NORTEL

Ethernet Routing Switch

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

Software Release 6.1.4

1. Release Summary

Release Date: 12-Aug-2010
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_614010.img	Agent code image	15,848,388
5xxx_614011s.img	Agent code image (SSH)	16,382,284

5. Version of Previous Release

Software Version 6.1.3.

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 Ability to set password, username and type of security for any switch in stack (Q02132910, Q02143365)

The 6.1.4 release includes the ability to set password, username and type of authentication for any switch in stack.

CLI Support

Configuring the type of authentication

The type of authentication can be set with the following commands:

cli password <serial| telnet> <local | none | radius | tacacs> - applies the setting to current running mode (standalone or stack);

*cli password **stack** <serial | telnet > <local | none | radius | tacacs>* - applies the settings to entire stack;

*cli password **switch** <serial | telnet > <local | none | radius | tacacs>* - applies the settings to the unit where the serial console run CLI commands or to base unit if command is run from telnet;

*cli password **switch <all | 1-8>** <serial | telnet> <local | none | radius | tacacs>* - applies the settings to all units if "ALL" parameter is used or to the unit specified by number from 1 to 8.

The type of authentication can be viewed with the following command:
show cli password type

Configuring the password
The password can be set with the following commands:

cli password <ro | rw> - applies the setting to current running mode (standalone or stack);

*cli password **stack** <ro | rw>* - applies the settings to entire stack;

*cli password **switch** <ro | rw>* - applies the settings to the unit where the serial console run CLI commands or to base unit if command is run from telnet;

*cli password **switch <all | 1-8>**<ro | rw>* - applies the settings to all units if "all" parameter is used or to the unit specified by number from 1 to 8.

If a unit will join an existing stack the stack passwords are propagated to the joined unit too, but the switch password of the joined unit remains what was set before join. The administrator of the units needs to be sure that the switch passwords are compliant with password security rules if the unit joins a stack where password security was enabled.

Configuring the username
The username can be set with the following commands:

username <word> <ro | *rw>* - applies the setting to current running mode (standalone or stack);

username <word> ***stack*** *<ro* | *rw>* - applies the settings to entire stack;

username <word> ***switch*** *<ro* | *rw>* - applies the settings to the unit where the serial console run CLI commands or to base unit if command is run from telnet;

username <word> ***switch <all | 1-8>*** *<ro* | *rw>* - applies the settings to all units if "all" parameter is used or to the unit specified by number from 1 to 8.

default username [switch [all | *<1-8>]* | *stack] [ro* | *rw]* – applies the default settings.

The username / password settings can be viewed with the following command:
show cli password [unit <1-8>]

The command *"username…"* can be used to update the default RO and RW usernames. It cannot be used to create additional usernames.

Configuring the password security

When enabling password security with the command "*password security enable",* if one of password does not comply with password security rules, the command fails and the user is asked to change it using "*cli password…*" command according with these rules.

"default username" command will set to default value both username and password, even if password security is enabled. It is the user responsibility to change the default values in order to have proper security in place.

SNMP
The SNMP interface was not modified, the functionality remains the same as in pre 6.1.4 releases.

Web
The WEB interface was not modified, the functionality remains the same as in pre 6.1.4 releases.

Console Menu Interface
The console menu interface was not modified, the functionality remains the same as in pre 6.1.4 releases.

ASCII Generator

In stack just stack settings of password security are saved. If we default the stack after saving ASCII configuration file and then try to bring back the setting from the ASCII file, the settings of switch password security are lost.

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

Base unit crashed with data exception in PP task (**Q02119687**)

Invalid binding entries via DHCP engineering menu caused fluctuations in the binding table within seconds. (**Q02143834**).

IGMP reports received from Client with TTL greater than 1 were forwarded and when an ERS 8600 connected to an ERS 5520 received the IGMP report with TTL set any value but 1, it dropped the packet (**Q02141971**)

Problems changing switch passwords (**Q02132910**).

Custom user password profiles were not consistently applied to all units in the stack (**Q02143365**)

TACACS authentication caused an exception (**Q02126732**)

In a Triangular IST/SMLT environment, with ERS 8300 as core and ERS 5520 as edge switches, with ARP Inspection enabled, the edge switches lost Arp entry for its default gateway and thus the gateway was no longer reachable. (**Q02153086**)

Under certain conditions, broadcast traffic looped into the stack could generate a broadcast storm (**Q02162104**).

8. Outstanding Issues

None.

9. Known Limitations

CLI password type for switch is changing from TACACS to Local when we change software image (**wi00557586**)
This issue happens only when the authentication type for switch is set to TACACS.
Workaround: Remove the switch settings for authentication type before downloading the new software.

Password security goes from enable to disable when upgrade/downgrade (**wi00557570**).
When upgrading from 6.1.4 to 6.2.0, if the password security is enabled, it will become disabled after upgrade. This issue will be fixed with 6.2.1 release.
When downgrading from 6.1.4 release to a 6.1.x release, if the password security is enabled, it will become disabled.
Workaround: Enable password security.

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 .

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