Ethernet Routing Switch 5510/5520/5530
Software Release 5.1.3

1. Release Summary

Release Date: 19-December-2008
Purpose: Software patch release to address customer found software issues.

2. Important Notes Before Upgrading to This Release

For customers upgrading from older software versions, a series of upgrades are required to prevent configuration corruption under certain circumstances. This upgrade path includes the following releases: 4.0, 4.1, 4.2 and 5.0.

3. Platforms Supported

Ethernet Routing Switch 5510/5520/5530

4. Notes for Upgrade

For details on updating the software on your Ethernet Routing Switch, please see "*Nortel Ethernet Routing Switch 5500 Series, Configuration — System*" for software release 5.1 (NN47200-500 v03.01). To download this document, go to http://www.nortel.com/support, and select **Routers & Routing Switches**. Under Ethernet Routing Switches, select either **Ethernet Routing Switch 5510, 5520, or 5530-24TFD**. Click on **Documentation** in the gray banner to view a list of all documentation for the product.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
5530_500004_diag.bin	Diagnostic image	812,036
5530_513024.img	Agent code image	6,010,560
5530_513025s.img	Agent code image (SSH)	6,258,324

5. Version of Previous Release

Software Version 5.1.2

6. Compatibility

This software release is managed with Java Device Manager (JDM) release 6.0.2 or later.

7. Changes in This Release

7.1. New Features in This Release

7.1.1. *EAP and NEAP Separation*

The purpose of this new feature is to allow distinct configuration options and functionality for EAP/NEAP clients. In previous versions, there is no option to disable EAP authentication without disabling NEAP clients.
In the 5.1.3 release, the user can choose to disable EAP and have only NEAP clients connected. In this case, EAP packets are no longer processed and the device will only forward traffic for authenticated NEAP clients.

CLI Commands:

(config-if)# eap multihost eap-protocol-enable	allow and process EAP packets (as before)
(config-if)# no eap multihost eap-protocol-enable	drop all EAP packets
(config-if)# default eap multihost eap-protocol-enable	allow and process EAP packets (as before)
(config-if)# show eapol multihost interface <port#>	display the new parameter
(config)# eap multihost eap-protocol-enable	allow and process EAP packets (as before)
(config)# no eap multihost eap-protocol-enable	drop all EAP packets

Per port and global SNMP support is available. See the bsee.mib file for details on the following SNMP objects:

bseeMultiHostEapProtocolEnabled
bseePortConfigEapProtocolEnabled

This feature also has ACG support for global and per port settings.
When upgrading from 5.1.2 to 5.1.3 the default value for eap-protocol-enable is “enabled” (to keep existing functionality).

7.1.2. Port-mirroring on 802.1x (EAP) port

Due to potential security risks, an EAP port could not be monitored or a mirror port, and a mirror port could not be set as an EAP port.

An enhancement is provided in this release to enable port-mirroring on EAP ports. Three new global commands to enable or disable port mirroring on EAP ports are provided under the EAP sub-commands/group. The format of the commands is:

EAPol allow-port-mirroring

no EAPol allow-port-mirroring

default EAPol allow-port-mirroring

The user will be provided with a warning message about the potential security risk in each one of the following situation:

When enabling the feature

If the user is mirroring an EAP port or try to enable EAP on a mirror port

When disabling the feature and there are still mirroring ports with EAP enabled

7.1.3. RADIUS request for ADAC MACs

ADAC MACs are allowed on an EAP enabled port subject to the following requirements:

Global EAP is enabled and Interface EAP is enabled (status = auto)
Global EAP multihost for configured NonEAP MACs is allowed
Interface EAP multihost for configured NonEAP MACs is allowed
ADAC is globally enabled
ADAC is locally enabled as a Telephony Port

Uplink and CallServer Ports cannot be non-EAP-enabled at the same time. Similarly, ADAC cannot be enabled locally on a port that is EAP enabled but is not configured for multi-host and to allow non-EAP MACs.

When a new MAC is seen on an EAP port and is allowed based on ADAC credentials, a dummy radius request as for a non-EAP radius MAC authentication will be sent. This is for servers to learn the MAC to update their databases. Any response from radius for an ADAC authenticated MAC will be ignored.

7.1.4. Filter Limiting

The 55xx 5.1.3 release includes a new functionality that enables the user to configure the maximum number of protocol-based VLAN filters that are available in the 5520 and 5530 hardware. 5510 has the capability for only 7 protocol VLAN entries. Due to this hardware limitation, any combination of 55xx stacks that included 5510s was limited to 7 entries. With this new feature, a user can configure a stack of 5520/5530 units (5510s not allowed) to take full advantage of the maximum of 16 protocol VLANs available in 5520/30. The default setting for the feature is based on the older 5510 configuration and a reboot is required to put the revised setting into use.

In a stack which has a 5520 or 5530 as a base unit and contains one or more 5510s, the 5510s will not join the stack after reboot and will be isolated and have their base light blinking indicating they are not in the stack.

When one attempts to disable the feature in a stack which contains one or more 5510s, the user will be warned that 5510s will no longer be part of the stack. In addition, the user is warned of a potential loss of stack after reboot. This is due to the fact that 5510s won't join the stack so that the cascade connectors will not have a continuous path between units preventing inter-unit communication and stack formation.

If a unit joins a stack and has a different setting for filter limiting than the setting on the base unit, the new unit's setting will be changed and the unit will be rebooted and will join the stack after reboot.

Command formats:

qos filter-limiting enable	(Enable filter limiting)
no qos filter-limiting enable	(Disable filter limiting)
show qos filter-limiting	(Display current and next boot settings)
qos default filter-limiting	(Sets next boot value to Enabled)

The output of the show qos filter-limiting command displays the current and next boot settings:

Filter Limiting current setting: Enabled
Filter Limiting next boot setting: Enabled

Support for filter limiting is provided in the ASCII configuration file.

Note that if one saves an ASCII configuration that has filter limiting disabled with more than 7 protocol VLANs and applies that configuration file to a switch/stack that has filter limiting enabled, only the first 7 protocol VLANs will be configured and subsequent protocol VLANs will cause errors. When this is loaded via the CLI, error messages will be displayed but the ASCII configuration file processing will continue. When loaded via JDM, the first error will cause the process to stop.

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

Nortel RoHS (AA14030001-E5), 10G XFP fails during continuous data transfer (**Q01862257**).

OSPF multicast addresses should not be configured for unknown-mcast-allow-flood with OSPF enabled (**Q01900472**)

IGMP general queries were not sent over MLT after a reboot (**Q01900952**).

When IGMP was disabled and then re-enabled, IGMP general queries were not sent over MLT (**Q01900995**).

The command ‘show mac-address-table port x/x =’ did not produce an output (**Q01887303-03**).

When using the Web Interface, the option to select 1000Mbs/Full for ports 25-48 was missing (**Q01909355**)

Setting the parameter "ip ospf cost" did not show in the ASCII configuration (**Q01918262**).

A specific configuration using QoS policies generated an error in 5.1.1 (**Q01911158**).

The DHCP mode could not be changed from the default value (**Q01854140**).

Ports with STP configured on them remained in blocking although the original loop had been cleared (**Q01924699**).

With STP configured over DMLT trunks, traffic flow over the DMLT stopped while STP converged (**Q01899528-01**).

User Based Policies were not properly aging out (**Q01901832-01**).

The DHCP offer packets were dropped when MAC Security was enabled (**Q01864504-01**).

Under certain conditions, an error is generated when loading an ASCII configuration (**Q01920225**)

When EAP was reinitialized, authentication would fail on the first attempt and then would authenticate correctly after approximately 30 seconds (**Q01840171**).

Static routes became inactive after a few days (**Q01930428**).

VLACP operational status was not consistently displayed in NNCLI (**Q01931070**).

OSPF multicast addresses should not be configured for unknown-mcast-allow-flood with OSPF enabled (**Q01900472**).

Non-EAPOL client sends MAC address as password with periods at the start and end of the password (**Q01936857**).

5530 did not correctly process the MST BPDUs that were transmitted from some non-Nortel core switches (**Q01886438**).

There were connectivity issues with IP phones when ARP inspection was enabled (**Q01951221**).

The Timestamp sent out for the IPFIX flows was 0 (**Q01771425-01**)

Enabling port-mirroring on a stack of 5 to 8 units could cause stack instability (**Q01948148-01**).

Under certain conditions, “Intra-stack communication failure” error was displayed when trying to download a binary configuration (**Q01785951-01**).

VLACP port flaps could cause invalid Forwarding Data Base and ARP tables (**Q01933842**).

8. Outstanding Issues

Q01953520 – Using the web browser to enable EAP is not always successful.

9. Known Limitations

When upgrading from any previous release to 5.1.3 the following EAP enhancements will have their settings defaulted:

Dynamic VLAN assignment from RADIUS server for EAP and non-EAP authentication device
EAP/NEAP Separation
Use most recent radius vlan

To avoid loosing specific configuration related to these EAP enhancements, it is recommended to save these setting using an ASCII configuration file before upgrading to 5.1.3 and restore them after upgrade.

10. Documentation Corrections

For other known issues, please refer to the product release notes and technical documentation available from the Nortel Technical Support web site at: http://www.nortel.com/support .

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Technical Support on the web at: http://www.nortel.com/support