NORTEL

Ethernet Routing Switch 5510/5520/5530

Software Release 5.1.4

1. Release Summary

Release Date: 07-May-2009
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_514020.img	Agent code image	6,019,328
5530_514021s.img	Agent code image (SSH)	6,264,716

5. Version of Previous Release

Software Version 5.1.3

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

7.1.1 802.1 AB MED Enhancement

The purpose of this feature is to allow an IP Phone to get voice traffic VLAN ID, DSCP and priority and tagged/untagged traffic type information through LLDP-MED Network Policy TLV.

1. LLDP PDUs exchange

On a switch port, multiple devices can be seen – LLDP-MED devices (devices that can send LLDP with MED extensions) – and other non LLDP MED devices.

The following behavior will be for a port with LLDP enabled, Med-Capabilities TLV enabled, Network Policies enabled and configured.

When an IP Phone sends a LLDP PDU with MED capabilities the switch will notice that it has a MED endpoint device on that port and will reply with a PDU containing the Network Policies TLVs together with the other non-MED TLVs already set for transmission. (The LLDP-MED standard specifies that if med- capabilities TLV are not received from an endpoint device on a port then no other MED TLVs except med-capabilities will be sent to the user in a PDU).

The VID, DSCP, L2 priority and tagging information is sent to the IP Phone through LLDP-MED Network Policy TLV.

At any time, an endpoint device can send LLDP PDUs with Network Policy TLVs containing the Unknown flag set in order to notify the switch that the network policy is unknown but required and to specifically request from the switch the network policies for that application type. The switch shall reply with a PDU containing the Network Policy TLV.

2. Network Policy configuration

Each port will be able to add and delete the voice network policy and for each network policy to configure:

- VLAN, tagging options
- DSCP
- L2 Priority

Configuration of the VLAN at a per port basis will make possible the usage of multiple VLANs for voice traffic per switch, as required.

There has to be noted that these VLANs for voice traffic do not refer to ADAC Voice-VLAN; ADAC automatically creates its Voice-VLAN and also it automatically configures on ADAC telephony ports the Network Policy TLV for voice application type with VID = ADAC Voice-VLAN ID.

The default values for the DSCP and priority are the TIA-MED standards default – set to zero value.

3. Configuration options and user interface

The configuration options will be under the LLDP commands.
The command to add a per port voice network policy is:

```
(config-if)# lldp med-network-policies [port <portlist>] voice
            [dscp <DSCP>] |
            [priority <priority>] |
            [tagging <tagged | untagged>] |
            [vlan-id <VID>]
```

The command to delete a per port voice network policy is:

```
(config-if)# no lldp med-network-policies [port <portlist>] voice
```

The command to default – delete the network policy is:

```
(config-if)# default lldp med-network-policies voice
```

The command to display the configuration for each port and the status of the applied policies will look like:

```
(config-if)# show lldp med-network-policies [port <portlist>] voice
-------------------------------------------------------------------------------
                    lldp voice network-policies
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
   Port  Voice    Tagging    DSCP  Priority
         VlanID
-------------------------------------------------------------------------------
   1/1    1       tagged     1     6
   1/2    20      tagged     23    7
```

If no network policy is created/enabled on a port then nothing will be displayed on that line for the port.

NOTE: For now, only the voice option is implemented.

Warnings to the user:
If a user configures on a port a specific voice VLAN then warning messages will be displayed if:
   if ADAC is enabled on a port then a warning message will be displayed to the user;
   if the port is not a member of the VLAN with VID set on the Network Policy;
   if enable ADAC on a port and MED voice Network Policy is already configured on that port.

Only CLI will be supported as the user interface in this initial release of the feature.

4. Network Policy operation on the switch for an IP Phone

When a device with phone and MED capabilities is seen on a port the configured Network Policy for voice application type will be sent on that port to the MED devices.

5. 802.1AB Network Policies and ADAC policies

MED Network Policy for voice application type cannot be enabled on a port at the same time that ADAC is enabled on that port. This will be prevented and error message will be displayed to the user if the user tries to enable both MED Network Policies for voice application type and ADAC on the same port.

When enabling ADAC on a port:

test will be performed to see if user configured MED Network Policy for voice application type was created; if it was created then a warning message will be displayed for that port and the settings will not be applied:

```
“Cannot enable ADAC on MED Voice Network Policy enabled interfaces”
```

When adding a user configured voice Network Policy on a port:

test will be performed to see if ADAC is enabled on that port; if enabled then no policy will be added and a warning message will be displayed:

```
“Cannot enable MED Voice Network Policy on ADAC enabled interfaces”
```

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

Port Mirroring not functional under certain configurations (**Q01959329**)

Unable to modify newly created IPFIX rules (**Q01965294**)

STP port state changes when Port-Mirroring was enabled (**Q01951054-01**)

ARP entries did not age out when ARP timer was set to 5 min (**Q01895080-01**)

Stack instability occurred when “show ip route” CLI command with overlapping routes was used (**Q01963468**)

SLPP packets looped over MLT ports during VLACP link flap (**Q01926412**)

Invalid ASE LSA generation when direct redistribution was enabled (**Q01985487-01**)

When the option “eapol multihost non-eap-use-radius-assigned-vlan” was enabled the switch kept sending re-authentication to radius server every 10 minutes (**Q01994731-01**)

DHCP-relay was not properly forwarding the DHCP packets (**Q01998739**)

Under certain circumstances, the VRRP settings were not saved after reboot (**Q01993843-01**)

The VRRP address of the management VLAN was not always preserved after reboot (**Q01997145-01**)

Some times static routes got disabled after link to next hop was broken (**Q02002640-01**)

8. Outstanding Issues

None.

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

10. Documentation Corrections

When saving a binary configuration containing SNMP v3 parameters and then downloading it to another switch (same type and model), the SNMP v3 functionality will cause an error on the new switch. This behavior is normal and is a security feature of SNMPv3. After loading a binary configuration created on a different switch, the SNMPv3 users need to be re-created (**Q01930052).**

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 .

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel.

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