Ethernet Routing Switch

5510/5520/5530/5698TFD(-PWR)/5650TD(-PWR)/5632FD

Software Release 6.1.2

1. Release Summary

Release Date: 22-December-2009
Purpose: Software patch release to address customer and internally 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. Customers upgrading to release 6.0.1 and later versions from software versions prior to Release 6.0, must first upgrade to Release 6.0. Please see "Ethernet Routing Switch 5000 Series Release Notes - Release 6.0" for details on how to upgrade your Ethernet Routing Switch to Release 6.0.

3. Platforms Supported

Ethernet Routing Switch 5510/5520/5530/5698TFD(-PWR)/5650TD(-PWR)/5632FD

4. Notes for Upgrade

Please see "Nortel Ethernet Routing Switch 5000 Series, Configuration – System, Software Release 6.1" (NN47200-500, available at http://www.nortel.com/support). Under Technical Support, select Routers & Routing Switches followed by Ethernet Routing Switch 5510, 5520, 5530-24TFD, 5698TFD(-PWR), 5650TD(-PWR) or 5632FD) for details on how to upgrade your Ethernet Routing Switch.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
5xxx_60009_diags.bin	Diagnostic image	2,464,972
5xxx_612028.img	Agent code image	15,818,424
5530_612029s.img	Agent code image (SSH)	16,360,068

5. Version of Previous Release

Software Version 6.1.1.

6. Compatibility

This software release is managed with Java Device Manager (JDM) release 6.2 or later.

7. Changes in This Release

7.1. New Features in This Release

7.1.1 Dynamic VLAN assignment from RADIUS server for EAP and non-EAP authenticated devices

In this release both EAP and non-EAP clients may be authenticated and assigned to a VLAN when in MHMA mode. In other modes, VLAN assignment is ignored.

In order to utilize this feature, the user must enable the *radius-non-eap-enable* globally and at the interface (port) level. Once enabled, EAP and non-EAP MACs will be assigned to configured VLANs.

NNCLI configuration
New CLI commands are provided for Radius assigned VLANs for EAP and Non-EAP MACs:

EAPol multihost use-radius-assigned-VLAN
no EAPol multihost use-radius-assigned-VLAN
default EAPol multihost use-radius-assigned-VLAN
EAPol multihost non-EAP-use-radius-assigned-VLAN
no EAPol multihost non-EAP-use-radius-assigned-VLAN
default EAPol multihost non-EAP-use-radius-assigned-VLAN

7.1.2 802.1X Authentication, NEAP / MAC-based Authentication, and Guest VLAN functionality on the 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.

NNCLI configuration
Use the commands in this section to allow a non-EAP phone to function with the Guest VLAN enabled.

Enabling EAPOL VoIP VLAN

Perform this procedure to enable the EAPOL multihost VoIP VLAN.

Prerequisites

• Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Enable the EAPOL multihost VoIP VLAN by using the following command: **`eapol multihost voip-vlan <1-5> {[enable] [vid <1-4094>]}`**

Variable definitions

The following table defines variables you can use with the **`eapol multihost voip-vlan <1-5> {[enable] [vid <1-4094>]}`** command.

Variable	Value
Enable	Enables VoIP VLAN
voip-vlan <1-5>	Sets number of VoIP VLAN from 1 to 5
vid <1-4094>	Sets VLAN ID, which ranges from 1 to 4094.

Disabling EAPOL VoIP VLAN

Perform this procedure to disable the EAPOL multihost VoIP VLAN.

Prerequisites

• Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Disable the EAPOL multihost VoIP VLAN by using the following command: **`no eapol multihost voip-vlan <1-5> [enable]`**

Variable Definitions

The following table defines variables you can use with the **`no eapol multihost voip-vlan <1-5> [enable]`** command.

Variable	Value
Enable	Disables VoIP VLAN.
voip-vlan <1-5>	Sets the VoIP VLAN number, range is 1 to 5.

Configuring EAPOL VoIP VLAN as the default VLAN

Perform this procedure to configure the EAPOL multihost VoIP VLAN as the default setting.

Prerequisites

• Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Configure the EAPOL multihost VoIP VLAN by using the following command: **`default eapol multihost voip-vlan <1-5> [enable][vid]`**

Variable Definitions

The following table defines variables you can use with the **`default eapol multihost voip-vlan <1-5> [enable] [vid]`** command.

Variable	Value
enable	Disables VoIP VLAN.
Vid	Default VoIP VLAN ID.
voip-vlan <1-5>	Sets the VoIP VLAN number, range is 1 to 5.

Displaying EAPOL VoIP VLAN

Perform this procedure to display information related to the EAPOL multihost VoIP VLAN.

Prerequisites

• Log on to the Global Configuration mode in NNCLI.

Procedure steps

Step	Action
1	Display information related to the EAPOL multihost VoIP VLAN by using the following command: **`show eapol multihost voip-vlan`**

Device Manager configuration

Enabling VoIP VLAN

Perform this procedure to activate the VoIP VLAN.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Security, Security.**
2	Click the **EAP VoIP Vlan** tab.
3	Configure VoIP vlans as required.
4	Click **Apply**.

Variable Definitions

The following table defines variables you can use to enable VoIP VLAN.

Variable	Value
MultiHostVoipVlanIndex	Sets the VoIP VLAN number, range is 1 to 5.
MultiHostVoipVlanEnabled	True-Enables the VoIP VLAN False-Disables the VoIP VLAN
MultiHostVoipVlanId	Sets the VLAN ID, which ranges from 1 to 4094

7.1.3 802.1X Authentication and NEAP functionality with Radius, but with Radius response using VLAN names instead of VLAN ids

The 802.1X or non-EAP with VLAN names functionality enhances the switch to match RADIUS assigned VLANs based on either the VLAN number or a VLAN name. Prior to this release, a match occurred based on the VLAN number of the Tunnel-Private-Group-Id attribute returned by the RADIUS server.

Now you can use the VLAN number or names for configuring VLAN membership of EAP or non-EAP clients.

The Tunnel-Private-Group-Id attribute is converted to either a VLAN ID or VLAN name, based on the first character of the returned attribute. If the first character in the attribute is a number, the switch processes it as a VLAN number. In other cases, the attribute is taken as a VLAN and matched on the full string. The maximum length of a VLAN name can be 16 characters. You do not have to configure this feature as this mode is always enabled.

7.1.4 802.1X Authentication and NEAP with Fail-Open functionality

This feature provides network connectivity for EAP-enabled or non-EAP-enabled ports to 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 clients are re-authenticated and, as appropriate, moved to the assigned VLANs, allowing normal network connectivity.

Every three minutes, the switch checks whether the RADIUS servers are reachable. If the switch cannot connect to the primary and secondary RADIUS servers after a specified number of attempts, the switch declares the RADIUS servers unreachable, moving all authenticated devices into the Fail-Open VLAN.

Moving the clients into the Fail-Open VLAN prevents the clients from being disconnected when the re-authentication timer expires, providing limited network connectivity.

To provide the level of connectivity as required by corporate security policies, configure the Fail-Open VLAN for the network. For example, when the Fail-Open VLAN is configured to provide access to corporate IT services, the VLAN may exclude financial and other sensitive resources since client re-authentication is impacted.

When a client operates in the Fail-Open VLAN without RADIUS servers reachable, 802.1X logoff messages received from the EAP supplicant are not processed by the switch.

For an EAP or non-EAP enabled port, by default, the Fail-Open VLAN feature is disabled. When the RADIUS servers are unreachable and the Fail-Open VLAN is defined:
- the port becomes a member of both the EAP Fail-Open VLAN and EAP Fail-Open VoIP VLANs
- the switch sets the PVID of the switch port to the EAP Fail-Open VLAN
- all the EAP-enabled ports move to the Fail-Open VLANs on all units in a stack

SPECIAL NOTES
When the switch is operating in Fail-Open mode, it does not send EAP authentication requests to the RADIUS Server and instead performs a dummy re-authentication of the client within the Fail-Open VLAN.

When the port transitions from normal EAP operation to Fail-Open, the end client is not aware that the port has transitioned to a different VLAN. Depending upon the association of the IP addressing scheme to VLANs, it is necessary for the client to obtain a new IP address when transitioning to or from the Fail-Open VLAN.
An enhancement calls for the port to be administratively turned off, and then back on again when the port transitions between Fail-Open VLAN. If the PC is directly connected to the switch, this results in the client automatically refreshing the IP address. If the PC is located behind an IP handset, another switch, or a hub, the client must perform a manual renewal of the IP address.
After the switch accesses the RADIUS server and authentication succeeds, the ports move to the Guest VLAN, or to configured VLANs. The entries are aged to allow the continued authentication of all incoming MAC addresses on the port.

If there is at least one authenticated MAC address on the port, it blocks all other unauthenticated MAC addresses on the port. You must turn on the debug counters to track server reachability changes.

Use the procedures in this section to configure the 802.1X non-EAP with Fail-Open VLAN using NNCLI.

Note: The switch does not prevent the Radius Assigned VLAN from being the same as the Fail-Open VLAN. This means that if you configure the Fail-Open VLAN name or ID the same as one of the VLAN names or IDs which can be returned from the RADIUS server, then EAP or NEAP clients could be assigned to the Fail-Open VLAN even though RADIUS remains reachable.

NNCLI configuration

Enabling EAPOL Fail-Open VLAN

Perform this procedure to enable the EAPOL Fail-Open VLAN.

Prerequisites

• Log on to the Global configuration mode using NNCLI.

Procedure steps

Step	Action
1	Enable the EAPOL Fail-Open VLAN by using the following command: **`eapol multihost fail-open-vlan {[enable] [vid <1-4094>]}`**

Variable Definitions

The following table defines variables you can use with the **`eapol multihost fail-open-vlan {[enable] [vid <1-4094>]}`**command.

Variable	Value
Enable	Enables fail-open-vlan.
Vid <1-4094>	Specifies a guest VLAN ID in a range from <1-4094>.

Disabling EAPOL Fail-Open VLAN

Perform this procedure to disable the EAPOL Fail-Open VLAN.

Prerequisites

• Log on to the Global configuration mode using NNCLI.

Procedure steps

Step	Action
1	Disable the EAPOL Fail-Open VLAN by using the following command: **`no eapol multihost fail-open-vlan [enable]`**

Variable Definitions

The following table defines variables you can use with the **`no eapol multihost fail-open-vlan [enable]`** command.

Variable	Value
Enable	Disables the Fail-Open VLAN.

Setting EAPOL Fail-Open VLAN as the default

Perform this procedure to set the EAPOL Fail-Open VLAN as the default.

Prerequisites

• Log on to the Global configuration mode using NNCLI.

Procedure steps

Step	Action
1	Set the EAPOL Fail-Open VLAN as the default by using the following command: **`default eapol multihost fail-open-vlan [enable][vid]`**

Variable Definitions

The following table defines variables you can use with the **`default eapol multihost fail-open-vlan [enable] [vid]`** command.

Variable	Value
enable	Disables the Fail-Open VLAN.
vid	Sets the default Fail-Open VLAN ID.

Displaying EAPOL Fail-Open VLAN

Perform this procedure to display information related to the EAPOL Fail-Open VLAN.

Prerequisites

• Log on to the privileged exec mode and configuration mode using NNCLI.

Procedure steps

Step	Action
1	Display the status of the fail-open VLAN by using the following command: **`show eapol multihost fail-open-vlan`**

Device Manager configuration

Enabling EAPOL multihost Fail-Open VLAN

Perform this procedure to enable the EAPOL multihost Fail-Open VLAN.

Prerequisites

• Guest Vlan and failopen vlan do not have the same vid.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Security, Security**.
2	Click the **EAPol** tab.
3	Select the **MultihostFailOpenVlanEnabled** option.
4	Click **Apply**.

Job aid

The following example procedure specifies the use of VoIP VLAN and Fail-Open VLAN.

Step	Action
1	Specify VoIP VLANs. These must not be Fail-Open VLANs or Guest VLANs on any port.
2	Specify Fail-Open VLAN. This must not be VoIP VLANs or Guest VLANs on any port.
3	Specify Guest VLANs. These must not be VoIP VLANs or Fail-Open VLANs.
4	Enable non-phone-enable on a specific port and globally.
5	Enable GuestVlan on the same port and globally.
6	Enable FailOpen globally.

7.1.5 Support for DDI SFPs

This release includes support for newer SFP GBICs which include DDI functionality. The new SFPs will be recognized by the agent. Usage of the DDI SFP parameters and display of their values will be supported in a future release**.**

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

If the IST is disabled, then it's possible to delete the MLT while it's still configured as SMLT but when MLT with the same ID was re-created later, inconsistent configuration resulted (**Q02012165**).

Switch instability resulted after deleting a VLAN running multiple instances of RSTP when the switch is in RSTP mode (**Q02073016**).

Prior to any EAPoL activity, the switch checks the availability of the Radius server by sending an ICMP packet to a configured Radius IP address. If this fails (due to a firewall) the EAP will not function (**Q02025072-01**).

Data exception error in "tMCMgr" task when executing the “show ip mroute” command (**Q02070133**).

10G ports coming online too early (**Q02078638**)

During HP Openview queries of the ifIndex. the corresponding entries for the IfAdminStatus and IfOperStatus are down for those two mibs and it is not possible to manage the switch.
(**Q02073525-01**)

BPDUs are sent after STP is disabled causing MLT port blocking (**Q02082301-01**).

Manually executed post diagnostic tests show errors (**Q02082310**).

On a stack of 5530-24TFD units running 6.0.3,.when a large numbers of small VLANS (150 VLANS, minimum 2 port each) are created, then the traffic will not be delivered on some of them (**Q02039074-01**).

8. Outstanding Issues

SMLT traffic stopped after powering off one unit and then booting another unit in stack. This issue will be resolved in 6.1.3, the workaround for it is to disable and then enable the IST (**Q02084874**).

9. Known Limitations

EAP settings will be lost when downgrading from SW version 6.1.2 to 6.1.0 or 6.1.1 **(Q02084401).**

10. Documentation Corrections

None.

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 .