Ethernet Routing Switch 4500
Software Release 5.4.1

1. Release Summary

Release Date: 23-Sep-2010
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 "*Ethernet Routing Switch 4500 Series, Configuration — System*" for software release 5.4 (NN47205-500 v06.0x) available at http://www.avaya.com/support for details on how to upgrade your Switch.

File Names For This Release

File Name	Module or File Type	File Size (bytes)
4500_5303_diag.bin	Diagnostic image	1,589,514
4500_541012.img	Agent code image	7,347,344
4500_541013s.img	Agent code image (SSH)	7,610,624

5. Version of Previous Release

Software Version 5.4.0.

6. Compatibility

This software release is managed with Enterprise Device Manager (EDM) Revision number: 19932 which is integrated into the agent software.

7. Changes in This Release

New Features in This Release

Ability to set password, username and type of security for any switch in stack (wi00484374)

The 5.4.1 release includes the ability to set password, username and type of authentication for a specified unit in a stack. Previously the password settings were applied to all units in the stack or to a standalone switch,

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 base unit of stack or to the unit in the stack to where the console cable and session is currently being executed;

*cli password **switch <all | 1-8>** <serial | telnet> <local | none | radius | tacacs>* - applies the settings to specified units in the stack.

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

show cli password type [unit <1-8>]

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 base unit of stack or to the unit in the stack to where the console cable and session is currently being executed;

*cli password **switch <all | 1-8>**<ro | rw>* - applies the settings to the specified units in the stack.

If a new or replacement unit will join an existing stack the stack passwords will be propagated to the newly joined unit, but the switch password will not be changed. The administrator 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 base unit of stack or to the unit in the stack to where the console cable and session is currently being executed;

*username <word> **switch <all | 1-8>** <ro | rw>* - applies the settings to specified units in the stack.

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 / EDM

The SNMP / EDM interface was not modified, the functionality remains the same as in pre 5.4.1 releases.

ASCII Generator

The ASCII configuration file only stores the password settings for stack operations and not for each unit in the stack. If you default a stack and restore the ASCII configuration, if individual switch passwords were stored on each switch, these will not be restored, but will have to be created manually.

Old Features Removed From This Release

None.

Problems Resolved in This Release

The 'show interfaces gbic-info' command now correctly displays the status of the port after an SFP is removed (**wi00555071** / **Q02139059-02**)

In certain situations when an ARP entry was deleted from an internal list this would previously cause a task exception on the Base Unit or Temporary Base Unit (**wi00554897** / **Q02119687-01**)

DHCP Snooping: The "show ip dhcp-snooping binding" command now correctly displays all entries in the DHCP snooping binding table, which corresponds to those preset via SNMP or EDM (**wi00554888** / **Q02124324**)

802.1X: EAP authentication now succeeds on the first attempt when using default EAP default values as EAP now waits until the port is in a forwarding state before commencing authentication (**wi00554900** / **Q02154743**)

SNMP: When performing multiple SNMP get of the etherStatsStatus value, the switch no longer produced a task exception and stack instability (**wi00555060** / **Q02156778**)

LLDP: After rebooting a stack, all IP Phones will now correctly receive the correct VLAN-ID via LLDP (**wi00664788**)

DHCP Snooping: When a windows client using PXE environment is shutdown, the DHCP Snooping entry is now correctly cleared from the switch (**wi00691367**)

RIP: The switch now accepts RIP updates with a destination address of all ones (255.255.255.255) which is sometimes common in configurations with Cisco routers **(wi00703940)**

Static Routing: The situation in which a static route would sometimes become inactive and would not recover without a unit reboot has now been rectified (**wi00692260**)

Port Statistics: OutDiscards packets are no longer incorrectly counted as filtered packets (**wi00692576**)

ADAC, MLT: When MLT/DMLT is set as the ADAC uplink port(s) the ASCII configuration file now produces the correct output (Q02144052-02)

QoS: When performing repeated and multiple changes to QoS role combinations the switch no longer produces a task exception and stack instability (Q02160389)

ADAC: The ADAC Voice-VLAN ports are now correctly set after making a change to the uplink ports (wi00700962)

Security: Password security will not be enabled if passwords do not meet the minimum requirement and have at least 10 characters – this is the correct mode of operation (wi00729543)

8. Outstanding Issues

None.

9. Known Limitations

CLI password type for a switch is changing from TACACS to Local when a new software image is loaded (**wi00701033**) Workaround: This issue happens only when the authentication type for switch is set to TACACS, as a workaround, remove the switch settings for authentication type before downloading new switch software.

Password security goes from enable to disable when upgrade/downgrade (**wi00701016**).
When downgrading from 5.4.1 release to 5.4.0 release, if the password security is enabled, it will become disabled. Workaround: after the downgrade to 5.4.0, manually re-enable password security after the downgrade.

Password history is set to 0 after downgrade to 5.4.0. (wi00704283)
Workaround: after the downgrade to 5.4.0, manually reconfigure password-history value after the downgrade.

10. Documentation Corrections

For other known issues, please refer to the product release notes and technical documentation available from the Avaya Technical Support web site at: http://www.avaya.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 Avaya Technical Support on the web at: http://www.avaya.com/support or for legacy products at: http://www.nortel.com/support.