



NORTEL

Nortel Ethernet Routing Switch 8600

Release Notes — Software

Release 7.0

Release: 7.0
Document Revision: 04.AV

www.nortel.com

NN46205-402

Nortel Ethernet Routing Switch 8600
Release: 7.0
Publication: NN46205-402
Document status: Draft
Document release date: 22 February 2010

Copyright © 2008-2010 Nortel Networks. All Rights Reserved.

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

THE SOFTWARE DESCRIBED IN THIS DOCUMENT IS FURNISHED UNDER A LICENSE AGREEMENT AND MAY BE USED ONLY IN ACCORDANCE WITH THE TERMS OF THAT LICENSE.

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

All other trademarks are the property of their respective owners.

Contents

Software license	7
New in this release	11
Features	11
Other changes	12
List of new features removed from Release Notes	12
Nonsupported hardware for Release 7.0 and later	12
R mode	13
Introduction	15
Important notices	17
Software licensing	18
File names for this release	18
Important information and restrictions	21
SuperMezz, CPU memory, and upgrades	22
Compact flash card display on 8695 SF/CPU	22
Proper care of external compact flash and PCMCIA cards	22
EDM considerations	23
Using the EDM plug-in with COM	24
Installing EDM help files	24
I/O module considerations	25
MLT/LAG considerations	25
Console connection considerations	25
DHCP snooping considerations	25
Supported upgrade paths	25
General upgrade considerations	26
Upgrade considerations for 8692 SF/CPU with SuperMezz	26
Upgrade considerations for Release 7.0	26
Upgrading from 8692 SF/CPU with SuperMezz to 8695 CPU	26
Upgrade considerations: DOSFS with upgrades from pre-Release 5.0	27
Upgrade considerations: Power Management	28
Disabling power and cooling management	29
Upgrade considerations: IST	31
Pre-release 5.1 upgrades considerations: specifying license file location	32

Considerations for upgrades from 5.0.0.x release code	32
Supported software and hardware scaling capabilities	38
Hardware and software compatibility	41
Module type and feature compatibility	44
High Availability mode considerations	45
HA mode and short timers	46
Ongoing considerations	46
Module and chassis compatibility and performance considerations	46
High Performance chassis	47
Switch clustering topologies and interoperability with other products	48
SF/CPU protection and loop prevention compatibility	49
Switch behavior during boot cycle and redundant configuration files	49
Configuring primary, secondary, and tertiary boot sources	51
OSPF warning message	52
MPLS considerations	53
SNMP considerations	53
VLACP considerations	53
DVMRP considerations	54
SMLT considerations	54
RSMLT considerations	55
60 day trial license	55
Advanced filter guidelines	55
Supported standards, RFCs, and MIBs	56
Supported traps and notifications	56

Resolved issues

57

Platform resolved issues	57
Switch management resolved issues	57
MLT/SMLT resolved issues	58
Unicast routing resolved issues	58
Multicast routing resolved issues	59
CLI and NNCLI resolved issues	59
Quality of Service and filters resolved issues	59

Known issues and limitations

61

Release 7.0 known issues	61
Release 5.1 known issues	71
Platform known issues	72
Switch management known issues	74
Layer 2 known issues	75
MLT/SMLT known issues	75
Unicast routing known issues	76
Multicast routing known issues	77
CLI and NNCLI known issues	77
Quality of Service and filters known issues	78

Device Manager known issues	78
Release 5.1 known limitations	78
Platform limitations	79
Switch management limitations	81
Layer 2 limitations	81
MLT/SMLT limitations	82
Unicast routing limitations	82
Multicast routing limitations	83
QoS and filters limitations	83
Device Manager limitations	83
MIB limitations	84

Customer service	85
Updated versions of documentation	85
Getting help	85
Express Routing Codes	85
Additional information	86

Index	87
--------------	-----------

DRAFT

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.

DRAFT

New in this release

The following sections detail what's new in *Nortel Ethernet Routing Switch 8600 Release Notes — Software Release 7.0* (NN46205-402) for Release 7.0.

Features

The following sections are new or updated for Release 7.0:

- “SuperMezz, CPU memory, and upgrades” (page 22)
- “Compact flash card display on 8695 SF/CPU” (page 22)
- “Proper care of external compact flash and PCMCIA cards” (page 22)
- “EDM considerations” (page 23)
- “Installing EDM help files” (page 24)
- “Using the EDM plug-in with COM” (page 24)
- “Installing EDM help files” (page 24)
- “Console connection considerations” (page 25)
- “DHCP snooping considerations” (page 25)
- “Supported upgrade paths” (page 25)
- “General upgrade considerations” (page 26)
- “Upgrade considerations for Release 7.0” (page 26)
- “Upgrading from 8692 SF/CPU with SuperMezz to 8695 CPU” (page 26)
- “Upgrade considerations: DOSFS with upgrades from pre-Release 5.0” (page 27)
- “Configuration file modifications for BGP upgrades from release 4.x code” (page 34)
- “Considerations for upgrades from 5.0.0.x release code” (page 32)
- “Configuration file modifications for BGP upgrades from release 4.x code” (page 34)

- “SMLT switch cluster upgrade considerations” (page 35)
- “Supported software and hardware scaling capabilities” (page 38)
- “Hardware and software compatibility” (page 41)
- Table 5 "Module and component compatibility" (page 42)
- “Module type and feature compatibility” (page 44)
- “Module and chassis compatibility and performance considerations” (page 46)
- “SMLT considerations” (page 54)
- “RSMLT considerations” (page 55)
- “High Availability mode considerations” (page 45)
- “Considerations for upgrades from 5.0.0.x release code” (page 32)
- “Resolved issues” (page 57)
- “Known issues and limitations” (page 61)

Other changes

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

List of new features removed from Release Notes

With Release 7.0, the Release Notes do not list all new features for this release. For information on new features, see *Ethernet Routing Switch 8600 Release 5.1 to Release 7.0 Delta* (NN46205-205).

Nonsupported hardware for Release 7.0 and later

Release 7.0 and later does not support any classic modules:

- 8608GBE module
- 8608GBM module
- 8608GTE module
- 8608GTM module
- 8608SXE module
- 8616GTE module
- 8616SXE module
- 8624FXE module
- 8632TXE module
- 8632TXM module

- 8648TXE module
- 8648TXM module
- 8672ATME module
- 8672ATMM module
- 8683POSM module
- 8690 SF/CPU module
- 8691 SF/CPU module
- Web Switching Module (WSM)
- 8660 Service Delivery Module (SDM)
- 8661 SSL Acceleration Module (SAM)
- Media Dependent Adapters for the 8672ATME and 8672ATMM Modules
- Breaker Interface Panel
- 8001AC power supply
- 8002DC power supply
- 8003AC power supply

Finally, Release 7.0 supports the 8692 SF/CPU only if it is equipped with SuperMezz. The 8692 SF/CPU without SuperMezz is not supported with Release 7.0.

References to these modules are removed from this document.

ATTENTION

In release 7.0, the 8003 chassis is no longer supported. It is replaced by the 8003-R chassis.

R mode

With Release 7.0, M mode is no longer supported. The software runs in R mode by default. References to R mode are removed from this document.

DRAFT

Introduction

This document describes important notices and known and fixed issues for Ethernet Routing Switch 8600 Software Release 7.0. Use this document to help you optimize the functionality of your Ethernet Routing Switch 8600.

ATTENTION

With Release 7.0, the Release Notes do not list the new features for this release. For information on new features, see *Ethernet Routing Switch 8600 Release 5.1 to Release 7.0 Delta* (NN46205-205).

Navigation

- [“Important notices” \(page 17\)](#)
- [“Resolved issues” \(page 57\)](#)
- [“Known issues and limitations” \(page 61\)](#)
- [“Customer service” \(page 85\)](#)

DRAFT

Important notices

This section describes the supported and unsupported hardware and software features in the Ethernet Routing Switch 8600 Software Release 7.0, and provides important information for this release.

Navigation

- [“Software licensing” \(page 18\)](#)
- [“File names for this release” \(page 18\)](#)
- [“Important information and restrictions” \(page 21\)](#)
- [“Supported software and hardware scaling capabilities” \(page 38\)](#)
- [“Hardware and software compatibility” \(page 41\)](#)
- [“Module type and feature compatibility” \(page 44\)](#)
- [“High Availability mode considerations” \(page 45\)](#)
- [“Ongoing considerations” \(page 46\)](#)
- [“Module and chassis compatibility and performance considerations” \(page 46\)](#)
- [“Switch clustering topologies and interoperability with other products” \(page 48\)](#)
- [“SF/CPU protection and loop prevention compatibility” \(page 49\)](#)
- [“Switch behavior during boot cycle and redundant configuration files” \(page 49\)](#)
- [“MPLS considerations” \(page 53\)](#)
- [“SNMP considerations” \(page 53\)](#)
- [“VLACP considerations” \(page 53\)](#)
- [“DVMRP considerations” \(page 54\)](#)
- [“SMLT considerations” \(page 54\)](#)
- [“60 day trial license” \(page 55\)](#)

- “Advanced filter guidelines” (page 55)
- “Supported standards, RFCs, and MIBs” (page 56)
- “Supported traps and notifications” (page 56)

Software licensing

The following table describes the license required to use specific features.

For more information about using the License Bank, see *Nortel Ethernet Routing Switch 8600 Administration* (NN46205-605).

Table 1
License and features

Base license	Advanced license	Premier license
<ul style="list-style-type: none"> • Basic features • IPv6 management • BGPv4 for up to 10 peers 	<ul style="list-style-type: none"> • all Base License features • Border Gateway Protocol version 4 (BGPv4) for more than 10 Peers • Bidirectional Forwarding Detection (BFD) • IPv6 Routing • Multicast Source Discovery Protocol (MSDP) • Packet Capture function (PCAP) 	<ul style="list-style-type: none"> • all Advanced License features • Virtual Routing and Forwarding, Lite version (VRF-Lite) • Multi-Protocol Border Gateway Protocol (MP-BGP) • IP-Virtual Private Network, Multi-Protocol Label Switching (RFC2547) (IP-VPN MPLS RFC2547) • IP-Virtual Private Network-Lite (IP-VPN-Lite – IP in IP) • Multicast virtualization for VRF-Lite (IGMP and PIM-SM/SSM)

Release 7.0 features are addressed under existing licenses.

Ethernet Routing Switch 8600 Release 5.1 and above includes a Premier trial license that is valid for 60 days from the date of install. After 60 days, the license expires and licensed features are no longer available after the system restarts.

File names for this release

This section describes the Ethernet Routing Switch 8600 Software Release 7.0 software files.

Before you upgrade, verify the MD5 signature for each new file. For upgrade procedures, see *Nortel Ethernet Routing Switch 8600 Upgrades — Software Release 7.0 (NN46205-400)*.

Table 2
Release 7.0 software files

Module or file type	Description	File name	Size in bytes
Software tar file	Tar file of all software deliverables (includes images that also contain encryption software)	pr86_7000.tar.gz	51.2 M
Ethernet Routing Switch images			
Boot monitor image for 8692 SF/CPU	8692 CPU and switch fabric firmware	p80b7000.img	1.1 M
Boot monitor image for 8695 SF/CPU	8695 CPU and switch fabric firmware	p80be7000.img	1.2 M
Run-time image for 8692 SF/CPU	Run-time image for 8692 SF/CPU	p80a7000.img	13.5 M
Run-time image for 8695 SF/CPU	Run-time image for 8695 SF/CPU	p80ae7000.img	12.6 M
Run-time image for R modules	Image for R modules	p80j7000.dld	1.6 M
Run-time image for RS modules	Run-time image for RS modules	p80k7000.dld	1.6 M
Run-time image for Enterprise Enhanced SF/CPU Daughter Card (SuperMezz)	Image for the SuperMezz card	p80m7000.img	13.6 M
3DES for 8692 SF/CPU	Encryption module for privacy protocol with Secure Shell (SSH)	p80c7000.des	55 K
3DES for 8695 SF/CPU	Encryption module for privacy protocol with Secure Shell (SSH)	p80ce7000.des	51 K
AES for 8692 SF/CPU	Encryption module for privacy protocol with Secure Shell (SSH)	p80c7000.aes (this image includes the 3DES image)	25 K

Table 2
Release 7.0 software files (cont'd.)

Module or file type	Description	File name	Size in bytes
AES for 8695 SF/CPU	Encryption module for privacy protocol with Secure Shell (SSH)	p80ce7000.aes (this image includes the 3DES image)	21 K
MIB	MIB files	p80a7000.mib	4.7 M
MIB (zip file)	Zip file containing MIBs	p80a7000.mib.zip	749 K
MD5 checksum file	md5 checksums of all Release 7.0 software files	p80a7000.md5	1 K
Firmware images			
FOQ for R modules	Feedback output queueing FPGA firmware	foq267.xsvf	5.1 M
BMC for R modules	BAP memory controller FPGA firmware	bmc776.xsvf	2.5 M
DPC for R modules	Dual port controller FPGA firmware	dpc184.xsvf	2.5 M
PIM8630GBR	Programmable I/O module FPGA firmware; for the 8630GBR only	PI_769.xsvf	2.2 M
Firmware for RS modules	Contains FOQ, BMC, DPC, mirroring, and loopback images	rs_dpm_fpga.bin	4.3 M
PIM images for RS modules	PIM FPGA firmware required for 8612XLRS module only	pim8612XLRS.bin	59 K
	PIM FPGA firmware required for 8634XGRS module only	pim8634XGRS.bin	76 K
	PIM FPGA firmware required for 8648GBRS module only	pim8648GBRS.bin	78 K
	PIM FPGA firmware required for 8648GTRS module only	pim8648GTRS.bin	53 K
Trace files			
MPLS trace file	Trace file for MPLS. This is autogenerated and appears on the PCMCIA after upgrade.	nbpdtrc.lo0	variable

Table 2
Release 7.0 software files (cont'd.)

Module or file type	Description	File name	Size in bytes
EDM Help files			
EDM help files	Help files for EDM GUI	ers8600v7.0.0.0_Help.zip	2.8 M
ERS 8600 EDM plug-in for COM			
EDM plug-in for COM	EDM plug-in for COM	ers8600v7.0.0.0.war	

Important information and restrictions

This section contains important information and restrictions that you should consider before you upgrade to Release 7.0.

Fixes from previous releases

The Ethernet Routing Switch 8600 Software Release 7.0 incorporates all the fixes from release 4.1.x up to and including 5.1.2.0.

Important information and restrictions navigation

- [“SuperMezz, CPU memory, and upgrades” \(page 22\)](#)
- [“Compact flash card display on 8695 SF/CPU” \(page 22\)](#)
- [“Proper care of external compact flash and PCMCIA cards” \(page 22\)](#)
- [“EDM considerations” \(page 23\)](#)
- [“Installing EDM help files” \(page 24\)](#)
- [“I/O module considerations” \(page 25\)](#)
- [“MLT/LAG considerations” \(page 25\)](#)
- [“Console connection considerations” \(page 25\)](#)
- [“DHCP snooping considerations” \(page 25\)](#)
- [“MLT/LAG considerations” \(page 25\)](#)
- [“Supported upgrade paths” \(page 25\)](#)
- [“General upgrade considerations” \(page 26\)](#)
- [“Upgrade considerations for Release 7.0” \(page 26\)](#)
- [“Upgrading from 8692 SF/CPU with SuperMezz to 8695 CPU” \(page 26\)](#)
- [“Upgrade considerations: DOSFS with upgrades from pre-Release 5.0” \(page 27\)](#)

- “Upgrade considerations: Power Management” (page 28)
- “Upgrade considerations: IST” (page 31)
- “Pre-release 5.1 upgrades considerations: specifying license file location” (page 32)
- “Considerations for upgrades from 5.0.0.x release code” (page 32)

SuperMezz, CPU memory, and upgrades

To support Release 7.0, the 8692 SF/CPU must be equipped with SuperMezz. 8692 SF/CPU without SuperMezz is not supported with Release 7.0. If the Release 7.0 software is booted with a non-SuperMezz 8692 SF/CPU, the line cards do not come online.

For Release 5.0 or later, Nortel recommends that the PCMCIA card for the 8692 SF/CPU with SuperMezz be at least 256 MB. (The 8695 SF/CPU comes with a 2 GB compact flash card.)

Compact flash card display on 8695 SF/CPU

The current 8692 with SuperMezz displays the external flash card as `/pcmcia`. The 8695 has a compact flash installed, but also displays the flash card as `/pcmcia`.

Proper care of external compact flash and PCMCIA cards

Do not remove the external compact flash or the PCMCIA before it is synchronized. To guarantee the external memory is in a consistent state before you remove it, use one of the following commands.

- `pcmcia-stop` (on 8692 SF/CPU)
- `dos-stop /pcmcia` (on 8695 SF/CPU)

Be sure to back up all configurations, as all files are lost if the card is corrupted.

To check and optionally repair a file system, you can use the `dos-chkdsk <device> repair` command (on all SF/CPU).

If the file system cannot be repaired, you must reformat the device using the `dos-format <device>` command (on all SF/CPU).

Both of the above commands delete all information on the memory, so be sure to backup all information before using either of the commands.

The above commands are available in the CLI or the boot monitor.

EDM considerations

For Enterprise Device Manager (EDM) to display and function correctly, use one of the following Web browsers:

- Mozilla Firefox, version 3.0
- Microsoft Internet Explorer, version 7.0

In EDM, the option for saving runtime configuration changes is not easily seen. To save current changes, go to **Configuration > Edit > Chassis** and under ActionGroup1, click on **SaveRuntimeConfig** and click **Apply**. (Q02114591)

In some cases, EDM functionality differs from that offered in Java Device Manager (JDM), including the following:

- **Single username and password combination for each VRF** With EDM, you cannot configure more than one username and password combination on each VRF.

- **RADIUS authentication**

The on-box EDM GUI does not support login using RADIUS authentication. Login with RADIUS authentication is supported using Configuration and Orchestration Manager (COM) with the off-box Ethernet Routing Switch 8600 EDM plug-in. (Q02060042)

- **CLI window launch**

On-box EDM is a browser-based solution that can run from any platform (Windows or Linux) and it does not offer the capability to launch a Windows-based command prompt window. In the COM with off-box Ethernet Routing Switch 8600 EDM plug-in, the CLI manager exists to launch CLI windows as needed.

- **Managing VRFs**

With on-box EDM, you cannot manage multiple VRFs from the GRT instance. To manage different VRFs, you must log out of the GRT instance and log in to the desired VRF. You can manage different VRFs using COM with the off-box EDM plug-in. Using the off-box EDM plug-in, you can switch VRF contexts from the GRT. (Q02100808)

- **Multiple port selection**

Multiple-port selection or monitoring is not supported in on-box EDM for this release.

As a workaround for monitoring multiple ports, you can select multiple ports, then undock the tabs for each port, placing the windows side-by-side. Using the off-box EDM plug-in, you can select multiple ports. (Q02100807)

Using the EDM plug-in with COM

The Configuration and Orchestration Manager (COM) is a Nortel off-box network management tool that supports an EDM plug-in for the Ethernet Routing Switch 8600. The EDM plug-in allows you to perform EDM functions within the off-box COM tool. For information on installing the EDM plug-in for COM, see *Nortel Configuration and Orchestration Manager Using the Product Interfaces* (NN47226-100).

To obtain the EDM plug-in software, go to the Nortel Technical Support site at www.nortel.com/support and choose **Network Management** and then **Configuration and Orchestration Manager**.

Installing EDM help files

While the EDM GUI is bundled with the Ethernet Routing Switch 8600 software, the associated EDM help files are not included. To access the help files from the EDM GUI, you must install the EDM help files on a TFTP or FTP server in your network.

Use the following procedure to install the EDM help files on a TFTP or FTP server.

Do not install the EDM help files on PCMCIA or Flash.

Step	Action
1	Retrieve the EDM help zip file from nortel.com or from the software CD.
2	On a TFTP or FTP server that is reachable from your 8600 switch, create a directory named: ERS8600_70_Help. If you are using FTP for this installation, be sure that the 8600 switch is configured with the appropriate host name and password using the <code>config bootconfig host user</code> and <code>config bootconfig host password</code> commands (or, using the NNCLI, <code>boot config host user</code> and <code>boot config host password</code>).
3	Unzip the EDM help zip file in the new FTP or TFTP server directory.
4	Using EDM on the 8600 switch, open the following folders: Configuration, Security, Control Path.
5	Double-click General .
6	Click the Web tab.
7	In the HelpTFTPSourceDir field, enter the FTP or TFTP server IP and the path of the online directory

where the files are unzipped, in the following format:
<TFTP-server-IP-address>:/ERS8600_70_Help.

- 8 To test that the help is working properly, select any tab (for example, **Edit > Chassis**) and click the **Help** button.

The appropriate EDM help page appears.

--End--

I/O module considerations

The 8648GTR module does not support packets larger than 9188 bytes at 100 Mbps. At 1000 Mbps, frames larger than 9188 bytes are supported.

MLT/LAG considerations

To maintain LAG stability during failover, use CANA: configure the advertised speed to be the same for all LACP links. For 10/100/1000 Mbps ports, ensure that CANA uses one particular setting, for example, 1000-full or 100-full. Otherwise, a remote device could restart Auto-Negotiation and the link could use a different capability.

It is important that each port uses only one speed and duplex mode. This way, all links in Up state are guaranteed to have the same capabilities. If Auto-Negotiation and CANA are not used, the same speed and duplex mode settings should be used on all ports of the MLT.

Console connection considerations

If you change the management IP setting using EDM or an SNMP device, the active console session is terminated. In this case, you must reopen the console session.

DHCP snooping considerations

When configuring DHCP snooping to utilize a remote DHCP server (DHCP Relay), you must ensure that the routing interfaces where the DHCP offer is received are configured as DHCP snooping trusted ports. This applies to all return paths; that is, primary and backup routing interfaces.

Supported upgrade paths

The Ethernet Routing Switch 8600 Software Release 7.0 supports upgrades from the following earlier releases:

- 4.1.8.2
- 4.1.8.3
- 5.0.1.x
- 5.1.x

If you want to upgrade to release 7.0 from any other release, first upgrade to one of the above releases and then upgrade to 7.0.

General upgrade considerations

The configuration file generated with Ethernet Routing Switch 8600 Software Release 7.0 and later contains options that are not backward-compatible with any previous Ethernet Routing Switch 8600 Software Releases.

Loading a Release 7.0 or later configuration file on a pre-7.0 runtime image generates errors and causes the image to stop loading the configuration file. The system will load with a default configuration.

Downgrades require previously saved configuration files (boot.cfg and config.cfg) and may require the removal of R and RS modules prior to downgrade.

Upgrade considerations for 8692 SF/CPU with SuperMezz

With an 8692 SF/CPU with SuperMezz enabled, the time needed to copy all the required upgrade images from a TFTP server to the SF/CPU (flash or PCMCIA) can be up to several minutes.

If you first disable SuperMezz or boot the software into monitor mode, the file transfer takes much less time.

Upgrade considerations for Release 7.0

Before you upgrade, read *Nortel Ethernet Routing Switch 8600 Upgrades — Software Release 7.0* (NN46205-400) and follow the outlined procedures.

If you are upgrading from a release prior to 5.0, you must reformat the DOSFS for the PCMCIA and flash. Steps are included in the upgrade procedures. See [“Upgrade considerations: DOSFS with upgrades from pre-Release 5.0”](#) (page 27).

You must take into consideration Power Management for this release; for more information, see [“Upgrade considerations: Power Management”](#) (page 28).

Upgrading from 8692 SF/CPU with SuperMezz to 8695 CPU

Use the following steps to upgrade from 8692 SF/CPU with SuperMezz to 8695 CPUs.

Note that the Ethernet Routing Switch 8600 must be running 7.0 code.

Step	Action
1	Disable the slot for the slave CPU.
2	Remove the slave 8692 SF/CPU with SuperMezz.
3	Insert the 8695 SF/CPU and stop at the boot monitor.
4	Copy the configuration file, boot configuration file, and images to the 8695 SF/CPU (use the internal IP for copy: 127.0.0.X - Where X=Slot # of CPU).
5	Boot the 8695 SF/CPU with correct images and configuration files.
6	Perform a failover from the master 8692 SF/CPU using the <code>config sys set action cpuswitchover</code> command.
7	Once the 8695 SF/CPU takes over, remove the slave 8692 SF/CPU with SuperMezz and insert another 8695 SF/CPU and stop at the boot monitor.
8	Copy the configuration file, boot configuration and images to the 8695 SF/CPU (use the internal IP for copy: 127.0.0.X)
9	Boot the 8695 SF/CPU with correct images and configuration files.

--End--

Upgrade considerations: DOSFS with upgrades from pre-Release 5.0

Release 5.0 introduced a unique signature to the Disk Operating System File System (DOSFS) volume label generated during `dos-format` and `format-flash` operations. This label provides clear identification about which DOSFS devices have been formatted with the latest DOSFS source code.

When you upgrade from pre-Release 5.0 software and boot an image with Release 7.0 or later, you may see boot messages like:

```
The /flash device mounted successfully, but it appears to have
been formatted with pre-Release 5.0 file system code.  Nortel
recommends backing up the files from /flash, and executing
dos-format /flash to bring the file system on the /flash device
to the latest ERS8600 baseline.
```

If you receive this message, Nortel recommends that you perform a one-time reformat of the DOSFS device (using `dos-format`) to set the DOSFS baseline. This is part of the upgrade procedures.

The one-time DOS reformat erases all files on the DOSFS device. Nortel recommends that you back up all files from the DOSFS device, reformat the device, and replace all files.

Be sure to back up hidden files as well. For information on hidden files, see *Nortel Ethernet Routing Switch 8600 Upgrades — Software Release 7.0* (NN46205-400).

Upgrade considerations: Power Management

The addition of the Power Management feature to Release 5.0 may require you to take special steps before you upgrade.

When you upgrade to Release 7.0 or later, Power Management is enabled by default. If Power Management detects that there are not enough power supplies in the system to successfully run the system, it shuts down the lowest-priority modules. This does not occur if you have enough available power.

You can calculate the number of power supplies required for your Ethernet Routing Switch 8600 system. To determine the number of power supplies required for your switch configuration, use the *Nortel ERS8600 Power Supply Calculator* (NN48500-519). This is available on the Nortel Technical Support Web site at www.nortel.com/documentation. Choose Routers & Routing Switches, and then Ethernet Routing Switch 8600. In the Documentation, Operations section, click the Configuration link. Navigate through the list until you find the calculator.

For Power Management configuration and conceptual information, see *Ethernet Routing Switch 8600 Administration* (NN46205-605).

Power Management operations

With Power Management, when the switch boots, users are notified if there is redundant power available in the system. This notification is based on the available power provided by the power supplies as compared to the power requirements of the installed modules.

R and RS modules are not brought up if there is insufficient power available. Although there is an override capability available, this should only be used for short periods of time or in emergencies—operating a chassis in an underpowered condition can lead to unpredictable results. Power management does not apply to switch fabric modules (8692 SF/CPU or 8695 SF/CPU).

The amount of system power is calculated based on the number, type, and input source voltage of the power supplies in the chassis. For 8005AC or 8005DI AC supplies, the system detects whether the supply is sourced

with 110 V or 220 V and uses the corresponding output power. For all other power supplies, the power output is the same, regardless of source voltage.

Switch fabrics are allotted highest priority and always power up. R and RS modules power up if there is sufficient power remaining to do so. If there is insufficient power to bring all R and RS modules online, they are powered up based on slot priority. By default, R and RS modules are powered up starting at slot 1 until there is insufficient power to bring the next module online.

If a chassis boots up and there are modules that are not online due to insufficient power, adding an additional power supply does not bring the modules online automatically. To bring the modules online, the system must be rebooted, or the module must be removed and reinserted into the chassis.

If a system boots and power supply failure occurs, one of the two following conditions result:

1. A system with redundant power continues to operate normally. The redundant power configuration compensates for a power supply failure.
2. A system with no redundant power continues to operate, however, if there is insufficient power to support all modules, an SNMP trap and syslog message are sent every five minutes notifying the user that the system is operating in an underpowered condition. This situation must be corrected as soon as possible.

Disabling power and cooling management

Disable Power Management to successfully upgrade even though not enough power supplies are installed to run all I/O modules.

If you already have enough power supplies, you do not need to disable Power Management.

You can calculate the number of power supplies required for your Ethernet Routing Switch 8600 system. To determine the number of power supplies required for your switch configuration, use the *Power Supply Calculator for ERS 8600* (NN48500-519). This is available on the Nortel Technical Support Web site at www.nortel.com/documentation. Choose Routers & Routing Switches, and then Ethernet Routing Switch 8600.

ATTENTION

Nortel recommends that you do not disable Power Management, and that you instead install the required power supplies before upgrade. However, if you must disable Power Management for a short period of time, install the required supplies as quickly as possible.

RS modules do not come up when the high-speed cooling module is not installed.

ATTENTION

Although you can override the fan check for the high-speed cooling module, this should only be done for short periods of time or in emergencies—operating a chassis with RS modules without the high-speed cooling module can lead to unpredictable results.

Step	Action
1	Save the pre-7.0 configuration file. <code>save config.cfg</code>
2	Edit the configuration file offline using an editor like VI or EMACS. You can either: <ul style="list-style-type: none">• Use the CLI to edit the file on the switch (the switch has a built-in VI-like editor). Use the <code>edit config.cfg</code> command.• Save the file as an ASCII file and transfer to another device for editing with a text editor like Notepad.• Transfer the file to a device and edit with VI or EMACS-like editor.
3	In the configuration file, add the following lines to the end of the flags section: <code>#!power power-check-enable false</code> <code>#!power fan-check-enable false</code> See the following job aid for an example of correct placement of these commands.
4	Save the file and, if you edited it off-switch, transfer the file back to the switch to use in the upgrade.

--End--

Job aid: configuration file and command placement

```

#
# MON MAY 19 22:43:41 2008 UTC
# box type : ERS-8010
# software version : REL5.0.0.0_B006
# monitor version : 5.0.0.0/006
# cli mode : 8600 CLI
#
#
# Asic Info :
# SlotNum|Name |CardType |MdaType |Parts Description
#
# Slot 1 -- 0x00000001 0x00000000
# Slot 2 -- 0x00000001 0x00000000
# Slot 3 -- 0x00000001 0x00000000
# Slot 4 8630GBR 0x2432511e 0x00000000 RSP=25 CLUE=2 F2I=1 F2E=1
FTMUX=17 CC=3 FOQ=266 DPC=184 BMC=776 PIM=257 MAC=4
# Slot 5 8692SF 0x200e0100 0x00000000 CPU: CPLD=19 MEZZ=4 SFM:
OP=3 TMUX=2 SWIP=23 FAD=16 CF=56
# Slot 6 -- 0x00000001 0x00000000
# Slot 7 -- 0x00000001 0x00000000
# Slot 8 -- 0x00000001 0x00000000
# Slot 9 -- 0x00000001 0x00000000
# Slot 10 -- 0x00000001 0x00000000
#
#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!flags r-mode false
#!resource-reservation max-vlan false
#!resource-reservation multicast 2048
#!flags multicast-check-packet true
#!flags system-monitor true
#!record-reservation filter 4096
#!record-reservation ipmc 500
#!record-reservation local 2000
#!record-reservation mac 2000
#!record-reservation static-route 200
#!record-reservation vrrp 500
#!system-monitor monitoring-enable true
#!system-monitor detection-time 30
#!power power-check-enable false <----- ADD THIS LINE
#!power fan-check-enable false <----- ADD THIS LINE

```

Upgrade considerations: IST

After an IST peer is upgraded and restarted, wait until the entire system is stable prior to upgrading the other IST peer. Stabilization time depends on the complexity and size of the network (for example, the number of MAC and ARP records, routes, and the protocols used). Wait for the Layer 3

protocols, especially multicast protocols, to settle before you restart the other peer. If Layer 3 protocols are not in use, wait until the FDB and ARP tables on both peers report a similar number of entries.

Pre-release 5.1 upgrades considerations: specifying license file location

If you upgrade to release 7.0 or later from a release prior to 5.1, you must specify the location of your license file in the boot configuration file. If you do not specify the location of your license file, you can encounter issues with your licensed features.

Procedure steps

Step	Action
1	<p>To specify the license file location, enter the following CLI command:</p> <pre>config bootconfig choice primary license-file <file></pre> <p>OR</p> <p>enter the following NNCLI command:</p> <pre>(config)# boot config choice primary license-file <file></pre>
	--End--

Note: The variable '<file>' supports the following values for the source of a license file on an ERS8600 switch:

- /flash/<file_name>
- /pcmcia/<file_name>
- <a.b.c.d>:<file_name>

Considerations for upgrades from 5.0.0.x release code

Users should read and reference the latest version of CSB 2008008618, Software Life-Cycle Management for the ERS 8600 product, before deciding to move to any code release.

ATTENTION

For switch cluster systems running 5.0.0.x code (where x is less than 2), intermediate upgrades first to 5.0.0.2, then to one of 5.0.1.x, or 5.1.x are required, versus a direct upgrade to 7.0.0.0. If not performed, direct console access will be required to recover the 'peer' switch cluster system still running 5.0.0.x code, after the first switch is upgraded. Direct upgrades to release 7.0.0.0 are supported from 4.1.8.2, 4.1.8.3, 5.0.1.x, and 5.1.x.

When upgrading a pair of IST Core peer switches, special care must be taken due to SMLT architectural changes. When moving from 5.0.0.x code to 5.0.1.x (or 5.1.x) code, the IST peer switch operation will be different during the upgrade process. When the first peer switch is upgraded (secondary SF/CPU first, and then primary SF/CPU), this switch will go into an ALL port lock state, with the IST_MLT being the only links/ports up and active. The SMLT connected portion of the network will continue to operate on the second IST Core switch, still running the 5.0.0.x image. The user should now wait approximately 5 minutes until the following message is seen on the upgraded 5.0.1.x (or 5.1.x) switch:

```
CPU5 [05/15/08 05:33:55] MLT ERROR SMLT initial table sync is
delayed or failed. Please check the peer switch for any partial
config errors. All the ports in the switch except IST will remain
locked.
```

The second IST Core peer switch can then be upgraded. When the first switch, now running 5.0.1.x (or 5.1.x), sees its IST MLT connection go down, it unlocks all its ports and starts learning and then forwarding traffic. This upgrade process will cause some user traffic impact, even for the SMLT connected portion of the network. The second IST Core switch, after upgrading, should show the following messages in its log. These should be checked to confirm proper upgrade and operation:

```
CPU5 [06/05/08 05:05:45] MLT INFO SMLT MAC/ARP Sync Requested:
CAUTION do not take ANY action with the peer at this time
CPU5 [06/05/08 05:05:46] MLT INFO SMLT MAC /ARP Sync is Complete
: Peer can now be used normally
```

After both IST Core peer switches are upgraded and the network is running 'normally', it is now recommended to power-cycle (reboot only for single SF/CPU systems) the one peer switch which was upgraded first so that a complete sync occurs.

After upgrading to 5.0.1.x (or 5.1.x) code, the upgrade process to 7.0.0.0 returns to the behavior previously documented. When one IST Core peer switch is upgraded, the SMLT portion of the network will continue operation without user impact on the other IST Core peer. The second IST Core peer switch can then be upgraded in the same manner, resulting in little to no user traffic impact for the SMLT connected portion of the network.

ATTENTION

In the upgrade procedures, boot the Secondary SF/CPU first and then wait 10 seconds and then immediately boot the Master SF/CPU. Do NOT wait for the Secondary SF/CPU to come up completely before booting the Master SF/CPU, or the Secondary SF/CPU may hang.

This new upgrade operation affects SMLT based networks moving from 5.0.0.x code to 5.0.1.x (or 5.1.x) code.

If you are upgrading from 4.1.8.2, 4.1.8.3, 5.0.1.x, or 5.1.x to 7.0 code, these releases of code have similar SMLT enhancements and therefore a normal IST Cluster upgrade can be done.

Upgrades from 4.1.8.x to 5.0.0.x code are NOT supported.

Note: After upgrading there is a very small potential for invalid (but not operationally affecting) ARP entries to show up in the ARP table. These entries start with an IP address with the number 0 (0.x.x.x). Running the command `show ip arp info 0.` will show if such entries exist. If entries are returned, please contact Nortel Support and request Level 2 GNPS assistance.



CAUTION

If after upgrading to 5.0.1.x or 5.1.x code, you want to downgrade to some other 5.0.0.x code, that downgrade **MUST** be done to 5.0.0.2 code instead of 5.0.0.0 or 5.0.0.1 code. If present, the user may still use the same 5.0.0.0 or 5.0.0.1 config files when performing the downgrade but the downgrade code release must be 5.0.0.2. Downgrades from 5.0.1.x or 5.1.x to 4.1.x code are supported as normal. (Q01971801)

Configuration file modifications for BGP upgrades from release 4.x code



CAUTION

Users using BGP with release 4.x code need to be aware of the following limitations regarding upgrading to 5.x or later code release. For any user using the `add-as-path` command in 4.x or earlier releases, a direct upgrade to 5.x or later code (including 5.0.0.x, 5.0.1.0, 5.1.0.0, or 7.0.0.0 code) will create issues with your BGP operation, as the format for this command has changed in 5.x and all future code releases. The usage of this command can be confirmed by looking at your current 4.x based configuration file (`config.cfg` by default) by using either CLI command `show config` or `more /flash/config.cfg`, and looking for entries under:

```
# IP AS LIST CONFIGURATION #
```

Entries such as this indicate usage of the command:

```
ip as-list 1 create ip as-list 1 add-as-path 100
permit "64521"
```

With 5.x code, the two commands have been replaced by a single command of format:

```
ip as-list <as-list id; 1-1024> create <member id  
in as-path; 0-65535> permit "<as-path: 0-65535>"
```

Prior to upgrading to 5.x code, if such config entries are in a 4.x config file, those entries must be manually converted to 5.x or later format before upgrading; the upgrade to 5.x or later code does not convert this command structure properly. Since both the 4.x and 5.x code files are plain ASCII text, the 4.x config file can be copied to any text editor (or edited locally on the 8600 switch with its Unix VI editor), edited (for example with MS Word) and then copied back before upgrading.

For example, the above 4.x config example:

```
ip as-list 1 create ip as-list 1 add-as-path 100  
permit "64521"
```

Must be changed to the following 5.x config format:

```
ip as-list 1 create 100 permit "64521"  
(Q01977204)
```

SMLT switch cluster upgrade considerations

With SMLT switch cluster upgrades, to maintain remote Telnet access to the switches, you must follow specific upgrade steps in some scenarios when upgrading to any higher release of code.

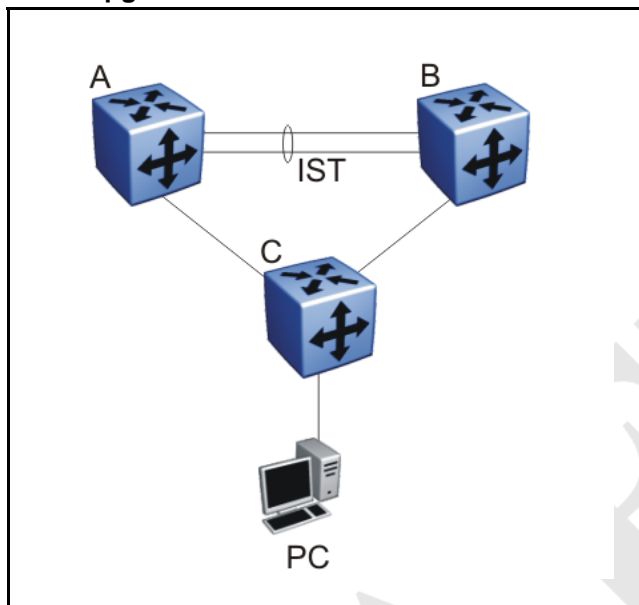
For device management during an upgrade, you can use one of the following options:

1. Direct serial console connection to the switch
2. Telnet access to the management IP
3. Telnet access to any of the in-band IP addresses on the switch

In scenarios 1 and 2, you can manage the switch effectively at all times during the upgrade, and therefore these scenarios require no additional considerations. However, in scenario 3, you can lose Telnet connectivity during the upgrade of the IST peers unless you follow the proper steps.

Consider the following figure, showing a triangle SMLT setup. In this case, the user intends to upgrade the IST peers (that are currently running 5.1.0.0) to 7.0.0.0.

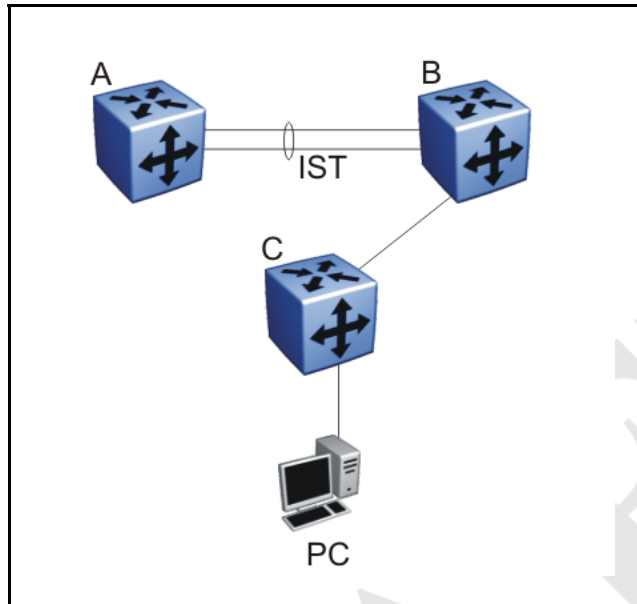
Figure 1
SMLT upgrade scenario



Assume the user Telnets from the PC to manage switch A and switch B. When the Telnet traffic generated by the PC arrives at switch C, depending on the MLT hashing algorithm, the traffic can be hashed to the link toward switch A or switch B. So, it is possible to have a situation where the Telnet management traffic destined for switch A flows through switch B and vice-versa.

Assume that the user upgrades switch A to 7.0.0.0. Due to the SMLT behavior, the network diagram now looks like the following figure.

Figure 2
SMLT upgrade scenario after upgrading switch A to 7.0.0.0



In this situation the PC cannot communicate with switch A, and as a result Telnet access to switch A is unavailable. For in-band management, you can alternatively Telnet first into switch B, and then Telnet to switch A from there.

The following are the recommended steps to perform this upgrade procedure while using Telnet in-band management:

1. Telnet to switch B from the PC
2. From switch B, Telnet to switch A
3. Upgrade switch A to 7.0.0.0, following the normal upgrade process. At this point, your Telnet session to switch A is lost, and eventually times out. After approximately a minute, Telnet to switch A again. This allows you to check the log messages on switch A. (At this point, you can possibly lose the Telnet connectivity to B in some situations depending on the MLT hashing occurring on switch C. If this occurs, re-open a Telnet connection to switch B.)
4. Upgrade switch B to 7.0.0.0 following the normal upgrade process. At this point, your Telnet session to switch B is lost. You can open a new Telnet session to switch A. After switch B completes the upgrade, you can then establish connectivity with switch B, either via Telnet from switch A, or via Telnet from the PC.

The same procedure applies for warm standby and hot standby scenarios. You must follow the upgrade directions for warm and hot standby cases provided in the upgrade document for individual chassis.

Note that you cannot use SSH in this upgrade scenario, as you cannot open SSH connections from one Ethernet Routing Switch 8600 to another. You must use Telnet.

Note: If switch A and switch B are running 5.0.0.x (where x is less than 2), the switches MUST be upgraded to 5.0.0.2 before upgrading to 5.0.1.0 (or 5.1.0.0), and then to 7.0.0.0.

Supported software and hardware scaling capabilities

The following table lists supported software and hardware scaling capabilities in Ethernet Routing Switch 8600 Software Release 7.0. The information in this table supersedes information contained in *Nortel Ethernet Routing Switch 8600 Planning and Engineering — Network Design* (NN46205-200), or any other document in the suite.

The capabilities described in this table are supported as individual protocols, not mixtures of protocols.

Nortel supports 25 Spanning Tree Groups (STG) in this release. Although you can configure up to 64 STGs (only 63 when a Web Switching Module is present), configurations including more than 25 STGs are not supported. If you need to configure more than 25 STGs, contact your Nortel Customer Support representative for more information about the support of this feature.

MLT is statically compliant with the 802.3ad standard (no support of LACP).

Table 3
Supported scaling capabilities

	Maximum number supported 8692SF with SuperMezz (R or RS series modules)
<i>Layer 2</i>	
MAC address table entries	64 000 32 000 when SMLT is used
VLANs (port- protocol-, and IEEE 802.1Q-based)	4000
IP subnet-based VLANs	800
Ports per Link Aggregation Group (LAG, MLT)	8
Aggregation groups 802.3ad aggregation groups Multi Link Trunking (MLT) group	128
SMLT links	128

Table 3
Supported scaling capabilities (cont'd.)

	Maximum number supported 8692SF with SuperMezz (R or RS series modules)
SLT (single link SMLT)	382
VLANs on SMLT/IST link	With Max VLAN feature enabled: 2000
RSMLT per VLAN	32 SMLT links with RSMLT-enabled VLANs
RSTP/MSTP (number of ports)	384, with 224 active. Configure the remaining interfaces with Edge mode
MSTP instances	32
<i>Advanced Filters</i>	
ACLs for each system	4000
ACEs for each system	1000
ACEs for each ACL	1000
ACEs for each port	2000: 500 inPort 500 inVLAN 500 outPort 500 outVLAN
<i>IP, IP VPN/MPLS, IP VPN Lite, VRF Lite</i>	
IP interfaces (VLAN- and brouter-based)	1972
VRF instances	255
ECMP routes	5000
VRRP interfaces	255
IP forwarding table (Hardware)	250 000
BGP/mBGP peers	250
iBGP instances	on GRT
eBGP instances	on 256 VRFs (including GRT)
BGP forwarding routes BGP routing information base (RIB) BGP forwarding information base (FIB)	BGP FIB 250 000 BGP RIB 500 000
IP VPN routes (total routes for each system)	180 000
IP VPN VRF instances	255
Static ARP entries	2048 per VRF 10 000 per system
Dynamic ARP entries	32 000
DHCP relay instances (total for all VRFs)	512

Table 3
Supported scaling capabilities (cont'd.)

	Maximum number supported 8692SF with SuperMezz (R or RS series modules)
Static route entries	2000 per VRF 10 000 per system
OSPF instances for each switch	on 64 VRFs (including GRT)
OSPF areas for each switch	5 per VRF 24 per system
OSPF adjacencies for each switch	80 200 per system
OSPF routes	20 000 per VRF 50 000 per system
OSPF interfaces	500 500 per system
OSPF LSA packet maximum size	6000 bytes
RIP instances	on 64 VRFs (including GRT)
RIP interfaces	200
RIP routes	2500 per VRF 10 000 per system
<i>Multiprotocol Label Switching</i>	
MPLS LDP sessions	200
MPLS LDP LSPs	16 000
MPLS RSVP static LSPs	200
Tunnels	2500
<i>IP Multicast</i>	
DVMRP passive interfaces	1200
DVMRP active interfaces/neighbors	80
DVMRP routes	2500
PIM instances	on 64 VRFs (including GRT)
PIM active interfaces	200 (200 for all VRFs)
PIM passive interfaces	1972 (2000 for all VRFs)
PIM neighbors	80 (200 for all VRFs)
MSDP peers	20
MSDP maximum SA messages	6144
Multicast streams: with SMLT/ without SMLT	2000/4000
Multicast streams per port	1000

Table 3
Supported scaling capabilities (cont'd.)

	Maximum number supported 8692SF with SuperMezz (R or RS series modules)
IGMP reports/sec	250
<i>IPv6</i>	
IPv6 interfaces	250
IPv6 tunnels	350
IPv6 static routes	2000
OSPFv3 areas	5
OSPFv3 adjacencies	80
OSPFv3 routes	5000
<i>Operations, Administration, and Maintenance</i>	
IPFIX	384 000 flows per chassis
RMON alarms with 4000K memory	2630
RMON events with 250K memory	324
RMON events with 4000K memory	5206
RMON Ethernet statistics with 250K memory	230
RMON Ethernet statistics with 4000K memory	4590

Hardware and software compatibility

The following table describes your hardware and the minimum Ethernet Routing Switch 8600 software version required to support the hardware.

Table 4
Chassis, power supply, and SF/CPU compatibility

Item	Minimum software version	Part number
Chassis		
8010co	10-slot	3.1.2 DS1402004-E5 DS1402004-E5GS
8010	10-slot	3.0.0 DS1402001-E5 DS1402001-E5GS

Table 4
Chassis, power supply, and SF/CPU compatibility (cont'd.)

Item			Minimum software version	Part number
Chassis				
	8006	6-slot	3.0.0	DS1402002-E5 DS1402002-E5GS
	8003-R	3-slot	7.0.0.0	DS1402011-E5
Switching fabric/CPU				
	8692 SF/CPU	Switching fabric	Unsupported in release 7.0 and above.	DS1404065-E5
	8692SFw/SuperMezz	8692SF Switch Fabric/CPU with factory-installed Enterprise Enhanced CPU Daughter Card (SuperMezz).	4.1.0	DS1404066-E5
	Enterprise Enhanced CPU Daughter Card (SuperMezz)	Optional daughter card for the 8692 SF/CPU	4.1.0	DS1411025-E5
	8695 SF/CPU	Switching fabric	7.0	DS1404120-E5
Power supplies				
	8004AC	850 W AC	3.1.2	DS1405x08
	8004DC	850 W DC	3.1.2	DS1405007
	8005AC	1462 W AC	4.0.0	DS1405012
	8005DI AC	1462 W Dual input AC	5.0	DS1405018-E6
	8005DI DC	1462 W Dual input DC	5.1	DS1405017-E5
	8005DC	1462 W DC	4.0.x	DS1405011

Table 5
Module and component compatibility

Modules and components			Minimum software version	Part number
Ethernet R modules				
	8630GBR module	30-port Gigabit Ethernet SFP	4.0.0	DS1404063

Table 5
Module and component compatibility (cont'd.)

Modules and components			Minimum software version	Part number
	8648GTR module	48-port 10/100/1000BASE-TX	4.0.x	DS1404092
	8683XLR module	3-port XFP (10.3125 Gb/s LAN PHY)	4.0.0	DS1404101
	8683XZR module	3-port XFP (10.3125 Gb/s LAN PHY and 9.953 Gb/s WAN PHY)	4.1.0	DS1404064
Ethernet RS modules				
	8648GTRS	48-port 10/100/1000 Mbps copper ports	5.0.0	DS1404110-E6
	8612XLRS	12-port 10 GbE LAN module	5.0.0	DS1404097-E6
	8634XGRS	24 100/1000 Mbps SFP ports 2 XFP ports 8 10/100/1000 Mbps copper ports	5.0.0	DS1404109-E6
	8648GBRS	48 100/1000 Mbps SFP ports	5.0.0	DS1404102-E6
Small form factor pluggable transceivers				
	1000BASE-SX SFP	850 nm LC connector	4.0.0	AA1419013-E5
	1000BASE-SX SFP	850 nm MT-RJ connector	4.0.0	AA1419014-E5
	1000BASE-LX SFP	1310 nm LC connector	4.0.0	AA1419015-E5
	1000BASE-XD CWDM SFP	From 1470 nm to 1610 nm LC connector	4.0	AA1419025-E5 to AA1419032-E5
	1000BASE-ZX CWDM SFP	From 1470 nm to 1610 nm LC connector	4.0	AA1419033-E5 to AA1419040-E5
	1000BASE-T SFP	Category 5 copper unshielded twisted pair (UTP), RJ-45 connector	4.0.0	AA1419043-E6
	1000BASE-SX SFP	850 nm DDI LC connector	5.0	AA1419048-E6
	1000BASE-LX SFP	1310 nm DDI LC connector	5.0	AA1419049-E6
	1000BASE-XD SFP	1310 nm DDI LC connector	5.0	AA1419050-E6

Table 5
Module and component compatibility (cont'd.)

Modules and components			Minimum software version	Part number
	1000BASE-XD SFP	1550 nm DDI LC connector	5.0	AA1419051-E6
	1000BASE-ZX SFP	1550 nm DDI LC connector	5.0	AA1419052-E6
	1000BASE-XD CWDM SFP	From 1470 nm to 1610 nm, DDI	5.0	AA1419053-E6 to AA1419060-E6
	1000BASE-ZX CWDM SFP	From 1470 nm to 1610 nm, DDI	5.0	AA1419061-E6 to AA1419068-E6
	1000BASE-BX bidirectional SFP	1310 nm, single fiber LC, up to 10 km	4.1.0	AA1419069-E6
	1000BASE-BX bidirectional SFP	1490 nm, single fiber LC, up to 10 km	4.1.0	AA1419070-E6
	1000BASE-BX bidirectional SFP	1310 nm, single fiber LC , up to 40 km	7.0	AA1419076-E6
	1000BASE-BX bidirectional SFP	1490 nm, single fiber LC, up to 40 km	7.0	AA1419077-E6
	1000BASE-EX	1550 nm, up to 120 km	5.0	AA1419071-E6
10 Gigabit Ethernet Small form factor pluggable transceivers				
	10GBASE-LR/LW XFP	1-port 1310 nm SMF, LC connector	4.0.0	AA1403001-E5
	10GBASE-ER/EW XFP	1-port 1550 nm SMF, LC connector	4.0.x	AA1403003-E5
	10GBASE-SR/SW XFP	1-port 850 nm MMF, LC connector	4.0.0	AA1403005-E5
	10GBASE-ZR/ZW XFP	1550 nm SMF LC connector	4.1.0	AA1403006-E5
	10GBASE-LRM XFP	Up to 220 m over MMF, DDI	5.0.0	AA1403007-E6

Module type and feature compatibility

The following table shows the supported features for each module.

Feature	Module types	Comment
	R and RS	
ACL IN L2 to L4	yes	Ingress filtering ACT, ACL, ACE based
ACL OUT L2 to L4	yes	Egress filtering ACT, ACL, ACE based
ACL pattern matching	yes	Pattern match filtering for ingress and egress
Ingress policing L2 to L4	yes	450 policers per LANE (10x1 Gb/s, 1x10 Gb/s), total 10 800 policers
Egress shaping L2 to L4	yes	per port shapers, per queue shapers
Egress queues 64	yes	640 queues per LANE (10x1 Gb/s, 1x10 Gb/s), total 15 360 queues
SMLT over 10 Gbps	yes	in any mode available (8683XLR required)
Port mirroring	yes	Ingress R and RS modules: up to 20 ports per LANE Egress R module: 1 port per LANE; Egress RS module, up to 20 ports per LANE
SVLAN	no	
IPX routing	no	

High Availability mode considerations

High Availability mode (also known as HA-CPU) permits the synchronization of configuration and protocol states between the Master and Secondary CPUs.

For Release 7.0, HA-CPU supports the following in Hot Standby mode:

- platform configuration
- Layer 2 protocols: IGMP, STP, MLT, SMLT, ARP, LACP, VLACP
- Layer 3 protocols: RIP, OSPF, VRRP, RSMLT, VRF Lite

HA-CPU supports the following in Warm Standby mode. After failover, these protocols are restarted:

- DVMRP, PIM-SM, PIM-SSM
- BGP
- MPLS
- BFD
- IPv6

Hot Standby mode performs hitless failover, while Warm Standby mode restarts protocols after failover.

A reboot is necessary to make HA-CPU mode active.

HA-CPU does not currently support the following protocols or modules:

- PGM

In HA mode, Nortel recommends that you do not configure the OSPF Hello timers for less than one second, and the dead router interval for less than 15 seconds (Q01445505).

When using the CLI or NNCLI on a dual-CPU system with HA mode enabled, do not enter configuration commands on the Standby SF/CPU. Execute all configuration commands on the Master SF/CPU only.

If you use Layer 3 multicast routing protocols in HA mode, it takes approximately 30 seconds for the routing protocols to re-converge after an HA failover. This behavior occurs because multicast protocols are only partially supported by Release 7.0, and thus PIM and DVMRP are restarted upon failover. When PIM is enabled, it takes the same amount of time (approximately 30 seconds) to come up.

HA mode and short timers

Prior to Release 5.0, protocols that used short timers could bounce (restart) during HA failover. These protocols include VLACP, LACP, VRRP, OSPF, and STP. Release 5.0 and later support fast failover for configurations that use short timers. In Release 5.0 and later:

- all HA configurations that use R or RS modules, along with the 8692 SF/CPU with SuperMezz or the 8695 SF/CPU, support protocols with short timers. Fast failover under these conditions is supported.
- all HA configurations that use R or RS modules, along with the 8692 SF/CPU without SuperMezz or the 8695 SF/CPU support protocols with short timers. Fast failover under these conditions is supported.

Ongoing considerations

The following sections describe considerations that are not new for Release 7.0.0.0, but which still apply for 7.0.0.0.

Module and chassis compatibility and performance considerations

Release 7.0 and later do not support classic modules. Only R and RS line card modules are supported with release 7.0 and later. Also, the 8003 chassis is not supported with release 7.0 or later. The 8003-R chassis replaces the 8003 chassis.

For switch fabric modules, only the 8692 with SuperMezz and 8695 CP/SF are supported with release 7.0 and later.

In older chassis (those shipped before 2005), there is a difference between Standard and High Performance slots. In these chassis, an R or RS module installed in a Standard slot delivers increased port density. An R or RS module installed in a High Performance slot delivers increased port density and increased performance. Chassis manufactured in 2005 and later do not have this limitation, and have full high-performance slot support.

In older chassis, R and RS modules inserted in slots 2 to 4 and slots 7 to 9 of the 8010 10-slot chassis, and slots 2 to 4 of the 8006 6-slot chassis, always operate at high performance. R modules inserted into slot 1 and slot 10 of the 8010 chassis, and slot 1 of the 8006 chassis, can operate at high performance, but operate at standard performance depending on chassis revision (for more information about identifying chassis, see the following section). For information about relative performance per slot with two fabrics installed in existing 8010, 8010co, and 8006 chassis, see the following table.

Table 6
Pre-2005 8010, 8010co, and 8006 chassis performance

Module	Standard slot (Slots 1 and 10) full duplex	High Performance slot (Slots 2 to 4, Slots 7 to 9) full duplex
8630GBR	16 Gbps	60 Gbps
8683XLR	16 Gbps	60 Gbps
8648GTR	16 Gbps	32 Gbps
8683XZR	16 Gbps	60 Gbps
8612XLRS	16 Gbps	60 Gbps
8648GTRS	16 Gbps	40 Gbps
8648GBRS	16 Gbps	60 Gbps
8634XGRS	16 Gbps	60 Gbps

If you place an R or RS module into a Standard slot of a non-high performance chassis, you receive the following message:

For maximum performance, Nortel recommends placing R modules in Slots 2 to 4 or 7 to 9 as available. Please refer to release notes for additional details.

High Performance chassis

A chassis revision with an upgraded High Performance Backplane is available. The High Performance chassis is compatible with existing R, and RS modules.

Identify the High Performance Backplane by using the CLI or NNCLI. Use the CLI command `show sys info` or the NNCLI command `show sys-info` to show the chassis revision number. The HwRev field indicates if the chassis is High Performance or Standard. The following table provides the Hardware Revision details for each chassis model. For more information, see the Technical Tip *Identifying the new Ethernet Routing Switch 8600 Chassis* (TT-0507501A) on the Nortel Technical Support Web site.

Table 7
Chassis hardware revision

Chassis model	Hardware Revision	H/W Config
8006	05 or greater indicates high performance chassis	02 or greater
8010	06 or greater indicates high performance chassis	02 or greater
8010co	05 or greater indicates high performance chassis	02 or greater

Customers requiring High Performance Mode for all slots on an older Ethernet Routing Switch 8600 chassis can have their existing chassis exchanged and reworked. Call 1-800-4NORTEL and order service part number N0060024. The list price for this chassis re-work is US \$2000.00 for each chassis, and an advanced replacement unit is provided.

Switch clustering topologies and interoperability with other products

When the Ethernet Routing Switch 8600 is used with other Ethernet Routing Switch products, the switch clustering bridging, unicast routing, and multicast routing configurations vary with switch type. Nortel recommends that you use the supported topologies and features when you perform inter-product switch clustering. For more information, see *Switch Clustering (SMLT/SLT/RSMLT/MSMLT) Supported Topologies and Interoperability with ERS 8600 / 5500 / 8300 / 1600* (NN48500-555), available on the Nortel Technical Support Web site.

For specific design and configuration parameters, see *Converged Campus Technical Solutions Guide* (NN48500-516) and *Switch Clustering using Split-Multilink Trunking (SMLT) Technical Configuration Guide* (NN48500-518).

SF/CPU protection and loop prevention compatibility

Nortel recommends several best-practice methods for loop prevention, especially in any Ethernet Routing Switch 8600 Switch cluster environment. For more information about loop detection and compatibility for each software release, see *Converged Campus Technical Solution Guide — Enterprise Solution Engineering* (NN48500-516).

Switch behavior during boot cycle and redundant configuration files

Nortel recommends that you take special care when providing the boot option for your production systems. The Ethernet Routing Switch 8600 provides three boot configuration file choices, as well as a backup configuration file choice for each configuration file choice.

The default boot sequence directs the switch to look for its image and configuration files first on the PCMCIA card, then in the onboard flash memory, and then from a server on the network. The switch first checks for `/pcmcia/pcmbboot.cfg` and then checks for `/flash/boot.cfg`.

The PCMCIA card is the primary source for the files; the onboard flash memory is the secondary source; and the network server is the tertiary source. These source and file name definitions are in the boot configuration file. The boot source order is configurable.

The `config.cfg` file stores the configuration of the Ethernet Routing Switch 8600 and its modules. This is the default configuration file. You can specify a different configuration file for the switch to use for the boot process.

For more details about boot sources, see *Nortel Ethernet Routing Switch 8600 Administration* (NN46205-605).

In normal operation, Nortel recommends that the primary configuration file is saved on the `/flash` drive, and that the primary backup configuration file is saved on the `/pcmcia` drive. Using this configuration, if one file or drive gets corrupted, the switch can still boot from the other file or drive. When you change configuration files, Nortel further recommends that you save the last known good configuration using the secondary choice option.



CAUTION

Risk of network outage

If a switch cannot access a valid configuration file, it will fall into default configuration mode, which can cause a network outage.

Ensure that a valid configuration and a backup configuration file are always available.

ATTENTION

If you want to store only one simple backup configuration file, Nortel recommends that you use a default backup configuration file with the following information (only) included:

```
config ethernet 1/1-10/48 state disable
```

This ensures that all ports remain disabled if the backup configuration file is loaded for any reason.

The information in the following table describes how the switch behaves in different boot situations. If a configuration file is unspecified, this means that the `config bootconfig choice` command was not provided for the file. The switch action column describes the expected behavior in both CLI and NNCLI modes, unless otherwise specified.

Table 8
Switch behavior during boot cycle

Parameters	Switch action
A configuration file is not specified. The config.cfg file is present on the flash drive.	The switch boots config.cfg
The primary configuration file is specified. The configuration file is present on the flash drive.	The switch boots the specified configuration file.
The primary configuration file is specified. The configuration file is not present on the flash drive.	The switch boots with factory defaults (if <code>config boot flags verify-config</code> is <code>true</code> , and a backup configuration is not specified).
The primary configuration file is specified. The configuration file on the flash drive has a bad command.	The switch boots with factory defaults (if <code>config boot flags verify-config</code> is <code>true</code> , and a backup configuration is not specified).
The primary configuration file is specified. The configuration file on the flash drive has a bad command. The backup configuration file is specified, but it has a bad command.	The switch fails the first configuration file, and boots the second configuration file, ignoring the bad command.

Parameters	Switch action
The switch is configured to boot with factory defaults.	The switch boots with factory defaults.
The boot.cfg file is corrupt.	In CLI mode: The switch fails to load the boot.cfg file and creates a new boot.cfg file with a default boot configuration. In NNCLI mode: The switch fails to load the boot.cfg file and creates a new boot.cfg file with a default boot configuration. The switch comes up in CLI mode, which is the correct behavior because the NNCLI mode flag is false by default.

Configuring primary, secondary, and tertiary boot sources

Configure the boot sources so that the switch uses proper files from which to boot.

Step	Action
1	<p>To change the runtime configuration file locations, use the following command:</p> <pre>config bootconfig choice <primary secondary tertiary> [config-file <file> backup-config-file <file> image-file <file>]</pre> <p>For example, to specify the configuration file in flash memory as the primary, use the following command:</p> <pre>ERS-8610:6# config bootconfig choice primary config-file /flash/config.cfg</pre>
2	<p>To set the location for the I/O module driver image for the BootStrap protocol:</p> <pre>config bootconfig bootp image-name <image-name> <slot-number></pre> <pre>config bootconfig bootp secondary-image-name <image-name> <slot-number></pre> <p>For example, to specify an R module driver for slot 2 in flash memory, use the following command:</p> <pre>ERS-8610:6# config bootconfig bootp /flash/p80j50 xx.dld 2</pre> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>ATTENTION Nortel recommends that you store .dld files in flash memory, and that you always set the image-name to default.</p> </div>
3	<p>To set the boot source location for the SuperMezz image:</p> <pre>config bootconfig mezz-image image-name <image-name></pre>

For example:

```
ERS-8610:6#config bootconfig mezz-image  
image-name /flash/p80m50xx.img
```

--End--

The following example configures the primary and secondary sources as per Nortel recommendations.

Step	Action
1	Configure the primary configuration file choices: <pre>config bootconfig choice primary config-file /flash/primaryconfig.cfg config bootconfig choice primary backup-config-file /pcmcia/primaryconfig.cfg</pre>
2	Configure the secondary configuration file choices: <pre>config bootconfig choice secondary config-file /flash/secondaryconfig.cfg config bootconfig choice secondary backup-config-file /pcmcia/secondaryconfig.cfg</pre>

--End--

OSPF warning message

When you enable OSPF on a VLAN or a brouter port, if no OSPF area is associated with the interface (that is, the OSPF area for the interface is 0.0.0.0), the following warning message is displayed:

When enabling OSPF for a VLAN, this automatically creates area 0.0.0.0 for the switch, which once the VLAN is active (VLAN has active ports) will result in the advertisement of area 0.0.0.0 by this switch. If this is not the users intent, care must be taken to place the VLAN into some other properly configured area. Area 0.0.0.0 will always be present for the switch, BUT this area will only be advertised if some active VLAN exists and is assigned to area 0.0.0.0, which is the default assignment.

MPLS considerations

The MPLS maximum transmission unit (MTU) is dynamically provisioned (1522 or 1950 bytes) and it supports jumbo frames (9000 bytes). Packets that exceed the MTU are dropped. The allowed data CE frame size is MTU size minus MPLS encapsulation (header) size. For control frames (for example, LDP) the frame size is 1522 or 1950 bytes.

For the Ethernet Routing Switch 8600, the MPLS RSVP LSP Retry Limit is infinite by design (a setting of zero means infinite). When the limit is infinite, should a Label Switched Path (LSP) go down, it is retried using exponential backoff. The Retry Limit is not configurable.

In scaled environments, if MPLS LDP sessions flap and CPU utilization increases, then the default Hello Hold Timer of 60 seconds may not be long enough. If this situation occurs, Nortel recommends that you increase the Hold Timer to 120 or 180 seconds.

SNMP considerations

Release 5.0 introduced changes to SNMP behavior. SNMP is configured differently in the NNCLI than in the CLI. Auto-generation of several parameters and command structure changes means that several configuration procedures are no longer required in the NNCLI. For more information:

- Refer to CR Q01858455.
- For SNMP trap changes, see the NNCLI SNMP trap configuration section in *Nortel Ethernet Routing Switch 8600 Troubleshooting* (NN46205-703).
- For SNMP community-based changes, see *Nortel Ethernet Routing Switch 8600 Administration* (NN46205-605) in this document.

VLACP considerations

Nortel recommends the following:

- The best practice standard settings for VLACP are a short timer of no less than 500 milliseconds and a time-out scale of 5. Both faster timers and lower time-out scales are supported, but if any VLACP flapping occurs, increase the short timer and the time-out scale to their recommended values: 5 and 500, respectively.
- Do not use VLACP on any configured LACP MLTs because LACP provides the same functionality as VLACP for link failure. VLACP and LACP running on the same link is not supported.

- VLACP with short timers is not supported on interswitch trunk (IST) links. Use only long timers. For IST links, Nortel recommends that you do not set the VLACP long periodic timer to less than 30 seconds.
- Although the software configuration supports VLACP short timers of less than 30 ms, using values less than 30 ms is not supported in practice. The shortest (fastest) supported VLACP timer is 30 ms with a timeout of 3, which is used to achieve sub-100 ms failover (see “VLACP sub-100 ms convergence using SuperMezz” (page 78)). 30 ms timers are not supported in High Availability (HA) mode, and may not be stable in scaled networks. At this time, 30 ms timers are only supported between two Ethernet Routing Switch 8600 switches.

For more information on VLACP best practices, see *Nortel Ethernet Routing Switch 8600 Planning and Engineering — Network Design* (NN46205-200).

DVMRP considerations

For Distance Vector Multicast Routing Protocol (DVMRP) configurations of more than 1000 streams, you may have to increase protocol timeouts (for example, OSPF dead interval, and so on). Otherwise, traffic loss can occur.

SMLT considerations

Software Release 7.0 does not support PIM Multicast Border Router (MBR) functionality over SMLT.

Nortel does not support an additional redundant MLT group between two IST peers.

To improve SMLT failover and recovery behavior for large-scale networks, Nortel has optimized the IST protocol and rearchitected the SMLT state machines. This functionality improvement is mainly targeted for large-scale SMLT networks, where Layer 2 bridging, Layer 3 routing with VRRP BackupMaster or RSMLT, and Multicast SMLT (IGMP and PIM) are required. Using these optimizations, failover and recovery improvements occur for networks in which IST switches handle more than 5000 MAC address table entries, 5000 ARP table entries, and 100 multicast streams.

For proper network behavior, Nortel recommends that you operate both IST switches with either the new or old SMLT architecture. That is, both switches on either end of an IST must use the same SMLT architecture and therefore the same software release version. Interconnected IST pairs may run different software release versions.

The SMLT re-architecture is supported in releases 4.1.8.2, 4.1.8.3, 5.0.1.0+, 5.1.0.0+, and 7.0.0.0+.

RSMLT considerations

In an RSMLT configuration, to ensure peer forwarding when the peer is down, enter save config after the peer information is first learned by both peers, or at any later time when the peer RSMLT information changes.

Whenever the peer RSMLT information changes (for example, from adding or deleting VLANs, changing VLAN IDs, or changing VLAN IP addresses), messages appear in the log indicating a discrepancy between stored information and what the switch is receiving from the peer. For example:

```
CPU6 [03/07/09 01:25:19] IP WARNING Recvd Peer address not same as
stored address for Vlan 544. Save config for Edge-Support to use
this info on next reboot
CPU6 [03/07/09 01:25:19] IP WARNING Recvd Peer address not same as
stored address for Vlan 536. Save config for Edge-Support to use
this info on next reboot
CPU6 [03/07/09 01:25:19] IP WARNING Recvd Peer address not same as
stored address for Vlan 535. Save config for Edge-Support to use
this info on next reboot
```

When the preceding messages appear in the log, if the peer goes down, the switch does not forward the traffic for its peer for the indicated VLANs unless the configuration is saved.

60 day trial license

You are provided a 60 day trial period of Ethernet Routing Switch 8600, during which you have access to all features. In the trial period you can configure all features without restriction, including system console and log messages. The switch logs trial period messages even if no license features are used or tested during the trial period. If any valid license is loaded on the switch at any time, none of the trial period messages are logged. At the end of the trial period, a message appears notifying the user that the trial period has expired.

For additional information about trial licenses, see *Nortel Ethernet Routing Switch 8600 Administration* ((NN46205-605)).

Advanced filter guidelines

Use the following guidelines when you configure advanced Layer 2 to Layer 7 filters for R or RS module ports or for VLANs with R or RS module ports in them.

- Always use an ACT with only the proper attributes selected. If you must add ACEs with attributes that are not in the original ACT, you must create a new ACL associated with the new ACT.
- For filter optimization reasons, when you have multiple ACEs that perform the same task (for example: deny or allow IP addresses,

or UDP/TCP-based ports), you can configure one ACE to perform the task with either multiple address entries, or address ranges, or a combination of both. You can use this one ACE instead of using multiple ACEs.

For R and RS module ACLs, a maximum of 500 ACEs are supported. This maximum may not be achievable depending on the type of attributes used within an ACE. Since there are millions of combinations, note that certain combinations can overextend the system. In these cases, to help ensure stable system operation, reduce the number of ACEs and follow the previous guidelines.

**CAUTION****Risk of module reset or improper load of configuration file**

If the following messages appear on the console or in the log file, it is likely that there is a specific problematic combination of ACEs configured within an ACL. Such combinations are very unlikely to occur, but if you see these messages, first reduce the number of ACEs within the ACL until the messages stop. Next, contact Nortel Technical Support. Support will attempt to find a combination that does not cause this situation, and will provide the required filtering capabilities.

```
CPU5 [05/23/06 10:51:08] COP-SW ERROR Slot 3:
ercdAddCollapseBin: rcdRspMalloc failed for
INGRESS RSP memory allocation
```

```
CPU5 [05/23/06 10:51:08] COP-SW ERROR Slot 3:
ercdGetCollapseNode: collapse node creation
failed.
```

```
CPU5 [05/23/06 10:51:08] COP-SW ERROR Slot 3: erc
dFilterRdxResultUpdate: ercdGetCollapseNode()
Failed !!
```

Supported standards, RFCs, and MIBs

For information about supported standards, RFCs, and MIBs, see the Appendices in *Nortel Ethernet Routing Switch 8600 Planning and Engineering — Network Design* (NN46205-200).

Supported traps and notifications

For a complete list of log messages generated by Ethernet Routing Switch 8600 Software Release 7.0, see *Nortel Ethernet Routing Switch 8600 Logs Reference* (NN46205-701).

For a complete list of SNMP traps generated by Ethernet Routing Switch 8600 Software Release 7.0, see *Nortel Ethernet Routing Switch 8600 Troubleshooting* (NN46205-703).

Resolved issues

This section details all issues resolved for Release 7.0.

Platform resolved issues

Table 9
Platform resolved issues

CR references	Description
Q02004992	With an HA-enabled switch in synchronized state, if you perform a soft reset on the master CPU (boot), the standby CPU may attempt to become the master. In this case, the master CPU boots and comes up as the standby, and the standby CPU comes up as the master. At this time, the new master shows synchronized state but the standby shows two-way active state, which is wrong.

Switch management resolved issues

Table 10
Switch management resolved issues

CR references	Description
Q01845752-02	For the Ext-CP Limit feature, the congested time (milliseconds) should approximate to the configured system minimum congestion timer (config sys ext-cp-limit min-congestion-time). The default value for this system timer is 3000 milliseconds. Total rxDrop will indicate how many packets have been dropped due to the congestion. Note that at this time, this parameter display may be inaccurate.
Q01972504-04	Connection of the Out-of-Band Ethernet Management port to an In-Band I/O port is not recommended, as erroneous behavior on this network, such as a loop, can cause issue with the operation of the SF/CPU module (either 8695 or any 8692 model). The most common issue seen is a loss of file management, and inability to access the /pcmcia directory. A SF/CPU re-boot or reset is need to clear the condition. The current suggestion to not see such issue is not NOT connect the OOB port to any In-band I/O port. Such a configuration actually provides no extra value to managing the network. The same functionality can be accomplished, without concern for see the above potential situation, by creating a "management" VLAN and assigning a "management" IP address to the VLAN. If OOB management is a desire, then a true OOB management

CR references	Description
	network should be created, and the switches In-Band I/O ports should NOT be part of such a network design.

MLT/SMLT resolved issues

Table 11
MLT/SMLT resolved issues

CR references	Description
Q01982830	IPv6 over SMLT or RSMLT is not supported. The following 3 CRs also deal with support of IPv6 over SMLT which is considered an enhancement : Q01834803, Q01756551, 01750113.

Unicast routing resolved issues

Table 12
Unicast routing resolved issues

CR references	Description
Q02002237	At switch boot, IPv6 ND prefixes are created on the switch, but not in the config file. These ND prefixes are created with default valid-life and pref-life parameters. Modifying these values causes the following errors to display on the slave console: CPU6 [03/05/09 17:53:23] RCIP6 ERROR rcIpv6PrefixTblSetBody: Failed to modify valid life CPU6 [03/05/09 17:53:23] RCIP6 ERROR rcIpv6PrefixTblSetBody: Failed to modify preferred life These ND prefixes are not saved to the config file after a save config. As a workaround, delete and recreate any IPv6 ND prefixes created upon boot that are not in the config file.
Q01878778	In BGP update packets, the route origin community type shows the wrong value (0x01 instead of 0x03).
Q01787988	For IPv6 traffic, with an IPv6 dest-val of 2301::100 and a src-val of 1301::100, the egress port shown using <code>config sys set hash-calc</code> does not match the original egress port used to send traffic. The port shown by the command is different from the actual port used for traffic forwarding; traffic is forwarded correctly.
Q01449035	IPv6 addresses remain in the routing table after you disable the VLAN.

Multicast routing resolved issues

Table 13
Multicast routing resolved issues

CR references	Description
Q02013130	Traffic loss is experienced after link failure in PIM-SSM in full mesh topology, which is not supported in Release 5.1.
Q02003390	Traffic loss for new streams due to no (S,G) clean up on IST peers. When multiple senders are sending traffic for the same groups (1000 groups) in the same VRF one after another, there may be traffic loss for new streams because this exceeds 2000 (S,G) records in an SMLT/RSMLT environment, due to the (S,G) clean up issue on IST peers. Workaround: Do not send traffic immediately from senders on same groups before timeout or do not send IGMP reports from clients for that particular group for 255 seconds.

CLI and NNCLI resolved issues

Table 14
CLI and NNCLI resolved issues

CR references	Description
Q02021276	Configuration information for PIM virtual neighbours in VRF are saved under multiple headers. The general practice for saving configurations in config.cfg is to save configurations for all the VRFs under a single header. The configurations for PIM virtual neighbour do not follow the convention as a new header is created for each VRF.

Quality of Service and filters resolved issues

Table 15
Quality of service and filters resolved issues

CR references	Description
Q01904368	Unable to mirror IPv6 packets received on a port when the ACE filter action on that port is set to deny.
Q01917455	On RS modules, if you enable access-diffserv (<code>enable-diffserv true</code>) on ingress or egress ports, IPv6 traffic on the ports is dropped and the IPv6 neighbor state changes to INCOMPLETE.
Q01814530-02	ACE filters applied to IST ports may malfunction after the switch reboots. Workaround: Disable and enable the malfunctioning ACE.

DRAFT

Known issues and limitations

Use the information in this section to learn more about known issues and limitations. Where appropriate, use the workarounds provided for these.

Navigation

- [“Release 7.0 known issues” \(page 61\)](#)
- [“Release 5.1 known issues” \(page 71\)](#)
- [“Release 5.1 known limitations” \(page 78\)](#)

Release 7.0 known issues

The following sections list known issues in Ethernet Routing Switch 8600 Release 7.0. These are to be resolved in a future release.

CR	Subsystem	Description
Q01981779	IPv6	The switch cannot learn a given IPv6 neighbor's address on more than one interface (including link-locals). If the same address is learned on more than one interface, this can cause the switch to generate errors, such as: swF:5# CPU5 [01/19/09 03:27:21] RCIP6 ERROR rcip6RpcOutChangeResEntrySubCid: REPLACE neighbor to HW FAILED. nbr ip address:
Q02033342	CLI display	In the output from the <code>show ipv6 route info</code> CLI command, the last 4 columns can appear to be shifted too far to the right. The space is allocated for completely addressed IPv6 addresses. The display of 80 characters is the standard for each line.
Q02051417	EDM	If you use EDM to export MLT configuration data (using the MultiLink/LACP Trunks tab, LACP tab, or IST/SMLT Stats tab under Configuration, VLANs, MLT/LACP), the display of the exported data is misaligned with the table header row. Although the data display is misaligned, the data values are correct.

CR	Subsystem	Description
Q02053644	BGP route policies	<p>BGP in/out route policies can be applied to IPv6 as well as IPv4, using the following command:</p> <pre>config ip bgp neighbor <addr> route-policy in <policy-name> <add del> [ipv6]</pre> <p>The <code>ipv6</code> option is used only for route policies that are applicable for IPv6 BGP routes. When configuring IPv4 route policies, omit the <code>ipv6</code> option.</p>
Q02056344	RSTP statistics on MLT	<p>If you disable a member port of an MLT that is running RSTP and then display statistics for the disabled port (for example, using the <code>show spanning-tree rstp port statistics <slot/port></code> CLI command), the command output indicates that the port is still sending and receiving BPDUs. This is the normal display behavior for MLT ports. When the system displays the RSTP statistics for MLT ports, the statistics are taken from the designated port and displayed for all member ports. Even if a port is disabled, it is still a member of the MLT and hence the designated port's statistics are displayed for the disabled port. However, there are actually no packets going out the disabled port.</p>
Q02018739	IGMPv3	<p>If you change the IGMP version at the interface level from IGMPv3 to IGMPv2 and back to IGMPv3, this sets the operating version permanently to the default value of IGMPv2. All switches in the network revert to IGMPv2 and all IGMPv3 membership reports are discarded. This also deletes the IGMP group table information.</p> <p>This is in accordance with the RFC, which states that downgrade is supported but upgrading is not.</p>
Q02045966	IPv6 VRRP	<p>In a triangle SMLT, if you delete VRRP peers on the SMLT aggregation switches, the VRRP addresses on the data closet switch are not immediately cleaned up in the IPv6 neighbor table (<code>show ipv6 neighbor info</code>). The table shows IPv6 neighbor states as <code>Incomplete</code>. The neighbor addresses are only aged out 30 minutes after the traffic is stopped from the neighbor, in accordance with the ND RFC. In addition, the Ethernet Routing Switch 8600 does not immediately delete router neighbors. Instead, it places them in the <code>Incomplete</code> state when they no longer exist.</p> <p>In this case, the virtual addresses are removed by the neighbor 30 minutes after deleting the VRRP virtual routers on the two switches.</p>
Q02054029	PIM with square SMLT	<p>The maximum number of groups in a BSR message on square SMLT is 66.</p>

CR	Subsystem	Description
Q02066205	Port logging and KHI	<p>The following two issues are related to port logging and port KHI:</p> <ol style="list-style-type: none"> 1. Setting the duplex value on a port that has auto-negotiate enabled results in a port up/down log message, and also produces a port up/down event in the <code>show khi port</code> command output. 2. Setting the duplex value on a port that has auto-negotiate disabled results in a port up log message, and also produces port up events in the <code>show khi port</code> command output.
Q01943780	BGP+	<p>IPv6 Tunnel-to-tunnel forwarding is not supported. The impact of this issue for BGP+ is as follows.</p> <p>Scenario-1 Host1-----8600-A ----N/W-1---- 8600-B -----N/W-2----8600-C-----Host2</p> <p>here: 8600 A, B and C are Dual stack routers. N/W-1 and N/W-2 consist of single stack (IPv4 only) routers (multiple hops).</p> <p>In this scenario two possibilities exist for tunneling configurations:</p> <ul style="list-style-type: none"> • eBGP+ between A-B and B-C (this scenario is not supported) • eBGP+ connection from A to C and eBGP connections between A-B and B-C (this is the only working solution) <p>Scenario-2 Host1-----8600-A ----N/W-1---- 8600-B-----8600-D-----N/W-2--- -8600-C-----Host2</p> <p>here: 8600 A, B, C and D are Dual stack routers, and the tunnels are between A-B and D-C and B-D B and D are in one AS while A and C are in two different ASs. B and D need to have synchronization enabled along with the iBGP+ connection.</p> <p>The requirement here would be to have the IGP install the routes in the route table so that the next hop is no longer the tunnel.</p>

CR	Subsystem	Description
Q02053131	RSMLT (dual-stack)	<p>On a dual-stack RSMLT VLAN (that is, IPv4 and IPv6 are configured on the same VLAN), if you delete and re-create IPv4 on the VLAN, then IPv4 forwarding does not work properly. The workaround is to disable RSMLT on the VLAN before creating IPv4 on the VLAN, if it is already configured with IPv6 RSMLT.</p> <p>Note that if the intention is to permanently delete IPv4 from a VLAN, then there is no need to disable RSMLT.</p> <p>In addition, if you delete and re-create IPv6 on an IPv4 RSMLT VLAN, you do not need to disable and reenable RSMLT on the VLAN.</p>
Q02057757	NNCLI	<p>In the CLI, entering "!" allows the commands in the history to be run again as follows:</p> <pre>Usage: history history commands substitution syntax !! : run last command !<number> : run command <number> !<str> : run last command that matches <str> !<substr> : run last command that matches <substr> ^<sstr>^<rstr> : replace <sstr> with <rstr> in last command</pre> <p>However, this functionality is not supported in the NNCLI.</p>
Q02058144	MVR	<p>If MVR is enabled on the global level for a particular vrf and save configuration is done, the "MVR ENABLE" command would be repeated two times in the configuration file. If the MVR is disabled after being enabled for the particular VRF, the configuration file would show the "MVR DISABLE" command followed by the "MVR ENABLE" command. This is done intentionally and is required for proper working of MVR on the ERS 8600 switch. The first "MVR ENABLE" command for a particular VRF does the job for allocating memory for all the structures required by MVR to run on the concerned VRF. The subsequent "MVR DISABLE" or "MVR ENABLE" command does the job of disabling or enabling the MVR feature on the VRF. The memory for MVR structures is never de-allocated unless the VRF is deleted or the switch is rebooted.</p> <p>Please do not edit the configuration file and delete either "MVR DISABLE" or "MVR ENABLE" command considering them duplicate or redundant.</p>

CR	Subsystem	Description
Q02077395	EDM	With EDM, if you attempt to delete forwarding database (FDB) entries (using the Forwarding tab under Configuration > VLAN > VLANs), an error is displayed and the FDB entries are not deleted. To delete FDB entries, you must use the <code>config vlan <vid> fdb-entry flush</code> command (in the CLI) or the <code>vlan mac-address-entry <vid> flush</code> command (in the VLAN Interface Configuration mode of the NNCLI).
Q02082668	EDM and RIP	In CLI, the RIP Domain field displayed using the <code>show ip rip info</code> command appears in decimal, while in EDM, the RIP Domain field (in the Interface tab under Configuration > IP > RIP) appears in hexadecimal.
Q02078914	EDM and OSPF	In the Virtual If EDM tab, under Configuration>IP>OSPF , you can modify the hello interval to a value that is not a multiple of the dead interval, and no warning message appears to indicate that this is not a valid configuration.
Q02085265	EDM and ACEs	In the ACE Common EDM tab (under Configuration > Security > DataPath > ACL Filters > ACL > ACE), to configure the RedirectNextHopIpv6 parameter, you must first verify that the PktType field for the corresponding ACL (under Configuration > Security> DataPath > ACL Filters > ACL) shows ipv6. If the ACL is configured for ipv4, then the RedirectNextHopIpv6 configuration does not take effect. If you do configure the RedirectNextHopIPv6 field on an IPv4 ACL, while the IPv6 value is not saved, the RedirectNextHop field (for IPv4) can be populated with an erroneous IPv4 address. Be sure to delete the erroneous IPv4 address.
Q02086884	EDM and IST	In EDM, no warning or information messages are displayed on enabling or disabling an IST (under Configuration > VLAN > MLT/LACP > MultiLink/LACP Trunks). In the CLI, when enabling IST on the MLT, the following information message is displayed: INFO : The spanning tree protocol is disabled on the port (s) with IST enabled! And when disabling the IST, the following warning message is displayed: WARNING : Disabling IST may cause loop in the network! Do you really want go DISABLE IST (y/n) ? y No similar messages are displayed with EDM.

CR	Subsystem	Description
Q02087376	EDM and SSM-snoop	<p>In EDM, if you attempt to enable SSM-snoop (under Configuration > IP > IGMP > Interface) without first enabling IGMP snoop, no warning message is displayed indicating that you must enable IGMP snoop. In the CLI, the following message appears:</p> <pre>WARNING: IGMP SNOOP should also be enabled with IGMP SSM-SNOOP</pre> <p>Similarly, no warning message is displayed in EDM if you disable IGMP snoop without first disabling SSM-snoop. In the CLI, the following message appears:</p> <pre>WARNING: IGMP SSM-SNOOP should also be disabled with IGMP SNOOP</pre>
Q02088725	EDM and VRRP	<p>In EDM, if you set the VRRP FasterAdvInterval parameter (under Configuration > IP > VRRP > Interface) to a value that is not a multiple of 200 ms, no warning is displayed. A message similar to the following from the CLI should appear:</p> <pre>WARNING: Input value is not a multiple of 200ms, Fast Adv Interval adjusted to 200ms.</pre> <p>The warning is displayed if you modify the FasterAdvInterval under Configuration > VLAN > VLANs > IP > VRRP.</p>
Q02091549	EDM and DVMRP	<p>In EDM, under Configuration > IP > DVMRP > Interface Advance, if you double-click the InPolicy or OutPolicy parameter and then click the Refresh button, the displayed pop-up window disappears.</p> <p>One workaround is to keep the lower scrollbar to the left-most position, in which case the refresh works and the popup window does not disappear.</p>
Q02087492	CLI	<p>With protocol-ID based VLANs, the DSAP/SSAP entry must be a four-digit hexadecimal number in the range 0x0 to 0xffff. If the first letter in the four-digit hexadecimal format entered is an invalid digit, an 'out of range' error is displayed.</p> <p>However, the CLI can accept four-digit numbers that include nonhexadecimal letters (for example: bbhh, 3dhj, abzz, and so on). If the trailing digits are invalid digits, the value is accepted and the valid part of the given number is extracted (for example: if bhhh is entered, the switch extracts a value of 0x000b).</p>

CR	Subsystem	Description
Q02087372/ Q02056314	Platform	<p>After a reboot, a COP software error message similar to the following may be displayed on the switch:</p> <pre>CPU5 [10/30/09 11:23:06] COP-SW ERROR 27806496: LtrId = 152,LtrPrio=0,ltrStatus= 15 (LTR_SYNC_MSG_S LOT_INUSE),msgId=152,msgState = 1,Slot=4</pre> <p>You can ignore this message as it does not cause any functional issues.</p>
Q02088077	SMLT	<p>Consider a triangle SMLT network where the edge switch is connected to each IST switch using SMLT over MLT. On either of the IST switches, if you delete and re-add the SMLT interface to the edge switch, duplicate traffic to the edge switch can result.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Before re-creating the SMLT on the MLT interface, shut down the ports of the MLT, and reenale them after assigning the SMLT ID. 2. After deleting the SMLT-ID, delete and re-create the MLT.
Q02066194	KHI	<p>The <code>show khi performance</code> command displays the status of any suspended tasks, but does not display a timestamp of when the task was suspended.</p>
Q02088992	Anycast RP	<p>With Anycast RP enabled, multicast traffic cannot be sent over an IST even when there is an active receiver connected to the IST pair switch. Workaround: The receivers must be connected to the IST pair through edge switches on one extended VLAN. They cannot be connected directly to either of the IST pairs.</p>
Q02088297	EDM and VRF	<p>In EDM, after a port is assigned to a VRF, the user can manage this port from the assigned VRF including creating an IP Brouter port, OSPF interface, and a RIP interface. From the GRT, the user can manage the basic functionality for the port, for example disabling and enabling the port, but cannot manage the IP functionality for the port. If the user configures an IP address on a port from the VRF, the GRT cannot display this data, and no IP functionality on this port can be managed from the GRT. Due to this problem, EDM shows no data or wrong values in the GRT from the Edit > Port > IP path.</p>
Q02081336	8695 SF/CPU	<p>On reboot of the 8695 SF/CPU, the following message appears:</p> <pre>SWA_7000-slot6:0x51aa300 (ttNetTask): mBlkClFree -- Invalid mBlk</pre> <p>This is an intermittent error message that can be safely ignored.</p>

CR	Subsystem	Description
Q02080990	KHI	<p>If you reset a slot that is passing traffic, the following KHI errors can result:</p> <pre>:5# CPU5 [11/04/09 06:52:01] KHI WARNING Port 4/2 is experiencing Packet Errors :5# CPU5 [11/04/09 06:52:01] KHI WARNING Port 4/4 is experiencing Packet Errors, Frames Long Errors :5# CPU5 [11/04/09 06:52:13] KHI WARNING Port 4/6 is experiencing Packet Errors, FCS Errors :5# CPU5 [11/04/09 06:52:24] KHI WARNING Slot 4 Middle Lane is experiencing Ingress RSP Errors - PM EME1 Parity Error :5# show bootconfig CPU5 [11/04/09 06:53:48] KHI WARNING Slot 4 Middle Lane is experiencing Ingress RSP AM Short Packets :5# CPU5 [11/04/09 06:53:48] KHI WARNING Slot 4 Middle Lane is experiencing F2X Errors - F2I Ingress SPI-4.2 Abort Received</pre>
Q02053536	EDM and IP VPN	<p>The work flow for creating an IP VPN route target in EDM differs from that for the CLI or NNCLI. If you want to create a route target through EDM, you must perform the following steps:</p> <ol style="list-style-type: none"> 1. Select IP > IPVPN > Route Target > Insert. 2. Enter a valid index and IP address in the respective fields. 3. Click Insert. 4. Select IP > VRF > Insert to create a VRF. 5. Select IP -> IPVPN > VPN > Insert to create an IPVPN for the VRF just created. 6. For the IPVPN just created, change the importRTList or exportRTList to associate the route target (put the route target index for importRTList or exportRTList) with the IPVPN.
Q02096944	BGP	<p>If BGP confederation and route reflectors are configured, the maximum number of routes is 150k; in a normal situation, the maximum is 250k.</p>
Q02076555	EDM and BGP	<p>In EDM, under IP > BGP > Aggregates, if you modify the parameters of an existing Aggregate entry (for example AsSetGenerate, SummaryOnly, SuppressPolicy, AdvertisePolicy, and AttributePolicy) and click Apply, the change is not displayed accordingly in some cases. To display the correct values, refresh the EDM screen. This issue can also occur when you delete an Aggregate entry.</p>
Q02089610	EDM and IPv6 OSPF	<p>EDM allows you to configure the IPv6 OSPF stubmetric parameter (under IPv6 > OSPF > Areas) beyond the valid range of 0-65535 without producing an error.</p>

CR	Subsystem	Description
Q02089739	VRRP	<p>In a triangular SMLT setup with VRRP, if you delete the VRRP instance on the master router, the following error may appear:</p> <pre>*Dist-1-187:3# CPU3 [11/06/09 02:41:41] RCIP6 ERROR rcip6RpcOutChangeResEntryState: ify_arte lookup failed fe80:0:0:0:212:83ff:fe7c:2204 cid 16779277</pre> <p>There is no traffic impact from this issue.</p>
Q02091105	EDM and STG	<p>Under VLAN > Spanning Tree > STG, if you attempt to remove a port from an STG, a warning similar to the following should be displayed:</p> <pre>WARNING:Port (s) 3/13 will be removed from the VLAN (s) as well Do you want to continue (y/n) ?</pre>
Q02092358	EDM and ACL	<p>In EDM, under Security > Datapath > ACL filters > ACL > ACE > IP > Source Address, if the error message <code>UndoFailed</code> is returned, the value entered is illegal or improper.</p>
Q02094865	Platform	<p>With the new KHI enhancements, the switch produces more messages at boot up. These messages only indicate issues if they appear concurrently with switch operational issues.</p>
Q02097130	EDM and PCAP	<p>Under Edit > Diagnostics > PCAP > PcapGlobal, if you modify the <code>BufferSize</code> field to a value that consumes too much memory, an <code>UndoFailed</code> error is displayed. EDM should display an error similar to the following:</p> <pre>Possible Memory allocation failure - please refer to logs in PCAP engine</pre>
Q02097283	BGPv6 route preferences	<p>There is no way using CLI, NNCLI, or EDM to change route preferences for BGPv6 routes only. The switch provides a single option that can change route preference for BGPv4 and v6.</p>
Q02098500	Platform	<p>When rebooting the master CPU, the following warning messages may appear on the 8695 SF/CPU:</p> <pre>nyhq-csbu-udb:6# 0x51bb4e0 (tNetTask): duplicate IP address 2f50ef10 sent from ethernet address f4:e3:b1:0d:14:00</pre> <p>In addition, the following messages may appear on either the 8692 or 8695 SF/CPU:</p> <pre>CPU6 [11/24/09 12:15:49] MLT WARNING smltTick: pollCount = 51 > 50. But IST Channel active and resetCount = 0 < 3. Resetting pollCount and staying active!. CPU5 [11/24/09 12:17:44] IP INFO the RsmLT circuit of vlan 18 is existed already in slave CPU</pre>

CR	Subsystem	Description
Q02099222	IST	After rebooting an IST switch, the following error message may appear on the IST peer: COP-SW-IPV6 ERROR Slot 7: ercdDeleteIPv6Record: Failed to lookup entry in gIPv6RadixTbl. Status: 18 There are no functional impacts from this issue.
Q02099531	EDM and Route Policies	In EDM, under the IP > Policy > Route Policy tab, if you double-click the MatchAsPath or MatchCommunity fields, values are duplicated in the pop-up window. If you assign one of the duplicate values to the MatchAsPath or MatchCommunity field, it gets applied. Once applied, do not attempt to assign the other duplicate value to the MatchAsPath or MatchCommunity field; otherwise an error is displayed.
Q02099875	SMLT full mesh	In full mesh SMLT, if a VLAN IP is changed, the IST peer is not displaying the new IP address in the topology table. Workaround: save the config file where the IP address was changed and reboot the switch with that config file. After the switch comes back up, the IST peer will learn the new IP address with topology.
Q02100377	CLI	In the CLI, you can configure a DNS host name of up to 256 characters. The CLI should limit the DNS host name to 64 characters.
Q02098992	CLI	The <code>config ethernet <slot/port> fc-pause-0 <enable disable></code> command for configuring Ethernet ports does not apply to R/RS modules. This command will be removed in a future release.
Q02091957	EDM and ACE	Under Security > Datapath > ACL filters > ACL > ACE , if you select an existing ACE and click Action/Debug , and then click the ellipsis (...) to select a DstMltId from the pop-up window, to remove the selected value, you must deselect the DstMlt value and also deselect either the associated DstPortList or the DstVlanId to remove it as well.
Q02100062	Platform	After a reboot of an HA switch, the following error may appear: CPU6 [12/10/09 02:32:53] COP-SW-IP ERROR Slot 4: ercdProcIpRecMsg: Failed to Add ECMP IP Record. IpAddr:xxx.xxx.xxx.xxx IpMask: xxx.xxx.xxx.xxx NumEcpRouteRecs: 1 retCode: 18 No traffic issues are seen with this issue.
Q02091999	DNS host name	The CLI can support a DNS host name of up to 256 characters; however, EDM can only support up to 64 characters. Therefore, do not configure a DNS host name greater than 64 characters.
Q02100726	EDM Help	The current online help for many tabs opens a page with the field variable definitions. However the associated procedure for the current tab is listed on a separate HTML page which cannot be reached from the variable definitions page.

CR	Subsystem	Description
Q02101603	CLI	When running in HA mode, the login prompt may scroll on the console screen. This issue does not appear if the CLI timeout is set to the default value of 900. As a workaround, restore the CLI timeout to the default value of 900 (using CLI or EDM [Security > control path > general > CLI]).
Q02102285	KHI	KHI may report a false positive of bad packets on a 10-Gig port, even when nothing is plugged into the port. In addition, the error message refers to the lane rather than the port. For information on which ports are associated with which lanes, refer to <i>Nortel Ethernet Routing Switch 8600 Planning and Engineering — Network Design Guide (NN46205-200)</i> .
Q02102162	MLT	The 8600 switch allows you to configure more than the supported maximum of 128 MLTs. Do not configure more than 128 MLTs on the switch as this is not a supported configuration.
Q02076924	PIM-SM	In a PIM-SM network, if a single-attached multicast source is removed from the network, its entries are never removed from the mroute tables and the entries continue to be displayed under show ip mroute info .
Q02109487	EDM help	In this release, EDM help is unavailable for the EDM Quick Start pages (Configuration > Quick Start > Quick Start). Therefore, in these pages, the Help button is disabled.
Q02107441	DDI	If you enable DDM monitoring on a switch with non-DDM GBICs installed, the switch generates a message (HAL INFO GBIC) every 5 seconds to the console and to the log file for each non-DDM GBIC installed.
Q02111397	IGMP	For the IGMP <code>stream-limit-max-streams</code> parameter, if the default value is changed, the new stored value appears incorrectly in the show commands and in the config.
Q02111203	DHCP Relay with IP Multinetting	Once packets come into the switch through an IP Multinetting port, the switch internally reclassifies the packets and assigns the packets to the IP-multinetting-associated IP-subnet VLAN. From that point on, all upper layer protocols, including DHCP, only see the associated IP-subnet VLANs, instead of the IP-Multinetting VLAN. Therefore, configure any Layer 3 features on the IP-subnet VLAN rather than on the IP-Multinetting VLAN. For example, configure DHCP-relay on the associated IP-subnet VLANs, rather than the IP-Multinetting VLAN.

Release 5.1 known issues

The following sections list known issues in Ethernet Routing Switch 8600 Release 5.1. These are to be resolved in a future release.

Platform known issues

Table 16
Platform known issues

CR references	Description
Q02025261	With multiple HA failovers, intermittent connectivity issues may occur.
Q01993610	Line RDI is not generated properly as a result of LOS on the 8683XZR module in WAN mode.
Q01993661	When an RDI-P is received on the XZR module, a "Path RDI" should be shown under the active alarm; however, a "Path AIS" appears.
Q02005338 Q02013534	With DWDW XFP AA1403001-E5, wavelength is displayed in CLI as 1307nm or 1307.5nm, but the faceplate is labelled as 1310nm. The wavelength specifications provided by the XFP manufacturer and reported by the Ethernet Routing Switch 8600 system can vary slightly because of hexadecimal to decimal (and decimal to hexadecimal) rounding.
Q01947384	Ping does not work when the source IP option is set to a circuitless IP interface.
Q01993806	Three SONET Alarms are wrongly decoded by the 8683XZR module: <ul style="list-style-type: none"> • Path PLM is interpreted as Path SLM • Path PDI is interpreted as Path SLM Path • TIM is interpreted as No Defect <p>These three alarms are not supported by Ethernet Routing Switch 8600 Release 5.1.</p>
Q02013161	With an FPGA upgrade, the PCMCIA is not checked for a file before an error message is displayed. The switch does not search in PCMCIA before displaying the error message, wrongly stating that no such file exists even if the PCMCIA has that file. The switch should search in PCMCIA along with FLASH also. The issue is present for all FPGA upgrade commands.
Q02002324	When Autonegotiation is enabled on two switches that are connected to each other using RS modules, and the auto-negotiation-advertisement parameter is set to default on one switch and to 1000-half on the other switch, ping does not work.
Q02006487	When an 8683XZR module in WAN mode receives a LOF, the port correctly detects the LOF, but it does not send out a Line RDI.
Q02006504	When an 8683XZR module in WAN mode receives a P-PLM (path label mismatch), the alarm raised is path SLM. Path PLM is the SONET term and path SLM is the SDH term. To be consistent, the SONET term should be used when the port is in SONET mode.

CR references	Description
Q02008247	<p>With DWDM XFPs, the <code>show system pluggable-optical-modules</code> threshold status is incorrect during transition from a "High Alarm" to a "Low Alarm".</p> <p>When the Rx power is high (beyond the threshold), the threshold status indicator shows "High Alarm", which is correct. However, when the Rx optics is pulled, then the state remains at "High Alarm," even though the indicated power level is -38.200 dBm (which is a "Low Alarm"). The high alarm does not clear in this scenario until the Rx power level goes back to normal.</p>
Q01991485	<p>If two Ethernet Routing Switch 8600s are connected using two Ethernet WAN ports using SONET framing and the ports are operationally up, when one of the two ports is changed from SONET framing to SDH framing, no alarm is received. An alarm is needed for the SONET and SDH mismatched connection.</p>
Q02023608	<p>On 8612XLRS modules with DDM enabled, wait 3 minutes after module initialization before you enter <code>show sys pluggable-optical-modules</code> commands to avoid errors during the initialization.</p>
Q01727720	<p>In the output for the <code>show port error main port <slot/port></code> command, the <code>FRAMES LONG</code> counter does not increment when the 8648GBRS port receives frames larger than the system MTU size. The same behavior is observed on 8648GTR ports and Gigabit ports on the 8634XGRS.</p>
Q01877552-01	<p>Configuring Distributed MLT on ERS8600 using 8608GBE cards could lead to a ports being put in different STP states in the MLT.</p>
Q01927867-01	<p>On an ERS8600 running OSPF, the command <code>show vlan info ports <vlan-id></code> display provides inadequate spacing between the column head VLAN ID and PORT MEMBER when the ports to be displayed are OSPF passive port members.</p>
Q01986390	<p>Force Topology CLIP (Circuitless IP) becomes unconfigured after an HA-CPU failover. Under these considerations, the user must reconfigure the parameter if configured differently than the default value.</p>
Q01967211-01	<p>When the remote mirroring destination/termination (RMT) port is used for both local port mirror and remote port mirror, the sniffer can't decode the mirrored traffic and report them as malformed packets. When the RMT port is either used for a remote port mirror or local port mirror, the sniffer can decode the mirrored traffic correctly.</p> <p>When a RMT is configured on an interface, do not configure the same interface as a local "mirroring port". This causes packet corruption on the locally mirrored traffic.</p> <p>In ERS 8600, an interface can be configured as either a local or a remote mirroring destination. The RMT port is exclusively used in Remote mirroring tunnel. The Remote mirroring Destination/Termination port should be disabled to perform local mirroring.</p>

CR references	Description
Q01832726	In a SuperMezz R mode HA-CPU system configured with a dead interval of 3 seconds, when the Master is removed, OSPF neighborship is lost for interfaces configured with low timers (for example, 1 s Hello and 3 s Dead Interval). If failover is triggered by soft-resetting the Master CPU, or the dead interval is 10 s, this issue does not occur. Workaround: Remove the Master CPU during a maintenance window or other low-traffic periods. Or, increase the dead-interval to 10 s.
Q01841910	When using High Availability mode, the Secondary SF/CPU crashes if it cannot find the backup primary configuration file, even if there is a backup configuration file. Workaround: Ensure that the configuration files on both the Master and Secondary SF/CPU have the same R mode setting (either enabled or disabled).
Q01872749	If you reset an RS module, a FATAL COP message may be logged. Reset is a maintenance command which should not be used under normal circumstances. Workaround: If you must reset an RS module that is passing traffic, first disable the slot, then reset the slot.

Switch management known issues

Table 17
Switch management known issues

CR references	Description
Q01924118	When configuring SSH on the switch, -C and -C2 compression options are accepted, but should be rejected. Subsequent SSH connection are also accepted with no message to the user. The switch should prompt the user with a message stating compression is not supported.
Q01576692-01	With RADIUS accounting of SNMP, when the switch sends start, interim, and stop requests, the packets do not contain the SNMP community string value.
Q01576083	You can connect through HTTP to an Ethernet Routing Switch 8600 interface that has an IPv4 address, but not to an interface that has an IPv6 address.
Q01831409	Using the CLI, when you configure an SNMPv3 target address with an IPv6 address in short format and a port (for example 100::2:162), the software incorrectly assigns part of the IPv6 address as the port number. Workaround: Specify the IPv6 address in long format along with the port number (for example, 1:2:3:4:5:6:7:8:162), or use Device Manager to configure the address.

Layer 2 known issues

Table 18
Layer 2 known issues

CR references	Description
Q01449886	The switch can send VLACP PDUs at the short timeout interval when the long timeout interval is configured.
Q01735063	When the Link Aggregation Control Protocol (LACP) adds a new port to a link aggregation group (LAG), it brings all the ports of the LAG down, which brings the entire interface down. As a result, the multilink trunk is deleted and the VLAN interface is deleted. This causes OSPF to go down.
Q01750113	If you disable RSMLT on a VLAN of a full-mesh triangle SMLT network that carries IPv6 traffic, up to 50% of the IPv6 traffic can be lost. Workaround: Do not disable RSMLT.
Q01850453	When you convert a single-port MLT to a multiple-port MLT, you cannot set the LACP key for the newly-added ports and form a LAG until you change the key for all ports. You may also receive the following type of error: CPU6 [03/26/08 10:51:50] LACP INFO lacpOperDisablePort: LACP operationally disabled on port 8/23 because the port's capability doesn't match key 64's capability. Workaround: Change all ports to a different key, then change back to the old key. After setting aggregation back to true, the LAG can form.

MLT/SMLT known issues

Table 19
MLT/SMLT known issues

CR references	Description
Q2016922	For an IP VPN-lite configuration, where an edge 8600 Cluster is configured to use an SMLT configuration toward the core (most likely square or full-mesh RSMLT), SMLT fast failover cannot always be guaranteed for this portion of the network.
Q01998049	In RSMLT environments, if an IST peer is powered off for durations longer than the RSMLT holdup-timer, when the powered off peer comes back up on-line, one may see a traffic loss for up to 30 seconds. If this amount of time is unacceptable, it is recommended to perform one of the follow two actions. The recommended action is to configure the RSMLT holdup-timer to infinity on the on-line IST peer, power up the off-line IST peer, and once the SMLT cluster is stabilized, re-configure the RSMLT holdup-timer back to the default setting of 180 seconds. The alternative action is to power up the off-line IST peer during a maintenance windows.

Unicast routing known issues

Table 20
Unicast routing known issues

CR references	Description
Q01946521	In OSPF Router LSA updates, the V-bit is not set, and is always 0.
Q02008788	In a square SMLT environment, if OSPF is disabled and reenabled while the IST is down, the OSPF adjacency to one of the non-IST peer boxes may show ExStart state for 5 to 8 minutes. The condition does clear itself in that time frame, and will go to full adjacency.
Q01976924	With high route scaling (15 000 routes) and ECMP enabled, error messages can appear on the slave CPU, including: IP ERROR VRF-0: rcIpAddRoute: addIpRoute failed with -102 CPU5 [01/07/09 16:04:27] IPMC ERROR ipmSysAddSession FAIL: ipmcSysHashRidAlloc failed S 125.133.180.1 G 224.9.5.0 CPU5 [01/07/09 16:04:27] IPMC WARNING ipmcSysHashRidAlloc FAIL: HashRecIndex EOS 8194 S 125.128.168.1 G 224.9.8.0 InVlanid 14
Q02010177	The routing table does not use the preference value specified for a static route if the route has a static ARP entry as the next hop, after disabling and re-enabling the port.
Q01872074	When the switch is in IP VPN Lite mode, the "Assigned Number" portion of the Route Distinguisher (RD) cannot be modified. This occurs for CLI, NNCLI, and Device Manager. Workaround: To change the assigned number, the IP Address and the Assigned Number must be changed at the same time, or the RD must be deleted and re-added (using IP VPN delete).
Q01922909-01	On an ERS running BGP and OSPF, when BGP routes are redistributed into the OSPF domain and a route-policy is used to match and permit a prefix, the more specific prefixes do not get redistributed into the OSPF domain. Care must be taken when using such a configuration, to avoid unwanted traffic loss.
Q01464501	The switch does not send an ICMP Parameter Problem message with an ICMP code value of 1.
Q01720546	When an HA failover occurs, it produces BGP errors on the new Master: "CPU5 [07/31/07 11:05:09] BGP INFO PEER_ERROR PKT EVENT(172.16.100.5) Established: remove duplicate peer". No negative effects on functionality occur.
Q01867585	Configuring a BGP peer group with route-reflection causes configuration anomalies. In particular, you can configure three peers and only two come up; or you can disable route reflection and all peers stay up. Workaround: Do not use BGP route-reflection on any peer groups. BGP peer groups are not supported with route reflection enabled.

CR references	Description
Q01878638	When a VRF with an IP VPN configuration is deleted messages of the following type are displayed on the console: RCMPLS WARNING ipVpnIImAdd line 983: UTAL_LookupArp() failed for NextHop 30.1.30.151 vrfId 100. These messages do not affect functionality.
Q01881289	When a port is untagged and Penultimate Hop Popping (PHP) is set to implicit-null, IP VPN traffic is sent to the wrong queue. The issue occurs on the last-hop Label Switch Router (LSR) (the LSR that sends the service label). Workaround: For untagged ports, set PHP to explicit-null or disabled.

Multicast routing known issues

Table 21
Multicast routing known issues

CR references	Description
Q02011440	SSM channel set to false on receiving traffic
Q02021453	RPF checks fail with MSDP peer configured in iBGP configuration. Workaround: Use default Peer or do not use iBGP configuration.
Q01866720	The output of the <code>show ip pim interface</code> command indicates that the operational status (OPSTAT) is down even if the PIM interface is enabled and active. This does not impact traffic. The reason for the discrepancy is that Spanning Tree has not converged. Once the convergence completes, the table is updated properly.

CLI and NNCLI known issues

Table 22
CLI and NNCLI known issues

CR references	Description
Q02000473	After enabling Hsecure on the switch and saving the configuration, the CLI prompt should not be returned to the user until the configuration save is complete. Currently, the switch displays the following error: Another show or save in progress. Please try the command later.
Q01467778 Q02010136	The System Messaging Platform (SMP) command <code>config log transferFile <ID> filename <str></code> , used to modify the default file name, does not function properly. The optional filename string does not work. Instead, the transferFile name is always the standard SMP log file name of xxxxx.sss, where xxxxx is the last three bytes of the chassis base MAC address, and sss is the SF/CPU slot number. Nortel recommends that you not use this command.
Q01948346	The <code>copy</code> command does not work properly with FTP debug turned on.

CR references	Description
Q02010142	When sending traps to an Element Manager, the switch only uses the IP address specified by the first entered <code>sender-ip <dest-ip> <source-ip></code> command. It is possible to specify multiple sender IPs and each should use a different IP as specified in this command. The switch uses the IP address of the physical VLAN of the first entry in the target-address table.
Q01623093	In the CLI, when you enter the <code>config/ip/static-route# create <ipaddr/mask> next-hop ?</code> command, only the <code>vrf <value></code> parameter is shown in response. In spite of this, you can still configure all parameters: <code>config/ip/static-route# create <ipaddr/mask> next-hop <ipaddr> cost <value> [preference <value>] [local-next-hop <value>] [next-hop-vrf <value>]</code>
Q01794612	Entering the CLI <code>reset</code> command for an SF/CPU module with SuperMezz should implement a cold boot on both the SF/CPU and SuperMezz, but instead incorrectly performs a warm boot on the SuperMezz and correctly performs a cold boot on the SF/CPU.

Quality of Service and filters known issues

Table 23
QoS and filters known issues

CR references	Description
Q01793851	RS modules do not support egress flow-based mirroring for IP VPN Lite traffic.
Q01868828	If you enable mirroring on an ACL-based filter whose actions re-mark the DSCP bit, the DSCP bit and QoS egress queues are incorrectly assigned.

Device Manager known issues

Table 24
Device Manager known issues

CR references	Description
Q01883183	When using Device Manager, IP VPN routes in a VRF are not flushed when the import route target (RT) is deleted. Workaround: To delete the routes, before you delete the RT, in the IP-VPN, VPN tab, ensure that the import RT field is not selected.

Release 5.1 known limitations

Use the information in this section to learn more about known limitations. These CRs are classified as operation not to be changed.

Platform limitations

Table 25
Platform limitations

CR references	Description
Q01279047-01	Disabling Auto-negotiation on 1000BASE-T ports with speed of 1000 Mbps can result in inconsistent behavior. Auto-negotiation cannot be disabled on the 8648GTR module, but can be disabled on an 8630GBR with an SFP. Workaround: Nortel recommends that you enable Auto-negotiation on all 1000BASE-T ports when they operate at 1000 Mbps.
Q01347146-01	Single Fiber Fault Detection is supported on the ERS 8600 but should a user run into any issues with its operation, it is recommended that the user uses VLACP to achieve the same functionality. Workaround: Disable SFFD and instead use VLACP.
Q01464922	An 8630GBR module using Single Fiber Fault Detection (SFFD) connected to an Ethernet Switch 470 does not recognize a single-fiber fault. SFFD is not supported when an Ethernet Routing Switch 8600 is connected to an Ethernet Switch 470. Workaround: Disable SFFD and instead use VLACP.
Q01971595	Pasting configurations, either via console or telnet/SSH, is not recommended and if performed should only be done one line at a time, versus larger text files. This is independent of any control the user may have over how 'slow' their actual input maybe. The reason for is that neither the console or telnet/SSH functions are high priority, and the switch could be servicing some other task and therefore miss lines in the config paste. Optionally, use TFTP/FTP and 'source' the file.
Q01938504	When VLACP is configured, the log message "LACP WARNING Received MAC-mismatched PDUs on port <port number>, MAC <mac address>, Please check your VLACP configuration." is sometimes observed. In the event of a VLACP misconfiguration, this message will be logged continuously in the log file, and the configuration should be corrected. If VLACP is not misconfigured and the message is observed sporadically, it should be disregarded as there is no impact to traffic.
Q01774929	The event of discontinuing logging to PCMCIA by the executing the CLI command pcmcia-stop is not logged into the log file.
Q01848350	ERS8600 could take a minimum of about 10 seconds to populate an OSPF learned route into the Route Table Manager as it does not rebuild its router LSAs immediately when the neighbor router changes to FULL state.
Q01937023	A "save config" executed from the standby CPU will result in the pcap.cfg data replacing the configuration data stored in config.cfg on the standby CPU. Changes to the standby CPU configuration should ONLY be executed from the master CPU, via either "save config" (savetostandby flag set true or "save config standby <config file name>".

CR references	Description
Q01926665-02	SLT configurations where the SLT port and all the IST_MLT ports are configured on the same physical module (non-best practice design; IST_MLT should always be a D-MLT), the switch can experience FDB entry learning issues for MAC addresses learned across the IST; this can lead to connectivity loss. This condition can occur if the module is physically swapped out during switch operation, or if the module is disabled/enabled via CLI or JDM. If seen and to resolve, FDB entries will be relearned after the fdb-ageout time, or can be manually relearned by performing an fdb-entry flush on the relevant VLANs.
Q01932414	On an ERS8600 running VLACP, if the value of VLACP timer is not set to a multiple of 10, VLACP may not function properly because the VLACP port may not be able to send out any VLACP PDUs. VLACP timers must always be set to some multiple of 10.
Q01880938-01	LACP short timers for RSMLT/SMLT configurations must be set to 550 milliseconds or higher.
Q01885138-04	Traffic loss has been observed for 1-2 seconds after a port link up occurs. This is caused by the edge box transmitting traffic immediately upon connecting to the aggregation (IST core) box. As soon as the link is enabled, it takes a while before VLACP engages and stops the traffic from flowing on that link.
Q01986615	If you have a IPVPN Lite route, with multiple IGP nexthops towards the MP-BGP network (by virtue of ECMP being enabled in VRF 0) and ECMP is also enabled in a non-zero VRF, then the VRF route is installed multiple times in Route Table Manager (RTM). The datapath will therefore use each IGP nexthop, as expected. Now, if the user disables ECMP in the VRF, the additional ECMP routes from the non-zero VRF are deleted but the IPVPN lite route is not removed. If then some network failover happens, under these circumstances, the system incorrectly thinks that the underlying route is still available. This could cause unwanted traffic interruption. Work around: Restart IPVPN if this event occurs.
Q01972028	When operating in HA mode, if the Standby and Master SF/CPUs are rebooted quickly in succession within a few seconds in that order, a race condition can occur in which R/RS line cards do not get rebooted as part of the Standby and Master reboot process. Instead they get rebooted in a delayed fashion during the new Master SF/CPU initialization. However, they would function normally after that. To avoid this delayed reboot condition and an unnecessary alarm, Nortel recommends to not reboot both the Standby and Master SF/CPUs in quick succession or simultaneously. By leaving a gap of around 10 seconds, this problem could be avoided.
Q01470456	When the Packet Capture Tool (PCAP) buffer fills up, a Standby SF/CPU exception can occur. The exception only occurs if you use a console connection to the Standby SF/CPU. This only occurs when the autosave feature is enabled and is set to transfer to a network device. The issue does not occur when you save to a PCMCIA card.

CR references	Description
Q01450708	When you create an MLT with more than one port that ends in an 8648GTR module, and the MLT is connected to a 10/100 Mbps device with Auto-negotiation enabled, the link state for the first port is 100 Mbps full duplex and state of all other MLT ports is 10 Mbps half duplex. Workaround: Adjust the speed and duplex modes manually on a per-port basis.
Q01644085	When a copper GBIC is present in an 8630GBR module port with Auto-Negotiation disabled, the port is always in an up state, even if no Ethernet cable is plugged in. Workaround: Auto-Negotiation must be enabled for GBIC ports running 1 Gigabit Ethernet. Keep Auto-Negotiation enabled.

Switch management limitations

Table 26
Switch management limitations

CR references	Description
Q01393349-01	On the ERS8600 switch, the <code>-f</code> option cannot be used with SSH non interactive commands.
Q01380593, Q01194685	The switch does not add standby ports to a link aggregation group (LAG) properly. Currently, the Ethernet Routing Switch 8600 supports a maximum of eight ports, active or standby, in any one LAG.
Q01436111	The switch does not display all SNMPv3 target parameters when you enter the <code>show config</code> command. This is the expected behavior.

Layer 2 limitations

Table 27
Layer 2 limitations

CR references	Description
Q01449886	The switch can send VLACP PDUs at the short timeout interval, even though the long timeout interval is configured. This operation has no negative affect on VLACP operation, to other ERS 8600s, or to any other Nortel ERS switches running VLACP.
Q01352932	In a pure Layer 2 point-to-point configuration, using VLACP fast timers, 100 ms convergence is not guaranteed when ECMP is implemented on top of the link. Keep the configuration as simple as possible, with routed VLANs, but without ECMP. For fast convergence, Nortel recommends that you use RSMLT rather than ECMP.
Q01453004	With HA enabled, the switch does not flush the VR ARP entry from the ARP table when you delete the VR ID from both switches.

CR references	Description
Q01454547	You can configure Link Aggregation/MLT group IDs from 1 through 256. The switch supports a total of 128 MLT groups. Nortel suggest that users start numbering S-SMLT or SLT IDs to avoid overlapping MLT IDs in the 1 through 128 range. Note: SLT IDs range from 1 through 512. If you start at 129, a switch can support the full capacity of 383 SLT ports or IDs.
Q01810668	When you install an RS module and have SMLT and LACP configured, LACP goes down, and the switch shows the message "swA:6# CPU6 [01/09/08 14:39:28] LACP INFO lacpOperDisablePort: LACP operationally disabled on port x/y because the port's capability doesn't match key z's capability". Workaround: Globally disable and enable LACP to bring the ports back to the MLT. Further, for reliable LACP operation, use CANA, or, if CANA is not supported, enforce a speed and duplex mode on all 10/100/1000 Mbps and 10/100 Mbps ports. See " MLT/LAG considerations " (page 25).

MLT/SMLT limitations

Table 28
MLT/SMLT limitations

CR references	Description
Q01971344	In the case of a full-mesh SMLT configuration between 2 Clusters running OSPF (more likely an RSMLT configuration) because of the way that MLTs work in regards to CP generated traffic, it is highly recommended that the MLT port (or ports) that form the square leg of the mesh (versus the cross connect) be placed on lowered number slot/port, than the cross connections. The reason for this is because CP generated traffic is always sent out on the lowered numbered ports when active. Using this recommendation will keep some OSPF adjacency up if all the links of the IST fail. Otherwise the switches which have a failed IST could lose complete OSPF adjacency to both switches in the other Cluster and therefore become isolated.

Unicast routing limitations

Table 29
Unicast routing limitations

CR references	Description
Q01845219-01	The QoS value of unicast packets is retained when forwarded to the CP as exception packets. If enough packets with high QoS setting are received, this could negatively affect CP handling of other packets. In general, unicast packets being sent to CP is abnormal, and the root cause of that situation should be investigated and resolved as a first step.
Q01835057	To maintain backward-compatibility with pre-5.0 releases, if the management IP address network mask is equal to the natural network mask, then the mask is not displayed in response to the <code>config bootconfig net mgmt info</code> command. If the configured network mask is not equal, it will be shown. This is the correct behavior.

Multicast routing limitations

Table 30
Multicast issues

CR references	Description
Q01437712	The <code>show ip pim mroute</code> command may display an incorrect incoming port after the corresponding SMLT port is disabled and re-enabled.
Q01439217-01	The switch sends no ICMP message when it receives IPv6 packets destined to an IPv6 multicast address with a destination header option type equal to 0x80.

QoS and filters limitations

Table 31
QoS and filters issues

CR references	Description
Q01443034	The CLI allows you to configure mutually-exclusive Access Control Template (ACT) properties.
Q01450812	The <code>show qos stats policy all</code> command does not display correct statistics.

Device Manager limitations

Table 32
Device Manager issues

CR references	Description
Q01374909	<p>Device Manager does not allow all fields to be configured for PING and Trace Route. This is as designed.</p> <p>Trace Route does not allow the following fields:</p> <ul style="list-style-type: none"> • TargetAddressType • DSField • SourceAddressType • IfIndex • MiscOptions • StorageType • CreateHopsEntries • Type <p>PING does not allow the following fields:</p> <ul style="list-style-type: none"> • TargetAddressType • StorageType

CR references	Description
	<ul style="list-style-type: none">• Type• SourceAddressType• IfIndex• DSField
Q01445777	The Device Manager scroll bars on the ACL-Insert ACL-ActID interface do not function properly.

MIB limitations

Table 33
MIB issues

CR references	Description
Q01274812-01	The description for rcStgTaggedBpduVlanId is incorrect. The range -2147483648 to 2147483647 should read 1 to 1024.

Customer service

Visit the Nortel Web site to access the complete range of services and support that Nortel provides. Go to www.nortel.com, or go to one of the pages listed in the following sections.

Navigation

- “Updated versions of documentation” (page 85)
- “Getting help” (page 85)
- “Express Routing Codes” (page 85)
- “Additional information” (page 86)

Updated versions of documentation

You can download and print the latest versions of Nortel Ethernet Routing Switch 8600 NTPs and Release Notes directly from the Internet at www.nortel.com/documentation.

Getting help

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

If you purchased a Nortel service program, you can get help by contacting one of the Nortel Technical Solutions Centers found at <http://www.nortel.com/callus>; or visit our Technical Support site at <http://www.nortel.com/support>.

Express Routing Codes

An Express Routing Code (ERC) is available for many Nortel products and services.

When you use an ERC, your call is routed to a technical support person who specializes in supporting that particular product or service. To locate an ERC for a product or service, go to <http://www.nortel.com/erc>.

Additional information

Use the information in the following table to access other areas of the Nortel Web site.

For information about	Contact
Contact Us	www.nortel.com/contactus
Documentation feedback	www.nortel.com/documentfeedback
Products (marketing)	www.nortel.com/products
Partner Information Center (PIC)	www.nortel.com/pic
Register	www.nortel.com/register
Search	www.nortel.com/search
Services	www.nortel.com/services
Training	www.nortel.com/training

Index

A

Advanced filters
 guidelines 55

B

boot source
 SuperMezz 51

C

chassis
 High Performance 47
compatibility
 module and chassis 46
 module and component 42
 module and feature 44
 software and hardware 41

D

DOSFS 27
DVMRP considerations 54

F

file names 18

H

HA mode
 considerations 45

I

I/O module considerations 25
IST and VLACP considerations 53

K

known issues
 CLI and NNCLI 77
 Device Manager 78
 Layer 2 75
 MLT/SMLT 75
 multicast routing 77
 platform 72
 QoS and filters 78
 switch management 74
 unicast routing 76

L

license
 temporary 55
limitations
 Device Manager 83
 Layer 2 81
 MIB 84
 MLT/SMLT 82
 multicast routing 83
 platform 79
 QoS and filters 83
 switch management 81
 unicast routing 82
loop prevention 49

M

MIB 56
MLT/LAG considerations 25
MPLS
 and MTU 53

N

nonsupported modules 12
notifications 56

P

- performance
 - module and chassis 46
- power and cooling management 29

R

- resolved issues
 - CLI and NNCLI 59
 - IP unicast 58
 - multicast 59
 - platform 57
 - QoS and filters 59
 - switch management 57
- RFC 56

S

- scaling 38
- SF/CPU
 - protection and loop prevention 49
- SMLT
 - and switch clustering 48
- SMLT considerations 54
- SNMP considerations 53
- Software licensing 18
- SuperMezz 22

T

- traps 56

U

- upgrade considerations 26
 - changes to procedures 32
 - IST 31
 - power management 28
 - pre-5.0.0.x software 32
- upgrade paths 25

V

- VLACP and IST considerations 53

Nortel Ethernet Routing Switch 8600

Release Notes — Software Release 7.0

Release: 7.0
Publication: NN46205-402
Document status: Draft
Document revision: 04.AV
Document release date: 22 February 2010

Copyright © 2008-2010 Nortel Networks. All Rights Reserved.

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

THE SOFTWARE DESCRIBED IN THIS DOCUMENT IS FURNISHED UNDER A LICENSE AGREEMENT AND MAY BE USED ONLY IN ACCORDANCE WITH THE TERMS OF THAT LICENSE.

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

All other trademarks are the property of their respective owners.

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

www.nortel.com

