Part No. 316859-J
June 2006

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Ethernet Routing Switch 1600 Series Software Release 2.1

NORTEL

Trademarks

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice.

Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Nortel Networks software license agreement

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

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

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or

modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

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

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

4. General

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

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

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

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

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

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

Contents

Introduction

These Release Notes for the Nortel* Ethernet Routing Switch 1600 Series, Software Release 2.1 describe the hardware and software and any known issues that exist in this release.

Note: The information in these Release Notes supersedes applicable information in other documentation.

The following topics are discussed in this document:

A list of related publications can be found on page 42.

See *Getting Started* (321821-A) for a documentation suite index that contains Documents listed by function, new features mapped to documents, and a document subject list.

For more information, see How to get help on page 44.

Note: For Release 2.1 the document suite has been restructured to conform to the Ethernet Routing Switch Series 8300 document suite. A Quick Start Guide, *Quick Start Guide* (321819-A), and a Getting Started book, *Getting Started* (321821-A) have also been added. The Quick Start Guide provides basic instruction about installing the hardware and performing basic configuration for an Ethernet Routing Switch 1600 Series switch. Getting Started provides procedures for setting up and starting the Ethernet Routing Switch 1600 Series switch using the Command Line Interface (CLI) as well as a documentation suite index.

File names for this release

Table 1 describes the Ethernet Routing Switch 1600 Series, Software Release 2.1 software files.

The Ethernet Routing Switch 1600 Series switch Software Release 2.1 contains the following files:

Table 1 Release 2.1 software files (Sheet 1 of 2)

Software File Name	Description
p16a2100.img	Run-time image file
p16b2100.img	Boot image
p16c2100.img	3DES encryption module for SSH NOTE 1
p16c2100.des	DES SNMPV3 encryption module NOTE 1
p16a2100.mib.zip	MIB zip file
p16a2100.mib	Concatenated text file containing all MIBs
p16b2100.had	Boot image, pre-boot monitor code NOTE 3
p16a2100.md5	MD5 checksum file NOTE 2
jdm_6000.exe	Supported Device Manager version (Windows* 95 and later)

Table 1 Release 2.1 software files (Sheet 2 of 2)

Software File Name	Description
jdm_6000_solaris_sparch.sh	Supported Unix Device Manager version (Solaris SPARC only)
jdm_6000_hpux_pa-risc.sh	Supported HP-UX Device Manager version
jdm_6000_linux.sh	Supported Linux Device Manager version
NOTE 1: SSH and SNMPv3 provide increased security and are optional. These software files are available only on the Nortel web site. See Finding the latest updates on the Nortel web site on page 44. **NOTE 2**: For more information about using the MD5 checksum command, see *Upgrading to Ethernet Routing Switch 1600 Series Software Release 2.1* (321327-B). **NOTE 3**: The pre-boot monitor code upgrades the switch to a new bootrom code that supports SMLT failover features. **CAUTION**: Ensure that the switch does not experience power interruption during installation of the pre-boot monitor code, p16b2100.had, image. The p16b2100.had image can perform an emergency recovery of all other images and power interruption during installation requires system recovery. Recovery after a power interruption can be done only by the manufacturer. If a power interruption occurs during installation of the pre-boot monitor code, use the Return Merchandise Authorization, RMA, procedure to return equipment to the manufacturer for recovery.	

Use the files in Table 2 to perform an upgrade only from version 1.2.x to version 2.1.

Table 2 Upgrade files for release 1.2.x to 2.x upgrade

Software file name	Description
p16a1310.img	Upgrade file NOTE 2
p16c1310.img	Encryption-enabled upgrade file NOTE 1 and NOTE 2
NOTE 1: SSH and SNMPv3 provide increased security and are optional. These software files are available only on the Nortel web site. See Finding the latest updates on the Nortel web site on page 44. Use the p16b2100.had file with the upgrade file to upgrade from release 1.2.x to release 2.x.	
NOTE 2: Use the upgrade file, p16a1310.img or p16c1310.img, to upgrade your switch from Release 1.2.x to Release 2.1. If you are upgrading an encryption-enabled system, ensure that you use the encryption-enabled upgrade file. Encryption-enabled upgrade files are available only on the Nortel web site. See Finding the latest updates on the Nortel web site on page 44. Use the p16b2100.had file with the upgrade file to upgrade from release 1.2.x to release 2.x. For more information about upgrading the Ethernet Routing Switch 1600 Series, see *Upgrading to Ethernet Routing Switch 1600 Series Software Release 2.1* (321327-B).	

Table 3 lists the standards supported in Ethernet Routing Switch 1600 Series, Software Release 2.1.

Table 3 IEEE Standards supported in Release 2.1

Supported Standards	Description
802.1D	MAC bridges and Spanning Tree Protocol
802.1p	VLAN tagging and prioritization
802.1Q	VLAN tagging and prioritization
802.1s	Multiple Spanning Tree protocol (MSTP)
802.1w	Rapid Spanning Tree protocol (RSTP)
802.3 CSMA/CD Ethernet ISO/IEC 8802	ISO/IEC 8802-3
802.3ab	Gigabit Ethernet 1000 BaseT 4 pair Cat5 UTP
802.3i 10BaseT	ISO/IEC 8802-3
802.3u 100BaseT	ISO/IEC 8802-3
802.3x	Flow Control
802.3z	Gigabit Ethernet

Table 4 lists the Request for Comments (RFC) documents supported in Ethernet Routing Switch 1600 Series, Software Release 2.1.

Table 4 RFCs supported in Release 2.1 (Sheet 1 of 2)

Supported RFCs	Description
RFC 768	User Datagram Protocol (UDP)
RFC 783	Trivial File Transfer Protocol (TFTP)
RFC 791	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transport Control Protocol (TCP)
RFC 826	Address Resolution Protocol (ARP)
RFC 854	Telnet protocol
RFC 1058	Routing Information Protocol version 1 (RIPv1)
RFC 1112	Internet Group Management Protocol version 1 (IGMPv1)
RFC 1541 and 1542 (updated by RFC2131)	Bootstrap Protocol and Dynamic Host Control Protocol (BootP and DHCP)

Table 4 RFCs supported in Release 2.1 (Sheet 2 of 2)

Supported RFCs	Description
RFC 1591	Domain Name Server (DNS) Client
RFC1812	Router requirements
RFC 1866	Hypertext Markup Language (HTML) v2.0
RFC 2068	Hypertext Transfer Protocol (HTTP)
RFC 2131	Dynamic Host Control Protocol (DHCP)
RFC 2138	Remote Authentication Dial-in User Service (RADIUS) Authentication
RFC 2139	RADIUS Accounting
RFC 2236	Internet Group Management Protocol version 2 (IGMPv2)
RFC 2328	OSPFv2 protocol
RFC 2362	Protocol Independent Multicast–Sparse Mode (PIM-SM)
RFC2453	RIPv2 protocol
RFC 2474 and 2475	Differential Services (DiffServ)
RFC 2597 and 2598	DiffServ per hop behavior
RFC 2819	Remote Monitoring (RMON) Alarms, Events, Statistics, and Groups

The Ethernet Routing Switch 1600 includes an SNMPv1/v2/v2c/v3 agent with Industry Standard MIBs, as well as private MIB extensions, to ensure compatibility with existing network management tools.

All of the MIBs listed in Table 5 are provided with any version of code. To obtain a file called mib.zip, containing all of the MIB, as well as a special file called mib.txt, containing the order of MIB compilation, consult the Nortel web site at www.nortel.com/support.

Table 5 Supported network management MIBs

Standard MIB name and description	IEEE/RFC	MIB file name
EAPoL (802.1x)	802.1x	ieee8021x.mib
IANA Interface Type	N/A	iana_if_type.mib
Network Management of Transport Control Protocol/Internet Protocol (TCP/IP) based internets MIB2	RFC1213	rfc1213.mib
A convention for defining traps for use with the SNMP	RFC1215	rfc1215.mib
Remote Network Monitoring Management Information Base (RMON) NOTE: The Ethernet Routing Switch 1600 supports alarms, events, statistics, and history.	RFC1271	rfc1271.mib
RIP version 2 MIB extensions	RFC1389	rfc1389,mib
Definitions of Managed Objects for Bridges	RFC1493	rfc1493.mib
Interface MIB	RFC1573	rfc1573.mib
Definitions of managed objects for the Ethernet-like interface types	RFC1643	rfc1643.mib
Routing Information Protocol version 2 (RIPv2) MIB extension	RFC1724	rfc1724.mib
SNMPv3: Architecture for describing SNMP management frameworks	RFC2571	rfc2571.mib
SNMPv3: Message processing and dispatching for SNMP/SNMPv3	RFC2572	rfc2572.mib
SNMPv3: SNMP applications - defines MIB modules for specifying targets of management operations, for notification filtering, and for proxy forwarding	RFC2573	rfc2573.mib
SNMPv3: USMv3 of SNMPv3 MIB for remote monitoring and managing security model configuration parameters	RFC2574	rfc2574.mib
SNMPv3: MIB for remote management of configuration parameters for View-based Access Control Model (VACM)	RFC2575	rfc2575.mib

Table 6 lists the proprietary MIBs available for the Ethernet Routing Switch 1600 series switch.

Table 6 Supported network management MIBs, proprietary

Proprietary MIB name	MIB file name
Rapid City MIB	rapid_city.mib
SynOptics Root MIB	synro.mib
Other SynOptics definitions	s5114roo.mib
Other SynOptics definitions	s5tcs112.mib
Other SynOptics definitions	s53mt103.mib
Nortel RSTP/MSTP proprietary MIBs	nnrst000.mib, nnmst000.mib
Nortel IGMP MIB	rfc_igmp.mib
Nortel VRRP MIB	vrrp_rcc.mib
Nortel IP Multicast MIB	ipmroute_rcc.mib
Nortel PIM MIB	pim-rcc.mib
OSPF Version 2 MIB, Nortel proprietary	rfc1850t_rcc.mib

Supported software and hardware capabilities

This section lists the current values for supported capabilities (Table 7) and the maximum supported hardware and software routes for RIP and OSPF (Table 8) for Software Release 2.1. Unless otherwise noted, values represented in Table 7 are maximum values. Actual values are dependent on implementation.

Table 7 lists the maximum hardware and software capabilities for Ethernet Routing Switch 1600 Series, Software Release 2.1.

Table 7 Hardware and software capabilities (Sheet 1 of 2)

Hardware/Software	Capabilities
Hardware records - MAC	8000
Dynamic ARP entries	1372
Static ARP entries	32

Table 7 Hardware and software capabilities (Sheet 2 of 2)

Hardware/Software	Capabilities
VLANs	2047 **Note:** The range of valid ID numbers is greater than the maximum number of supported VLANs. The range for VLAN IDs is 1- 4000.
Protocol-based VLANs	11
Spanning Tree Group	64 (ID 1 to 64)
Multiple Spanning Tree	8 supported (includes CIST)
Aggregation groups*	7
Ports per MLT group	up to 4 per aggregation group
IP interfaces	64
VRRP IDs	64
Static IP routes	up to 512 with configuration
RIP routes	1918 (see Table 8 on page 15)
OSPF areas per switch	4
OSPF adjacencies (neighbors) per switch	32
OSPF routes per switch	1918 (see Table 8 on page 15)
OSPF virtual link per Area	1
MTU**	1518 (1522 for tagged ports)
Multicast streams	64 (S, G)
IGMP Snoop VLANs	256
* Aggregation groups are statically compliant with the IEEE 802.3ad standard.These groups should be of the same type. ** Jumbo frames are not supported in Release 2.1. IP Subnet-based VLANs are not supported in Release 2.1. DVMRP is not supported in Release 2.1.	

Table 8 describes the maximum supported hardware and software routes for RIP and OSPF.

Table 8 Maximum supported hardware and software routes for RIP and OSPF

Hardware size			
Ratio	**UC prefix (entry)**	**MC prefix (entry)**	
100/0	1916	0	
75/25	1404	64*	
50/50	892	64*	
* 64 assumes sequential numbering of the IP multicast group prefix (x.x.x.y, sequential number of the y value) NOTE: See these Change Requests in Known limitations and considerations in this release: Q01325124 and Q01273341on page 33, PIM/Scaling.			
Software size			
Ratio	**Route entry**	**ARP entry**	**IPMC entry**
100/0	1884/32	1884/32	0
75/25	1372/32	1372/32	64*
50/50	860/32	860/32	64*
Note: Route entry and ARP entry values indicate dynamic routes/static routes. For example, the 75/25 ratio for Route entry indicates 1372 dynamic routes with 32 static routes.			

In Software Release 2.1, the Ethernet Routing Switch 1600 Series switch supports the SFP (Small Form-factor Pluggable) modules listed in Table 9.

Table 9 Supported SFP modules

Product number	Model
AA1419013	1-port 1000Base-SX connector type: LC
AA1419014	1-port 1000Base-SX connector type: MT-RJ
AA1419015	1-port 1000Base-LX connector type: LC
AA1419025	1-port 1000BaseCWDM- 1470nm wavelength- 40km
AA1419026	1-port 1000BaseCWDM- 1490nm wavelength- 40km
AA1419027	1-port 1000BaseCWDM- 1510nm wavelength- 40km
AA1419028	1-port 1000BaseCWDM- 1530nm wavelength- 40km
AA1419029	1-port 1000BaseCWDM- 1550nm wavelength- 40km
AA1419030	1-port 1000BaseCWDM- 1570nm wavelength- 40km
AA1419031	1-port 1000BaseCWDM- 1590nm wavelength- 40km
AA1419032	1-port 1000BaseCWDM- 1610nm wavelength- 40km
AA1419033	1-port 1000BaseCWDM- 1470nm wavelength- 70km
AA1419034	1-port 1000BaseCWDM- 1490nm wavelength- 70km
AA1419035	1-port 1000BaseCWDM- 1510nm wavelength- 70km
AA1419036	1-port 1000BaseCWDM- 1530nm wavelength- 70km
AA1419037	1-port 1000BaseCWDM- 1550nm wavelength- 70km
AA1419038	1-port 1000BaseCWDM- 1570nm wavelength- 70km
AA1419039	1-port 1000BaseCWDM- 1590nm wavelength- 70km
AA1419040	1-port 1000BaseCWDM- 1610nm wavelength- 70km
AA1419043	1-port 1000BASE-T Small Form Pluggable (SFP), 8-pin modular connector (RJ-45).

Upgrading the switch to Release 2.1 software

Refer to *Upgrading to Ethernet Routing Switch 1600 Series Software Release 2.1* (321327-B) for detailed procedures to upgrade the switch.

Caution: Ensure that the switch does not experience power interruption during installation of the pre-boot monitor code, p16b2100.had, image. The p16b2100.had image can perform an emergency recovery of all other images and power interruption during installation requires system recovery. Recovery after a power interruption can be done only by the manufacturer. If a power interruption occurs during installation of the pre-boot monitor code, use the Return Merchandise Authorization, RMA, procedure to return equipment to the manufacturer for recovery.

Following is a list of available upgrade and downgrade procedures:

- Software Release 1.x to 2.1 Automatic Upgrade Procedure
- Software Release 1.x to 2.1 Manual Upgrade Procedure
- Software Release 2.x Upgrade Procedure using the CLI
- Software Release 2.x Upgrade Procedure using the JDM
- Software Release 2.1 to 1.x Downgrade Procedure

Note: Read the entire upgrade procedure before attempting to upgrade the switch. Upgrade procedures cause interruption of normal switch operation. Back up your runtime configuration and boot configuration before starting the upgrade process.

Software upgrade is supported from Release 1.2.x upward. An intermediate release, Release 1.3.1, has been created to manage the translation of the 1.2.x configuration file (because of the differences between the Release 1.2.x and the Release 2.1 CLI) and to collect some required information (such as TFTP Server IP Address) to support the upgrade process from Release 1.2 to Release 2.1. During the upgrade process, a new configuration file is created based on the

Ethernet Routing Switch 8000 CLI. The Release 1.3.1 upgrade process translates the 1.2.x configuration files to Release 2.1 and generates a file containing a list of CLI commands that require manual intervention. See CLI commands that require manual translation on page 35.

Caution: Nortel recommends that you back up your configuration prior to upgrading the software from Release 1.2.x to Release 1.3.1 because your configuration is lost when the flash memory is reformatted during the upgrade process.

If you are upgrading an encryption-enabled system, when the upgrade to Release 2.1 is complete you must manually load the encryption-enabled upgrade files to enable encryption on your upgraded system.

New hardware for this release

There is no new hardware for this release.

New software features in this release

This section describes the new software features, by function, for the Ethernet Routing Switch 1600 Series Software Release 2.1compared to Release 1.2.

Platform

Release 2.1 supports the following list of new Platform features:

- File system–based on the Ethernet Routing Switch Series 8600 file system
- CLI compatible with Ethernet Routing Switch Series 8300 and Series 8600

  The NNCLI is not supported in Release 2.1.

Layer 2

Release 2.1 supports the following list of new Layer 2 features:

- Single Link Trunking (SLT)
- Split MultiLink Trunking (SMLT)

IP Subnet Based VLANS are not supported in Release 2.1.

For more information, see *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (321717-B) and *Configuring VLANs, Spanning Tree, and Static Link Aggregation using Device Manager* (321718-B).

To provide interoperability between the Ethernet Routing Switch 1600 Series and the Ethernet Routing Switch Series 8300 and 8600, Release 2.1 supports the Nortel Spanning Tree Group (STG) proprietary implementation.

The Ethernet Routing Switch 1600 Series switch boots in Spanning Tree Mode (STP) by default.

To change the mode, do the following :

- Execute the following command:

  ```
  ERS1624>:1/config/bootconfig/flags# spanning-tree-mode
  <mstp|rstp|default>
  ```

- Save the boot config file.
- Reboot the switch.

Layer 3

Release 2.1 supports the following new Layer 3 features:

- VRRP Backup Master
- Routing Policies
- ICMP Router Discovery

Multicast

Release 2.1 supports the Protocol Independent Multicast–Sparse Mode (PIM-SM).

Distance Vector Multicast Routing Protocol (DVMRP) is not supported in Release 2.1.

For more information, see *Configuring IP Routing and Multicast Operations using the CLI* (321711-A) and *Configuring IP Routing and Multicast Operations using Device Manager* (321712-B).

Network Management

Release 2.1 supports SNMPv3.

For more information, see *Configuring Network Management using the CLI and Device Manager* (321816-A).

QoS and Filtering

The Release 2.1 QoS and Filtering feature is expanded from 4 to 8 queues.

For more information, see *Configuring QOS and Filters using the CLI and Device Manager* (321822-A).

Security

Release 2.1 supports the following new Security features:

- 802.1x Extensible Authentication Protocol (EAP)
- EAP and RADIUS MAC centralization–allows users to mix non-EAP and EAP stations on the same port and also allows mobility for these stations because MAC is configured once, centrally, with the RADIUS server
- Remote Dial In User Service (RADIUS) authentication
- RADIUS accounting – centralization of management access with accounting allows users to record management sessions by criteria like time of day, duration, and traffic.

- SNMPv3

For more information, see *Configuring and Managing Security using the CLI* (321714-B) and *Configuring and Managing Security using Device Manager* (321713-B).

Problems resolved in this release

The following topics are considered in this section:

Table 10 describes issues resolved in the Ethernet Routing Switch 1600 Series Software Release 2.1.

Table 10 Resolved issues, by type of issue (Sheet 1 of 6)

CR reference	Description
Hardware	
	No updates for this section

Table 10 Resolved issues, by type of issue (Sheet 2 of 6)

CR reference	Description
Software	
Platform	
	No updates for this section.
CLI	
Q00620617	When you disable STP ports using the CLI `config ports state disabled` command, it means that STP no longer works on the specified ports and they remain in the forwarding state.
Q00872911	This CR is not applicable to Release 2.1 because the operating system differs from the previous release. Care should be taken when modifying the max_static route size to ensure that other administrators are not concurrently modifying the configuration. This is because this command will automatically do a save and reboot. Others attempting to do a save will interfere with this process.
Q00599270	This CR is not applicable to Release 2.1 because the operating system differs from the previous release. You can accidentally remove your IP address when executing the CLI `reset config` and `reset system` commands.
Q00651775	This CR is not applicable to Release 2.1 because the operating system differs from the previous release. While the 1600 Series switch allows you to have multiple administrator accounts, you cannot delete or modify the default admin account username `rwa`.
Q00637504	This CR is not applicable to Release 2.1 because the operating system differs from the previous release. When you attempt to use the up-arrow key to recall a CLI command whose length is over 80 characters, and either move the cursor or use <Backspace> to delete, the cursor moves up a line. This problem typically occurs when the Telnet session's window width is set to more than 80 characters.
Q00654586	This CR is not applicable to Release 2.1 because the operating system differs from the previous release. The question mark (?) is not recognized by the CLI in the 1600 Series switch. Press <CR> to obtain help by way of the *Next possible completions* option.
Q00699418	You cannot partially disable link aggregation ports. You must either disable or enable all of the ports.

Table 10 Resolved issues, by type of issue (Sheet 3 of 6)

CR reference	Description
Q00615078	When you enter the `show iproute` command, the route preference ranges and defaults that display as output are different in the Ethernet Routing Switch 1600 switches than they are in the Ethernet Routing Switch 8600. For example, the 8600 contains route preferences that range from 0 to 175, with 0 being the highest priority. By contrast, the 1600 route preferences range from 0 to 10, with 10 being the highest priority. Note that as far as the route protocol behavior is concerned, both the Ethernet Routing Switch 1600 and 8600 are the same.
Q00720617	Once you remove a port from an untagged port list, its PVID becomes 0.
Device Manager (JDM)	
Q00873714	The Device Manager uninstaller gives an out-of-memory exception.
Q00636659	JDM shows multicast packets as NUcastPkts, or Non-Unicast packets. There are no separate rows for multicast and broadcast packets in the JDM graph.
Q00728030	System names are limited to 15 characters.
Q00715696	In the CLI, the IP routing table shows the gateway IP for the local subnet as the local IP interface. In the JDM, however, the next-hop for the local subnet displays as IP 0.0.0.0.
Q00719409	Note that this issue is not relevant for the Ethernet Routing Switch 1600 since it has no separate management port.By default, the management port on the Ethernet Routing Switch 1612G and 1624G switches is part of the default VLAN. Thus, there is no way to manage this port from the JDM. Instead, it is recommended that you use the CLI.
Layer 2	
Q00788268	After creating the protocol-based VLAN, you can not dynamically change the EtherType or Protocol ID. You must first delete the VLAN, then recreate it with the new EtherType and Protocol ID.
Q01014687	When the Ethernet Routing Switch 1600 is running in RSTP or MSTP mode, any port that receives a legacy STP BPDU migrates to STP-compatible mode. However, the Ethernet Routing Switch 1600 has no log event for this situation. Although the port has migrated to STP, in Device Manager (JDM), the port's OperVersion will not update to STP-compatible mode. JDM will continue to show the port operating in the original MSTP or RSTP mode.
Q00621524	When you connect two Ethernet Routing Switch 1600 switches and configure link aggregation on both of them, traffic transmits without any problem. However, if link aggregation is disabled on one of the switches, a network loop occurs since the switch with link aggregation enabled only sends out BPDUs on the master port. This causes all the ports on the switch with link aggregation disabled to go into forwarding mode, thus causing a network loop. Be aware that this scenario only occurs when the Ethernet Routing Switch 8600 compatibility option is turned off. This option ensures that the Spanning Tree Protocol (STP) running over a Local Area Group (LAG) is compatible with the 8600. Ensure that this compatibility option is turned on.

Table 10 Resolved issues, by type of issue (Sheet 4 of 6)

CR reference	Description
Q00640319	When an Ethernet Routing Switch 1600 Series switch and an Ethernet Routing Switch 8600 are connected with 2 MLT links, STP works properly as long as the 8600 is the designated root bridge. When the 1600 is the designated root bridge, however, only one of the MLT ports on the 8600 side transitions to the appropriate STP state (forwarding), while the rest remain in the listening state. This can cause problems, such as the 8600 dropping control traffic received on the ports that are in listening state. It is strongly recommended that you use the option to make the 1600 work in 8600 compatibility mode, **and** configure the 8600 as the root bridge. Configuration **must** be performed using the Command Line Interface. You cannot configure this using the Device Manager (JDM).
Layer 3	
Q00804183	VRRP–Nortel Networks guarantees the following combination of VRRP and OSPF routes: VRRIDs OSPF routes LSDB entries Areas 4 760 4284 4 8 740 4164 4 16 715 4014 4 24 675 3885 4 32 650 3735 4 **NOTE**: Scaling limits from Release 1.2 no longer apply. Release 2.1 meets the expected scalability of 64 VRRP instances with maximum OSPF routes.
Q00803727	VRRP–When you implement VRRP between an Ethernet Routing Switch 1600 and an Ethernet Routing Switch 8600, do not configure the authentication field. Ethernet Routing Switch 8600 does not support VRRP authentication as defined in the RFC. If you enable authentication on the Ethernet Routing Switch 1600, you could encounter a situation where both routers would be master.
Q00804959	VRRP–Once you modify an IP interface used for a VRRP, the VRRP interface will be removed. However, the total number of VRRP interfaces remains unchanged (even though the total number of VRRP interfaces should decrement by one)
Q00566603-01	IP–The 1600 Series switch does not support an IP deny policy, and thus, cannot deny some unwanted routes. For RIP, the route preference is lower than OSPF external type 1 and 2 routes. Because of this, if the 1600 works as an Autonomous System Border Router (ASBR), it redistributes those OSPF external type 1 and 2 routes back to the OSPF network. Also, the ASBR picks RIP instead of OSPF for those OSPF external routes.
Q00718213	RIP–When you create or modify a RIP interface, the status follows the RIP global state automatically. For example, if RIP is globally enabled, once you modify the interface, it is also enabled.
Q00711011	OSPF–The Hello and DeadInterval timers are the only OSPF timers supported on the 1600 Series switch CLI and JDM. The standard MIB contains other OSPF timers which are read/write and may be set with other SNMP tools. However, be aware that these are *not* supported.

Table 10 Resolved issues, by type of issue (Sheet 5 of 6)

CR reference	Description
Q00961939	OSPF–When using GBICs in MLT configurations, OSPF may take a long time to become stable if the MLTs are configured in "force mode 1000_full".
Multicast	
Q00844463	The accuracy of the CP limit feature for the multicast frames (IGMP) is plus or minus 100 frames. **NOTE**: This design issue is not applicable to Release 2.1.
Bandwidth management	
	No updates for this section.
Web Management Interface	
Q00718412	In the Web management interface, under Network Monitoring > Address Table > OSPF > OSPF LSDB table –If you filter by LSDB Type: ASExtLink, do not enter a value into the AREA ID since the external links are not associated with an area.
Network Management	
Q00815285	A telnet session automatically expires, triggered by the serial port logout timer (there is only one timer for both console and telnet sessions). To configure serial port logout timer, use the following CLI command: `config serial_port auto_logout never |2_minutes}5_minutes|10_minutes|15_minutes`
Security	
Q00801010	You must create a TACACS+ server prior to selecting TACACS+ as an authentication type in either the JDM or CLI.
Q00797922	TACACS+ does not properly support authenticating Web access to the switch. Because the switch can handle this authentication locally, Nortel recommends that you configure Web Access in this manner. **NOTE**: This limitation is not applicable to Release 2.1
Q00872906	The CLI command config authentication allows entry of a 3rd parameter, but returns an error message that the chosen authentication method cannot exceed two. **NOTE**: This limitation is not applicable to Release 2.1
Miscellaneous	
Q00718504	Be aware that the JDM and CLI use different terms to refer to ingress filtering. The JDM uses ingress filters while the CLI uses ingress checking. Both terms refer to the same set of features. **NOTE**: This limitation is not applicable to Release 2.1.

Table 10 Resolved issues, by type of issue (Sheet 6 of 6)

CR reference	Description
Q00719351	The Ethernet Routing Switch 1600 Series switch does not support the swL2IGMPMaxIpGroupNumPerVlan MIB. **NOTE**: This limitation is not applicable to Release 2.1.
Q00720343	**NOTE**: This limitation is not applicable to Release 2.1. If the management port is left in the default VLAN in the Ethernet Routing Switch 1600 switch, multiple packets are sent by the management port. This problem occurs because in the Ethernet Routing Switch 1600 default configuration all ports are in the same, default VLAN. Before you move all the ports out, those ports forward traffic to one another. After connecting to the Ethernet Routing Switch 1612 and 1624, Nortel recommends that you isolate the management port by placing it in its own VLAN. Do this through the CLI, as JDM does not support this capability. To do so, use the following procedure: Create a VLAN named mgmt or management with VLAN ID 4094 as follows: create vlan mgmt vid 4094 Configure the System IP interface and attach it to VLAN mgmt as follows: config ipif System ipaddress x.x.x.x/x vlan mgmt state enable Use the following CLI command to verify that the mgmt_port is in the VLAN mgmt: show vlan Note that this problem is related to Q00705437 which involves the same overall issue, with a different result.
Q00718397	The Transmit counter for Bridge Protocol Data Units (BPDUs) on the Gigabit ports will not increment. This occurs with the Gigabit ports on all three models of the 1600 Series switch. To monitor STG/RSTP/MSTP/BPDU statistics, use the `show ports stats stg` command.

Known limitations and considerations in this release

The following topics are considered in this section:

Table 11 describes issues known to exist in the Ethernet Routing Switch 1600 Series Software Release 2.1.

Table 11 Known limitations, by type of issue (Sheet 1 of 9)

CR reference	Feature	Description
Hardware		
Q01299661	Connectivity	When a 1600 Series switch using a DLink Gbic is connected to an 8600 Series switch with an 8608 SX line card the console, telnet, or JDM sessions can be unresponsive for up to one minute when the neighbor experiences a power cycle or software reboot.

Table 11 Known limitations, by type of issue (Sheet 2 of 9)

CR reference	Feature	Description
Software		
Platform		
Q01148274 Q01148347	Autonegotiate, Mixed mode	If you configure your system to operate in mixed mode with GBIC ports the following problems may occur. If a GBIC port is set to autonoegotiate, the far-end link must also be set to autonegotiate. The current release does not support mixed mode with GBIC ports. GBIC port link behavior in auto-negotiate mode is incorrect when the port state of a link partner is forced to 1000_Full. Uplink port LEDs in auto-sense mode do not go out and link state does not go down.
Q01219004	Configuration, Upgrade, Downgrade	There is a conflict between the VLAN ID setting ranges - version 1.x is 1..4094 and version 2.0 is 1..4000. **SOLUTION:** After upgrade or downgrade is complete, reconfigure the VLAN ID settings for the appropriate software version.
Q01402147	DFCDL	Some SDRAM setting information appears during system startup if the device uses Samsung E 2004, Samsung G Auto, or a new SDRAM with Auto Adjustment feature. These messages have no impact on system operation. Following are the messages which may appear: Set DFCDL table: Table index 0 - Value: 0x00000000 Table index 1 - Value: 0x00001040 .... Table index 62 - Value: 0x000279dd Table index 63 - Value: 0x000279de coreSnapshotFdbInit : Init done coreSnapshotFdbInit : Init done 0x1e5ba70 (rcStart): ppStart1600: successful TAPI gmirrLibInit library initialization, error 0
Q01201523	High secure flag	The high secure flag–bootconfig flags hsecure–is not supported in Release 2.1.
Q01208133	Port Mirroring	Mirroring fails if the mirrored port and mirroring port are in different Spanning Tree Groups. **WORKAROUND** Ensure that a mirroring port is in the same Spanning Tree Group as a mirrored port.

Table 11 Known limitations, by type of issue (Sheet 3 of 9)

CR reference	Feature	Description
Q01363944	Unicast/Multicast ratio	Asic Unicast/Multicast ratio now has a default ratio of 75/25 when you perform a factory default restoration of the configuration. This differs from Release 1.x which did not restore the configuration to a factory default, but retained the user-configured setting.
Layer 2		
Q01237394	IP interface	IP interface MAC address displays as 00.00.00.00.00.00 if you shut down the IP interface by disabling all ports in the VLAN.
Q01283905	MSTP	In certain configurations with an extremely high number of topology loops, topology changes can reduce system performance. An extremely high number of topology loops is considered, for example, 30 VLANS where each VLAN has 10 topology loops. A topology change is, for example, changing the root bridge router.
Q01256212	MSTP	There is no global enable and disable option for MSTP. If you disable MSTI and CIST on a per port basis, Bpdu packets are dropped, not forwarded.
Q01245689	MSTP	The CIST PathCost parameter does not display when you invoke the show port info mstp cistinfo command. **WORKAROUND**: Use the config ether <slot/port> mstp cist info command to to view the CIST PathCost information.
Q01288796	RSTP	Rapid Spanning Tree Protocol (RSTP) does not converge on multilink trunking (MLT) ports on Cisco 6500 CATOS releases 8.8-5-1 and 8.8-5-3 and an Ethernet Routing Switch Series 1600 switch.
Q01357019	SMLT	Do not use MT-RJ Small Form-factor Pluggable (SFP) GBICs for SMLT configurations. Recovery time increases by approximately one second per MT-RJ in a full switch failure test if you use MT-RJ SFP GBICs for SMLT configurations.
Q01371928	SMLT	Do not use force mode (autonegotiate disabled) between Ethernet Routing Switch 1600 switches when SMLT ports are configured. Recovery time increases if you use force mode in this configuration.
Q01379448	SMLT	If a station moves within the network with SMLT configured, the move is not seen for up to 15 minutes; that is, until the MAC ages out. **PROPOSED SOLUTION**: Reduce the FDB age-out time to minimize the time it takes for moves to be detected.
Q01341626	SMLT	Multiple VRRP IDs can be configured with the same VrID but the system will not function correctly. **SOLUTION**: Do not configure multiple VRRP IDs with the same VrID.

Table 11 Known limitations, by type of issue (Sheet 4 of 9)

CR reference	Feature	Description
Q01392504 Q01393395	SMLT, Multicast	In an SMLT configuration with PIM enabled, Nortel recommends that you do not configure Multicast receivers in IST switches or in Core areas.
Q01395688	SMLT, Multicast	If the sender is on a Layer 2 edge switch of an SMLT configuration and the sender port is disabled, the sender entry is not purged until the port is re-enabled.
Q01396190	SMLT, Multicast	When the PIM DR and PIM RP are on different iST switches, some traffic can be lost. **SOLUTION**: In an SMLT configuration, do not configure PIM RP in the same switch where the non-DR of the incoming VLAN resides.
Q01400968	SMLT, Multicast	In an SMLT configuration with PIM enabled, Nortel recommends that you do not extend the SMLT VLAN to a non-SMLT device.
Q01248609	STP	Do not use any Multicast control packet MAC addresses as STP BPDU MAC addresses.
Q01162520	Unknown MAC Discard	When an allowed MAC is learned on one port and then moved to another port, the MAC entry is not learned.
Q01162518	Unknown MAC Discard	Manually allowed MAC entries can be lost when the same MACs are received from another port configured as auto-learn.
Q01161751	Unknown MAC Discard	The Autolearn MAC learning function does not add the dynamic learned MAC address entries to the Allow MAC table after your disable or enable the three setting flags for activation, autolearn, and lock-autolearn-mac. **WORKAROUND**: Use the command `config ether slot#/port# action flushMacFdb` to flush out all existing MACs so the Autolearn MAC learning function can re-learn FDB entries.
Q01165950	VLAN	If you have all ports assigned to all VLANS and attempt to untag all of the ports, the untag operation generates the VLAN error message vlanDelMac:msgQSend failed.
Q01184453	VLAN	If tagged frames from a different VLAN ID are sent into an untagged port, CPU utilization increases. **CAUTION**;: Do not send tagged frames from a different VLAN ID into an untagged port.
Q01202109	VLAN	The Ethernet Routing Switch 1600 Series supports 2047 VLANS. One VLAN is used internally for ports not bound to any VLAN. Refer to New software features in this release on page 18.
Q01386046	VLAN	If you do not configure the VLAN before you execute the command `config vlan <vlan_id> ports info` then an incorrect VLAN ID may display in the error message.

Table 11 Known limitations, by type of issue (Sheet 5 of 9)

CR reference	Feature	Description
Layer 3		
Q01329829	Directed Broadcast	Directed Broadcast Suppression is not supported.
Q01194759	ICMP	An advertisement with Lifetime equal to zero is not sent when the advertise flag is set to False.
Q01216266	IP, OSPF	When you change the import-summary configuration from false to true, the link state update is incomplete. **SOLUTION**: To get the summary Link State Advertisements into the stub area, toggle the OSPF admin state. Toggling the OSPF admin state initiates SPF and the Link State Advertisements are imported.
Q01212971	IP, OSPF	Authentication Key configuration display behavior differs between an OSPF IP Interface and an OSPF Virtual IP Interface. Authentication Key function is not affected. For example; on an IP Interface, when Authentication is turned off, the key no longer displays; while for an OSPF Virtual IP Interface, when Authentication is turned off, the key continues to display.
Q01233606	IP, OSPF	OSPF Accept/In filter for route policy does not filter type 1 and type 2 external routes propagated from the advertising router.
Q01212054	IP, OSPF	If you set the retransmit interval setting to 0 the switch bursts OSPF Data Description Packets continuously when it receives the neighbor hello packet. This continues until the dead interval expires (40 seconds). **WORKAROUND**: Do not set the retransmit interval setting to 0.
Q01174157	IP, RIP	When the RIP interface receives a RIP request packet for a complete routing table, the switch responds at the next scheduled transmission (in 30 seconds instead of immediately).
Multicast		
Q01303686	IGMP	The IGMP sender table may not contain the IGMP sender unless you use a PIM-enabled interface.
Q01304703	IGMP	If the last 23 bits of Multicast IP addresses are the same, they map to the same multicast MAC address and cannot be distinguished from each other. For example, if a client joins IP group address A it may receive the traffic from IP group address C because the groups have the same Multicast MAC address.
Q01166814	IGMP	Because the mapping of Multicast IP address to Multicast MAC addresses is not unique, only one multicast MAC address is entered into the IGMP Sender Table.

Table 11 Known limitations, by type of issue (Sheet 6 of 9)

CR reference	Feature	Description
Q01155294	IGMP	When you request Help for IGMP on a VLAN the following parameters are not displayed: • robustval • query-max-resp • last-memb-query-int
Q01162481	IGMP	An incomplete group IP is accepted as a static IGMP member. For example, if you configure 224.1.1 as a static IGMP member, the switch adopts the configuration of 224.1.1.0.
Q01322116	PIM	Use the trace command `Pimdbgtrace` on a telnet session only. Do not use this command with a console connection.
Q01366606	PIM	Routing of multicast datagrams with a group address of x.0.0.13 is not supported. Refer also to CR Q01369313.
Q01369313	PIM	Forwarding of any multicast datagrams with a destination address of x.0.0.y (where x is in the range from 224 to 239 and y is in the range from 0 to 255 inclusive) is not supported. Refer also to CR Q01366606.
Q01331170	PIM	In an extended VLAN with MLT (where the Ethernet Routing Switch 1600 Series is the intermediate device and Ethernet Routing Switch 8600 series switches are upstream neighbors), MLT failure and recovery between the Ethernet Routing Switch 1600 Series and the Ethernet Routing Switch 8600 series can result in unstable traffic. **SOLUTION**: Do not install an Ethernet Routing Switch 1600 series switch in an extended VLAN that has an Ethernet Routing Switch 8600 on both ends.
Q01330190	PIM	An entry cannot be built in the mroute table and data cannot be forwarded for the second sender when senders from a different source (sending traffic to the same group) belong to the same network. **SOLUTION**: Do not configure multiple senders serving the same group in the same subnet.
Q01329813	PIM	PIM-SM Static RP is not supported in Release 2.1.
Q01287247	PIM	If there is an intermediate switch between the sender switch and the Rendezvous Point (RP), when an Ethernet Routing Switch 1600 Series is designated as the RP, the RP may continue to receive traffic after Shortest Path Tree (SPT) switchover if both the sender and receiver are on the same switch.
Q01251555	PIM	Circuitless IP is not supported on PIM-SM.

Table 11 Known limitations, by type of issue (Sheet 7 of 9)

CR reference	Feature	Description
Q01275238	PIM	Querier (*,G) entry cannot be created in mroute table after failover on a non-DR. If two IGMP routers are active in the same VLAN, the router with the lowest IP address is elected as the querier and any Layer 2 snoop-enabled switches exchange IGMP information with this querier (router with the lowest IP address). If the same two routers are subsequently PIM-enabled, the router with the highest IP address is elected as the PIM DR. While the Layer 2 hosts attempt to communicate with the lower IP querier, the host reports cannot reach the PIM domain. To communicate properly with the PIM-enabled routers, the Layer 2 switch must send IGMP reports to the non-querier (the PIM DR) **WORKAROUND**: Enable Multicast Router Discovery on the switch and routers.
Q01325124 Q01273341	PIM, Scaling	Refer to Table 8 on page 15 for scaling values. If your configuration over-subscribes the stated values, scaling problems may occur and error messages may appear in two separate, but related, cases when the scaling limits are exceeded. 1. The addition of too many multicast sources (S,G) may fill the table directly and the following message appears: apiAddNewSesion: ipv4AddMcRoute did not add the session and returned Error 2. If the table is near capacity and a reboot or failover of a link occurs, addition of new S,G is prevented (a certain amount of free memory is required to allow additions and deletions). The scaling numbers given leave enough spare capacity to avoid this problem, but, if the network administrator does not monitor the number of multicast sources and groups in the network to ensure that they remain within the limit, the table fills and new S,G addition is prevented. New PIM Multicast session creation fails and the following error messages appear : ipv4GetMcRouteInfo failed for tapiAddNewSesion: ipv4AddMcRoute did not add the session and returned Error Passport-1648T:1# CPU1 [08/25/37 01:48:24] PIM WARNING k_chg_mfc FAIL New Session 172.168.40.101 224.1.2.56 is failed **CAUSE**: Multicast scaling has a limit. **WORKAROUND**: To achieve best results, use sequential group IP addresses.
Traffic Management		
Q01272583	Filter, L4	L4 Redirect is not supported when the destination IP is a Multicast IP.
Q01278761	Filter, L4	IGMP drop rules do not take effect when PIM is enabled on the switch.

Table 11 Known limitations, by type of issue (Sheet 8 of 9)

CR reference	Feature	Description
Q01219027	QoS	The `config vlan <id> fdb-entry qos-level` command is not saved in the config.cfg file.
Network Management		
Q01361831	Access policies	Access policies for the SNMP service are unavailable in this release. **WORKAROUND**: Use SNMPv3 to selectively provide access to specific users and specific parts of the MIB.
Q01364992	MLT	The procedure to enable tagging on an MLT differs between the CLI and the device manager.
Q01395671	Telnet, Rlogin	You cannot open the maximum number of Telnet and Rlogin sessions simultaneously.
Command Line Interface		
Q01201501	CLI password	CLI password aging, and CLI password history are not supported in Release 2.1.
Device Manager (JDM)		
Q01370201	Statistics	Some bridging and routing statistics are unavailable through the Device Manager. **WORKAROUND**: Use the CLI.
Web Management Interface		
Q01169519	Bridging Multicast table entries	There is a discrepancy between the Web and the CLI for Bridging Multicast table entries. The Web indicates 99 entries and the CLi indicates 128 entries.
Q01351648	MIB, SNMP	The Web interface does not display the correct product type.
Q01177400	RADIUS	On the Web page the RADIUS Server Statistics table is empty.
Q01177397	RADIUS	On the Web page the RADIUS Server Table is empty.
Q01256235	SNMPv3	SNMPv1users can access the SNMPv3 MIB from other MIB tools.
Q01256220	SNMPv3	A user cannot log on if the user EngineID differs from the device EngineID. **SOLUTION**: Do not create a new account with an EngineID that differs from the device EngineID.
Q01248626	SNMPv3	When a new SNMPv3 user is created and assigned to a non-existent group there is no warning message.
Q01248630	SNMPv3	When an SNMP-V3 group member is deleted, an incorrect error message appears. The error message incorrectly refers to group entry when it should refer to the specific user.

Table 11 Known limitations, by type of issue (Sheet 9 of 9)

CR reference	Feature	Description
Q01150214	VLANs	When you use the Web browser to read VLAN port information an Exception message appears. This situation is associated with large number of VLANs and tagged ports. **SOLUTION**: Press **Enter** to continue operating the console.
Security		
Q01372064	Filters	When you configure a flow-classifier template to security mode and configure the security source or destination mask as 0.0.0.0, no error or warning messages are generated. When you then try to configure a rule with the security source set as IP, you receive a consistency check error. **SOLUTION**: Do not use 0.0.0.0 as a source or destination mask.
Q01201583	High secure bootconfig flag, Passwords	The high secure bootconfig flag, implemented in the Ethernet Routing Switch 8600, is not available in the Ethernet Routing Switch 1600 Series Release 2.1. **CAUTION**: Nortel recommends that you change the passwords and community strings immediately, that you manually disable nonsecure services such as FTP and telnet, and that you use only SNMPv3 or SSH/SCP.
Miscellaneous		
There are no Change Requests for this section.		

CLI commands that require manual translation

During the upgrade process a new configuration file is created based on the Ethernet Routing Switch 8000 CLI. The version 1.3 upgrade process translates the 1.2.x configuration files to version 2.1 and generates a file containing a list of 1.2.x CLI commands that cannot be automatically upgraded.

Commands in Table 12 are not translated during the upgrade process.

Table 12 CLI commands not translated during software upgrade (Sheet 1 of 5)

Command	Comments
Platform	
config log_state <username> [enabled|disabled]	No 8000 equivalent CLI
config remote_user log state [enabled|disabled]	No 8000 equivalent CLI

Table 12 CLI commands not translated during software upgrade (Sheet 2 of 5)

Command	Comments
enable snmp authenticate traps	config sys set sendAuthenticationTrap true
disable snmp authenticate traps	config sys set sendAuthenticationTrap false
enable snmp traps	No 8000 equivalent CLI
disable snmp traps	No 8000 equivalent CLI
disable post	No 8000 equivalent CLI
enable telnet {<tcp_port_number 1-65535>}	8000 implementation does not permit TCP port number configuration
config password_aging<day 1-999>	No 8000 equivalent CLI
config secure_mode [normal|high]	No 8000 equivalent CLI
DNS Relay	
config dnsr [[primary|secondary] nameserver <ipaddr>|[add|delete] static <domain_name 32><ipaddr>]	No 8000 equivalent CLI
disable dnsr {cache | static }	No 8000 equivalent CLI
enable dnsr {cache | static }	No 8000 equivalent CLI
SNTP (Simple Network Time Protocol)	
config sntp Unicast Polling Interval {<value 1 - 1440>}	No 8000 equivalent CLI
Port configuration	
config scheduling ports [<portlist> | all] class_id <value 0-2> max_packet <value 6-255>	No 8000 equivalent CLI
config ports [<portlist>| all]learning disabled	No 8000 equivalent CLI
config mgmt_port {speed [auto | 10_half | 10_full | 100_half |100_full] | flow_control [enabled | disabled] | state [enabled |disabled]}	Refer to *Upgrading to Ethernet Routing Switch 1600 Series Software Release 2.1* (321327-B)
STP/FDB/VLAN	
config stp fbpdu enable (MSTP/RSTP/STP)	No 8000 equivalent CLI
enable stp (MSTP)	No 8000 equivalent CLI
disable stp (MSTP)	No 8000 equivalent CLI
create mac_priority vlan <vlan_name> dst_mac_addr <macaddr> priority <value 0-7>	No 8000 equivalent CLI
create fdbfilter vlan <vlan_name> mac_address ff-ff-ff-ff-ff-ff	No 8000 equivalent CLI

Table 12 CLI commands not translated during software upgrade (Sheet 3 of 5)

Command	Comments
create vlan <vlan_name 32> [ip-subnet <network_address>{arp_classification_id <vlanid 1-4094>}	No IP Subnet VLAN support in version 2.x
config ipif <ipif_name 12> directed-broadcast [enabled|disabled]	No 8000 equivalent CLI
config vlan_ports [<portlist> | all] ingress_checking [enabled | disabled]	No 8000 equivalent CLI
config vlan_ports [<portlist> | all] acceptable_frame [all|onlyTagged]	No 8000 equivalent CLI
IGMP Snooping	
config igmp_snooping [<vlan_name 32> |all] host_timeout <sec 1- 16711450>	No 8000 equivalent CLI
config igmp_snooping [<vlan_name 32> |all] router_timeout <sec 1-16711450>	No 8000 equivalent CLI
config igmp_snooping [<vlan_name 32> |all] leave_timer <sec 1- 16711450>	No 8000 equivalent CLI
config igmp_snooping querier [<vlan_name 32> |all] { query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-65535> }	No 8000 equivalent CLI
disable igmp_snooping {filtering}	No 8000 equivalent CLI
enable igmp_snooping {filtering|forward_mcrouter_only}	No 8000 equivalent CLI
ARP/IP/DVMRP/IGMP/VRRP	
config arp_req_rate_limit <value 10-100>	No 8000 equivalent CLI
enable arp_req_rate_limit	No 8000 equivalent CLI
disable arp_req_rate_limit	No 8000 equivalent CLI
create arpentry <ipaddr> <macaddr>	No 8000 equivalent CLI
config ipif <ipif_name 12>{ state [enabled|disabled]}	No 8000 equivalent CLI

Table 12 CLI commands not translated during software upgrade (Sheet 4 of 5)

Command	Comments
create ipif <ipif_name 12> <network_address> <vlan_name 32> { state [enabled|disabled]}	No 8000 equivalent CLI
config dvmrp [ipif <ipif_name 12>| all] {metric <value 1-31>| probe <sec1-65535>| neighbor_timeout <sec 1-65535>| state [enabled|disabled]}	No DVMRP support in version 2.1, Pim-SM only
enable dvmrp & disable dvmrp	No 8000 equivalent CLI
disable dvmrp	No 8000 equivalent CLI
config igmp [ipif <ipif_name 12>|all state [enabled|disabled]	No 8000 equivalent CLI
disable vrrp	No 8000 equivalent CLI
create vrrp ipif <ipif_name 12> {authtype [none|simple authdata <string>|ip authdata <string>]}	No 8000 equivalent CLI
create vrrp ipif <ipif_name 12>preempt true	No 8000 equivalent CLI
Routing/RIP/OSPF	
config rip [ipif <ipif_name 12>|all] {authentication [enabled <password 16> | disabled]}	No 8000 equivalent CLI
create route redistribute dst rip src [local | static | ospf[all|internal|external|type_1|type_2|inter+e1|inter +e2]]{metric <value>}	No 8000 equivalent CLI
create ospf host_route <ipaddr> area <area_id>	No 8000 equivalent CLI
Security TACACS+/MD5 keys/SSH	
config authentication admin [console | telnet | ssh | all] {tacacs+ | local | none}	No 8000 equivalent CLI
config authentication admin local_password	No 8000 equivalent CLI
config authentication login [console | telnet | ssh | all] {tacacs+ | local | none}	No 8000 equivalent CLI
config login_authen response_timeout <sec 1-255>	No 8000 equivalent CLI
enable admin	No 8000 equivalent CLI

Table 12 CLI commands not translated during software upgrade (Sheet 5 of 5)

Command	Comments
create md5 key <key_id 1-255> <password 16>	No 8000 equivalent CLI
config ssh user <username> authmode [hostbased [hostname <string 31> | hostname_IP <string 31> <ipaddr>] | password | publickey|none]	No 8000 equivalent CLI
config ssh algorithm [3DES|AES128|AES192|AES256|arcfour|blowfish|cast128|twofish128|twofish192|twofish256|MD5|SHA1|RSA|DSA] [enabled|disabled]	No 8000 equivalent CLI
config ssh authmode publickey[enabled|disabled]	No 8000 equivalent CLI
config ssh authmode hostbased enabled|disabled]	No 8000 equivalent CLI
config ssh server authfail <int 2-20>	No 8000 equivalent CLI
config ssh server port <tcp_port_number 1-65535>	No 8000 equivalent CLI
config ssh server rekey [10min|30min|60min|never]	No 8000 equivalent CLI
Traffic Control	
config traffic control [<portlist>|all] threshold <percentage 10-100> {dlf [enabled threshold <pps 0-1488100> | disabled] }	No 8000 equivalent CLI
config ethernet 1/1-1/52tx-flow-control disable	No 8000 equivalent CLI
config ethernet 1/1-1/52tx-flow-control	No 8000 equivalent CLI

CLI commands that translate with limitations

The upgrade process also translates some commands with limitations.

Commands in Table 13 are translated with limitations during the upgrade process.

Table 13 CLI commands translated with limitations during the software upgrade (Sheet 1 of 3)

Phase 1 (Release 1.x)	Phase 2 (Release 2.x)	Limitation
Platform (boot mode)		
config serial_port { baud_rate [9600|19200|38400|115200] | auto_logout [never|2_minutes|5_minutes|10_minutes|15_minutes] }	config bootconfig cli timeout <seconds >	If the timeout option was set to never in the original config, it defaults to the maximum value(65535).
enable telnet {<tcp_port_number 1-65535>}	config bootconfig flags telnetd <true|false >	Telnet port defaults to 23 during upgrade.
enable web {<tcp_port_number 1-65535>}	config web-server enable config web-server http-port <1..49515 >	The maximum port number is 49515. Any port outside this range defaults to 49515.
Simple Network Time Protocol (SNTP)		
config time Daylight-Saving-Time state [enabled|disabled] config time Daylight-Saving-Time offset <value 0-840> config time Daylight-Saving-Time start <hour 0-23> <day 1-31> <month 1-12> end <hour 0-23> <day 1-31> <month 1-12> "	config bootconfig tz dst-offset <minutes> config bootconfig tz dst-end <Mm.n.d/hhmm | MMddhhmm> dst-start <Mm.n.d/hhmm | MMddhhmm>	If state enabled is configured then all Daylight-Saving settings convert. If state is disabled, then all settings are lost.
Spanning Tree (MSTP/RSTP/STG)		
config stp ports <portlist> {externalCost [auto | <value 1-200000000>] |hellotime <value 1-10> | protocol-migration [true|false] |edgeport [true|false] | p2p [forcetrue|forcefalse|auto]| state [enable | disable]}	config ethernet <slot#>/<port#>-<slot#>/<port#> mstp cist hello-time <timeval 100-1000>	All STP time values are expressed in 1/100 second in Phase 2.
config stp mst_ports <portlist> instance_id <value 0-7> {internalCost [auto | <value 1-200000000>]}	config ethernet <ports> mstp msti <1-63> pathcost <intval 1-200000000>	Phase 2 does not support auto cost . Therefore it is set to the default value in MSTP/RSTP/STG. NOTE: The default value differs between protocols and MLT).

Table 13 CLI commands translated with limitations during the software upgrade (Sheet 2 of 3)

Phase 1 (Release 1.x)	Phase 2 (Release 2.x)	Limitation
Spanning Tree (MSTP)		
config stp_vlan instance_id add <vidlist>	config vlan <id#> create byport-mstprstp <instance-id 0-63>	In Phase 1, VLAN_1 can be assigned to any MST instance. In Phase 2, VLAN_1 must be in CIST.
FDB		
config fdb aging_time <sec 10-630>	config vlan <vid> fdb-entry aging-time <seconds>	The Phase 1 global aging time is assigned to all VLANs in Phase 2.
create fdbfilter vlan <vlan_name> mac_address <macaddr>	config vlan <vid> fdb-filter add <mac> port <value> drop <value>	The `config vlan <vid> fdb-filter add <mac> port <value> drop <value>` command is executed on all ports in the VLAN in Phase 2.
VLAN		
config 802.1p default_priority [<portlist> | all] priority [0 | 4 | 6 | 7]	config ethernet <ports> qos qos-level <0…6>	In Phase 2, the "priority" range is 1..6. Any priority "7" setting is converted to a value of 6.
create vlan <vlan_name 32> {vid <vlanid 1-4094>}		VLAN ID range is [1..4000] in Phase 2. All VLAN IDs greater than 4000 are lost after conversion.
IGMP Snooping		
config router_ports <vlan_name 32> [add|delete] <portlist>	config vlan <vid> ip igmp mrouter <ports>	In Phase1, an mrouter can be configured without enabling IGMP Snoop. In Phase 2, if IGMP Snoop is disabled on the VLAN no "mrouter" port can be configured.
ARP		
config arp_aging time <value 0-65535>	config ip arp aging <minutes>	In Phase 2 the maximum ip arp aging value is 32767. Any value greater than 32767 defaults to 32767.
OSPF		
create ospf area <area_id> type [normal | stub {stub_summary [enabled|disabled] | metric <value 0-65535>}]	config ip ospf area <ipaddr> create config ip ospf area <ipaddr> stub <true|false> config ip ospf area <ipaddr> stub-metric <stub-metric>	The *`stub_summary [enabled|disabled]`* option is not available in Phase 2.

Table 13 CLI commands translated with limitations during the software upgrade (Sheet 3 of 3)

Phase 1 (Release 1.x)	Phase 2 (Release 2.x)	Limitation
Traffic Control		
config traffic control { [<portlist>|all] { broadcast [enabled |disabled] | multicast [enabled | disabled] |	config ethernet <ports> bcast-mcast-rate-limit <1..100> [<enable|disable >]	1. The default Bcast and Mcast rate limit percentage value is 20. 2. Only if both Bcast and Mcast are disabled in Phase 1 will Bcast and Mcast be disabled in Phase 2.

Documentation additions and corrections

The document suite has been redefined to conform to the Ethernet Routing Switch 8300 document suite.

See *Getting Started* (321821-A) for a listing of the Ethernet Routing Switch 1600 Series Release 2.1 documents by function, a map of Release 2.1 new features to documents, and a subject list by document.

Related information

This section lists information sources that relate to the Ethernet Routing Switch 1600 Series, Software Release 2.1.

Publications

Refer to the following publications for information on Ethernet Routing Switch 1600 Series, Software Release 2.1:

- *Installing and Using Device Manager* (316857-C)
- *Release Notes for the Ethernet Routing Switch 1600 Series, Software Release 2.1* (316859-J)
- *Installing the Ethernet Routing Switch 1600 Series Switch* (316860-D)

- *CLI Command Line Reference for the Ethernet Routing Switch 1600 Series* (316862-D)
- *Upgrading to Ethernet Routing Switch 1600 Series Software Release 2.1* (321327-B)
- *Configuring IP Routing and Multicast Operations using the CLI* (321711-B)
- *Configuring IP Routing and Multicast Operations using Device Manager* (321712-B)
- *Configuring and Managing Security using Device Manager* (321713-B)
- *Configuring and Managing Security using the CLI* (321714-B)
- *Configuring VLANs, Spanning Tree, and Static Link Aggregation using the CLI* (321717-B)
- *Configuring VLANs, Spanning Tree, and Static Link Aggregation using Device Manager* (321718-B)
- *Configuring Network Management using the CLI and Device Manager* (321816-A)
- *Managing Platform Operations* (321817-A)
- *Quick Start Guide* (321819-A)
- *System Messaging Platform Reference Guide* (321820-A)
- *Getting Started* (321821-A)
- *Configuring QOS and Filters using the CLI and Device Manager* (321822-A)
- *Network Design Guidelines* (321823-A)
- *Nortel Ethernet Routing Switch 1600 Series Release 2.1 Regulatory Information* (322751-A)

How to get help

This section explains how to get help for Nortel products and services.

Finding the latest updates on the Nortel web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software for Ethernet Routing Switch 1600 Series, click one of the following links:

Link to	Takes you directly to the
Latest software	Nortel page for **Ethernet Routing Switch 1600 Series** software located at www.nortel.com
Latest documentation	Nortel page for **Ethernet Routing Switch 1600 Series** documentation located at www.nortel.com

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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.