important files, including hidden files. See “Job aid: files present on SF/CPU modules” (page 75).
	--End--

Variable definitions

Use the information in the following table to help you perform this procedure.

Variable	Value
`<tftpipaddress>`	Specifies the IP address of the TFTP server.

Generating reference data

Use show commands to generate data to determine if the software upgrade is successful. After upgrade. the switch and network should operate as they did before the upgrade. Nortel recommends that you keep

track of important parameters and ensure they are unchanged after an upgrade. The following procedure gives examples of how to generate reference data. Choose the parameters that are most important to your network.

If these parameters remain unchanged before and after the upgrade, the upgrade is likely successful. Otherwise, you may need to downgrade to a previous release or perform troubleshooting procedures.

Procedure steps

Step	Action
1	Determine the number of routes in the routing table: **`show ip route info`**
2	Record the number of routes.
3	Determine Address Resolution Protocol (ARP) information: **`show ip arp info`**
4	Determine the total number of Internet Group Management Protocol (IGMP) groups: **`show ip igmp group`**
5	Determine the total number of multicast routes: **`show ip mroute interface`** **`show ip mroute route`**
6	Determine Open Shortest Path First (OSPF) parameters: **`show ip ospf show-all`**
7	Use the following command to view other IP show commands that you can use: **`show ip ?`**

--End--

Upgrading the software on a single SF/CPU system

Use this CLI procedure to upgrade the SF/CPU software on a nonredundant Ethernet Routing Switch 8300 SF/CPU. This procedure shows how to upgrade using the flash memory as the file storage location; you can use other storage locations.

CAUTION
Risk of bootconfig file corruption
Operating a system with different versions of the runtime image and boot monitor image can cause a corrupt bootconfig file. If the boot.cfg file is corrupt, replace it with a saved version or recreate the file.

Prerequisites

- Back up the switch configuration files. For more information about backing up and copying files, see “Backing up configuration files” (page 40) or “Copying files” (page 70).
- You must be able to access www.nortel.com/support.
- Determine if you need to disable access policies and do so if required. See “Disabling access policies” (page 78).

Procedure steps

Step	Action
1	Download Release 4.1 software. For more information about how to download software, see “Downloading the software” (page 65).
2	Use the management console port, Secure Shell (SSH), or a Telnet session to connect to the Ethernet Routing Switch 8300 CLI.
3	Copy the required software files to flash memory. If you use TFTP or FTP, use the IP address of the SF/CPU. To determine the required files, see Table 1 "Software files" (page 27). For instructions about copying files, see “Copying files” (page 70).
4	Confirm that the software files are successfully copied by using the **`dir`** command. Ensure the new files are listed.
5	Ensure the new files are error-free. See “Verifying the MD5 checksums” (page 79).
6	Configure the boot source to point to the new runtime image file (p83a4100.img) on flash: **`config bootconfig choice primary image-file /flash/p83a4100.img`**
7	To specify the location of the I/O module image, enter the following command

config bootconfig bootp image-name /flash/p83r4100.dld

8 Save the configuration files:

save bootconfig

9 To verify that the changed primary image file settings are in the boot.cfg file, enter the following command :

more boot.cfg

Confirm that the image location and name are correct.

10 To boot the Ethernet Routing Switch 8300 with the new boot-monitor image, enter the following command:

boot /flash/p83b4100.img -y

This step causes an interruption to user traffic.

The switch boots using the new image file. The system takes a longer time to come up than a normal reboot because the system must write the new boot monitor to flash memory.

If you interrupt the auto-boot process, you may have to issue the **boot** command again.

--End--

Upgrading the software on a dual SF/CPU system

Use this procedure to upgrade the SF/CPU software on a system that contains redundant SF/CPUs. This procedure shows how to upgrade using the flash memory as the file storage location; you can use other storage locations.

CAUTION
Risk of data loss
Nortel does not support different software versions, for example, Releases 3.0.3.0 and 4.0.0.0, on the Master and Secondary SF/CPUs except for during an upgrade process. Operating a system with different versions of the runtime image and boot monitor image can corrupt the bootconfig file. If the boot.cfg file is corrupt, replace it with a saved version, or recreate the file.

The Master and Secondary SF/CPU must have the same amount of memory.

CAUTION
Risk of failed upgrade
You must set the nocheck-sw-version flag to true before upgrade or the upgrade may fail. Steps are included in this procedure.

Prerequisites

- Back up the switch configuration files. See “Backing up configuration files” (page 40).
- You must be able to access www.nortel.com/support.
- If TFTP or FTP is required, ensure they are enabled. See “Enabling FTP and TFTP” (page 71).
- Determine if you need to disable access policies and do so if required. See “Disabling access policies” (page 78).

Procedure steps

Step	Action
1	Download the new software. For instructions, see “Downloading the software” (page 65).
2	Connect to the Master SF/CPU by using the management console port, SSH, or a Telnet session.
3	Copy the required software files to the Master flash memory. To determine the required files, see “New software files” (page 27). For instructions about copying files, see “Copying files” (page 70).
4	Ensure that the SaveToStandby flag is true: **`config bootconfig flags savetostandby true`** **`save bootconfig`** If this flag is true, whenever a configuration file is saved on the Master, it is also automatically saved on the Secondary.
5	If you plan to use licensed features, copy the license file to the flash. The path and file name default to /flash/license.dat until the Release 4.1 software is loaded. The license file must contain the correct chassis MAC address.
6	To confirm that the software files are successfully copied, use the **`dir`** command.
7	Ensure the new files are error-free. See “Verifying the MD5 checksums” (page 79).
8	Copy the runtime image file (and all other files copied to the Master SF/CPU flash, including the license file) to the Secondary SF/CPU.

For example:

copy /flash/p83a4100.img <IP address of standby CPU>:p83a4100.img

You can use the management IP address or the loopback address of the Secondary SF/CPU. The loopback addresses are 127.0.0.5 and 127.0.0.6, respectively, for slots 5 and 6.

OR

copy /flash/p83a4100.img peer:p83a4100.img

9 Ensure that the files are successfully copied to the Secondary SF/CPU:

peer telnet

dir

exit

10 On the Master SF/CPU, configure the boot configuration file to point to new runtime image file (p83a4100.img):

config bootconfig choice primary image-file /flash/p83a4100.img

11 To specify the I/O module image, enter the following command:

config bootconfig bootp image-name /flash/p83r4100.dld

Although you can specify the image name, Nortel recommends that you use the default option.

12 Configure the nocheck-sw-version flag to true:

config bootconfig flags nocheck-sw-version true

ATTENTION

If you do not set this flag to true, then a nocheck-sw-version flag mismatch may occur between the Master and Secondary SF/CPUs. In this case, you must change the upgrade procedure slightly: before the Secondary SF/CPU finishes the upgrade, boot the Master SF/CPU immediately. Do not wait for the Secondary to come back online.

To do this, if you use a remote connection, open two telnet sessions before rebooting the Secondary (one to each SF/CPU).

13 Save the configuration on both the Master and the Secondary SF/CPUs:

save bootconfig

14 To verify that the changed primary image file settings are in the boot.cfg file, enter the following command:

more boot.cfg

OR

show bootconfig choice

Verify that the primary image file is p83a4100.img.

15 To log on to the Secondary SF/CPU, enter the following command and log on:

peer telnet

16 To verify that the changed primary image file settings are in the Standby boot.cfg file, enter the following command:

more boot.cfg

OR

show bootconfig choice

Confirm that the image location and name are correct.

17 To boot the Secondary SF/CPU with the new boot monitor image, enter the following command:

boot /flash/p83b4100.img -y

While the Secondary reboots, the Telnet session established from the Master SF/CPU does not respond. Wait for the session to time out and return to the Master CPU prompt.

18 Ensure that the Secondary SF/CPU administrative status is up by entering the following command:

show sys info card

19 When the Secondary is up, upgrade the Master SF/CPU using the following command:

boot /flash/p83b4100.img -y

If you interrupt the auto-boot process, you may have to issue the **boot** command again.

If you are connecting remotely, the session stops responding. You will have to reconnect.

20 If desired, configure the nocheck-sw-version flag to false:

config bootconfig flags nocheck-sw-version false

21 Save the configuration:

save bootconfig

22 To ensure proper failover support of upgraded Secondary, do a final reset of both SF/CPUs when a maintenance cycle permits. Reset the Secondary SF/CPU first and, within two seconds, the Master CPU, using the following command:

reset -y

Perform this step by opening two telnet sessions or do a power reset to the chassis power supplies.

23 Logon to the Master SF/CPU and check that the correct software version is loaded.

--End--

Changing passwords

Change passwords after an upgrade to maintain the highest security levels. For more information about passwords, see *Nortel Ethernet Routing Switch 8300 Security, NN46200-605*.

ATTENTION
Passwords are stored in an encrypted format in a system file, rather than in the configuration file. Passwords are maintained across an upgrade, assuming that the hidden files are not modified. If required, change the passwords after upgrade to secure your system. All passwords are case-sensitive.

Procedure steps

Step	Action
1	To change a password, use one of the following commands as required: **config cli password ro <username> [<password>]** **config cli password rw <username> [<password>]** **config cli password rwa <username> [<password>]**
2	To view other options to configure, use the **config cli password ?** command.

--End--

Variable definitions

Use the information in the following table to help you perform this procedure.

Variable	Value
<username>	Specifies the user name.
<password>	Specifies the password for the user.

Backing up upgraded configuration files

After you complete the upgrade, save the new config.cfg and boot.cfg files to the PCMCIA card or another safe place. See “Backing up configuration files” (page 40).

Verifying the upgrade

Verify your upgrade to ensure proper switch operation.

Procedure steps

Step	Action
1	Repeat the procedure used in “Generating reference data” (page 41) and regenerate the same data. Compare the results. If you see substantial differences in this data, you may have to downgrade to the previous version and/or commence troubleshooting procedures. See “Downgrading the Ethernet Routing Switch 8300” (page 49).
2	To view bootconfig flags, enter the following command: **`config bootconfig flags info`** Ensure the flags are set correctly.
3	To view RADIUS settings, enter the following command: **`config radius info`** Ensure the settings are correct.
4	To check for alarms or unexpected errors, enter one the following commands: **`show log file tail`** **`show log file severity <value>`** where **`<value>`** can be one or more of INFO, ERROR, FATAL, or WARNING.
5	To ensure SNMP access policies are correctly configured, check to see if you can access the switch with Device Manager.

--End--

Downgrading the Ethernet Routing Switch 8300

Downgrade the Ethernet Routing Switch 8300 if an upgrade is not successful.

Prerequisites

- You need the previously saved configuration files (boot.cfg and config.cfg) for the release to which you intend to downgrade.

Procedure steps

Action

Install an older version of software.

Use the procedure found in the *Upgrading the Ethernet Routing Switch 8300* document that corresponds to the software release you intend to install. Ensure you use the previously saved configuration files for that release.

Ethernet Routing Switch 8300 upgrade using the NNCLI

Upgrade software to add new functionality to your Ethernet Routing Switch.

Upgrade times using the NNCLI are the same as for using the CLI. For more information about upgrade times, see “Ethernet Routing Switch 8300 upgrade time requirements” (page 38).

Prerequisites to Ethernet Routing Switch 8300 upgrade

CAUTION
Risk of service interruption
If you do not have a redundant SF/CPU system, the upgrade can cause an interruption to normal switch operation.

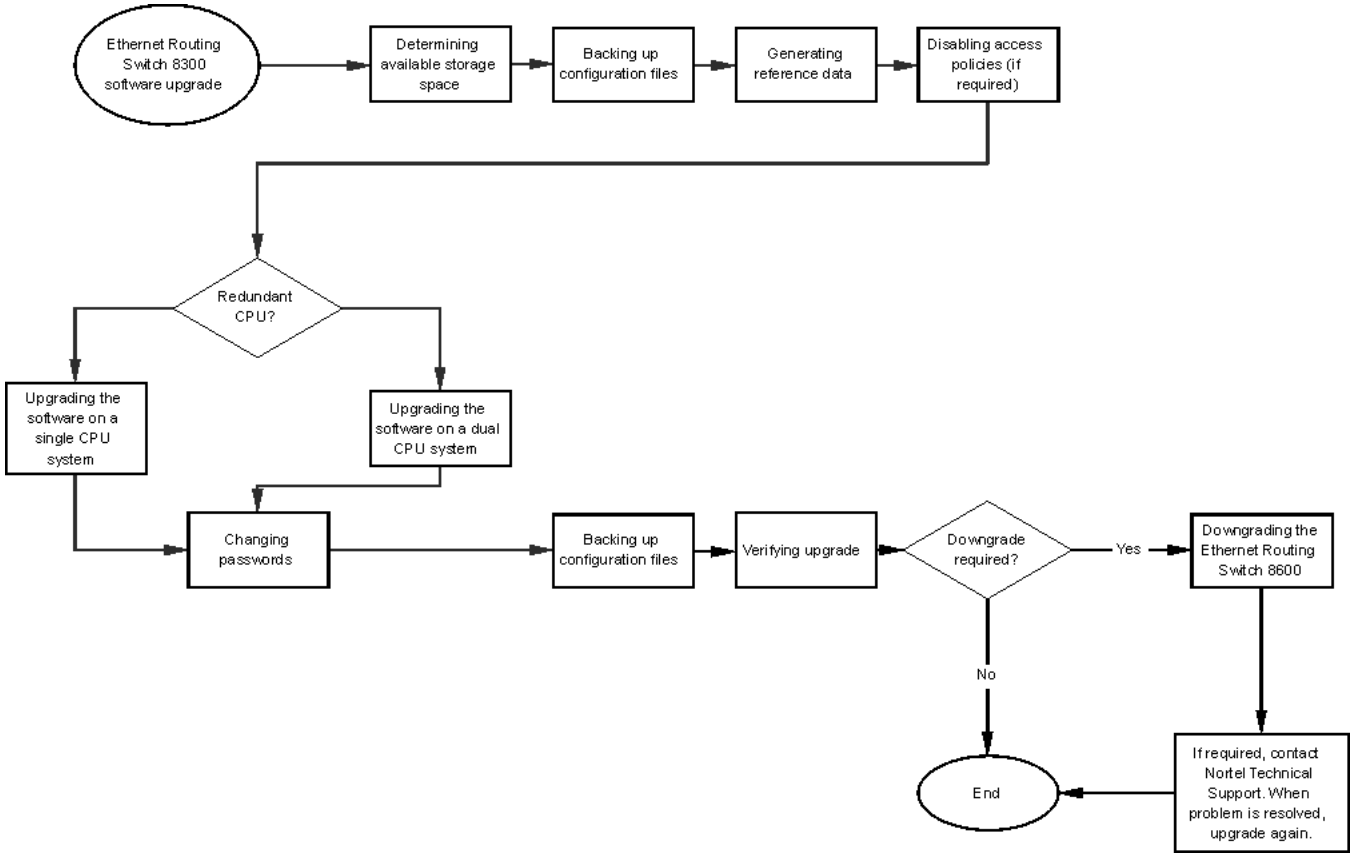
ATTENTION
All upgrade procedures assume that files use the default names. Use caution in any procedure if the file names are nondefault. Ensure all parameters associated with file names take into consideration the use of nondefault values.

- Read the latest release notes. See *Ethernet Routing Switch 8300 Release Notes — Software Release 4.1, NN46200-401*.
- Read the section “Safety Message Translations” (page 95).
- Read the section “Ethernet Routing Switch 8300 upgrade fundamentals” (page 25).
- You must be able to access the new software from the site www.nortel.com/support. You need a valid user or site ID and password.
- If necessary, schedule a time for the switch to be nonoperational.

Ethernet Routing Switch 8300 upgrade using the NNCLI tasks

This task flow shows you the sequence of tasks you perform to upgrade the Ethernet Routing Switch 8300. To link to any procedure, go to "Ethernet Routing Switch 8300 upgrade using the NNCLI navigation" (page 52).

Figure 2
Ethernet Routing Switch 8300 upgrade using the NNCLI tasks



Ethernet Routing Switch 8300 upgrade using the NNCLI navigation

- “Verifying the upgrade” (page 62)
- “Downgrading the Ethernet Routing Switch 8300” (page 63)

Determining available storage space

Determine whether the switch has enough storage space to store the new software.

Prerequisites

- Access PrivExec mode.

Procedure steps

Step	Action
1	To view the free space and files in flash memory, enter the following command: **dir** The bottom of the table shows available space: `total: 64155648 used: 40067072 free: 24088576 bytes`
2	If you must remove files to make space, use the **rm** command: **rm <WORD 1-99>** where **<WORD 1-99>** is /pcmcia/<file>, /flash/<file>, or /flash1/<file>. **ATTENTION** Older load, boot, and configuration files may be required if the upgrade is unsuccessful. Make sure you back up these files to a safe place before you remove them.

--End--

Backing up configuration files

Before you upgrade your switch software, make copies of the configuration files. If an upgrade is unsuccessful, use backup configuration files to return the switch to its previous state.

Prerequisites

- If you are using FTP or TFTP, ensure the switch allows Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP) access. See “Enabling FTP and TFTP” (page 71).
- For more details about copying files, see “Copying files” (page 82).
- Access PrivExec mode.

Procedure steps

Step	Action
1	Determine the configuration file names: **show boot config choice**
2	Save the configuration files. Assuming the files use the default file names, enter: **save config** **save bootconfig** **save config standby config.cfg** **save bootconfig standby boot.cfg** If the SaveToStandby flag is true, you do not need to save the files to the Secondary.
3	Copy the files to a safe place. For example, to copy to a PCMCIA card: **copy /flash/boot.cfg /pcmcia/boot_backup.cfg** **copy /flash/config.cfg /pcmcia/config_backup.cfg**
4	Ensure you also back up all other important files, including hidden files. See “Job aid: files present on SF/CPU modules” (page 75).
	--End--

Generating reference data

Use show commands to generate data to determine if the software upgrade is successful. After upgrade. the switch and network should operate as they did before the upgrade. Nortel recommends that you keep track of important parameters and ensure they are unchanged after an upgrade. The following procedure gives examples of how to generate reference data. Choose the parameters that are most important to your network.

If these parameters remain unchanged before and after the upgrade, the upgrade is likely successful. Otherwise, you may need to downgrade to a previous release or perform troubleshooting procedures.

Prerequisites

- Access PrivExec mode.

Procedure steps

Step	Action
1	Determine the number of routes in the routing table: **show ip route** Record the number of routes.
2	Determine Address Resolution Protocol (ARP) information: **show ip arp**
3	Determine the total number of Internet Group Management Protocol (IGMP) groups: **show ip igmp group**
4	Determine the total number of multicast routes: **show ip mroute interface** **show ip mroute route**
5	Determine Open Shortest Path First (OSPF) parameters: **show ip ospf** **show ip ospf neighbors interface**
6	Use the following command to view other IP show commands that you can use: **show ip ?**

--End--

Upgrading the software on a single SF/CPU system

Use this procedure to upgrade the SF/CPU software on a nonredundant Ethernet Routing Switch 8300 SF/CPU. This procedure shows how to upgrade using the flash memory as the file storage location; you can use other storage locations.

CAUTION
Risk of bootconfig file corruption
Operating a system with different versions of the runtime image and boot monitor image can cause a corrupt bootconfig file. If the boot.cfg file is corrupt, replace it with a saved version or recreate the file.

Prerequisites

- Back up the switch configuration files. See “Backing up configuration files” (page 53).
- You must be able to access www.nortel.com/support.
- Access Global Configuration mode.
- Determine if you need to disable access policies and do so if required. See “Disabling access policies” (page 91).

Procedure steps

Step	Action
1	Download the new software. For instructions, see “Downloading the software” (page 65).
2	Connect to the Ethernet Routing Switch 8300 by using the management console port. SSH, or a Telnet session.
3	Copy the required software files to flash memory. If you use TFTP or FTP, use the IP address of the SF/CPU. To determine the required files, see “New software files” (page 27). For instructions about copying files, see “Copying files” (page 70).
4	Confirm that the software files are successfully copied by using the **dir** command. Ensure the new files are listed.
5	Ensure the new files are error-free. See “Verifying the MD5 checksums” (page 91).
6	Configure the boot source to point to the new runtime image file (p83a4100.img): **boot config choice primary image-file /flash/p83a4100.img**
7	To specify the location of the I/O module image, enter the following command **boot config bootp image-name /flash/p83r4100.dld**

8 Save the configuration files:

```
save bootconfig
```

9 To verify that the changed primary image file settings are in the boot.cfg file, enter the following command :

```
show boot config choice
```

Confirm that the image location and name are correct.

10 To boot the Ethernet Routing Switch 8300 with the new boot-monitor image, enter the following command:

```
boot /flash/p83b4100.img
```

If you interrupt the auto-boot process, you may have to issue the **boot** command again.

This step causes an interruption to user traffic.

The switch boots using the new image file. The system takes a longer time to come up than a normal reboot because the system must write the new boot monitor to flash memory.

--End--

Upgrading the software on a dual SF/CPU system

Use this procedure to upgrade the SF/CPU software on a system that contains redundant SF/CPUs. This procedure shows how to upgrade using the flash memory as the file storage location; you can use other storage locations.

CAUTION

Nortel does not support different software versions, for example, Releases 3.0.3.0 and 4.0.0.0, on the Master and Secondary SF/CPUs except for during an upgrade process. Operating a system with different versions of the runtime image and boot monitor image can corrupt the bootconfig file. If the boot.cfg file is corrupt, replace it with a saved version, or recreate the file.

The Master and Secondary SF/CPU must have the same amount of memory.

CAUTION

Risk of failed upgrade

You must set the nocheck-sw-version flag to true before upgrade or the upgrade may fail. Steps are included in this procedure.

Prerequisites

- Back up the switch configuration files. See “Backing up configuration files” (page 53).
- You must be able to access www.nortel.com/support.
- If TFTP or FTP is required, ensure it are enabled. See “Enabling FTP and TFTP” (page 71).
- Access Global Configuration mode.
- Determine if you need to disable access policies and do so if required. See “Disabling access policies” (page 91).

Procedure steps

Step	Action
1	Download the new software. For instructions, see “Downloading the software” (page 65).
2	Connect to the Master SF/CPU by using the management console port, SSH, or a Telnet session.
3	Copy the required software files to the Master flash memory. To determine the required files, see “New software files” (page 27). For instructions about copying files, see “Copying files” (page 82).
4	Ensure that the SaveToStandby flag is true: **`boot config flags savetostandby`** **`save bootconfig`** If this flag is true, whenever a configuration file is saved on the Master, it is also automatically saved on the Secondary.
5	If you plan to use licensed features, copy the license file to the flash. The path and file name default to /flash/license.dat until the Release 4.1 software is loaded. The license file must contain the correct chassis MAC address.
6	To confirm that the software files are successfully copied, use the **`dir`** command.
7	Ensure the new files are error-free. See “Verifying the MD5 checksums” (page 91).

8 Copy the runtime image file (and all other files copied to the Master SF/CPU flash, including the license file) to the Secondary SF/CPU.

For example:

```
copy /flash/p83a4100.img <IP address of standby CPU>:p83a4100.img
```

You can use the management IP address or the loopback address of the Secondary SF/CPU. The loopback addresses are 127.0.0.5 and 127.0.0.6, respectively, for slots 5 and 6.

OR

```
copy /flash/p83a4100.img peer:p83a4100.img
```

9 Ensure that the files are successfully copied to the Secondary SF/CPU:

```
peer telnet
```

```
dir
```

```
exit
```

10 On the Master SF/CPU, configure the boot configuration file to point to new runtime image file (p83a4100.img):

```
boot config choice primary image-file /flash/p83a4100.img
```

11 To specify the I/O module image, enter the following command:

```
boot config bootp image-name /flash/p83r4100.dld
```

Although you can specify the image name, Nortel recommends that you use the default option.

12 Configure the nocheck-sw-version flag to true:

```
boot config flags nocheck-sw-version true
```

ATTENTION

If you do not set this flag to true, then a nocheck-sw-version flag mismatch may occur between the Master and Secondary SF/CPUs. In this case, you must change the upgrade procedure slightly: before the Secondary SF/CPU finishes the upgrade, boot the Master SF/CPU immediately. Do not wait for the Secondary to come back online.

To do this, if you use a remote connection, open two telnet sessions before rebooting the Secondary (one to each SF/CPU).

13 Save the configuration on both the Master and the Secondary SF/CPUs:

```
save bootconfig
```

14 To verify that the changed primary image file settings are in the boot.cfg file, enter the following command:

more boot.cfg

OR

show boot config choice

Verify that the primary image file is p83a4100.img.

15 To log on to the Secondary SF/CPU, enter the following command and log on:

peer telnet

16 To verify that the changed primary image file settings are in the Secondary boot.cfg file, enter the following command:

more boot.cfg

OR

show boot config choice

Confirm that the image location and name are correct.

17 To boot the Secondary SF/CPU with the new boot monitor image, enter the following command:

boot /flash/p83b4100.img

While the Secondary reboots, the Telnet session established from the Master SF/CPU does not respond. Wait for the session to time out and return to the Master CPU prompt.

18 Ensure that the Secondary SF/CPU administrative status is up by entering the following command:

show sys-info card

19 When the Secondary is up, upgrade the Master SF/CPU using the following command:

boot /flash/p83b4100.img

If you interrupt the auto-boot process, you may have to issue the **boot** command again.

If you are connecting remotely, the session stops responding. You will have to reconnect.

20 If desired, configure the nocheck-sw-version flag to false:

no boot config flags nocheck-sw-version

21 Save the configuration:

save bootconfig

22 To ensure proper failover support of upgraded Secondary, do a final reset of both SF/CPUs when a maintenance cycle permits. Reset the Secondary SF/CPU first and, within two seconds, the Master CPU, using the following command:

reset

Perform this step by opening two telnet sessions or do a power reset to the chassis power supplies.

23 Logon to the Master SF/CPU and check that the correct software version is loaded.

--End--

Changing passwords

Change passwords after an upgrade to maintain the highest security levels.

ATTENTION
Passwords are stored in an encrypted format in a system file, rather than in the configuration file. Passwords are maintained across an upgrade, assuming that the hidden files are not modified. If required, change the passwords after upgrade to secure your system. All passwords are case-sensitive.

Prerequisites

- Access Global Configuration mode.

Procedure steps

Step	Action
1	To change a password, use one of the following commands as required: **cli password <WORD 1-20> read-only [<WORD 0-20>]** **cli password <WORD 1-20> read-write [<WORD 0-20>]** **cli password <WORD 1-20> read-write-all [<WORD 0-20>]**
2	To view other password options, use the **cli password ?** command.

--End--

Variable definitions

Use the information in the following table to help you perform this procedure.

Variable	Value
<WORD 1-20>	Specifies the user name.
<WORD 0-20>	Specifies the password for the user. For more password options, enter **cli password <WORD 1-20> ?**

Backing up post-upgrade configuration files

Action
After you complete the upgrade, save the new config.cfg and boot.cfg files to the PCMCIA card or another safe place. See "Backing up configuration files" (page 40).

Verifying the upgrade

Verify your upgrade to ensure proper switch operation.

Prerequisites

- Access PrivExec mode.

Procedure steps

Step	Action
1	Repeat the procedure used in "Generating reference data" (page 41) and regenerate the same data. Compare the results. If you see substantial differences in this data, you may have to downgrade to the previous version and/or commence troubleshooting procedures.
2	To view bootconfig flags, enter the following command: **show boot config flags** Ensure the flags are set correctly.
3	To view RADIUS settings, enter the following command: **show radius** Ensure the settings are correct.
4	To check for alarms or unexpected errors, enter one the following commands: **show log file tail** **show log file severity <WORD 0-25>**

where **<WORD 0-25>** specifies INFO, ERROR, WARNING, or FATAL.

5 To ensure SNMP access policies are correctly configured, check to see if you can access the switch with Device Manager.

--End--

Downgrading the Ethernet Routing Switch 8300

Downgrade the Ethernet Routing Switch 8300 if an upgrade is not successful.

Prerequisites

- You need the previously saved configuration files (boot.cfg and config.cfg) for the release to which you intend to downgrade.

Procedure steps

Action
Install an older version of software. Use the procedure found in the *Upgrading Ethernet Routing Switch 8300* document that corresponds to the software release you intend to install. Ensure you use the previously saved configuration files for that release.

Common procedures

The following sections describe common procedures that you can use for the Ethernet Routing Switch 8300. You can use these procedures during upgrade or as part of normal system operations.

Navigation

Downloading the software

Download the new software to upgrade the switch. You can download each file separately, or you can download all files in a zipped folder.

Prerequisites

- Before you download the software, review the sections "New software files" (page 27).

Procedure steps

Step	Action
1	From your browser, access the Nortel Technical support portal www.nortel.com/support.
2	Navigate to the required files by selecting: • Routers & Routing Switches • Ethernet Routing Switch 8300 • Software, Releases
3	Download the required files.
	--End--

Upgrading Device Manager

Upgrade Device Manager so that you can use Device Manager to configure the latest new software features and capabilities. Install the latest version of Device Manager to access switches that run the latest software. The Device Manager software version and the switch software must match for the correct information to be shown and accessible.

Prerequisites

- Uninstall the previous version of Device Manager or install the new version in a different directory. Multiple versions of Device Manager can be stored on a PC or UNIX machine if each version is stored in a separate directory.

Procedure steps

Step	Action
1	Save the configuration and boot files.
2	Back up all important files, including the license, configuration, and boot files.
3	Download the latest version of Device Manager.
4	Uninstall the previous version of Device Manager.
5	Install the new version of Device Manager.
6	If you installed the software in a new folder, copy the dm.ini file from the previous version of Device Manager to the new Device Manager folder.
7	Open Device Manager and ensure it operates correctly. In the unlikely event that you encounter problems, reinstall the previous version of Device Manager and contact Technical Support.

--End--

Job aid: Device Manager settings file

Device Manager saves previously visited IP addresses to a settings file dm.ini. Uninstalling Device Manager does not remove the settings file. The dm.ini file containing IP addresses visited from a previous Device Manager release is automatically used by a new Device Manager version installed in the same directory. Manually move or copy the dm.ini file from a previous version of Device Manager to the new Device Manager installation in a different directory.

In a Windows environment, the settings file is called dm.ini and is created in the Device Manager installation directory. In a UNIX or Linux environment, the settings file is called ~/.jdm/dm.ini.

Common procedures using the CLI

The following sections describe common procedures that you can use for the Ethernet Routing Switch 8300. You can use these procedures during upgrade or as part of normal system operations.

Navigation

Saving configuration files

Save configuration files in the mode that you want to use. Although you cannot convert configuration files from one mode to another, you can save them in either CLI or NNCLI mode.

Procedure steps

Step	Action
1	When in CLI mode, to save a configuration file in CLI mode, enter: **`save config`**

save bootconfig

2 When in CLI mode, to save a configuration file in NNCLI mode, enter:

save config mode nncli

save bootconfig mode nncli

--End--

Copying files

Copy files as part of an upgrade procedure to back up files or to move files to another location.

When you copy files, you can rename the files. Use caution. All procedures in this document use the default file names. Upgrades can be unsuccessful if the wrong file names are used.

ATTENTION
If a failure occurs while you copy a file using TFTP (for example, a TFTP server is not available), the file is deleted.

Procedure steps

Step	Action
1	Use the **copy** command: **copy <filename> <filename>** For example: **copy /flash/config.cfg /pcmcia/config_backup.cfg** The first parameter you specify is where the file resides, and the second parameter is the location for the new file.
2	To copy files using a TFTP server, ensure the TFTP server is operating and then use the following command: **copy <tftp IP address>:<filename> /<location>/** For example: **copy 111.111.1.11:p83a4100.img /flash/p83a4100.img**

--End--

Variable definitions

Use the information in the following table to help you perform this procedure.

Variable	Value
<filename>	Specifies the file name and the path.
<location>	Specifies the file name and the path for file storage on the switch
<tftp IP address>	Specifies the IP address of the TFTP server.

Enabling FTP and TFTP

Enable FTP and TFTP to use these protocols on the Ethernet Routing Switch 8300. You can use FTP or TFTP servers to store upgrade files. To save a file to a Secondary SF/CPU, enable TFTP on the Secondary SF/CPU. Reboot the switch to enable FTP or TFTP.

Procedure steps

Step	Action
1	To enable the FTP daemon, enter the following command: **config bootconfig flags ftpd true**
2	To enable the TFTP daemon, enter the following command: **config bootconfig flags tftpd true**
3	To save the boot configuration file, enter the following command: **save bootconfig standby boot.cfg**
4	Reboot the SF/CPU so that the changes take effect, and the protocols are enabled: **boot -y**

--End--

Configuring boot sources

If the boot source location or image name is not default, specify its location or name. To specify boot source locations and file names, use the following procedure. You can also use these commands to change the order in which the boot sources (flash memory, PCMCIA card, FTP or TFTP server) are accessed. If you move a .dld file from its default location, be sure to specify its new location.

ATTENTION
Nortel recommends that you store .dld files in flash memory.

Procedure steps

Step	Action
1	To change the runtime configuration file locations, use the following command: **config bootconfig choice <primary|secondary|tertiary> [config-file <file>|backup-config-file <file>|image-file <file>|license-file <file>]** For example, to specify the configuration file in flash memory as the primary, use the following command: **config bootconfig choice primary config-file /flash/config.cfg**
2	To set the location for the I/O module driver image for the BootStrap protocol: **config bootconfig bootp image-name <image-name> [<slot-number>]** For example, to specify the I/O module driver for slot 2 in flash memory, use the following command: **config bootconfig bootp /flash/p83r4100.dld 2**

--End--

Variable definitions

Use the data in the following table to help you use the **config bootconfig choice <primary|secondary|tertiary>** command.

Variable	Value
backup-config-file <file>	Identifies the backup boot configuration file; **file** is the device path and file name, up to 256 characters including the path.
config-file <file>	Identifies the boot configuration file; **file** is the device path and file name, up to 256 characters including the path.
image-file <file>	Identifies the image file; **file** is the device path and file name, up to 256 characters including the path.
info	Shows the current boot choices and associated files.
license-file <file>	Identifies the license file; **file** is the device path and file name, up to 256 characters including the path.

Use the data in the following table to help you use the **config bootconfig bootp** command.

Variable	Value
image-name <image-name> [<slot-number>]	Identifies the I/O module image. **<file>** is the device and file name, up to 256 characters including the path. **<slot-number>** identifies the image with a particular slot.
info	Shows the current boot choice and associated files.

Replacing a SF/CPU module in a single CPU chassis

Replace a single SF/CPU module in a single chassis to replace a faulty SF/CPU or to upgrade the SF/CPU to a newer model.

CAUTION
Risk of traffic loss
This procedure causes an interruption to user traffic. Schedule a time for the switch to be nonoperational.

If you are replacing an 8393SF/CPU with an 8394SF/CPU, the configurations of the 1 gigabit ports on the 8393SF/CPU need to be reprogrammed on the 8394SF/CPU 10 gigabit ports. Some manual reconfiguration may be necessary.

If the flash is not accessible on a faulty SF/CPU, obtain the files from another source, which can be another network device, such as a TFTP or FTP server. Alternatively, the files can be rebuilt using the Customer Spec Book or the configuration from the VRRP peer Ethernet Routing Switch 8300.

CAUTION
Risk of equipment damage
To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack.

Prerequisites

- You can access the console port and the Ethernet management port.

Procedure steps

Step	Action
1	Save the configuration files. **save config**

save bootconfig

2. Place all required files onto the PCMCIA card.

   For more information, see "Job aid: files present on SF/CPU modules" (page 75) and "Copying files" (page 70).

3. Power down the switch to stop all traffic.

4. Disconnect the cables from the management and console ports.

5. Remove the old SF/CPU.

   For instructions, see *Nortel Ethernet Routing Switch 8300 Installation — Modules, NN46200-305*.

6. Insert the new SF/CPU.

7. Reconnect the cables to the Ethernet management and console ports.

8. Replace the PCMCIA card.

9. Logon to the SF/CPU.

10. Copy all required files from the PCMCIA card to the SF/CPU flash memory, including the license.

11. Re-hide any hidden (.txt) files.

    See "Hiding files" (page 74).

12. Boot the system:

    boot -y

13. Verify that the license, image, and configuration loaded properly:

    show sys sw

    show license

--End--

Hiding files

Hide files for security reasons, and to keep them safe from accidental deletion. Hidden files are listed in "Job aid: files present on SF/CPU modules" (page 75).

Procedure steps

Action
To hide files, use the attrib "+h" command. For example, to hide a file located on the flash named shadov.txt: **attribute /flash/shadov.txt "+h"**

Job aid: files present on SF/CPU modules

The following files can be present on the SF/CPU flash memory of an Ethernet Routing Switch 8300. The files present on the flash depend on the hardware and software configuration present on the switch. For more information about the most up-to-date filenames, see *Release Notes — Software Release 4.1, NN46200-401*. The information in the Release Notes takes precedence over the information in this document.

Table 4
Required files

File type	Name
Configuration	• config.cfg • boot.cfg
Images	• p83a4100.img (runtime) • p83b4100.img (boot monitor) • p83c4100.img (encryption module)
Encryption module	• p83c4100.aes
DLD image file	• p83r4100.dld
License files	• license.dat • *.dat, if files are renamed
Hidden files	• shadov.txt • passvord.txt (if hsecure is enabled) • snmp_usm.txt • snmp_comm.txt

Replacing both SF/CPU modules in a dual CPU chassis

Use this procedure to replace both SF/CPU modules in a redundant SF/CPU configuration. You can use this procedure when you upgrade switch fabrics from the 8393 to the 8394SF/CPU.

CAUTION
Risk of traffic loss
This procedure causes an interruption to user traffic. Schedule a time for the switch to be nonoperational.

If you are replacing an 8393SF/CPU with an 8394SF/CPU, the configurations of the 1 gigabit ports on the 8393SF/CPU need to be reprogrammed on the 8394SF/CPU 10 gigabit ports. Some manual reconfiguration may be necessary.

For information about configuring a SF/CPU as Master, see *Nortel Ethernet Routing Switch 8300 Administration, NN46200-604*.

CAUTION
Risk of traffic loss or corruption
When you replace the active SF/CPU module in a redundant SF/CPU system, wait until the new Master stabilizes before you insert any other modules. Do not replace I/O modules until the new SF/CPU becomes the Master SF/CPU.

If you have only one SF/CPU and you swap the SF/CPU, all the SNMP password files, including the hidden file, are lost. Either reconfigure the trap receivers and community strings each time you change the SF/CPU module, or save these hidden files to a PCMCIA card.

Do not replace modules in a switch while the switch boots. If you do, the switch may not recognize the module, which causes module initialization failure.

CAUTION
Risk of equipment damage
To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack.

Procedure steps

Step	Action
1	Use Telnet or the console port to connect to the Master SF/CPU.
2	Ensure both SF/CPUs have the same configuration. To do so, enter: **`save config standby <filename>`** **`save bootconfig standby <filename>`**
3	Remove the Secondary SF/CPU.
4	Install the new SF/CPU.
5	Save the configuration files: **`save config standby <filename>`** **`save bootconfig standby <filename>`**

6 If you are using licensed features, ensure that the license file is present on the Secondary. Also, ensure all required files are on the Secondary. See “Job aid: files present on SF/CPU modules” (page 75).

7 Remove the Master SF/CPU.

The Secondary becomes the new Master.

8 Install the second new SF/CPU.

9 Copy the configuration and license files to the Secondary SF/CPU.

10 Boot the Secondary.

11 Boot the Master.

12 Ensure both the Secondary and Master have all required files.

--End--

Variable definitions

Use the following table to help you use the commands in this procedure.

Variable	Value
<filename>	Specifies the destination path and filename in the format /pcmcia/<filename> or /flash/<filename>
<slotnum>	Specifies the slot number of the module to be disabled.

Hot swapping an I/O module

Use this procedure to hot swap an Ethernet Routing Switch 8300 I/O module. You can use this procedure when you upgrade to the latest modules.

CAUTION
Risk of traffic loss or corruption
Do not replace modules in a switch while the switch boots. If you do, the switch may not recognize the module, which causes module initialization failure.

CAUTION
Risk of equipment damage
To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack.

Procedure steps

Step	Action
1	Connect to the Master SF/CPU.
2	To avoid possible packet loss, Nortel recommends that you disable the module, although this is not strictly required: **config slot <slotnum> state disable**
3	If you disabled the module, confirm that the module is disabled. The Online LED of the module is amber when the module is disabled. You can also verify that the module is disabled by using the following command: **show tech**
4	Remove the module.
5	Insert the new module. The chassis automatically enables the new module.
6	Confirm that the new module is operational: **show tech** As well, the Online LED of the module lights up.
7	Confirm that traffic is traversing the module as normal.
	--End--

Variable definitions

Use the following table to help you use the commands in this procedure.

Variable	Value
<slotnum>	Specifies the slot number of the module to be disabled.

Disabling access policies

Access Policies must be disabled at the global level before upgrading from Release 2.3 to 4.1 if access through Device Manager is required immediately after upgrade.

After the software upgrade is complete, an access policy for the SNMPv3 group must be provisioned in Access Policies SNMP Groups table before enabling access policies at the global level.

For more information about SNMP, see *Nortel Ethernet Routing Switch 8300 Security, NN46200-605* and *Nortel Ethernet Routing Switch 8300 Administration, NN46200-604*.

Procedure steps

Action
To disable access policies: **config sys access-policy enable false**

Verifying the MD5 checksums

Use the MD5 checksums to ensure the integrity of the new software files before you use them to upgrade. Corrupted files can cause the upgrade to fail.

For more information about the **md5** command, see "MD5 information" (page 36).

Procedure steps

Step	Action
1	To calculate the message digest for files in flash memory or on a PCMCIA card, and to display the output on screen, enter the following command: **md5 <filename>** For example: **md5 *.img**
2	If, for any file, the checksum does not match, retransfer the file and run the **md5** command again.
	--End--

Variable definitions

Use the data in the following table to help you use the **md5 <filename>** command.

Variable	Value
wildcard character (*)	Calculates the MD5 checksum of all files.
-a	Adds data to the output file instead of overwriting it. You cannot use the -a option with the -c option.

Variable	Value
-c	Compares the checksum of the specified file by **<filename>** with the MD5 checksum present in the checksum file name. You can specify the checksum file name using the -f option. If the checksum file name is not specified, the file /flash/checksum.md5 is used for comparison. If the checksum file name and the default file are not available in flash memory, the following error message is displayed: `Error: Checksum file <filename> not present.` The -c option also: • calculates the checksum of files specified by **filename** • compares the checksum with all keys in the checksum file, even if the file names do not match • shows the results of the comparison

-f <checksum-file-name>	Stores the result of MD5 checksum to a file in flash memory or on a PCMCIA card.
	
	If the output file specified with the -f option is one of the:
	
	• reserved file names on the switch, the command fails and the error message is displayed:
	`Error: Invalid operation.`
	
	• files for which MD5 checksum is to be computed, the command fails and the error message is displayed:
	`Error: Invalid operation on file <filename>`
	
	If the checksum file name specified by the -f option exists on the switch (and is not one of the reserved file names), the following message is shown:
	
	`File exists. Do you wish to overwrite? (y/n)`

-r	Reverses the output and can be used with -f option to store the output to a file. The -r option cannot be used with the -c option.

Common procedures using the NNCLI

The following sections describe common procedures that you can use for the Ethernet Routing Switch 8300. You can use these procedures during upgrade or as part of normal system operations.

Navigation

Saving configuration files

Save configuration files in the mode that you want to use. Although you cannot convert configuration files from one mode to another, you can save them in either CLI or NNCLI mode.

Prerequisites

- Access PrivExec mode.

Procedure steps

Step	Action
1	When in NNCLI mode, to save configuration files in NNCLI mode, enter: **save config** **save bootconfig**
2	When in NNCLI mode, to save a configuration file in CLI mode, enter: **save config mode cli** **save bootconfig mode cli**

--End--

Copying files

Copy files as part of an upgrade procedure to back up files or to move files to another location.

When you copy files, you can rename the files. Use caution. All procedures in this document use the default file names. Upgrades can be unsuccessful if the wrong file names are used.

ATTENTION
If a failure occurs while you copy a file using TFTP (for example, a TFTP server is not available), the file is deleted.

Prerequisites

- Access PrivExec mode.

Procedure steps

Step	Action
1	Use the **copy** command: **copy <file> <file>** For example: **copy /flash/config.cfg /pcmcia/config_backup.cfg** The first parameter you specify is where the file resides, and the second parameter is the location for the new file.

2 To copy files using a TFTP server, ensure the TFTP server is operating and then use the following command:

copy <tftp IP address>:<filename> /<location>/

For example:

copy 111.111.1.11:p83a4100.img /flash/p83a4100.img

--End--

Enabling FTP and TFTP

Enable FTP and TFTP to use these protocols on the Ethernet Routing Switch 8300. You can use FTP or TFTP servers to store upgrade files. To save a file to a Secondary SF/CPU, enable TFTP on the Secondary SF/CPU. Reboot the switch to enable FTP or TFTP.

Prerequisites

- Access Global Configuration mode.

Procedure steps

Step	Action
1	To enable the FTP daemon, enter the following command: **boot config flags ftpd**
2	To enable the TFTP daemon, enter the following command: **boot config flags tftpd**
3	To save the boot configuration file, enter the following command: **save config standby boot.cfg**
4	Reboot the SF/CPU so that the changes take effect, and the protocols are enabled: **boot**

--End--

Configuring boot sources

If the boot source location or image name is not default, specify its location or name. To specify boot source locations and file names, use the following procedure. You can also use these commands to change

the order in which the boot sources (flash memory, PCMCIA card, FTP or TFTP server) are accessed. If you move a .dld file from its default location, be sure to specify its new location.

ATTENTION
Nortel recommends that you store .dld files in flash memory.

Prerequisites

- Access Global Configuration mode.

Procedure steps

Step	Action
1	To change the runtime configuration file locations, use the following command: **boot config choice <primary|secondary|tertiary> [config-file <WORD 0-256>|backup-config-file <WORD 0-256>|image-file <WORD 0-256>|license-file <WORD 0-256>]** For example, to specify the configuration file in flash memory as the primary, use the following command: **boot config choice primary config-file /flash/config.cfg**
2	To set the location for the I/O module driver image for the BootStrap protocol: **boot config bootp image-name <WORD 0-127> <1-10>** For example, to specify the I/O module driver file in flash memory, use the following command: **boot config bootp image-name /flash/p83r4100.dld**

--End--

Variable definitions

Use the data in the following table to help you use the **boot config choice <primary|secondary|tertiary>** command.

Variable	Value
backup-config-file <WORD 0-256>	Identifies the backup boot configuration file; **<WORD 0-256>** is the device and file name, up to 256 characters including the path.

Variable	Value
config-file <WORD 0-256>	Identifies the boot configuration file; **<WORD 0-256>** is the device and file name, up to 256 characters including the path.
image-file <WORD 0-256>	Identifies the image file; **<WORD 0-256>** is the device and file name, up to 256 characters including the path.
license-file <WORD 0-256>	Identifies the license file; **<WORD 0-256>** is the device and file name, up to 256 characters including the path.

Use the data in the following table to help you use the **boot config bootp** commands.

Variable	Value
image-name <WORD 0-127> <1-10>	Identifies the image file for I/O modules. **<WORD 0-127>** is the device and file name, including the path, of up to 128 characters. **<1-10>** is the slot number.

Replacing a SF/CPU module in a single CPU chassis

Replace a single SF/CPU module in a single chassis to replace a faulty SF/CPU or to upgrade the SF/CPU to a newer model.

CAUTION
Risk of traffic loss
This procedure causes an interruption to user traffic. Schedule a time for the switch to be nonoperational.

If you are replacing an 8393SF/CPU with an 8394SF/CPU, the configurations of the 1 gigabit ports on the 8393SF/CPU need to be reprogrammed on the 8394SF/CPU 10 gigabit ports. Some manual reconfiguration may be necessary.

If the flash is not accessible on a faulty SF/CPU, obtain the files from another source, which can be another network device, such as a TFTP or FTP server. Alternatively, the files can be rebuilt using the Customer Spec Book or the configuration from the VRRP peer Ethernet Routing Switch 8300.

CAUTION
Risk of equipment damage
To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack.

Prerequisites

- You can access the console port and the Ethernet management port.
- Access privEXEC mode.

Procedure steps

Step	Action
1	Save the configuration files. **save config** **save bootconfig**
2	Place all required files onto the PCMCIA card. For more information, see "Job aid: files present on SF/CPU modules" (page 87) and "Copying files" (page 70).
3	Power down the switch to stop all traffic.
4	Disconnect the cables from the management and console ports.
5	Remove the old SF/CPU. For instructions, see *Nortel Ethernet Routing Switch 8300 Installation — Modules, NN46200-305*.
6	Insert the new SF/CPU.
7	Reconnect the cables to the Ethernet management and console ports.
8	Replace the PCMCIA card.
9	Logon to the SF/CPU.
10	Copy all required files from the PCMCIA card to the SF/CPU flash memory, including the license.
11	Re-hide any hidden (.txt) files. See "Hiding files" (page 74).
12	Boot the system: **boot**
13	Verify that the license, image, and configuration loaded properly: **show sys software** **show license all**

--End--

Hiding files

Hide files for security reasons and to keep them safe from accidental deletion. Hidden file names are listed in “Job aid: files present on SF/CPU modules” (page 87).

Prerequisites

- Access PrivExec mode.

Procedure steps

Action
To hide files, use the attrib "+h" command. For example, to hide a file located on the flash named shadov.txt: **`attribute /flash/shadov.txt "+h"`**

Job aid: files present on SF/CPU modules

The following files can be present on the SF/CPU flash memory of an Ethernet Routing Switch 8300. The files present on the flash depend on the hardware and software configuration present on the switch. For more information about the most up-to-date filenames, see *Release Notes — Software Release 4.1, NN46200-401*. The information in the Release Notes takes precedence over the information in this document.

Table 5
Required files

File type	Name
Configuration	• config.cfg • boot.cfg
Images	• p83a4100.img (runtime) • p83b4100.img (boot monitor) • p83c4100.img (encryption module)
Encryption module	• p83c4100.aes
DLD files (I/O module)	• p83r4100.dld

Table 5
Required files (cont'd.)

File type	Name
License files	• license.dat • *.dat, if files are renamed
Hidden files	• shadov.txt • passvord.txt (if hsecure is enabled) • snmp_usm.txt • snmp_comm.txt

Replacing both SF/CPU modules in a dual CPU chassis

Use this procedure to replace both SF/CPU modules in a redundant SF/CPU configuration. You can use this procedure when you upgrade switch fabrics from the 8393 to the 8394SF/CPU.

CAUTION
Risk of traffic loss
This procedure causes an interruption to user traffic. Schedule a time for the switch to be nonoperational.

If you are replacing an 8393SF/CPU with an 8394SF/CPU, the configurations of the 1 gigabit ports on the 8393SF/CPU need to be reprogrammed on the 8394SF/CPU 10 gigabit ports. Some manual reconfiguration may be necessary.

For information about configuring a SF/CPU as Master, see *Nortel Ethernet Routing Switch 8300 Administration, NN46200-604*.

CAUTION
Risk of traffic loss or corruption
When you replace the active SF/CPU module in a redundant SF/CPU system, wait until the new Master stabilizes before you insert any other modules. Do not replace I/O modules until the new SF/CPU becomes the Master SF/CPU.

If you have only one SF/CPU and you swap the SF/CPU, all the SNMP password files, including the hidden file, are lost. Either reconfigure the trap receivers and community strings each time you change the SF/CPU module, or save these hidden files to a PCMCIA card.

Do not replace modules in a switch while the switch boots. If you do, the switch may not recognize the module, which causes module initialization failure.

CAUTION
Risk of equipment damage
To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack.

Procedure steps

Step	Action
1	Use Telnet or the console port to connect to the Master SF/CPU.
2	Ensure both SF/CPUs have the same configuration. To do so, enter: **`save config standby <filename>`** **`save bootconfig standby <filename>`**
3	Remove the Secondary SF/CPU.
4	Install the new SF/CPU.
5	Save the configuration files: **`save config standby <filename>`** **`save bootconfig standby <filename>`**
6	If you are using licensed features, ensure that the license file is present on the Secondary. Also, ensure all required files are on the Secondary. See "Job aid: files present on SF/CPU modules" (page 87).
7	Remove the Master SF/CPU. The Secondary becomes the new Master.
8	Install the second new SF/CPU.
9	Copy the configuration and license files to the Secondary SF/CPU.
10	Boot the Secondary.
11	Boot the Master.
12	Ensure both the Secondary and Master have all required files.

--End--

Variable definitions

Use the following table to help you use the commands in this procedure.

Variable	Value
<filename>	Specifies the destination path and filename in the format /pcmcia/<filename> or /flash/<filename>

Hot swapping an I/O module

Use this procedure to hot swap an Ethernet Routing Switch 8300 I/O module. You can use this procedure when you upgrade to the latest modules.

CAUTION
Risk of traffic loss or corruption
Do not replace modules in a switch while the switch boots. If you do, the switch may not recognize the module, which causes module initialization failure.

CAUTION
Risk of equipment damage
To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack.

Prerequisites

- Access Global Configuration mode.

Procedure steps

Step	Action
1	Connect to the Master SF/CPU.
2	To avoid possible packet loss, Nortel recommends that you disable the module, although this is not strictly required: **shutdown <1-10>**
3	If you disabled the module, confirm that the module is disabled. The Online LED of the module is amber when the module is disabled. You can also verify that the module is disabled by using the following command: **show tech**
4	Remove the module.
5	Insert the new module. The chassis automatically enables the new module.
6	Confirm that the new module is operational: **show tech**

As well, the Online LED of the module lights up.

7 Confirm that traffic is traversing the module as normal.

--End--

Variable definitions

Use the following table to help you use the commands in this procedure.

Variable	Value
<1-10>	Specifies the slot number of the module to be disabled.

Disabling access policies

Access Policies must be disabled at the global level before upgrading from Release 2.3 to 4.1 if access through Device Manager is required immediately after upgrade.

After the software upgrade is complete, an access policy for the SNMPv3 group must be provisioned in Access Policies SNMP Groups table before enabling access policies at the global level.

For more information about SNMP, see *Nortel Ethernet Routing Switch 8300 Security, NN46200-605* and *Nortel Ethernet Routing Switch 8300 Administration, NN46200-604*.

Procedure steps

Action
In Global Configuration mode, disable access policies: **no access-policy**

Verifying the MD5 checksums

Use the MD5 checksums to ensure the integrity of the new software files before you use them to upgrade. Corrupted files can cause the upgrade to fail.

For more information about the **md5** command, see “MD5 information” (page 36).

Prerequisites

- Access Global Configuration mode.

Procedure steps

Step	Action
1	To calculate the message digest for files in flash memory or on a PCMCIA card, and to display the output on screen, enter the following command: **md5 <filename>** For example: **md5 *.img** It takes some time to compute the message digest.
2	If, for any file, the checksum does not match, retransfer the file and run the md5 command again.

--End--

Variable definitions

Use the data in the following table to help you use the **md5 <filename>** command.

Variable	Value
wildcard character (*)	Calculates the MD5 checksum of all files.
-a	Adds data to the output file instead of overwriting it. You cannot use the -a option with the -c option.
-c	Compares the checksum of the specified file by **<filename>** with the MD5 checksum present in the checksum file name. You can specify the checksum file name using the -f option. If the checksum file name is not specified, the file /flash/checksum.md5 is used for comparison. If the checksum file name and the default file are not available in flash memory, the following error message is displayed: Error: Checksum file <filename> not present.

Variable	Value
	The -c option also: • calculates the checksum of files specified by **filename** • compares the checksum with all keys in the checksum file, even if the file names do not match • shows the results of the comparison

-f <checksum-file-name>	Stores the result of MD5 checksum to a file in flash memory or on a PCMCIA card.
	
	If the output file specified with the -f option is one of the:
	• reserved file names on the switch, the command fails and the error message is displayed:
	`Error: Invalid operation.`
	• files for which MD5 checksum is to be computed, the command fails and the error message is displayed:
	`Error: Invalid operation on file <filename>`
	
	If the checksum file name specified by the -f option exists on the switch (and is not one of the reserved file names), the following message is shown:
	
	`File exists. Do you wish to overwrite? (y/n)`

-r	Reverses the output and can be used with -f option to store the output to a file. The -r option cannot be used with the -c option.

Appendix
Safety Message Translations

This appendix contains translations of caution, warning, and danger messages that appear in this document.

Electrostatic discharge

This section translates the electrostatic discharge caution message.

CAUTION
Risk of equipment damage
To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack.

CAUTION
ATTENTION
Risque d'endommagement de l'équipement

To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack.

CAUTION
ACHTUNG
Risiko eines Geräteschadens

Um Schäden durch elektrostatische Entladung zu verhindern, tragen Sie bei der Instandhaltung dieses Produkts immer ein antistatisches Band am Handgelenk, welches mit einer ESD-Buchse verbunden ist.

CAUTION
PRECAUCIÓN
Riesgo de daño del equipo

Para prevenir el daño producido por una descarga electrostática, use siempre una pulsera antiestática conectada a un enchufe ESD.

CAUTION
CUIDADO
Risco de danos ao equipamento

Para evitar danos com descarga eletrostática, sempre use uma pulseira antiestática que esteja conectada a uma tomada ESD.

CAUTION
ATTENZIONE
Rischio di danni all'apparecchiatura

Per evitare danni derivanti da scariche elettrostatiche, indossare sempre un polsino antistatico collegato a una presa ESD.

Index

M

N

P

R

S

T

U

Nortel Ethernet Routing Switch 8300

Upgrades — Software Release 4.1

Printed in Canada, China, and the United States of America
Release: 4.1
Publication: NN46200-400
Document status: Standard
Document revision: 04.03
Document release date: 30 June 2008

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

www.nortel.com

ATTENTION

For information about the regulatory and safety precautions, read "Regulatory Messages and Safety Precautions" in this guide.

For information about the software license, read "Software license" in this guide.