avaya.com

Ethernet Routing Switch 2500 Series
Software Release 4.3.1

1. Release Summary

Release Date: 20-December-2010
Purpose: Software patch release to address customer and internally found software issues.

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 2500 (all models).

4. Notes for Upgrade

Please see “Ethernet Routing Switch 2500 Series Overview — System Configuration” (NN47215-500, available at http://www.avaya.com/support - click Products, select Ethernet Routing Switch 2500 Series from the A-Z list, then select Documentation > View All Documents) for details on how to upgrade your Switch.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
2500_10015_diag.bin	Diagnostic image	1,265,238
2500_431024.img	Agent code image	6,237,340
2500_431025.img	Agent code image (SSH)	6,340,580

5. Version of Previous Release

Software Version 4.3.0

6. Compatibility

This software release is managed with Enterprise Device Manager (EDM) Revision number: 20564 which is integrated into the agent software.

7. Changes in This Release

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

The 4.3.1 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",* 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 interface was not modified, the functionality remains the same as in pre 4.3.1 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

When a GBIC was removed, it still showed up as inserted (***wi00555064***)

MAC Security writes to NVRAM with no configuration changes is no longer an issue (**wi00489666**)

Core stack failure logging a SW exception: "Task PP, Type Data Access, PC" is now fixed (***wi00555066***)

A base unit failure logging a SW exception in the SNMP task is now resolved (***wi00554865***)

After a switch reboot, 20% of the IP phones had the incorrect VLAN id (***wi00664793***)

Synchronization between DHCP binding table and IPSG table was some times lost in a PXE environment (***wi00691369***)

OutDiscards were wrongly counting filtered packets (***wi00692579***)

Static routes going inactive did not recover before a unit reset (***wi00692264***)

EAP authentication failure resulted on the first attempt with EAP default values (***wi00691678)***

Static ARP entries were removed after clearing ARP or power loss (***wi00733358***)

Setting the speed/duplex of a shared port to 100/Full resulted in an inactive link (***wi00554866***)

8. Outstanding Issues

A fiber connection on a shared port with speed set to 100 does not fully link up (**wi00482642**)

Username remains intact after defaulting usernames and passwords by using ASCII config (**wi00841068**)

9. Known Limitations

CLI password type for the switch changes from TACACS to local with a new SW image (**wi00701033**)
Workaround:
This issue happens only when the authentication type for the switch is set to TACACS
Remove the switch settings for authentication type before downloading a new image.

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 .