Release Notes

Nortel Ethernet Routing Switch 5000 Series

Release Notes for Release 6.2

Document Status: **Standard**

Document Number: **NN47200-400**

Document Version: **06.01**

Date: **July 19, 2010**

NORTEL

Contents

New in this release

The following sections detail what's new in Nortel Ethernet Routing Switch 5000 Series Release 6.2.

Features

See the following sections for information about feature changes.

Other changes

Enterprise Device Manager (EDM) navigation has been enhanced. To access command tabs from the EDM navigation tree, the documented procedures specify using a double-click to open the tab in the work area. With the enhancement, you can access all objects in the navigation tree with a single click.

Introduction

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for the Nortel Ethernet Routing Switch 5000 Series, Release 6.2

The Nortel Ethernet Routing Switch 5000 Series includes the following switch models:

- Nortel Ethernet Routing Switch 5510-24T
- Nortel Ethernet Routing Switch 5510-48T
- Nortel Ethernet Routing Switch 5520-24T-PWR
- Nortel Ethernet Routing Switch 5520-48T-PWR
- Nortel Ethernet Routing Switch 5530-24TFD
- Nortel Ethernet Routing Switch 5698-TFD
- Nortel Ethernet Routing Switch 5698-TFD-PWWR
- Nortel Ethernet Routing Switch 5650-TD
- Nortel Ethernet Routing Switch 5650-TD-PWR
- Nortel Ethernet Routing Switch 5632-FD

Configurations can vary from a standalone switch to a stack of up to 8 switches. A stack can consist of any combination of switches. One benefit of operating Nortel Ethernet Routing Switch 5000 Series switches in a stack is management efficiency; a stack is managed with a single IP address and software is available as a single image across all models.

These release notes provide the latest information about the current software release, as well as operational issues not included in the documentation.

For a complete list of documentation in the Nortel Ethernet Routing Switch 5000 Series suite, see *Nortel Ethernet Routing Switch 5000 Series Documentation Roadmap* (NN47200-103).

The information in this document supersedes applicable information in other documents in the suite.

Important notices and new features

This section contains a brief synopsis of the new features in Release 6.2 and important notices.

Navigation

Feature document location

The following table contains a list of key software features and their location in the documentation suite.

Table 1 Where to find information about key software features

Feature	Document
QoS Traffic Profile Support	*Nortel Ethernet Routing Switch 5000 Series Configuration - Quality of Service* (NN47200-504)
SMLT configuration	*Nortel Ethernet Routing Switch 5000 Series Configuration - VLANs, Spanning Tree, and Link Aggregation* (NN47200-502)

New features in Release 6.2

Software Release 6.2 provides the following new features and feature enhancements.

Enterprise Device Manager

Enterprise Device Manager (EDM) replaces both the Java-based Device Manager and Web-based management. EDM is an embedded element management and configuration application for Ethernet Routing Switch 5000 Series switches. EDM uses a Web-based graphical user interface for the convenience of full integration onto the switch, but it retains the look and feel of Device Manager.

ATTENTION: With the introduction of Enterprise Device Manager (EDM) the use of Device Manager (sometimes referred to as JDM) is no longer supported because the use of JDM to control the switch could lead to potential corruption of the switch configuration.

ATTENTION: If you upgrade the software on your switch, and if you are managing the switch with EDM, then you should refresh the browser cache on your end device to ensure that EDM loads the latest tabs for all respective features.

802.1AB (LLDP) MED Network Policy

You can configure 802.1AB MED network policies to dynamically configure voice VLAN, DSCP, priority, and VLAN tagging on the switch for voice traffic received from an IP phone. When you enable LLDP and configure the MED network policies on the switch, the switch sends the network policies to the IP Phone. The IP phone processes the data in the LLDP PDU and transmits the voice traffic with the appropriate VLAN ID, VLAN tagging, DSCP and priority information.

You can configure MED network policies on a switch port that has ADAC enabled. The network policies have priority over the ADAC configuration on the port.

802.1X authentication and Wake on LAN

The Wake on LAN (WoL) networking standard allows you to remotely turn on a computer when it is in a sleeping state. Wake on LAN comprises components on the end device, network, and control system. You can use this tool while performing maintenance activities on systems during off hours.

802.1X or Non-EAP and Guest VLAN on same port

This feature removes previous limitations by providing the ability to simultaneously configure 802.1X, Non-EAP and Guest VLAN on the same port for a more universal port configuration. In this release you do not have to configure a port to support Guest VLANs or Non-EAP or 802.1X; one port can support all 3 functions.

802.1X or Non-EAP Last Assigned RADIUS VLAN

You can use the 802.1X or Non-EAP Last Assigned RADIUS VLAN function to configure the switch to always honor the last received RADIUS-VLAN assignment on a port.

802.1X or Non-EAP with Fail Open VLAN

This feature provides network connectivity for EAP-enabled or non-EAP-enabled ports to reach specific network resources when the switch is not able to reach the RADIUS server. When connectivity to the RADIUS server is lost, the system moves all authenticated devices into the configured Fail Open VLAN. When connectivity to the RADIUS server is restored, the system moves devices back to their previously-authenticated networks.

802.1X or Non-EAP with VLAN name

With this feature, you can enable the Ethernet Routing Switch 5000 Series to match RADIUS assigned VLANs based on either the VLAN number or a VLAN name. Previously, a match was based on the VLAN number of the Tunnel-Private-Group-Id attribute returned by the RADIUS server.

Autodetection and Autoconfiguration (ADAC) Uplink Enhancements

Autodetection and Autoconfiguration (ADAC) Enhancements provide increased flexibility in deployments that use Auto-Detect Auto-Configuration (ADAC) as follows:

- expanded support for up to 8 ADAC uplinks and 8 call-server links - individual ports or any combination of MLT, DMLT or LAG - per switch or stack
- non-ADAC VLANs retained in NVRAM through resets

For greater flexibility in ADAC call server configuration, ADAC is able to support up to 8 call-server links per switch or stack. More than one call server port is required because system deployments may have multiple devices, for example a signaling server and a media gateway, connected to a switch. The call server could be an individual port or any combination of MLT/DMLT or LAG connections.

Currently when ADAC is operational, a user can not change the non-ADAC VLANs on the port (without disabling ADAC, changing the VLAN and then re-enabling ADAC), which leads to usability issues that limit the deployment of ADAC.

The ADAC enhancements provide the ability to change the non-ADAC VLANs on a port irrespective of the ADAC status of the port. Any such changes in the underlying port VLAN assignment are saved as normal to NVRAM and ASCIII configurations.

Automatic QoS 802.1AB MED interoperability

Automatic QoS 802.1AB MED interoperability enhances automatic QoS implementation on the switch so you can use both features simultaneously. With the enhancement, if you configure 802.1 AB MED, the switch publishes the private Automatic QoS DSCP value to the end device rather than the default value defined by the network policy.

Automatic QoS and ADAC Interoperability

Automatic QoS and ADAC Interoperability enhances automatic QoS implementation on the switch so you can use Automatic QoS and ADAC simultaneously. In this release you can enable ADAC and configure Automatic QoS on the port so that ADAC can use the Automatic QoS DSCP markings.

Cisco CLI commands

The new CISCO type commands are available through auto-completion and also appear when you use the help menu (question mark). The equivalent NNCLI commands are still available, but are hidden.

You can use the following IOS CLI commands:

Table 2 Cisco CLI commands

ARP	
arp [A.B.C.D] [H.H.H] [port] [vlan id]	• A.B.C.D is the IP address • H.H.H. is the MAC address • port is the port to which the ARP entry is assigned
no arp A.B.C.D	Disables ARP for the specified IP address.
show arp	Displays ARP settings.
STP	
spanning-tree mode	Sets the Spanning Tree mode as one of the following: • mst • rstp • stpg
spanning-tree mode mst	This command changes STP operation to MSTP
show spanning-tree mode	Displays the Spanning Tree mode.
VLAN	
show vlan id [vlan ID]	Displays the VLAN ID.

Content-based forward to next hop (formerly source address-based route selection)

Routing is improved in this release with the introduction of source address-based route selection. Applied on a per VLAN basis, source address-based addresses can be an IP address or subnet and a TCP/UDP port or range of ports.

DHCP enhancements

The DHCP Snooping table entries have been increased to 1,024 so that you can deploy a full stack of 8 units using IP Phones and PCs.

You can add and delete DHCP snooping table entries manually so that devices assigned to static IP addresses can appear in the DHCP Snooping table and be protected by Dynamic Address Resolution Protocol (DARP) and IP Source Guard, which rely on the DHCP Snooping table to protect statically configured IP devices.

DHCP option 82 support

DHCP option 82 support is an extension of Dynamic Host Configuration Protocol (RFC3046 and RFC3993) that enables the switch to send information about DHCP clients to the authenticating DHCP server. When you enable option 82, in either Layer 2 or Layer 3 mode, the switch inserts additional port-based identification information into the DHCP packets traversing the switch enroute to the DHCP server. The DHCP server stores this additional identification information within the IP allocation record to assist in tracking of end device locations.

Dual Syslog Server support

In Release 6.2, you can use the Dual Syslog Server Support feature to configure a second syslog server to run in tandem with the first. If you configure Dual Syslog Server Support, the system sends syslog messages simultaneously to both servers to ensure that syslog messages are logged, even if one of the servers becomes unavailable.

EAP/NEAP separation

The EAP/ NEAP separation command allows you to disable EAP clients without disabling NEAP clients.

Energy Saver

Energy Saver (ES) can reduce network infrastructure power consumption without impact to network connectivity. ES reduces direct power consumption by up to 40% because it uses intelligent switching capacity reduction in off-peak mode. ES can also use Power over Ethernet (PoE) port power priority levels to shut down PoE ports and provide more power savings.

Enhanced QoS engine

Release 6.2 introduces an enhanced QoS engine to provide more efficient resource use.

Filter Limiting

Enabled by default, Filter Limiting limits the maximum number of user-defined protocol VLANs to 7. When you disable Filter Limiting, you can create up to 16 user-defined protocol VLANs. The ERS 5510 switch supports a maximum of 7 user-defined protocol VLANs and cannot join a stack if you disable Filter Limiting.

Full IGMPv3

Release 6.2 supports Full IGMPv3 with the addition of source filtering for IGMPv3 Snooping. Six group record types for IGMPv3 Snooping are supported.

IPv4 Tunneling for IPv6

IPv4 Tunneling for IPv6 supports communication between IPv6 networks across an IPv6 domain using manually configured tunnels.

IPv6 Automatic Address Assignment

When IPv6 routing is enabled for an interface, or when an IPv6 IP address is configured on an interface, the system automatically creates an IPv6 local route entry in the IPv6 routing table.

The following limitations apply to IPv6 automatic address assignment:

- works only on ERS 5600 units
- works only when IPv6 forwarding is enabled

- only one IPv6 address per interface

The IPv6 automatic address assignment supports the following:

- 256 prefixes (you can assign more than one prefix per VLAN)
- 1 local route, corresponding to a global IPv6 address, for each IPv6 prefix created with EUI 2 or 3 is added to the IPv6 routing table ; that is, if EUI for a prefix is equal to 2 or 3, a global IPV6 address with type “Random” is assigned to the interface

IPv6 Routing DHCP Relay

Ethernet Routing Switch 5000 Series switches support IPv6 DHCP Relay per RFC 3315.

IPv6 Static Routing

IPv6 Static Routing supports configurable IPv6 static routes and per-VLAN IPv6 routes to provide:

- multiple configurable IPv6 interfaces associated with VLANs (limitation: only 1 IPv6 interface associates with 1 VLAN)
- multiple configurable static entries in the IPv6 routing table
- router functionality based on the routing table
- configuration of prefix lists advertised to the host of stateless autoconfiguration

IPv6 Static Routing is supported only on ERS 5600 switch models.

MAC Security enhancement

In Release 6.2, if you want to lock ports out of MAC-based security, you can use the MAC Security enhancement to specify which ports to lock out.

Multicast group scaling

This release provides three levels of improved multicast group support as follows:

- ERS 5510 supports 250 multicast groups
- ERS 5520 and ERS 5530 support 492 multicast groups
- ERS 5600 supports 992 multicast groups

In a hybrid stack, multicast group support conforms to the lowest common denominator. If the stack contains an ERS 5510, then 250 multicast groups are supported; if the stack contains an ERS 5520 or 5530, then 492 multicast groups are supported.

Multiple Hosts with Multiple VLANs for EAP-enabled Ports

The Multiple Hosts with Multiple VLANs for EAP-enabled ports (MHMV) feature can direct multiple hosts on a single port to different VLANs. You can use MHMV to separate voice and data traffic on the same port.

PIM-SM support

PIM-SM support extends to both pure and hybrid stack configurations.

Port Mirroring - Bi-directional monitor port

You can enable bi-directional traffic on the monitor port to allow a connected IDS/IPS device to disable the port when it detects traffic posing a threat to the network. Also, when you enable bidirectional port mirroring, you can manage ERS 5000 on that port.

QoS DSCP mutation

QoS DSCP mutation extends Quality of Service trusted interface support by using the mapping tables, rather than filters, to permit remarking of DSCP values on egress. The enhancement adds an egress DSCP value to the DSCP-to-COS mapping table; the switch uses the ingress DSCP value to set the Class of Service (COS) and remark the DSCP value on egress. You can use the DSCP mutation operation to match and remark targeted DSCP values. The DSCP-to-COS Mapping Table can be easily extended to specify DSCP mutation values and to apply these automatically on Trusted interfaces.

In the current QoS implementation of Trusted interface class, the IPv4 traffic received on trusted interfaces is remarked at the layer 2 level, that is, the 802.1p user priority value is updated based on the DSCP value in the packet at ingress and the installed DSCP-to-CoS mapping data. The remarked CoS value is used for queuing at egress and, possibly, for downstream packet processing in a tagged VLAN environment. In some cases, you may need to remark the packet DSCP value at egress as well, based on the incoming DSCP value and, with Release 6.2, you can use QoS DSCP mutation to do this.

QoS Egress Queue Shaping

You can use QoS Egress Queue Shaping to configure egress shaping based on a per queue basis without traffic interruption.

Both port-based shaping and per-port per-egress queue shaping are supported in this release. The enhancement allows the traffic flow to be shaped at a CoS level and you can implement the egress queue shaping to provide control on a per queue basis.

QoS Lossless Buffering Mode for Data Center Applications

QoS lossless buffering mode is critical in data center applications, where reliable data transfer is more important than enhanced throughput. With lossless buffering mode, when a port receives volumes of traffic greater than port bandwidth, the port sends flow control (pause) frames to the sender. QoS lossless buffering is supported on ERS 5600 series switches only.

Route scaling

Up to 4000 routes, twice the number of routes available in the previous release, are available for the ERS 5600 Series products.

Running configuration NNCLI display command enhancements

The show running-config NNCLI command enhancements change the operation of the show running-configuration command. By default, show running-configuration displays only parameters that differ from the default configuration. You can use the verbose qualifier to display the entire ASCII configuration for the switch or stack. You can also use the module qualifier in the command to display the ASCII configuration for a specific feature.

The operation of the copy running-config tftp NNCLI command has been modified. By default, copy running-config tftp copies the complete contents of the running configuration file to a specified file on the TFTP server. With Release 6.2, you can use the module qualifier in the command to display the ASCII configuration for a specific feature, or you can use the verbose qualifier to copy the entire ASCII configuration for the switch or stack.

The operation of the copy running-config usb NNCLI command has been modified. By default, copy running-config usb copies the complete contents of the running configuration file to a USB mass storage device. With Release 6.2, you can use the module qualifier in the command to display the ASCII configuration for a specific feature, or you can use the verbose qualifier to copy the entire ASCII configuration for the switch or stack.

Secure Shell File Transfer Protocol (SFTP over SSH)

For enhanced network security, Secure FTP for secure file transfer over an SSH session is available in this release.

SFP support

Release 6.2 supports the following additional SFPs:

- AA1419050-E6
- AA1419051-E6
- AA1419052-E6
- AA1419053-E6
- AA1419054-E6
- AA1419055-E6
- AA1419056-E6
- AA1419057-E6
- AA1419058-E6
- AA1419059-E6
- AA1419060-E6
- AA1419061-E6
- AA1419062-E6
- AA1419063-E6
- AA1419064-E6
- AA1419065-E6
- AA1419066-E6
- AA1419067-E6
- AA1419068-E6

- AA1419071-E6
- AA1403007-E6
- AA1419074-E6
- AA1419075-E6
- AA1419076-E6
- AA1419077-E6

Split Multi-link Trunk (SMLT) consistency with the Ethernet Routing Switch 8600

In Release 6.2, Split Multi-link Trunk (SMLT) configuration is enhanced to more closely reflect the Ethernet Routing Switch 8600 configuration.

Split Multi-link Trunk (SMLT) over Link Aggregation Control Protocol (LACP)

SMLT over LACP improves trunking resilience and handling in fail-over situations, for example, when a stack breaks.

Software Licensing enhancements

Software Licensing is a mechanism that allows you to use designated features, according to the license level that you purchase. In Release 6.2 the licensing process is simplified so that if you purchase a license, it remains valid when you upgrade to a version of software that includes additional features included in the license level; that is, you do not have to regenerate the license file, remove the old license from your switches and reload a new license file. Licensing is further simplified for a stack scenario. Automatic Unit Replacement has been updated to enable automatic update of a license for any replacement stack unit, including the Base Unit.

Trace command

A Trace command is available that is supported in OSPF, RIP, SMLT, IPMC, IGMP, and PIM in 4 levels for each module or application.

Unicast storm control

Unicast storm control blocks all unicast traffic when the traffic rate exceeds a user-configurable threshold, also known as a high water mark. Unicast storm control then allows all unicast traffic to proceed when the traffic rate drops below a user-configurable threshold, also known as a low water mark.

Regardless of the blocking state of unicast traffic, all broadcast and multicast traffic continues to forward unless the traffic is blocked or limited by other means like broadcast rate limiting.

VLAN Scaling

VLAN Scaling can support up to 4,096 concurrent VLAN IDs with the scaling and demonstration capacity limited to 1,024 simultaneous VLANs.

The ERS 5000 Series offers the VLAN 4K scaling feature. This feature is controlled by the demo command and appropriate password provided to activate the functionality. This feature allows you to extend the number of VLANs supported by a device up to 4k. The scaling limits for each platform can be determined based on the business need and available system resources. All the VLAN configured applications can work properly with the maximum configured of VLANs. The standard scaling limit is 256, 512, 1024, or 4094 VLANs.

In ERS 5000 Series Release 6.2, the target scaling number is a maximum of 1024 active VLANs with full support.

No other capabilities extension for Layer 2 or Layer 3 will be enhanced as a result of VLAN scaling.

Release file names

The following table describes the Nortel Ethernet Routing Switch 5000 Series software components for this release.

Table 3 Release 6.2 software components

File type	Description	File name	File size
Standard runtime combo image software version 6.2	Standard non SSH combo image for the Ethernet Routing Switch 5000 Series	5xxx_620008.img	18286980
Secure runtime combo image software version 6.2	Standard SSH combo image for the Ethernet Routing Switch 5000 Series	5xxx_620009s.img	19045448
Combo diagnostic version 6.0.0.10	ERS 5000 Combo diagnostic software	5xxx_60010_diags.bin	2465180
Enterprise Device Manager Help files	EDM Help files zip	ERS5000_Help_EDM.zip	1,508,380 bytes
MIB Definition File	MIB Definition File	Ethernet_Routing_Switch_5xxx_MIBs_6.2.0.zip	1589703
COM Plugin	ERS 5000 plugin for COM	ers5000v6.2.0.0.war	2,854,983

Software upgrade

The procedures in this section are used to upgrade the diagnostic and agent software. Use the procedures to upgrade to Software Release 6.2.

ATTENTION: There is no upgrade path from any agent software release earlier than 6.0 to Software Release 6.2. Devices running older agent software must first be upgraded to a version of Software Release 6.0 before upgrading to Software Release 6.2. Note that the diagnostic software running on the device cannot be earlier than 6.0.0.6.

Upgrading diagnostic software

Use the following procedure to upgrade the diagnostic software image.

1. Access the NNCLI through a Telnet or Console connection.
2. Enter Privileged EXEC mode using the `enable` command.

3. Use the command `download address <ip_address> diag <image_name> [no-reset] [use]` to transfer the diagnostic image to the device.

   The following table describes the parameters for the download diag command.

   Table 4

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the diagnostic image is hosted.
diag <image_name>	The name of the diagnostic image file on the TFTP server.
no-reset	This parameter specifies that the device will not reset after the upgrade is complete.
use	This parameter specifies that the software download will occur from a USB device instead of the network. This option is only valid with the 5530-24TFD and 5600 Series devices.

The upgrade process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process.

When the process is complete, the device automatically resets unless the no-reset parameter was used. The software image initiates a self-test and returns a message when the process is complete.

During the download process the switch is not operational.

Upgrading agent software

Use this procedure to upgrade agent software.

1. Access the NNCLI through a Telnet or Console connection.
2. Enter Privileged EXEC mode using the `enable` command.
3. Use the command `download address <ip_address> {primary | secondary} {image <image_name> | image-if-newer <image_name> | poe_module_image <image_name>} [no-reset] [usb]` to transfer the agent image to the device.

The following table describes the parameters for the download agent command.

Table 5

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the agent image is hosted.
primary | secondary	Designates whether the image is stored in the primary or secondary image location. The default is primary.
image <image_name> | image-if-newer <image_name> | poe_module_image <image-name>	The name of the agent image file on the TFTP server. Each option is mutually exclusive. Use the option described with the following situation: To load the agent image under normal circumstances, use the image option. To load the agent image only if it is newer than the current image, use the image-if-newer option. To load the agent image if it is a PoE module image, use the poe_module_image option.
no-reset	Specifies that the device will not reset after the upgrade is complete.
usb	Specifies that the software download will occur from a USB device instead of the network. This option is only valid with the 5530-24TFD and 5600 Series devices.

The upgrade process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process.

When the process is complete, the device automatically resets unless the `no-reset` parameter was used. The software image initiates a self-test and returns a message when the process is complete.

During the download process the switch is not operational.

How to get EDM online help files for embedded EDM

Because help files are not included with the embedded EDM software files on the switch. a network administrator must copy the software-release-specific help files onto a TFTP server. Once the help files are downloaded to the TFTP server, the network administrator must configure the switch with the path to the help files on the TFTP server. You can use NNCLI or EDM to configure a path from your switch to the help files. After the path to the help files is configured, whenever an EDM user clicks the help button on the toolbar, the switch downloads and displays help information in the Web browser.

If you are using Configuration and Orchestration Manager (COM) to manage your switch, help resides with COM and you do not need to use these procedures.

For more information about EDM, see *Nortel Ethernet Routing Switch 5000 Series Fundamentals* (NN47215-102).

Downloading help files

Use this procedure to download EDM online help files.

Prerequisites

- An available TFTP server

1 To obtain EDM help files for the embedded element manager, do one of the following:

- Go to the Nortel Web site at *www.nortel.com/support* and locate the help files for the appropriate product.
- Select the help file from the software CD ROM.

2 Download the help file to a TFTP server.

How to configure the path to the embedded EDM help files

If you are using embedded EDM, use the procedures in this section to configure the path to the help files. You can configure the help file path with NNCLI or EDM.

Configuring the path to the help files using NNCLI

Use the following procedure to configure the path to the help files using NNCLI.

1. In NNCLI, go to the Global Configuration mode and use the following command: `edm-help-file-path <path name> tftp address <tftp address>`.

The following table describes the parameters for the edm-help-file-path command.

Table 6

Parameter	Description
path name	Specifies the path name you created for EDM help files. The path name is stored in NVRAM.
TFTP address	Specifies EDM TFTP server IP address. Use this address only for EDM help files. If you do not specify a TFTP server address, the system uses the address specified most recently. **WARNING**: Because the TFTP server address is stored in NVRAM, each time the system returns to the default configuration, you must reconfigure the path to EDM online help.

EDM help file path NNCLI example

Following is an example of an NNCLI EDM help file path:

```
edm help-file-path ERS 5000_62_Help tftp address 100.100.100.15
```

In the preceding example ERS 5000_62_Help is a folder that contains help files and the folder is located on a TFTP server at the 10.100.100.15 address.

Configuring the path to the help files using EDM

Use the following procedure to configure the path to the help files using EDM.

1. From the navigation tree, click Edit.
2. From the Edit tree, click File System.
3. Select the Help File Path tab.
4. In the Path dialog box, enter the path to the help file storage location.

   Example: tftp://xxx.xxx.x.x./file_name

Supported software and hardware capabilities

The following table lists the known limits for the Ethernet Routing Switch 5000 Series, Release 6.2 and Device Manager.

Table 7 Supported software and hardware capabilities

Feature	Maximum number supported
VLANs	1024 (1k)
Protocol-based VLANs	Depending on the protocol specified, the number of protocol VLANs supported at one time varies between 3 and 7. See *Nortel Ethernet Routing Switch 5500 Series Configuration - VLANs, Spanning Tree, and MultiLink Trunking* (NN47200-502) for more information.
Nortel NSNA VLANs	One Red VLAN per switch. Nortel recommends a maximum of five Yellow VLANs, five Green VLANs, and five VoIP VLANs per switch.
Nortel SNA ports	All ports. **Note**: The ERS 5530 has two 10 Gigabit (GB) ports that you can configure as uplink ports but not as dynamic ports.
IGMP maximum number of unique groups	Layer 2 and Layer 3 240 IGMP Op-Mode = 5510 492 IGMP Op-Mode = Non-5510 (Hybrid) 992 IGMP Op-Mode = Non-5510 (Pure)
EAPOL 802.1x supplicants	All ports
Number of routes (dynamic, static, and local)	4000 routes for ERS 5600 units and pure stacks (5600 units only) 2000 for ERS 5500 units and hybrid stacks (5500 and 5600 units)
ARP records	1500
Static ARP	256
IP interfaces	256
Static routes	512
Spanning Tree Groups	8
IPv6 DHCP relay forward paths	256
IPv6 static routes	512
IPv6 interfaces	256

Table 7 Supported software and hardware capabilities

Feature	Maximum number supported
IPv6 tunnels	4
Aggregation groups (link aggregation)	32
Ports per aggregation group	8
MAC addresses in fdb	16 Kb
OSPF areas	4 (3 areas plus area 0)
OSPF adjacencies	64
VRRP interfaces	64
ECMP	4 paths (not supported on ERS 5510 switches)
DHCP Snooping Binding table entries	1024
DHCP relay forward paths	512
IP Management routes	4
PIM-SM multicast entries	Up to 492 for ERS 55xx series. Up to 992 for ERS 56xx series. The hardware for ERS 55xx platforms supports a maximum of 492 IPMC forwarding entries. The ERS 56xx platforms support a maximum of 992 IPMC forwarding entries. These limitations are imposed on standalone ERS 5xxx devices and stacks with the added limitation that, on hybrid stacks, the lower limit of 492 IPMC forwarding entries is imposed. **NOTE**: These limits do not indicate that 492 or 992 entries will actually be available since the installation of IPMC entries in hardware is also determined by free entries being available in several hardware tables. Also, on ERS 5510 platforms, the available number of IPMC forwarding entries is 240. **NOTE**: ERS 5510 units cannot participate in PIM-SM due to hardware limitations.

Table 7 Supported software and hardware capabilities

Feature	Maximum number supported
Allow-flood IGMP multicast addresses	The maximum number of allow-flood multicast entries is determined by the number of VLANs on the device. Each entry in the allow-flood table applies to each current VLAN; for example, if 1 entry exists in the allow-flood table and 5 VLANS are configured, then there are 5 entries programmed in hardware. Currently, the hardware limit is 4096. **NOTE**: You should not exceed this limit. The limit for the maximum number of allow-flood addresses is 128 (1 VLAN).

Nortel Ethernet Routing Switch 5520 phone dongle

The part number for the Nortel Ethernet Routing Switch 5520 (5520-24T/48T-PWR) universal phone dongle is DY4311046.

Additional information about the software feature license file

When you create a license file to enable licensed features on an Ethernet Routing Switch 5000 series switch with the Nortel Electronic Licensing portal you must specify a file name. Follow the instructions on the License Certificate within the License Kit, or for more information, see *Nortel Ethernet Routing Switch 5000 Series Fundamentals* (NN47200-104.

You must use the following rules when you generate and name the file:

- A maximum of 63 alphanumeric characters
- Lower case only
- No spaces or special characters allowed
- Underscore (_) is allowed
- The dot (.) and three-character file extension are required

File name example: ascdefghijk_1234567890.lic

The format of the file that you upload to the license generation tool, and that contains the list of MAC addresses, must be as follows:

- ASCII file format
- One MAC address per line
- No other characters, spaces, or special characters allowed
- MAC addresses must be in hexadecimal, capitalized format, with each pair of characters separated by colons; for example: XX:XX:XX:XX:XX:XX
- The file must contain the correct MAC addresses. Any incorrect MAC addresses will result in the licensed features not working on the designated units.
- The number of MAC addresses must not exceed the number of MAC addresses allowed for the License Authorization Code entered for a particular file. For example:
  - AL1016001 - 2 MAC addresses (1 stack/standalone unit)
  - AL1016002 = 20 MAC addresses (10 stacks/standalone units)
  - AL1016003 = 100 MAC addresses (50 stacks/standalone units)
  - AL1016004 = 200 MAC addresses (100 stacks/standalone units)

Supported standards, MIBs, and RFCs

This section lists the standards, MIBs, and RFCs supported by the Nortel Ethernet Routing Switch 5000 Series.

Standards

The following IEEE Standards contain information that applies to the Nortel Ethernet Routing Switch 5000 Series:

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1X (EAPOL)
- IEEE 802.1ab (Link Layer Discovery Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)

RFCs

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

- RFC 768 (UDP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 894 (IP over Ethernet)
- RFC 951 (BootP)
- RFC 1112 (IGMPv1)
- RFC 1157 (SNMP)
- RFC 1213 (MIB-II)
- RFC 1271 (RMON)
- RFC 1350 (TFTP)
- RFC 1493 (Bridge MIB)
- RFC 1757 (RMON)
- RFC 1945 (HTTP v1.0)
- RFC 2131 (DHCP)
- RFC 2236 (IGMPv2)
- RFC 2362 (PIM-SM)
- RFC 2665 (Ethernet MIB)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2865 (RADIUS)
- RFC 3410 (SNMPv3)
- RFC 3411 (SNMP Frameworks)
- RFC 3412 (SNMP Message Processing)
- RFC 3413 (SNMPv3 Applications)

- RFC 3414 (SNMPv3 USM)
- RFC 3415 (SNMPv3 VACM)
- RFC 3576 (Dynamic Authorization Extensions to Remote Authentication Dial In User Service)

The following table lists IPv6 specific RFCs.

Table 8 IPv6 specific RFCs

Standard	Description	Compliance
RFC 1886	DNS Extensions to support IPv6	Supported
RFC 1981	Path MTU Discovery for IPv6‘	Supported
RFC 2460	Internet Protocol v6 (IPv6) specification	Supported
RFC 2461	Neighbor Discovery for IPv6	Supported
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Supported
RFC 3162	RADIUS and IPv6	Supported
RFC 3315	DHCPv6	Supported for IPv6 DHCP Relay
RFC 4007	Scoped Address Architecture	Supported
RFC 4022	Management Information Base for TCP	Mostly supported
RFC 4113	Management Information Base for UDP	Mostly supported
RFC 4193	Unique Local IPv6 Unicast Addresses	Not supported
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack and configured tunnels.
RFC 4291	IPv6 Addressing Architecture	Supports earlier version of RFC (3513)
RFC 4293	Management Information Base for IP	Mostly supported
RFC 4301	Security Architecture for the Internet Protocol	Not supported
RFC 4443	Internet Control Message Protocol (ICMP v6)	Supports earlier version of RFC (2463)

Resolved issues

The following table lists the issues resolved in the current software release.

Table 9 Resolved issues

Change Request number	Description
Q01219391	MAC Address table does not age out all MAC sources learned after the aging time has expired.
Q01470123	Passive static device behind a phone displayed as unknown after switch reboot.
Q01470123-01	Passive static device behind a phone displayed as unknown after switch reboot.
Q01728560	ADAC port configuration types not defined in manual.
Q01775378	Error message when disabling spanning tree learning.
Q01859874	Typed commands should not be sent remotely when log level is serious or critical.
Q01860782	A message is needed to confirm the successful upload of an ASCII configuration to USB with the PUSH button.
Q01862906	The Time Domain Reflectometer in the JDM displays an incorrect message for the Pin Short cable error.
Q01863512	MAC security Lifetime setting cannot be modified from the JDM.
Q01865091	MAC authorized clients are not reauthorized after a former base unit reenters the stack.
Q01895467	Some LLDP commands fail when configuring a device with an ASCII configuration file.
Q01895723	Metric for external routes jumps to 127174722 when a dummy vlink is created and deleted.
Q01906362	An NEAP client can change ports without a link down or age out timer event.
Q01909890	QoS-IGMP problems with known and unknown multicast options on 56xx ports.
Q01901336	Multicast traffic not forwarded through non-local static routes.

Table 9 Resolved issues

Change Request number	Description
Q01923408-02	Management VLAN IP address should always be used in relation to RADIUS.
Q01927698	PIM interfaces become disabled on a device.
Q01938607	Incorrect error message displayed during software download from an unreachable server.
Q01942783	Restoring a device with an ASCII configuration file fails when Layer 3 settings are present.
Q01943527	Inconsistency between IPv4 and IPv6 in binary configuration file.
Q01945909	Some ARP, OSPF, or VRRP packets are unexpectedly mirrored when using XrxYtx mirroring mode and the monitored port is in the Management VLAN or in SMLT VLANs.
Q01946214	MAC addresses are lost when a base unit fails.
Q01946284	LLDP-Med does not work in certain circumstances
Q01947050	ADAC system message logged after a stack is reset.
Q01948343	On a pure 56xx stack, port mirroring mode XrxYtx multiplies unicast traffic on port Y in certain scenarios.
Q01950071	VLACP enabling does not work in some circumstances.
Q01950147	The EAP-TLS or PEAP-MsChapV2 clients could be unexpectedly transitioned to the EAP Held state on a multihost enabled port.
Q01950311	Voice traffic is blocked on a non-base unit when ARP inspection is enabled on a VoIP VLAN.
Q01951600	Error performing MIB walk on 5632.
Q01954041	LLDP Med-Network-Policies Voice Tagging command issue.
Q01955272	PIM OIF may not get installed on IR.
Q01956922	Continuous IPv6 ping out stops working after 2147 ICMPv6 messages.
Q01978465	Telnet session hangs on ERS 5510-48T during an ASCII configuration download.

Table 9 Resolved issues

Change Request number	Description
Q02005019	ACG will fail when ports are added to VLANs if an STG was created, VLANs were added, the STG enabled and then ports added to VLANs (configuration control flexible and 1 port in 2 different VLANs).
Q02020938	After booting to default settings the syslog will display the message **ASCII failed at line 1**. This can be ignored. This only happens after a boot to default settings and not during a normal operation or reset of the switch. This does not affect subsequent ASCII downloads. The successful application of configurations can be confirmed using the `show logging` command. The bogus message will be the first in chronological order.

Known issues and limitations

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

Navigation

Known issues

See the following table for a list of known anomalies for the Ethernet Routing Switch 5000 Series Release 6.2.

Table 10 Known issues

Change Request number	Description

Q01319058	In a Nortel SNA setup, you may experience temporary loss of Nortel SNA functionality when UDP forwarding has approached maximum capacity. Workaround: Configure a filter on the port that connects to the SNAS (or depending on your configuration, on the port connected to the switch that, in turn, connects to the SNAS) to isolate Nortel SNA SSCP traffic received by the CPU.
	Use the following CLI commands to configure a filter:
	`qos ip-element <element_id> src-ip <ip_address/mask>`
	`qos classifier <value> set-id <value> element-type ip element-id <value>`
	`qos action <value> update-1p <value>`
	`qos policy <value> port <port_list> clfr-type class clfr-id <value> in-profile-action <action_id> prec <value>`

Q01893906	PIM will not function properly if the sender stops traffic and the SDR and DDR are on the same device.
Q01918300	VRRP may intermittently bounce when multiple protocols are configured on upstream routers with traffic and large routing updates.
Q01925597	Inconsistent display of pluggable modules in BigWave Stacks.
Q01943946	It may take more time than usual for traffic to re-converge (approximately 10 seconds) if a stack from the core is rebooted in a highly scaled SMLT configuration (100 VLANs).
Q01945335	Port mirroring mode XrxYtx on a 56XX device does not mirror broadcast, multicast and unknown unicast traffic if the X and Y mirrored ports are in different MLTs.
Q01979384-01	HTTP connections are not displayed by the `show ipv6 tcp connection` command.
Q01992383	PM Unicast doubled on monitor - hybrid stack, using xRx Or/And yTx modes.
Q01997912	The `show ip ospf neighbor detail` command that provides detailed information for OSPF LSDB should not be run when the terminal length is set to 0.
Q02001870	A non-PoE phone may display as Unknown and may need to be rebooted after a stack is rebooted.

Table 10 Known issues

Change Request number	Description
Q02004055	There is currently no command to disable the *metric* and *route-type* options for the `route-map <route_name> match` command and no command to disable the *ip preference, metric*, and *metric-type* options for the `route-map <route_name> set` command.
Q02007132	When the maximum of 10 DHCP clients are bound by IP Source Guard on MLT/LACP ports, if those ports go down, several IPSG binding table full messages will be logged. This is an incorrect behavior.
Q02009524	On a stack with 55xx units with all QoS filters or masks used, when ADAC tries to use another QoS mask / filter (unavailable because of exhausted resources), the system displays a commitFailed 1 message. The correct message is displayed for a 56xx or 55xx standalone device.
Q02009977-01	Specifying a range of ports for non-base units using the `poe poe-shutdown port X` command may cause IP Phones connected to those ports to remain powered on in some stack configurations.
Q02010212-01	Wait twice the configured MAC aging time after swapping two PCs behind 2 phones in an NSNA solution before plugging the PCs back in behind the phones.
Q02012264-01	After the reboot of a non-base unit in a stack of 2 with NSNA enabled, port 1/1 may shut down. Re-enable the port manually should this situation occur.
Q02014299	IPv6 traffic not destined for the switch or stack will not be processed by ERS 5500 Series units and therefore IPv6 neighbor cache entries will not be created for the devices exchanging traffic. This behavior is different on ERS 5600 Series units where entries are created if traffic passes them. In either instance the actual flow of IPv6 traffic is not influenced, just the contents of the neighbor cache.
Q02015511	If the UBP set is configured and the QoS agent is disabled when an EAP / Non EAP user authenticates, several log messages displaying QoS support is currently disabled will be produced.
Q02016370-01	If a PC is moved from behind a phone to another port or behind another phone, the PC won't age out on the old port after the aging time configuration in NSNA Fail Open. A new PC may in the old port may not be able to authenticate unless the phone is rebooted. **WORKAROUND**: Remove the PC from phone 1 and wait twice the configured aging time. Move the PC to the new port or phone. This ensures the ageout timer works as configured.
Q02016405	Can't see MAC add table for MLT ports after removing 55xx from a hybrid stack.

Table 10 Known issues

Change Request number	Description
Q02024644	The MAC security learning ports and security lists will present a display issue on 56xx units after upgrading to Release 6.1.
Q02029127	Commands may not be saved in the same format between different versions of an ACG file. These format differences do not affect the overall functionality of the stored commands. Some configuration management software may identify this as a change in configuration but it is only a change in the manner in which the command is stored in the file.
Q02050773	**OSPF**: Even though two LSA packets are sent (one with unicast destination address and one with multicast destination IP) only one LS ACK transmitted packet appears in the interface statistics table
Q02056133-02	**EDM**: To enable or disable EDM access use NNCLI commands `web-server enable` or `web-server disable.`
Q02059066	STP is re-enabled when moving SMLT ports from 1 STG to another.
Q02059865-01	**STACK**: EDM supports both Firefox and Internet Explorer; however, Firefox currently responds faster. There is an initial delay of 2 to 3 minutes when you use Internet Explorer.
Q02060814	**STACKING**: When you copy a binary configuration to an TFTP server, you may receive an **Intra-stack communication failure** message. This does NOT indicate a stack failure; it indicates that the command failed. **WORKAROUND**: If you receive the **intra-stack communication failure** message, execute the `copy binary` command until it succeeds.
Q02065172	**STACKING, NSNA**: In a stack with a large number of NSNA-enabled ports, a great deal of inter-unit messaging related to NSNA filter installation occurs at start-up. In some circumstances, processing of these messages may be delayed long enough for the message originator (typically the base unit) to consider the messages lost and an error to have occurred. However, message processing on the non-base units may have completed successfully after a minimal delay, allowing NSNA configuration to successfully complete. In this case, errors included in the system log may not signify actual configuration errors. If you receive error messages but suspect that NSNA configuration is complete, examine the NSNA-enabled ports to determine whether they correctly configured. If you find discrepancies, disable and re-enable NSNA.

Table 10 Known issues

Change Request number	Description
Q02068702	In the SMLT network, loop may be temporarily introduced on LACP-over-SMLT port. In order to prevent loop from happening it is required to configure all LACP-over-SMLT port in "Lacp Advance mode". Under this mode, LACP port stays in Blocking mode until it receives the first LACP PDU from its partner port. In 6.2 release, it is the user's responsibility to put all LAC-over-SMLT ports in "Lacp Advance Mode.
Q02077709	Do not see the ability to set Forced Stack Mode via the EDM interface.
Q02085548	**SFPs**: To ensure a proper match of the remote side, before you install an SFP set shared ports to auto-negotiate. Refer to NNCLI: default speed and default duplex
Q02087588	IPv6 Tunnel over IPv4 operational status is determined by combination of IPv6, IPv4 forwarding, and VLAN status. The IPv6 tunnel operational status is ACTIVE if IPv6, IPv4 forwarding is enabled and the VLAN status to which source IPv4 tunnel end point is UP (i.e. at least one port on VLAN is connected). Operational status ACTIVE does not indicate the liveliness or reachability of IPV4 remote tunnel end point.
Q02089575	Supported capabilities in Ethernet Routing Switch 5000 Series switches, the maximum supported PIM-SM entries should state up to 492 for 55xx Switches and up to 992 for 56xx Switches - not 500 and 1000.
Q02090303	**EDM LLDP Port MED**: When you insert a Local Policy, select either Voice or Voice policies. It is not recommended to select both options for the same Local Policy insertion.
Q02091856	**SLPP**: In a stack of 5 or more units that runs a complex configuration, for example, SMLT, LACP, SLPP, or OSPF, SLPP can fail to detect and prevent loops due to inadequate system resources. SLPP PDUs are not treated as high priority packets and are not processed on time. This does not happen on SLPP ports on base units.
Q02092550	**TDR**: Run TDR tests only for ports with Link Status UP. Test results can be inaccurate for ports with Link Status DOWN.
Q02092802	**DEMO LICENSE**: If you use a Demo License and you remove the Demo License, you must reboot the stack.
Q02099762	`show running-config defaults` When you execute the show running-config defaults or show running-config default specific commands the system may take up to 4 minutes to return results, depending on the complexity of the system: for example, an 8-high stack fully configured. This is considered normal behavior.

Table 10 Known issues

Change Request number	Description
Q02105783-01	The old RSTP Traps command is hidden (this means is not displayed when question mark is given and the command is not autocompleted when hitting TAB). Use the new commands found under 'snmp-server notification-control'. You can obtain a list of the current notification traps available using 'show snmp-server notification-control'.
Q02111347-02	**EDM**: 'Unresponsive script' warning appears in Firefox when hiding non-editable columns in 'EAPOL Multiple Port Config' section.
Q02114855	**STACKING**: After you reboot a non base unit in a stack, some logs can appear in the output for the show logging command. The log messages are generated by stack port state changes and you can disregard them. Example: Link Down Trap for Unit/Port: 0/Cascade.
Q02115658	**IPv6 DHCP Relay**: IPv6 DHCP Relay does not support Remote ID parameter (RFC 4649) in this release.
Q02117565	**EDM, RATE LIMITING**: Multiple port configuration for Rate Limiting may not work properly; the change allow rate of broadcast or multicast may produce an incorrect result. **WORKAROUND**: Use NNCLI to configure Rate Limiting.
Q02121563	In Lossless mode, when oversubscription exceeds 10 ports to 1 port, ingress ports must be spread across groups of 24 ports.
Q02121817-01	**Energy Saver**: When energy saver is activated or deactivated, the link on a port briefly transitions. This causes some devices to re-acquire connectivity. For copper uplink ports or critical devices, it is recommended to disable energy saver at the port level.
Q02121827-01	**EAP** authentication will be restarted on copper ports when Energy Saver transitions to active or inactive state. This occurs because Energy Saver is clearing the MAC address on the EAP client port when transitioning to the active or inactive state. EAP fiber port status does not change when Energy Saver is activated or deactivated.
Q02121828-01	**NEAP** authentication is restarted on copper ports when Energy Saver transitions to active or inactive state. This occurs because Energy Saver transition clears the MAC address on the NEAP client port. NEAP fiber ports EAP status does not change when Energy Saver is activated or deactivated
Q02122362	**EDM**: In this release EDM does not display syslog message severity. **WORKAROUND**: Use remote logging or NNCLI to gather syslog message severity information.
Q02123917	**PORT MIRRORING**: Port mirroring will mirror pruned multicast streams to the monitor port. However, the streams are not actually sent to the device because they are pruned.

Table 10 Known issues

Change Request number	Description
Q02125240	**EDM, Multiple Port Selection**: EDM can delete up to a maximum of 120 ports when you use multiple port selection. If you select more than 120 ports, some of the ports may not disabled.
Q02126101	**NSNA**: When you use an NSNA configuration on multiple units from a stack, after boot some NSNA errors may be present in the logs. NSNA will work as expected even if these errors are present.
Q02127471	**EDM, DOWNLOAD**: If you use EDM to perform a download without reset you may not be able to execute commands in NNCLI for up to 10 minutes.
Q02127479	**EDM, DOWNLOAD**: If you use the dnldImgIfNewer option in EDM to download a software image, when the image matches the current image on the switch the system displays an error message. Example: Error. commitFailed.
Q02128827	**STACK**: When you reset an entire stack, if all units reboot except the Base Unit, perform a manual reset of the base unit.
Q02129106	**EDM**: You cannot view and configure 802.1ab Dot1 settings for Local Protocol Vlan and Local Vlan Name using EDM. **WORKAROUND**: Use NNCLI to view and configure 802.1ab Dot1 settings for Local Protocol VLAN and Local VLAN name.
Q02130384-01	**Upgrade**: All trap notifications are enabled after you upgrade to R6.2.0 software, regardless whether you disabled them prior to the upgrade. For procedures to restore trap functionality, see “Trap restoration and reconfiguration after upgrade to Release 6.2” on page 49.
Q02131292	**ROUTING, DEFAULT GATEWAY**: If you enable and disable routing globally on the management VLAN the default gateway may not work. In R6.2 you can configure the switch with default gateway (using the command `ip default-gateway <next-hop>)` or default route (using the command `ip route 0.0.0.0.0.0.0.0 <next-hop>`). When IP Routing is disabled (Layer 2 mode) on the switch, the default gateway serves as the default route, that is the default gateway shown by the `show ip` command. When IP Routing is enabled (Layer 3 mode) on the switch, the default route specified is used, that is the 0.0.0.0 route shown by the `show ip route` command. You can enter up to 4 static routes, management static routes, to be used for management traffic only. These routes are used in software routing only and do not affect pure data plane traffic. **SOLUTION**: You must enable routing on the management VLAN to activate management static routes which you can use for separation of management and data traffic.

Table 10 Known issues

Change Request number	Description
Q02131637	**PoE**: After a stack reboot an IP Phone 1120E powered by PoE may not receive an IP address through DHCP. **WORKAROUND**: Restart PoE on the interface.
Q02131677	**LLDP MED NETWORK POLICIES**: You cannot assign custom DSCP values to Nortel 1120E IP Phones using LLDP MED network policies.
Q02131749	**Lossless Mode:** Lossless activates in oversubscription scenarios even if rate-limiting is applied to certain ingress streams and slowing them is not necessary. Lossless gives fair access to bandwidth, meaning that if you have 3 ingress streams of 100% line rate competing on 1 egress port, lossless will slow down the sender transmit rates to a 33-33-33 percentage, and it does this by sending pause frames. If you have 2 streams coming in at 100% and a third at 20%, lossless will not interfere with this stream, the egress percentages will be 40-40-20. If the third stream transmit rate exceeds 33%, lossless will begin to apply to it as well. In this situation, if applying a meter to this stream, limiting it at under 33%, lossless doesn't activate and doesn't interfere. However, if the third stream is either broadcast or multicast traffic and a rate-limiting setting is applied instead of a meter, lossless will activate - it will send pause frames to the sender. The egress rate of the stream is not affected, it will be the one imposed by the rate-limiting setting, but the transmit rate will vary because of the pause frames.
Q02132058, Q02118271	**EDM**: If you use more than 2 EDM sessions concurrently you may receive Request timed out messages and may not be able to open EDM sessions. **WORKAROUND**: Use the COM EDM plug-in for your product.
Q02132100	**EDM**: When you close and reopen a menu using embedded EDM, for example MSTP when the switch is in MSTP mode, your internet browser can become unresponsive for 25-35 seconds. However, the browser recovers. This does not occur when you use COM with the associated EDM plug-in (Offbox).
Q02133290	**UPGRADE**: A temporary loop can occur in a large network during upgrade. **WORKAROUND**: Use the procedure in "Preventing a loop during upgrade of a large network" on page 51.
Q02136898	It is recommended that you use SNMPv3 to achieve security, instead of using SNMPv1 and/or SNMPv2c with community strings.
Q02140511-01	**RADIUS, RADIUS reachability**: If you use the "radius reachability use-radius", the switch sends reachability requests with the username 'avaya' and a blank password. Because the Avaya ignition server does not allow accounts to be created with a blank password, the ignition server will log intrusion events when the dummy requests are regularly sent from the switch. **WORKAROUND**: Use ICMP reachability for ignition server reachability.

Table 10 Known issues

Change Request number	Description
Q02144010	**802.1ab MED**: Both LLDP MED and ADAC policies are supported on the same port. If both types of policies are created on the same port and you delete the LLDP policy you created, then the ADAC policy is also deleted.
Q02144889	**Lossless Mode**: In Lossless buffering mode, if you use ingress traffic with queue 1 + ingress traffic with queue 2, and the egress port is on a different asic from ingress ports, QoS queue shaper may limit the bandwidth for queue 1 under the min-rate and egress traffic may be under the expected rates.
Q02145350	**EDM, LLDP TLV**: To disable LLDP TLVs using multiple port configuration you must execute the following additional steps: 1. Double-click **TLVsTxEnable**. 2. Make a selection. 3. Click **OK**. 4. Double-click **TLVsTXEnable**. 5. Uncheck the selection made in step 2. 6. Click **OK**. 7. Apply the selection to multiple ports to disable the LLDP TLVs.
Q02147075	**IPv6 Static Routes**: In an IPV6 setup where static and backup static routes exist, if you disable the IPv6 routing on a neighbor next-hop router, the active route will remain active until ARP for the next-hop expires or until a neighbor solicit message is forced (ping, clear neighbor, clear neighbor mac address) or until you execute shutdown/ noshutdown on the respective interface.
Q02149708	**Energy Saver**: You must not select fiber ports when you use the Multiple Port Configuration menu to enable Energy Saver on a range of ports.
Q02149996	**EDM, MSTP**: If your environment contains a large number of stacks and a large number of ports and you click between the CIST Port, MSTI Bridges, and MSTI Port tabs, the system may display the **Unresponsive script dialog** because you have initiated a large data retrieval.
Q02150634	**AUR/DAUR**: The reboot process can take approximately 3 minutes to complete, after which the normal CLI commands will display the AUR status.

Table 10 Known issues

Change Request number	Description
Q02151530	**AUR, LICENSING**: After you perform automatic unit replacement (AUR) of a base unit, if the MAC address of the new unit introduced into the stack was not part of the original license, then, when you reboot the stack and execute the NNCLI command `show license all`, the output displays that 0 licenses are present. **WORKAROUND**: Licenses will be operational, or can be enabled, and you can verify the license state using the following NNCLI commands: • `show license all verbose` to check whether any bit is set in the License Vector in Use data • `show sys-info`: the Operational license field shows the current license state • `show system verbose`: Operational license field shows the current license state
Q02153392	The console could lock for up to 10 minutes if ACG is copied to the USB port after it was toggled (disabled and enabled) in a short period of time.
Q02154994	**QoS, MIXED STACK**: In a mixed stack environment with Trusted ports present on ERS 56XX units, transitioning from a QoS-disabled mode to a QoS-enabled mode may leave some Trusted ports on the 56XX units in the QoS-disabled state due to a temporarily incorrect resource requirements calculation. **WORKAROUND**: If trusted ports on 56XX units in a mixed stack remain in the QoS-disabled state, manually reassign the those ports to the appropriate Trusted interface group.

Q02156580	**AUR**: If you replace an ERS 56XX unit in a stack that uses AUR you must set the stack operation mode for the new unit before you introduce it to the stack.
	Hybrid stack
	After you set the replacement unit to default, at NNCLI Global Configuration mode prompt enter the following commands
	`stack oper-mode hybrid`
	`save config`
	Pure stack
	After you reset the replacement unit to default, at NNCLI Global Configuration mode prompt enter the following commands:
	`stack oper-mode pure`
	`save config`

Table 10 Known issues

Change Request number	Description
Q02156687	**EAP, IP ROUTING**: If you globally enabled EAP but disabled EAP on a specific port and traffic is dropped on that port, enable IP Routing.
Q02156864	**SLPP**: In a stack of 5 or more units that runs a complex configuration, for example, SMLT, LACP, SLPP, or OSPF, SLPP can fail to detect and prevent loops due to inadequate system resources. SLPP PDUs are not treated as high priority packets and are not processed on time. This does not happen on SLPP ports on the base unit.

Trap restoration and reconfiguration after upgrade to Release 6.2

Use the procedures in this section to restore and reconfigure trap functionality after you upgrade to Release 6.2 software. You can reconfigure trap notification, using either EDM or NNCLI.

Restoring trap notification functionality using NNCLI

Use the following procedure to restore trap notification functionality using NNCLI:

1. Use the following NNCLI command to remove traps created using R6.1 and before: `no snmp-server host X.Y.Z.T 'community name'.`

Reconfiguring traps using EDM

Use the following procedure to reconfigure traps using EDM:

2. From the navigation tree, click **Edit**.
3. From the Edit tree, click **Snmp Server**.
4. In the work area, select the **Community** tab.
5. Create a community string - you must specify the Notify View name.
6. In the work area, select the **Host** tab to create an SNMP host - use the community you created in the previous step.
7. On the **Host** tab, use the **Notification** button to activate or deactivate individual traps.

8 In the work area, select the **Notification Control** tab to activate or deactivate individual traps per device.

Reconfiguring traps using NNCLI with v1 host example, password security enabled

Use the following procedure to reconfigure traps using NNCLI - v1 host example with password security enabled:

1 To create a community, from the Global Configuration prompt, enter the following command:

```
snmp-server community notify-view nncli

Enter community string: CommunityName

Enter community string: CommunityName
```

2 To create an SNMP host using the community you created in the previous step, from the Global Configuration prompt enter the following command: `snmp-server host 10.100.68.3 port 162 v1 CommunityName filter TestFilter`.

Reconfiguring traps using NNCLI with v1 host example, password security disabled

Use the following procedure to reconfigure traps using NNCLI - v1 host example with password security disabled:

1 To create an SNMP community, from the Global Configuration prompt, enter the following command: `snmp-server community CommunityName notify-view nncli`.

2 To create an SNMP host using the community you created in the previous step, from the Global Configuration prompt enter the following command: `snmp-server host 10.100.68.3 port 162 v1 CommunityName filter TestFilter`.

Setting the Notification Type per receiver using NNCLI

Use the following procedure to set the Notification Type per receiver using NNCLI.

1. From the Global Configuration prompt, enter the following command: `snmp-server notify-filter TestFilter +org`.
2. From the Global Configuration prompt, enter the following command: `snmp-server notify-filter TestFilter -linkDown`.
3. From the Global Configuration prompt, enter the following command: `snmp-server notify-filter TestFilter -linkUp`.

Displaying Notification Types associated with the notify filter using NNCLI

Use the following procedure to display the Notification Types associated with the notify filter using NNCLI.

1. From the Global Configuration prompt, enter the following command: `show snmp-server notification notify filter`

Enabling or disabling the Notification Type per device using NNCLI

Use the following procedure to enable or disable the Notification Type per device using NNCLI.

1. From the Global configuration prompt, enter the following command: `no snmp-server notification-control linkDown`.
2. From the global Configuration prompt, enter the following command: `no snmp-server notification-control linkUp`.

Preventing a loop during upgrade of a large network

Use the following procedure to prevent a temporary loop during upgrade of a large network.

1. Shut down LAC/SMLT ports on system A.
2. Download the new software image to system A.
3. Enable LAC/SMLT ports on system A.

4 Shut down LAC/SMLT ports on system B.

5 Download the new software image to system B.

6 Enable LAC/SMLT ports on system B.

Ethernet Routing Switch 5000 Series considerations

The following table lists known ERS 5000 Series considerations.

Table 11 ERS 5000 Series considerations

Item	Description
1	Some terminal programs can cause the Console Interface to crash if you enter a RADIUS secret containing the character “k”. The issue has been reproduced using Tera Term Pro (version 2.3), as well as Minicom (version 2.1) on a Linux system.
2	Nortel recommends that you avoid using MAC security on a trunk (MLT).
3	Failed attempts to log in (using TACACS+ authentication and accounting) are not stored in the accounting file.
4	When switches are in MSTP mode and connected using a trunk (MLT), and at least one MSTI is configured, the switch can return an incorrect STPG root if you change the mode to STPG and reset the switches.
5	When you use the JDM/Web to configure and add VLAN ports to an STG other than the default STG, STG membership of the port may change. In that case, the new STG participation of that port will be disabled. **WORKAROUND**: Enable participation of the ports in the new STG after you enable the STG.
6	On the 5530-24TFD, the following (NT-OCP) SFPs cannot be inserted side-by-side, in neighboring slots, because of the SFP size. For a list of SFPs, see “SFPs that cannot reside in neighboring slots in the ERS 5530-24TFD” on page 53.
7	While downloading the image file, you may receive the following error message: "Error reading image file." **WORKAROUND**: Typically, this issue can be resolved by simply restarting the image download. If this does not resolve the issue, Nortel recommends that you try an alternate method to download the image to the switch (that is, the Web Interface).
8	The IPFIX sampling data rate cannot be changed because of a related hardware limitation.

Table 11 ERS 5000 Series considerations

Item	Description
9	Release 5.1 introduced a Demo License to enable OSPF, ECMP, VRRP, SMLT, and IPFIX for a period of 30 days. The trial license expires at the end of the 30-day period and the features, except SMLT, are disabled. The system sends traps advising of license expiration but SMLT remains enabled until the stack or unit is reset. Nortel recommends that, when you receive the first trap, the administrator begins to manually disable SMLT and ensure removal of any cabling loop. Because Spanning Tree Protocol needs to be disabled and, because SMLT is implemented through cabling, SMLT is not disabled with the other features because a network loop would form. After demo license expiry, when the stack or unit is reset, SMLT is disabled and a loop will form if there has been no intervention to remove or disable the ports participating in the IST. Demo license expiry traps: Five days prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 5 day(s). One day prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 1 day(s). At termination of demo license: bsnTrialLicenseExpiration: Trial license 1 has expired.
10	When you configure IPFIX to work with NetQoS, Nortel recommends that you disable the SNMP polling by NetQoS device. To do this, remove the community string associated with the ERS 5500 Series switch on NetQoS device.
11	Nortel recommends that you do not enable IP Source Guard on trunk ports.
12	Nortel recommends that you do not enable Critical-IP functionality with VRRP in an SMLT environment.

SFPs that cannot reside in neighboring slots in the ERS 5530-24TFD

The following list of SFPs states the manufacturer's part number and Nortel part number for SFPs that cannot reside in neighboring slots in the ERS 5530-24TFD.

- TRP-G1H5BC470N4 / AA1419025

- TRP-G1H5BC490N4 / AA1419026
- TRP-G1H5BC510N4 / AA1419027
- TRP-G1H5BC530N4 / AA1419028
- TRP-G1H5BC550N4 / AA1419029
- TRP-G1H5BC570N4 / AA1419030
- TRP-G1H5BC590N4 / AA1419031
- TRP-G1H5BC610N4 / AA1419032
- TRP-G1H7BC470N4 / AA1419033
- TRP-G1H7BC490N4 / AA1419034
- TRP-G1H7BC510N4 / AA1419035
- TRP-G1H7BC530N4 / AA1419036
- TRP-G1H7BC550N4 / AA1419037
- TRP-G1H7BC570N4 / AA1419038
- TRP-G1H7BC590N4 / AA1419039
- TRP-G1H7BC610N4 / AA1419040

VLACP issue

In some situations, when you use VLACP the ERS 5000 series switches remove a link from service due to variations in the arrival time of VLACP messages (VLACP PDUs) from the far end. The issue can exist between the ERS 5500 and ERS 5600 models and ERS 8300 and ERS 8600 models when the system runs short timers with a default timeout interval of 3 time-outs or less. The ERS 5500 and ERS 5600 switches maintain a rolling history of the last 3 received VLACP PDUs (by default) and calculate the time variance across and between these VLACP messages.

SOLUTION: Increase the VLACP timeout-scale value to 3 or more.

Port or ifIndex offset issue

If you use Software Release 6.0, specify switch_type ERS5500 at the SNAS for standalone switches or stacks.

Filter resource consumption

Applications consume filter resources, which are a combination of masks and filters, also known as rules.

A filter specifies the bit pattern to match.

A mask specifies the bit position to match and the evaluation precedence of the filters.

To enable some applications, for example BaySecure, Port Mirroring, and IGMP, a set number of masks and filters are required.

The following table summarizes the applications that require mask and filer resources.

Table 12 Application mask and filter resource requirements

Application	Category	Masks required	Filters required
Ethernet Routing Switch 5500 Series			
QoS (Auto QoS)	QoS	1	4
IGMP	Non QoS	2	10
Port Mirroring (MAC-based)	Non QoS	2	2
EAP Authentication (EAPoL packet filter)	Non QoS	1	1
BaySecure (ES 5520/30 only)	Non QoS	1	32
EAP MHMA Allowed Clients (5520/30)	Non QoS	1	32
IPFIX	Non QoS	1	1
QoS Interface Applications	QoS	17	17
NSNA MAC Intruder	Non QoS	1	32
NSNA (R/Y/G filters)	QoS	5	8
ADAC	Non QoS	1	1
RIP	Non QoS	1	1
UDP Broadcast	Non QoS	1	1
VRRP	Non QoS	1	3
OSPF	Non QoS	1	3

Table 12 Application mask and filter resource requirements

Application	Category	Masks required	Filters required
IP Source Guard	Non QoS	1	10
Ethernet Routing Switch 5600 Series			
Broadcast APR and ARP Inspection	Non QoS	1	1
DHCP Relay or DHCP Snooping or NSNA DHCP	Non QoS	1	2
QoS (default untrusted policy)	QoS	2	2
QoS (DAPP with status tracking)	QoS	1	1
QoS (Auto QoS)	QoS	1	4
Port Mirroring (MAC-based)	Non QoS	1	2
EAP Authentication (EAPoL packet filter)	Non QoS	1	2
IPFIX	Non QoS	1	1
NSNA MAC Intruder	Non QoS	1	32
NSNA (R/Y/G filters)	QoS	5	8
ADAC	Non QoS	1	1
RIP	Non QoS	1	1
UDP Broadcast	Non QoS	1	1
VRRP	Non QoS	1	3
OSPF	Non QoS	1	3
IP Source Guard	Non QoS	1	11
PIM	Non QoS	1	1

On the ERS 5500 Series switches 16 masks and 128 filters are available on each port. By default, 1 mask and 1 filter are consumed by the system for ARP filtering, leaving 15 masks and 127 filters available to QoS and other non QoS applications to configure dynamically.

On the ERS 5600 Series switches the resources are shared across groups of ports. For each group of ports there 16 masks and 256 filers available for each mask. By default, the system consumes one mask and one filter for ARP filtering on all ports, leaving 15 masks available for each group and 255 filters available for each mask and group for QoS and other non QoS applications to configure dynamically.

You can use the `show qos diag` command to assess the current filter resource usage for each port on ERS 5000 Series switches.

The `show qos diag` command displays the number of QoS masks and filters and non QoS masks and filters consumed on each port. You can determine whether an application that requires filter resources can be enabled on a port by verifying that the number of available masks and filters meets the mask and filter requirements of the application.

On ERS 5500 Series switches, the available masks and filters on a port can be determined by adding the total number of QoS and non QoS masks in use and the total number of QoS and non QoS filters in use on a port, then subtracting that number from 16 masks and 128 filters.

On the ERS 5600 Series switches, you can count the unused masks to determine the number of available masks for a port by using the output of the `show qos diag` command. The ERS 5600 Series switches share resources across a group of ports. The filters used by QoS or non QoS applications on a port for a specific mask determine the available filters for that mask for all ports from that group.

On the ERS 5600 Series switches, you can determine the number of filters available for a mask from a group of ports by adding the total number of QoS and non QoS filters in use and subtracting that number from 256. If the number of filters in use for a mask equals 256, you cannot use that mask on other ports from the same group.

Example - IP Source Guard on an ERS 5500 Series switch port

On ERS 5500 Series switches, you need 1 mask and 10 filters to enable IP Source Guard on a port. When you view the show qos diag command out you see that port 5 is currently using a total of 4 masks and 5 filters. This means that 12 masks and 123 filters are available for use. So you can enable IP Source Guard on port 5.

Example - IP Source Guard on an ERS 5600 Series switch port

On ERS 5600 Series switches you need 1 mask and 11 filters to enable IP Source Guard on a port. When you view the show qos diag command output you see that port 5 is currently using a total of 4 masks. IP Source Guard uses the next available mask and, from the command output, you can see that there are 256 filters available for mask 14. So you can enable IP Source Guard.

QoS Interface Security application

The QoS Interface Security application only runs on ERS 5500 Series switches. It targets a number of common network attacks. Support includes ARP spoofing prevention, DHCP snooping, DHCP spoofing prevention, detection for the common worms SQLSlam and Nachia, and the Denial of Service (DoS) attacks Xmas, TCP SynFinScan, TCP FtpPort, and TCP DnsPort. Due to the lack of filter resources (masks) to enable the whole QoS Interface Security application, you can select individual security applications.

The following table summarizes the mask and filter resource requirements for individual QoS Interface Security applications.

Table 13 Mask and filter resource requirements

QoS Interface Security application	Masks required	Filters required
ARP Spoofing Prevention	5	5
DHCP Snooping	1	1
DHCP Spoofing Prevention	2	2
DoS SQL Slam	1	1
DoS Nachia	1	1
DoS Xmas	1	1
DoS TCP SynFinScan	1	1
DoS TCP FtpPort	2	2
DoS TCP DnsPort	2	2
QoS BPDU blocker interface	1	1