Ethernet Routing Switch 4500 Series
Software Release 5.5.1

1. Release Summary

Release Date: 15-March-2012
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 4500 (all models except 4500-PWR+ and 4800s).

4. Notes for Upgrade

Please see "Ethernet Routing Switch 4500 Series, Configuration – System, Software Release 5.5" (available at http://www.avaya.com/support . Click Products, select Ethernet Routing Switch 4000 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)
4500_5303_diag.bin	Diagnostic image	1,589,514
4500_551016.img	Agent code image	7,527,336
4500_551017s.img	Agent code image (SSH)	7,795,740

5. Version of Previous Release

Software Version 5.5.0.

6. Compatibility

This software release is managed with Enterprise Device Manager (EDM).

7. Changes in This Release

7.1. New Features in This Release

None.

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

802.1AB (LLDP), Avaya TLVs: Avaya dot1q-framing and poe-conservation-request-level information is now correctly displayed after a unit is rebooted within the stack. (**wi00881470**)

802.1AB (LLDP), Large Configuration, Memory Leak: In some situations where the ERS 4500 switch was connected to a large number of 802.1AB neighbors a memory leak no longer occurs. (**wi00975239**)

802.1AB (LLDP), MED: LLDP Med TX-TLV information is now correctly displayed after a unit is rebooted within the stack. (**wi00881822**)

802.1AB (LLDP), Temporary Base Unit: When the stack is operating using the Temporary Base Unit (TBU) setting LLDP TX TLVs for all ports now works correctly. (**wi00928236**)

802.1X, EAP, Port Disconnect: When a devices supporting EAP is disconnected from a port, all EAP entries are now properly aged and removed. (**wi00895689**)

802.1X, EAP, RADIUS: During periods of high 802.1X authentication, the switch is now able to manage the large number of pending RADIUS requests when response from the RADIUS server may be slow. This previously resulted in an error message that the “Radius Queue is Full”. (**wi00895213**)

802.1X, EAP, STP: Avaya IP Phone 9608 now works correctly if the link is transitioned and 802.1X Multihost Multicast mode as well as Spanning Tree (STP) is enabled on the port. (**wi00898601**)

ADAC, Memory Leak: The memory leak which occurred in some situations where the ERS 4500 switch experiences significant number of link transitions with IP Phones connected is now addressed. (**wi00882779**).

Configuration, 256 Concurrent VLANs: An issue in which the configuration containing 256 VLANs for a stack of 8 switches was not correctly saved to the binary configuration and subsequently not able to be restored after stack reboot is now rectified. (**wi00952270**)

Configuration, 802.1AB (LLDP) dot1 TLVs: An issue in which the configuration containing lldp tx-tlv dot1 protocol-identity STP and EAP was not correctly saved to the binary configuration and subsequently not able to be restored after stack reboot is now rectified. (**wi00952270**)

Configuration, Large Size: A situation where a large configuration existed on a stack, now the upgrading and then subsequent downgrading of a stack will no longer result in the stack being incorrectly set to default configuration. (**wi00975223**)

Configuration, Patch Load Upgrade: In some instances where a customer has been running a special patch load, the upgrade to a standard maintenance release will no longer cause the loss of configuration. (**wi00975261**)

Configuration, Port VLANs, Secure Image: In some situations an issue where the port VLAN configuration was not correctly saved to the binary configuration and subsequently not able to be restored after stack reboot is now rectified. . (**wi00944336**)

Configuration, Unit Restore: A binary configuration file from a stack can now be correctly extracted to a unit when operating in standalone mode. (**wi00889880**)

Dynamic ARP Inspection (DAI), Unit Replacement: The Dynamic ARP Inspection trusted/untrusted state for each port is now correctly restored if a unit is replaced in an operational stack. (**wi00954473**)
EDM, ASCII Config: EDM now will correctly load an ASCII configuration file from the File System tab. (**wi00978114**)

IP Address, Downgrade: When downgrading from 5.5.1 to 5.4.x software the switch/stack IP Management address will now be correctly retained. (**wi00952333**)

IP Routing, Static: In some situations where the attempt to add an IP Static Route resulted in an incorrect warning message, this Static Route can now be correctly added to the switch without needing to perform a reboot. (**wi00973915**)

IPFix, Templates: IPFix Templates are now correctly sent to the collector, for example Scrutinizer 8.6.1. (**wi00931371**)

MAC Security, SNMP Trap: The SNMP Trap generated by MAC security now correctly shows the proper BoardIndex (Slot). (**wi00958930**)

MAC Security: Addresses are now correctly deleted from the MAC Security table when the "no mac-sec mac-address" command is issued. (**wi00869476**)

Management VLAN, MIB state: The following MIB instances ifOperStatus for ipAdEntIfIndex now correctly responds with an UP state as soon as a port is up in the Management VLAN. (**wi00975247**)

Passwords, Upgrade: When upgrading to 5.5.x software in some cases console or telnet passwords may no longer work. Please ensure that you refer to the section on Unified Authentication (see section 10). (**wi00937726**)

PoE: If the PoE module performs a power reset, then PoE will now be correctly restored to designated ports following the reset. (**wi00975232**)

QoS: The Ethertype field of ingress packets is now correctly processed by a QoS Layer 3 filter. (**wi00883329**)

Temperature Display: The correct switch temperature is now correctly displayed in MIB, EDM and CLI, in some cases the temperature previously displayed was double the actual temperature. (**wi00893478**)

TFTP, Memory Leak: The memory leak which occurred in some situations where the ERS 4500 switch when copying the running config to a TFTP server is now addressed. (**wi00961380**)

USB, larger than 8GB: The switch will now correctly recognize, display and access files on a USB device when the device is larger than 8GB in size. (**wi00926171**)

8. Outstanding Issues

None.

9. Known Limitations

None.

10. Documentation Corrections

wi00925480 - Telnet user credentials were lost (defaulted) after upgrading from 5.4 to 5.5

With the introduction of Release 5.5 and later Unified Authentication is supported on all ERS 4000 products. With Unified Authentication you can now manage only one set of local usernames and passwords for switches, whether the units are operating in stacked or standalone mode.

The unified authentication mechanism approach simplifies the design: using the current ‘cli password’ and ‘username’ commands the same set of read-write/read-only user name and passwords and authentication type is applied to stack as well as each standalone switch. The switch obsoletes and clear the switch passwords and username; so that when the unit is operating in either standalone or stacked mode we always use what was previously designated as the stack password and username.

When downgrading the software image from unified password to an older software image with separate switch and stack passwords all the switch setting (except IP address) will be defaulted, including authentication methods.

Special consideration needs to be given to the upgrade from an older software image with separate switch and stack passwords (any software image previous to 5.5 software image) to a 5.5 or 5.6 software image with unified password. When upgrading from a pre-5.5 software image with separate switch and stack set of credentials (password, username and authentication type) to 5.5, 5.6 or later software image, only the stack set of credentials will be preserved and used; the individual switch set of credentials will be lost and will be overwritten by the new unified / stack set of credentials.

The following message appears in system log :
“CLI pswd: A unified authentication method is now used. The local switch credentials are no longer supported”

For example, when a standalone unit had previously just switch set of credentials set (and no stack credentials), after upgrading to 5.5 or later software the previous stack set of credentials will overwrite the switch set of credentials and as a result the standalone switch will have default settings for the set of credentials.

Setting RADIUS or TACACS authentication requires that the switch or stack has a management IP address properly configured. Otherwise the user will be locked out of the system because the server providing authentication can never be reached.

Neither RADIUS nor TACACS+ servers can be configured without first having a management IP address. When the user tries to set RADIUS or TACACS authentication without having a RADIUS/TACACS server configured an error message appears in the console:
% You must configure Primary RADIUS Server and shared secret first
% You must configure Primary TACACS+ Server and shared secret first

With the unified authentication approach, when configuring RADIUS or TACACS+ on a Stack, the authentication type is also applied to each switch within the stack. Consideration need to be given for removal of a switch from the stack if a standalone switch IP address is not configured. If a switch within a stack does not have a standalone Switch IP address configured, then when either RADIUS or TACACS+ authentication is configured for the stack, this authentication method will not be applied to the respective standalone switch authentication and will only be applied to the stack and any switches with standalone IP addresses. The following log message appears in System log when such a configuration is made in stack:
“CLI pswd: Stack auth. type RADIUS/TACACS+ won't apply on switch (switch IP address not set). Local user/password used“

Known limitation:
For a standalone unit with an switch IP address set but no stack IP address set, if RADIUS or TACACS authentication is desired, the command “cli password serial/telnet radius/tacacs” will only set this for the standalone operation (and the stack mode will be left at type local).
After a reboot the stack credentials will overwrite switch credentials.

Workaround: To avoid this case, we recommend setting a stack IP address (even on standalone operating mode) before setting authentication type.

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 .