Ethernet Routing Switch 4500
Software Release 5.1.3

1. Release Summary

Release Date: 15-August-2008
Purpose: Software patch release to address customer found software issues.

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 4500 (all models).

4. Notes for Upgrade

Please see "Release Notes for the Ethernet Routing Switch 4500" (Part No. 322818-C, available at http://www.nortel.com/support, select Routers & Routing Switches, then select the appropriate Ethernet Routing Switch 4500 model) for details on how to upgrade your Switch

File Names For This Release

File Name	Module or File Type	File Size (bytes)
4500_5107_diag.bin	Diagnostic image	1,580,460
4500_513018.img	Agent code image	5,317,584
4500_513019s.img	Agent code image (SSH)	5,564,536

5. Version of Previous Release

Software Version 5.1.2.

6. Compatibility

This software release is managed with Java Device Manager (JDM) release 6.0.9.

7. Changes in This Release

New Features in This Release

RSTP Traps

RSTP Traps feature provide the ability to receive SNMP trap notifications and syslog log messages for a number of different RSTP events. RSTP Traps is configurable via CLI and ACG (no Web or JDM support is available). The following events are reported:

New Root Bridge

Port protocol migration

RSTP core memory allocation error

RSTP core buffer allocation error

The **CLI commands** are:

spanning-tree rstp traps
no spanning-tree rstp traps
default spanning-tree rstp traps

The default settings for RSTP traps are enabled.

ACG support will be represented by the presence of either of the following lines in the RSTP configuration section of the ASCII file:

spanning-tree rstp traps
or
no spanning-tree rstp traps

The events are notified as SNMP traps (see nnrst.mib) and also as system log messages.

The **SNMP traps definitions** are:

```
nnRstGeneralEvent NOTIFICATION-TYPE
  OBJECTS { dot1dBaseBridgeAddress, nnRstGenNotificationType }
  STATUS             current
  DESCRIPTION "Generated when any of the general events like protocol up or
               protocol down occurs"
  ::= { nnRstNotifications 1 }

nnRstErrorEvent NOTIFICATION-TYPE
  OBJECTS { dot1dBaseBridgeAddress, nnRstErrNotificationType }
  STATUS             current
  DESCRIPTION “Generated when any of the error events like memory failure or buffer
               failure or protocol migration or new root or topology change occurs"
  ::= { nnRstNotifications 2 }

nnRstNewRoot NOTIFICATION-TYPE
  OBJECTS { dot1dBaseBridgeAddress, nnRstDot1wOldDesignatedRoot,
            dot1dStpDesignatedRoot }
  STATUS             current
  DESCRIPTION "Generated whenever a new root bridge is selected in the topology"
  ::= { nnRstNotifications 3 }
```

```
nnRstTopologyChange NOTIFICATION-TYPE
  OBJECTS { dot1dBaseBridgeAddress }
  STATUS             current
  DESCRIPTION "Generated when topology change is detected "
  ::= { nnRstNotifications 4 }

nnRstProtocolMigration NOTIFICATION-TYPE
  OBJECTS { dot1dBaseBridgeAddress, nnRstDot1dStpVersion,
            nnRstPortNotificationMigrationType }
  STATUS             current
  DESCRIPTION "Generated when port protocol migration happens in the port"
  ::= { nnRstNotifications 5 }
```

The following messages will be logged into the system log for the above trap messages:
- Trap: RSTP General Event (Up/Down)
- Trap: RSTP Error Event (Mem Fail / Buff fail)
- Trap: RSTP New Root tt:tt:tt:tt:tt:tt:tt:tt
- Trap: RSTP Topology Change
- Trap: RSTP Protocol Migration Type: Send (RSTP/STP) for Port: t

The following OID has been implemented in order to provide SNMP control for RSTP traps notification:

```
nnRstSetNotifications OBJECT-TYPE
  SYNTAX   Integer32 (0..255)
  MAX-ACCESS   read-write
  STATUS   current
  DESCRIPTION "This object is used to enable and disable specific RSTP traps.
      Currently the following are defined
      0 - Notifications are not enabled.
      1 - General Notifications like protocol up or down
      2 - Exception Notifications like memory failure or buffer failure
          or port protocol migration or invalid packet rcvd in port
      3 - All the above Notifications "
  ::= { nnRstNotificationControlScalars 1 }
```

Radius Assigned VLAN Update for 802.1x - Use most recent Radius VLAN Enhancement

Existing Functionality

If use-radius-assigned-vlan option is enabled, the first valid radius-assigned-vlan (by EAP or Non-EAP authentication) on that port will be honored. Subsequent radius-vlan assignments will be ignored, for any user on that port. Note: If EAP VLAN is assigned after the Non-EAP VLAN, then the EAP VLAN takes precedence over the non-EAP with the port being moved from the Non-EAP VLAN to the EAP VLAN.

New Functionality (as implemented in 5.1.3 release)

The new functionality introduced with release 5.1.3 is to honor the last received radius-vlan assignments on a port. The last radius-assigned VLAN (either EAP or Non-EAP) will determine the VLAN membership and PVID replacing any previous radius-assigned VLAN values for that port.

Functional examples:
1. NEAP (Non-EAP) device authenticates on port X, the VLAN membership and PVID will be changed according to radius-vlan assignment if any. For example, let's say it will be added to VLAN 50.
2. Next. a PC authenticates on the same port X. That port will be removed from the VLAN 50 and moved into the new radius-vlan assigned with the new PVID, if a VLAN is assigned from the radius server.

The VLAN and the PVID will be changed every time a new valid radius-vlan assignment is processed on the port as a result of a new authentication.

Other functional example:
1. Multiple EAP and NEAP (non-EAP) clients authenticate on a port.
2. The EAP clients perform re-authentication; the non-EAP clients age out and are re-authenticated; the last VLAN assigned setting for either EAP or ENEAP clients will always be applied (meaning there is a potential for the VLAN to swap based on re-authentication).

CLI, SNMP and ACG interfaces are supported (no WebUI is available for this function)

CLI commands:

```
eap multihost use-most-recent-radius-vlan enable
no eap multihost use-most-recent-radius-vlan enable
```

ACG support will be represented by the presence of either of the following lines in the EAP configuration section of the ASCII

```
  eap multihost use-most-recent-radius-vlan enable
```

or

```
  no eap multihost use-most-recent-radius-vlan enable
```

SNMP Support

Global:

```
  bseeMultiHostUseMostRecentRadiusAssignedVlan OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "Controls whether to use most recent RADIUS-assigned VLAN."
    DEFVAL      { false }
    ::= { bseeObjects 21 }
```

Per Interface:

```
  bseePortConfigMultiHostUseMostRecentRadiusAssignedVlan OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "Controls whether to use most recent RADIUS-assigned VLAN."
    DEFVAL      { false }
    ::= { bseePortConfigEntry 18 }
```

Old Features Removed From This Release

None.

Problems Resolved in This Release

When the login timeout is set to a short time period, every time this timeout expired for the console port a message 'login timeout serial connection' was generated in the system log, which could fill up the log file with these messages (**Q01839829**)

For a MLT link, JDM incorrectly counted tagged packets that exceed 1518 byte as “FramesTooLong” (**Q01860630**)

When attempting to connect to a Nortel switch from a Cisco router using SSH an invalid protocol version exchange can cause the SSH session to not establish (**Q01837389-02**)

When telneting to another switch from the 4500 CLI and the remote switch IP address is changed, then all currently active telnet session from the switch CLI should be disconnected (**Q01812713-03**)

DHCP snooping incorrectly drops DHCP request packets which contain the padding option (0x00) in the vendor information field. Some Lexmark network printers use this padding option and consequently could not receive a DHCP reply when DHCP snooping was enabled. (**Q01895395**) (**Q01895523**)

If a telnet session to the switch has an active command running (for example tftp of a file) and that telnet session is terminated, a new telnet session will not be able to be established until the current command has completed (**Q01899506**)

8. Outstanding Issues

None.

9. Known Limitations

None.

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