Ethernet Routing Switch 4000 Series
Software Release 5.6.2

1. Release Summary

Release Date: 22-November-2012
Purpose: Software feature pack to address customer and internally found software issues.

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 4000 (all models).

4. Notes for Upgrade

Please see "Ethernet Routing Switch 4000 Series, Configuration – System, Software Release 5.6" (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)
4000_56108_boot.bin	Bootloader image for 4500-PWR+ & 4800 models.	322,522
4500_5303_diag.bin	Diagnostic image for ERS 4500 models (except 4500-PWR+).	1,589,514
4000_56201_diag.bin	Diagnostic image for ERS 4500-PWR+ & ERS 4800 models.	1,934,093
4000_56201_combodiag.bin	Combination diagnostics suitable for all ERS 4000 models.	3,523,607
4000_562026.img	Agent code image	8,702,404
4000_562027s.img	Agent code image (Secure / SSH)	9,098,848
4500_PoE_400.img	PoE Firmware for ERS 4500 (up to hardware revision 11: 4526T-PWR HW:11, 4550T-PWR HW:11, 4524GT-PWR HW:11, 4526GTX-PWR HW:11, 4548GT-PWR HW:11)	77,824
4500_PoE_400b15.img	PoE Firmware for ERS 4500-PWR (hardware revision 12 or later: 4526T-PWR HW:12, 4550T-PWR HW:12, 4524GT-PWR HW:12, 4526GTX-PWR HW:12, 4548GT-PWR HW:12)	77,923
4000_PoEplus_410B4.bin	PoE+ Firmware for 4526T-PWR+, 4550T-PWR+, 4826GTS-PWR+, 4850GTS-PWR+,	16,384
Ethernet_Routing_Switch_4000_MIBs_5.6.2.zip	Software Release 5.6.2 Management Information Base (MIB) Definition Files	2,047,880

Notes:

- The bootloader software is listed for completeness and is factory installed on new revision 10 hardware, there is no requirement for customer to update the bootloader.
- PoE firmware is listed for completeness, unless instructed by Avaya services; there is no requirement to load/update the PoE firmware.

The maximum filename length supported by the ERS 4000 product ranges from 30 to 255 characters:

Application	TFTP Filename Length	SFTP Filename Length	USB Filename Length
Agent Image	30	30	30
Diag Image	30	30	30
Binary Config	255	255	30
ACG Running-Config	255	255	30
ACG Script	254	254	30
SSH key	30	-	30
DHCP-snooping autosave	255	-	30

5. Version of Previous Release

Software Version 5.6.0 & 5.6.1

6. Compatibility

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

7. Changes in This Release

7.1. New Features in This Release

802.1X Fail_Open Continuity Mode.

Avaya ERS Stackable switches now provide three modes of operation for EAP/NEAP clients when the RADIUS Server(s) become unreachable.

1. Standard mode, in which clients will be moved back to the default port VLAN and policies if RADIUS re-authentication fails or the RADIUS servers become unreachable.
2. Fail_Open mode in which clients will be moved to a specified Fail_Open VLAN if defined, when the RADIUS servers become unreachable.
3. A new mode, Fail_Open Continuity Mode.

With Fail_Open Continuity Mode when an EAP or NEAP client is re-authenticated and the RADIUS server(s) are not reachable, the switch will maintain the client in the currently RADIUS assigned VLAN and any applicable policies. Similarly if the RADIUS servers become unreachable, the switch will maintain the client in the currently RADIUS assigned VLAN and any applicable policies.

When Fail_Open Continuity Mode is enabled, if the Fail_Open VLAN is defined, then if a new EAP or NEAP client cannot be authenticated due to RADIUS server reach ability issues, then the client will be placed into the designated Fail_Open VLAN. If no Fail_Open VLAN is defined, than the client will remain in the default VLAN on authentication failure.

CLI Command Syntax:
[no | default] eapol multihost fail-open-vlan { [continuity | enable] [vid <1-4094>] }
show eapol multihost fail-open-vlan

CLI Example:

```
ERS4000> ena
ERS4000# config t
Enter configuration commands, one per line.  End with CNTL/Z.
ERS4000# eapol multihost fail-open-vlan continuity
ERS4000# show eapol multihost fail-open-vlan
Fail Open VLAN Enabled: Continuity
Fail Open VLAN ID     : Null
```

802.1X User Based Policies

The goal of User Based Policies (UBP) is to allow user-specific QoS policy information to be applied to a port based upon user or device authentication. User information is retrieved from the RADIUS Server during EAP or NEAP Authentication and passed to the QoS Agent. The QoS Agent, in turn, looks up locally-defined policy criteria and applies that per port.

User Based Policies revolves around the new User Policy Table. User data, provided through interactions with EAP, is maintained in the User Policy Table. A user is associated with a specific interface, a user role combination, a user name string and, optionally, a user group string. Each user is also associated with session information. Session data is used to maintain state information for each user and users are also associated with a session group identifier. The group identifier is shared by users with the same role combination used to identify the policy criteria to be applied.

User roles are associated with a specific interface and user through the User Policy Table, these role combinations are independent of their Interface Role counterparts. They are not associated with an interface class and the default QoS processing associated with the interface through its association with an Interface Role. An interface cannot be assigned a user role unless it is “QoS enabled”. User roles are used to indicate user characteristics and may not be used to associate a policy with an interface.

If the user policy control attribute indicates that local control over user policy data is enabled the user role will be used to perform a local database lookup for a corresponding UBP filter set. If a matching filter set is found, it will be applied to the interface associated with the user, taking into account the current level of resources available on the interface. If resources are not available to install the specified filter set and the UBP support level is set to high security, the User Policy Table will not be updated and a failure indication will be returned to EAP amd an SNMP trap generated. If the support level is set to low, then the filter will not be applied.

UBP enhancements have been added to automatically include a user’s MAC address data in pre-defined UBP filter sets in certain scenarios. User role data is used to identify a filter set when local UBP support is enabled, if the filter set does not include data specifically identifying the user, support for multiple users with different filter set associations becomes an issue since all of the filter sets installed on an interface will then be applied to all users on that interface. When MAC address data is provided, the identified user role filter set data is cloned and filters intended to match the source MAC address of the user are added.

The operation of UBP feature will follow these basic steps:

- An NEAP device or EAP Client User logs in on a port with RADIUS Authentication.
- The switch sends the information to RADIUS for Authentication.
- The RADIUS server sends the Auth-Result and optionally UBP information for that device/user.
- EAP processes the UBP data and sends it to the QoS Agent, on Success.
- EAP also sends the Auth-Result to the EAP Client.
- QoS Agent processes the UBP data, the local policy database is consulted for applicable UBP filters.
- The QoS Agent validates and installs the policy components.
- From here on, this policy data will be applied on that user’s traffic.

RADIUS Vendor Attributes
Vendor Specific Attributes (VSAs) are used to provide UBP information from RADIUS. The following definitions are used:
Standard RADIUS Attribute = 26 (for VSA)
Vendor Id: 562 for Avaya.
Vendor Attribute Id: 110
Vendor Attribute Type: String
Allowed Values: UROLstring or UGRPstring
Max StringLength: 32.

CLI Syntax:
[no | default] eapol user-based-policies { [enable] [filter-on-mac enable] }
[no | default] eapol multihost non-eap-user-based-policies { [enable] [filter-on-mac enable] }
show qos user-policy
show qos ubp [name <name>]
qos ubp classifier name <name> [addr-type <addrtype>] [src-ip <src-ip-info>] [dst-ip <dst-ip-info>] [ds-field <dscp>] [protocol <protocoltype> | next_header <header>] [src-port-min <port> src-port-max <port>] [dst-port-min <port> dst-port-max <port>] [flow-id <flowid>] [src-mac <src-mac>] [src-mac-mask <src-mac-mask>] [dst-mac <dst-mac>] [dst-mac-mask <dst-mac-mask>] [vlan-min <vid-min> vlan-max <vid-max>] [vlan-tag <vtag>] [ethertype <etype>] [priority <ieee1p-seq>] [drop-action <drop | pass>] [update-dscp <0-63>] [update-1p <0-7>] [set-drop-prec <high-drop | low-drop>] [block <block-name>] [eval-order <1-65535>]
qos ubp set name <name> [committed-rate <64-10230000> Kbits/sec] [max-burst-rate <64-4294967295> Kbits/sec] [max-burst-duration <1-4294967295> Milliseconds] [drop-out-action <drop | pass>] [drop-nm-action <drop | pass>]
no qos ubp name <name> [eval-order <1-65535>]

CLI Example:
```
ERS4000> ena
ERS4000# config t
Enter configuration commands, one per line.  End with CNTL/Z.
ERS4000(config)# radius-server host 172.16.1.1
ERS4000(config)# radius-server key avayaPLM
ERS4000(config)# eapol multihost eap-protocol-enable
ERS4000(config)# eapol multihost allow-non-eap-enable
ERS4000(config)# eapol multihost radius-non-eap-enable
ERS4000(config)# eapol multihost non-eap-phone-enable
ERS4000(config)# eapol multihost use-radius-assigned-vlan
ERS4000(config)# eapol multihost non-eap-reauthentication-enable
ERS4000(config)# eapol multihost multivlan enable
ERS4000(config)# vlan create 100 name GVLAN type port
ERS4000(config)# eapol guest-vlan vid 100
ERS4000(config)# eapol guest-vlan enable
ERS4000(config)# eapol user-based-policies enable
ERS4000(config)# eapol user-based-policies filter-on-mac enable
ERS4000(config)# eapol multihost non-eap-user-based-policies enable
ERS4000(config)# eapol multihost non-eap-user-based-policies filter-on-mac enable
ERS4000(config)# qos ubp classifier name one dst-ip 10.1.1.1/32 ethertype 0x0800
drop-action enable eval-order 10
ERS4000(config)# qos ubp set name one track-statistics individual
ERS4000(config)# qos agent ubp high-security-local
ERS4000(config)# eapol enable
```

SLAMon Agent

Identifying occurrences of and isolating performance issues in a network has always been a difficult task. Embedding monitoring devices in the network infrastructure is one way to tackle this problem and this is the focus for SLA Monitor (SLAMon).

Through the use of coordinated network performance tests and efficiently distributed monitoring devices, an accurate picture of overall network health can quickly be developed. Areas in which performance is not up to expectations can then be specifically targeted for deeper analysis or troubleshooting, if necessary.

To support efficient configuration, issue detection and isolation, a centralized monitoring service is ideally suitable to coordinate monitoring agent actions and analyze tests results. The ability to easily and rapidly perform end-to-end network QoS tests and isolate issues requires distributed monitoring agents that are pervasive yet introduce minimal impact to the device's themselves. This divides the responsibilities of SLAMon into two main components of the SLAMon Server and SLAMon Agent.

The SLAMon agent support is available in the ERS 4000 switches with release 5.6.2. The agent operation will be largely transparent to the customer. The agent will be disabled by default (due to security considerations) and will require a single command to achieve minimum configuration on the switch.

The SLAMon agent also supports some local configuration capabilities as well as the ability to query the status of the SLAMon agent and server connection.

CLI Syntax:
PrivExec or global configuration Mode Commands:
show application slamon agent

Application Mode Commands:
[default] slamon agent-comm-port <0-65535>
[default] slamon agent ip address <IP address> [VRF name]
[default] slamon agent port <0-65535>
[no | default] slamon cli [enable]
[default] slamon cli-timeout <60-600>
[no | default] slamon cli-timeout-mode [enable]
[no | default] slamon oper-mode [enable]
[default] slamon server ip address <IP address> <secondary IP address>
[default] slamon server port <0-65535>

CLI Example:

```
ERS4000> ena
ERS4000# show application slamon agent
SLAMon Operational Mode: Enabled
SLAMon Agent Encryption: Not supported.
SLAMon Agent Address: 47.80.225.190
SLAMon Agent Port: 50011
SLAMon Agent Registration Status: Not Registered
SLAMon Registered Server Address: 0.0.0.0
SLAMon Registered Server Port: 0
SLAMon Server Registration Time: 0
SLAMon CLI Mode: Enabled
SLAMon CLI Timeout Mode: Disabled
SLAMon CLI Timeout: 60 seconds
SLAMon Configured Server Address: 0.0.0.0
SLAMon Configured Server Port: 0
```

```
SLAMon Configured Agent Address: 0.0.0.0
SLAMon Configured Agent Port: 0
SLAMon Agent-To-Agent Communication Port: 50012
SLAMon Configured Agent-To-Agent Communication Port: 0
ERS4000# config t
ERS4000 (config)# application
ERS4000 (config-app)# slamon agent ip address 10.30.56.100
ERS4000 (config-app)# slamon agent port 50056
ERS4000 (config-app)# slamon server ip address 135.10.100.1
ERS4000 (config-app)# slamon server port 50156
ERS4000 (config-app)# slamon agent-comm-port 50256
ERS4000 (config-app)# slamon oper-mode enable
ERS4000 (config-app)# exit
```

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

Reference Number	Description
Issues Resolved in 5.6.2	
wi01026335	**100FX SFP, Display:** The Avaya 100FX SFP (AA1419074-E6) is now correctly displayed as a supported SFP in variations of the switch which can support slow speed SFPs.
wi01054301	**801.2X, RADIUS Health Check:** The RADIUS health check password is now correctly encrypted with the server key when sending a reachability packet to the RADIUS server.
wi01047335	**802.1X, Clear MAC Address:** When issuing the clear mac-address-table address <x> command against an EAP/NEAP MAC address it is now correctly removed from the Layer2 MAC Address table.
wi01049393	**802.1X, RADIUS Reachability, ASCII Config:** RADIUS Reachability username is now correctly output when generating an ASCII configuration file.
wi01046960	**802.1X, RADIUS Reachability, IPv6, Log Messages:** Log messages related to RADIUS Server reachability are now correctly displayed when RADIUS servers are configured for IPv6.
wi01032441, wi01032439	**802.1X, RADIUS VLANs (RAV), DHCP Requests, Wrong VLAN:** When the switch boots, DHCP traffic is now correctly blocked until EAP/NEAP authentication starts. Previously DHCP request would be forwarded by the switch before EAP authentication, which could result in the end device obtained an IP Address which may be in the wrong VLAN is RADIUS Assigned VLANs (RAVs) are used.
wi01055405	**Diags, New Agent Software:** The diagnostics software has been updated to correctly recognise 5.7.0 and later agent code releases.
wi01053526	**Diags, PoE+, 4850GTS, Shared Ports:** An diagnostics internal loopback error which occurred when some devices were connected to the shared ports (47 or 48) on the 4850GTS or 4850GTS-PWR+ has now been addressed.
wi01055434	**Diags, PoE+, Warm Boot:** The diagnostics now correctly keeps PoE+ disabled during a warm boot process until control is passed to the agent software.
wi01034775	**EDM, ECMP:** The Maximum Path value in the ECMP configuration tab for EDM can now be changed from the default value of 1 and successfully applied to the switch.
wi01029886	**EDM, Help File, ASCII Config:** EDM Help file path is now correctly output when generating an ASCII configuration file.
wi01042035	**EDM, Password Display:** EDM now correctly shows console/web/telnet passwords when operating as a single unit or a stack.
wi01042931	**EDM, PoE Port status:** EDM now correctly displays PoE status when requesting output for a large number of PoE ports, rather than displaying “Request timed out” error.
wi01006349	**EDM, Username, Software Exception:** An issue which existed when a username longer than 2 characters was entered into EDM has now been addressed. The switch will no longer product a software exception.
wi01034869	**ERS 4500, PoE, Power failover:** ERS 4500-PWR models (4526T-PWR, 4550T-PWR, 4524GT-PWR, 4526GTX-PWR, 4548GT-PWR) with Hardware revision 12 or later will now correctly maintain PoE when switching to redundant power when the PoE firmware 4500_PoE_400b15.img is loaded on the units. Note: this firmware should not be loaded on to ERS 4500-PWR+, ERS 4800-PWR+ or ERS 4500-PWR with Hardware revision lower than HW revision 12.
wi01042478	**ERS 4500, Shard Ports, Duplex Settings:** User configured duplex settings are now correctly retained for the shared ports on ERS 4500 Gigabit models.
wi01043265	**ERS 4800, Port Mirroring:** Traffic is now correctly not mirrored on the switch then Port Mirroring Allow Traffic is Disabled

Reference Number	Description
wi01010344 wi01006771	**Memory Leak, IPFix:** A memory leak which could cause a switch to reset between 22-28 days when IPFiX is enabled has been rectified. The switch will no longer reset with a task exception after this period of time when IPFix is enabled.
wi01039472	**QoS:** The "show qos agent" output has been enhanced to provide information on the queue-set and buffer usage.
wi01034053	**SNMP Trap, IP Source Guard:** SNMP Traps for IP Source Guard for the last unit in a stack are now correctly enabled by default.
wi01042163	**Static MAC Address, MLT:** The switch will now correctly produce an error message if you try to enable an MLT which has a port with static MAC addresses configured.
wi01028451, wi01049826	**VLACP not working with Ethertype 8102:** Interoperability issues with VLACP using Ethertype 8102 (default Ethertype for SLPP-guard) have now been addressed.
Issues Resolved in 5.6.1	
wi00998403	**802.1AB (LLDP), Network Policy TLV:** The LLDP Network Policy TLVs are now correctly advertised if voice or voice-signalling parameters are configured on the switch.
wi00898601	**802.1X, EAP, STP, Avaya 9600:** Avaya IP Phone 9608 now works correctly if the link is transitioned and 802.1X Multi-host Multicast mode as well as Spanning Tree (STP) is enabled on the port.
wi00997610	**802.1X/NEAP, Wake-on-LAN (WOL):**The switch will now correctly forward a Wake-on-LAN packet for a device which has been authenticated as a Non-EAP (NEAP) device and which has gone to sleep.
wi01050193, wi01047238, wi01047286, wi01047012	**ADAC, MLT:** Issues related to incorrect operation of MLT ports in combination with ADAC when ADAC configurations are modified, disabled or the switch/stack transitions to standalone have now been addressed.
wi00938450	**ADAC, Unit Renumbering:** ADAC uplink settings are now correctly retained after renumbering of units in a stack.
wi00959485	**Autotopology, SONMP:** If the Ethernet Routing Switch 4000 is connected to a Virtual Service Platform 7000 (VSP 7000), the ERS 4000 now correctly display the VSP 7000 in the autotopology table.
wi00952270, wi00956069	**Configuration, 802.1AB (LLDP) dot1 TLVs:** LLDP tx-tlv dot1 protocol-identity STP and EAP TLVs are now correctly saved to the binary configuration and subsequently able to be restored after stack reboot.
wi00944336	**Configuration, Port VLANs, Secure Image:** Port VLAN configurations are now correctly saved to the binary configuration and subsequently able to be restored after stack reboot.
wi00888281	**Configuration, SNMP Trap Objects:** SNMP Trap Objects are now correctly saved to the binary configuration and subsequently able to be restored after stack reboot.
wi00889880	**Configuration, Unit Restore:** A binary configuration file from a stack can now be correctly extracted to a unit when operating in standalone mode.
wi00992892	**DHCP Relay Option 82:** An intermittently generated error message is no longer displayed when enabling or disabling dhcp-relay option82 on Layer3 VLAN interface.
wi00891087, wi00965814	**DHCP Snooping External Save, Filename:** The filename used for DHCP Snooping external save is now correctly retained if a stack transitions from stack to standalone with stack force mode enabled or if the Base Unit is changed within a stack.
wi00959866	**DHCP Snooping External Save, SNTP:** A guardrail is now implemented to prevent SNTP from being disabled if IP DHCP Snooping External Save is enabled on the switch.
wi00966939	**DHCP Snooping, Apple MAC Netboot:** When DHCP Snooping is enabled, the TFTP transfer for Apple MACs performing a netboot are now correctly forwarded by the switch and not truncated.
wi00965075	**EAP, MHMA, Fail_Open VLAN:** EAP Multi-Host mode can now be correctly enabled or disabled when Fail_Open VLAN is configured.

Reference Number	Description
wi00973504	**EAP, Port Mirroring:** An error is now correctly displayed if you attempt to enabling EAP on a mirrored port.
wi00949406	**ECMP, Route Display:** When ECMP is configured, the “show ip route” and the “show ip num-routes” commands now both display the correct number of routes.
wi00958809	**EDM plug-in, MAC Address Table:** After adding 1024 static MAC addressed, the number of MAC address entries is now correctly displayed when using EDM offbox plug-in.
wi00978114	**EDM, ASCII Config:** EDM now will correctly load an ASCII configuration file from the File System tab.
wi00958289	**EDM, ERS 4800, SFP:** In the switch physical view for Enterprise Device Manager (EDM), the link LEDs for the Fibre Optic ports on an ERS 4800 are now displayed correctly.
wi00958436	**EDM, MAC Address Table:** When you view the MAC address table from EDM, pressing the refresh button will no longer cause the output to scroll continuously.
wi00949529	**EDM, SFP:** When a device has been installed in the SFP port of a base unit in a stack it will now be correctly displayed as being present in EDM.
wi00994369	**ERS 4500, PoE:** The “show poe-main-status” command now correctly displays the available DTE power on newer hardware revisions of the ERS 4500-PWR models.
wi00952044	**ERS 4800, DMLT, Booting:** During power cycle or boot-up of an ERS 4800,the DMLT link will now function correctly. Traffic will not be forwarded on DMLT links until the unit is operational within the stack.
wi00947822	**ERS 4800, Port Mirroring:** When operating in xrxytx mode on an ERS 4800, traffic is now correctly forwarded and not flooded to the mirror to port when one of the mirror ports in disconnected.
wi00897184	**ERS 4800, Port Statistics:** The port statistics for ifOutDiscards are now correctly displayed on ERS 4800 switches.
wi00996178	**FAN MIB:** The reporting of intermittent FAN Failures by querying the switch MIB has now been rectified, so that the MIB status correctly reflects the FAN operational mode.
wi00889339	**IP Phone Automatic PoE Changes:** CLI help is now correctly displayed for the „no poe-ip-phone poe-limit’ command.
wi00934177	**IP Phone Automatic PoE Changes:** If a automatic power limit is configured lower than the static power port limit and is lower than the IP phone power consumption, then the port will no longer cycle through detecting, delivering and overload power states.
wi00993354	**IPFiX, IP Source Guard (IPSG**): If DHCP Snooping, Dynamic ARP Inspection and IP Source Guard (IPSG) are enabled on a port the switch will now return a timely error if IPFiX is attempted to be configured on the ports.
wi00931371	**IPFiX, Templates:** IPFiX Templates are now correctly sent to the collector, for example Scrutinizer 8.6.1.
wi00993842	**Jumbo Packets, UDP Forwarding:** Jumbo frames are now correctly forwarded when UDP forwarding is enabled on the switch.
wi00961451, wi00964606, wi00998809, wi00958930	**MAC Security, Access Violation Trap:** When MAC Security Access Violation traps are enabled on the port, the trap is now correctly generated as a result of a MAC security violation and it now displays the correct port index (s5SbsViolationPortIndx) is contained in the message.
wi00984489, wi00998420	**MAC Security, MAC Removed Trap:** When MAC Security MAC Remove traps are enabled, the trap message is now generated and it now displays the correct port index (s5EtrSbsMacRemoved) is contained in the message.
wi00928619	**MAC Security:** MAC addresses are now correctly deleted when the "no mac-sec mac-address" command is issued.
wi00950703	**Management IP Address, Bootp-when-needed, DHCP-when-needed:** If the switch is configured to use bootp-when-needed or dhcp-when-needed for the management IP address, you can now change the IP address after the agent code becomes operational.

Reference Number	Description
wi00961380	**Memory Leak, TFTP:** A memory leak which occurred in some situations on an ERS 4000 switch when copying the running config to a TFTP server is now addressed.
wi00939382	**MLT, Default Configuration:** When the switch configuration is factory defaulted, all MLT settings are correctly cleared.
wi01002256	**MSTP Mode, High CPU Load:** When MSTP is configured on a stack, a higher than expected CPU load is no longer observed.
wi00961473	**Multicast, Base Unit:** Multicast traffic is no longer incorrectly duplicated on the Base Unit in a stack when traffic matches igmp unknown-mcast-allow-flood criteria.
wi00933709	**NLSR, Show ip route:** The non local static routes (LCLNHOP) field in "show ip route static" output is now correctly displayed when the route is non-local.
wi00906995	**NTP:** The output for the “show clock” and “show ntp” commands have been improved to increase readability.
wi01049818	**OSPF, Missing Hellos:** The switch will now correctly send OSPF Hello Packets on reception of requests from an OSPF peer. Previously in some situations the switch would send out requests only every 10 seconds or longer which could result in loss of OSPF adjacency.
wi00941398	**PoE Traps, Base Unit:** The SNMP trap „bspeIpPhonePower’ is now correctly set if the Base Unit of a stack in a non-PWR or non-PWR+ unit.
wi00975621	**PoE+, Display:** When a port delivering PoE+ is disconnected by unplugging the device, the “show poe-port-status” command now correctly displays the PoE port status as ’Disabled’.
wi01008239	**PoE+, Display:** When removing the primary power supply from an ERS 4800-PWR+ or 4500-PWR+ unit which has a redundant power supply operational, the Available DTE power is now correctly displayed when issuing the “show poe-main-status” command.
wi00895972	**PoE+, SNMP Trap:** An SNMP trap is now generated when removing the power cord from the secondary (or redundant) power supply.
wi00883329	**QoS, Layer3 Filter:** The Ethertype field of ingress packets is now correctly processed by a QoS Layer 3 filter.
wi01004744	**QoS, Traffic Profile:** You can now modify a QoS action when a Traffic Profile is configured.
wi00991921	**RSTP, Port Priority:** Port priority values are now correctly applied when issuing the “spanning-tree rstp port x/y priority” command.
wi00941657	**Running Configuration, ADAC:** The “show running-config” command now produces the correct output for ADAC when the call-server port is set to tagall mode.
wi00995944	**Running Configuration, IPv6:** The “show running-config” command now produces the correct output for IPv6 Management addresses when no IPv6 addresses have been configured for individual units within the stack.
wi01000101	**Running Configuration, MAC Security:** The “show running-config” command now produces the correct output for the MAC Security intrusion timer.
wi01000147	**Running Configuration, PoE:** The “show running-config” command now produces the correct output for PoE when issued against non PoE units.
wi00952001	**Running Configuration, QoS:** The “show running-config” command now produces the correct output for QoS when specifying verbose mode.
wi00973089	**Running Configuration, SNMP Notification Control:** The “show running-config” command now produces the correct output for PoE SNMP Notification Control (pethPsePortOnOffNotification).
wi00941408	**Running Configuration, SNMP Notification:** The “show running-config” command now produces the correct output for SNMP notification section.
wi00986004	**Serial Security:** When enabling serial security is enabled on a switch, an intermittent error message is no longer displayed.
wi00976758	**SLPP Guard:** SLPP Guard now correctly functions in a stacked configuration to appropriately disable a port if a network loop is detected.

Reference Number	Description
wi00984718	**SNMP Notification Control, MAC Violation:** If SNMP notification control is set for „s5EtrNewSbsMacAccessViolation', the switch now correctly generated system log messages for MAC access violations.
wi00952333	**Software Downgrade, IP Address:** When downgrading to 5.4.x software the switch/stack IP Management address will now be correctly retained.
wi00992031	**Software Exception, 802.1X/EAP Scaling:** When the number of EAP/NEAP clients exceeds the recommended limits, issuing certain EAP commands such as "show eapol multihost status" no longer results in a software exception.
wi00978800	**Software Exception, DHCP Relay:** A software exception is no longer produced when DHCP Relay is enabled on a stack.
wi01008959	**Software Exception, ERS 4500 XFP, MLT:** When an ERS 4500 is configured for MLT/DMLT operation across a 10 Gigabit port which has an XFP installed, a software exception no longer occurs.
wi00960742	**Software Exception, SNTP, NTP:** Configure SNTP, NTP or clock commands via EDM, telnet, SSH or a console port connected to a non-Base Unit (NBU) in a stack will no longer result in a software exception.
wi00986026	**Software Exception, VLACP:** A software exception which occurred when running VLACP with fast timers and high amounts of ARP/broadcast traffic is now rectified.
wi00996200	**Software Exception:** An issue which resulted in a software exception with the name "tPDT" when processing certain traffic on MLT ports is now rectified.
wi00996154	**Software Upgrade, 802.1X/EAP:** After upgrading software, the per port EAP auto mode authentication state is now correctly maintained after the upgrade.
wi00898364	**Software Upgrade, MLT Configuration:** After upgrading software from a 5.4 private build, MLT port settings are now correctly maintained after the upgrade.
wi00961895	**Software Upgrade, MLT:** After upgrading software, the MLT shutdown-ports-on-disable state is now correctly maintained after the upgrade.
wi00961795	**Software Upgrade, Multicast:** After upgrading software, the Unknown multicast allow flood configuration state is now correctly maintained after the upgrade.
wi00937726	**Software Upgrade, Passwords:** When upgrading to 5.5.x or later software in some cases console or telnet passwords may no longer work. Please ensure that you refer to the section on Unified Authentication
wi00961775	**Software Upgrade, RADIUS Password Fallback:** After upgrading software, the RADIUS Password Fallback setting will no longer become disabled during the upgrade process.
wi00954473	**Stack, AUR, Dynamic ARP Inspection (DAI):** The Dynamic ARP Inspection trusted/untrusted state for each port is now correctly restored if a unit is replaced in an operational stack.
wi00909985	**Stack, AUR, QoS:** When a unit is replaced all of the previous units QoS settings are now correctly restored by AUR to the replacement unit.
wi00988314	**Stack, Temporary Base Unit Reset:** Traffic on other units in a stack are no longer impacted when the Temporary Base Unit (TBU) of a stack is reset.
wi00988318	**Stack, Unit Reset or Join:** Traffic on unit in a stack is no longer dropped for up to 35 second after that unit joins or re-joins the stack.
wi01042213	**Support Contact:** The support contact reported via the switch software now correctly indicates support@avaya.com
wi00893478	**Temperature Display: S**witch temperature is now correctly displayed in MIB, EDM & CLI.
wi01021689	**Upgrade from 5.3, Configuration, MLT Settings:** The MLT shutdown-ports-on-disable setting is now correctly maintained when upgrading the switch agent code software from release 5.3.x.
wi00930341	**USB, Diagnostics:** Diagnostics software can now correctly be downloaded from a USB device which is connected to units other than the Base Unit (BU) in a stack.

Reference Number	Description
wi00926171	**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.
wi00888446	**VRRP:** VRRP interface configurations are now correctly displayed for VLAN 4094.
Issues Resolved in 5.6.0	
wi00881470	**802.1AB (LLDP), Avaya TLV:** The information pertaining to Avaya proprietary TLVs of dot1q-framing and poe-conservation-request-level are now correctly displayed after reset of a unit within the stack.
wi00864797, wi00862420	**802.1AB (LLDP):** A memory leak which would occur in certain scenarios where the switch is processing a lot of 802.1AB (LLDP) packets is now addressed.
wi00881813, wi00881816	**802.1AB (LLDP):** If you reboot the Base Unit of a stack and then issue the command show lldp vendor-specific avayadotlq-framing on the Temporary Base Unit, the switches in the stack will no longer reset.
wi00881821, wi00881822	**802.1AB (LLDP):** Information is now correctly displayed for 802.1AB (LLDP) MED TX-TLV after a unit in the stack is powered down.
wi00928236	**802.1AB (LLDP):** When the stack is operating in Temporary Base Unit mode, you can now correctly change 802.1AB (LLDP) TLV information on units within the stack.
wi00862985	**802.1AB LLDPPDUs:** In simulations where high amounts of LLDPPDUs being generated, the stack continues to operate normally.
wi00931113	**802.1X, EAP, DHCP, Guest VLAN:** Devices which are connected to the Non-Base unit in a stack will now correctly receive a DHCP address when they are assigned into the Guest VLAN.
wi00827431	**802.1X, EAP, DHCP, Guest VLAN:** When the switch is booting, DHCP requests are no longer forwarded until 802.1X authentication is established or the device is placed into the Guest VLAN.
wi00895233	**802.1X, EAP:** During periods of high end device authentication (for example at commencement of the business day where a customer has a large number of users on a stack of 8 switches) the end devices are now correctly authenticated against the RADIUS server even if the RADIUS queue should become full awaiting responses from the server.
wi00895688	**802.1X, EAP:** Entries for 802.1X / EAP clients are now correctly aged out of the switch as well as the Layer 2 forwarding database (FDB) when devices are removed from the port or moved to a new port.
wi00930103	**ADAC:** When ADAC is configured to use one port of a MLT group as an uplink and the configuration is updated to add the other MLT links as an ADAC uplink, the Voice VAN is now correctly applied to all MLT ports rather than being removed from both MLT uplinks.
wi00885951	**Autotopology, SONMP:** If the Ethernet Routing Switch 4000 is connected to ERS 8800 with 8895CPU or 8810/8806,8803R chassis, the ERS 4000 will now correctly report these devices in the SONMP autotopology table.
wi00491271, wi00484313	**BX SFPs:** When you connect two BX SFPs (Part Code AA1419069-E6 and AA1419070-E6) between Gigabit ERS 4000 switches, a link issue which occurred if the vendor of the BX SFP is Luminet revision A (as identified by the vendor serial number starting with LUMNT) is now rectified.
wi00840626	**CLI, Password, Username:** When issuing commands cli password switch read-write/read-only the following message will appear: %CLI password: Switch authentication parameter is obsolete, changes have not been applied. Changes have been applied, see Unified Authentication for more details about new command syntax.
wi00855310	**EAP, NEAP IP Phone, DHCP Signature:** EAP authentication by DHCP signature now works correctly for legacy Avaya (Nortel) IP Phones and Avaya IP Phones.
wi00483813	**EDM, Energy Saver:** EDM now correctly displays the PoE Savings and PoE Priority in the energy saver ports tab.
wi00875776	**EDM, LLDP:** Neighbor PoE information is now available and correctly displayed in EDM.

Reference Number	Description
wi00855367	**EDM, Syslog:** EDM now supports the ability to configure syslog support under Configuration -> Edit -> Diagnostics -> System Log.
wi00876301	**EDM:** EDM now supports the configuration of http &/or https server mode.
wi00489779	**EDM:** EDM now supports the creation of Static MAC addresses in the Layer 2 FDB / MAC Address Table.
wi00843413	**EDM:** In the Interface tab, the 1000Half option is now correctly disabled if autonegotiation is enabled.
wi00862831	**Hotswap, SNMP Trap:** When a unit is replaced in a stack, the SNMP Trap s5CtrHotSwap is now correctly generated.
wi00838002	**IGMP Snooping & Proxy:** When issuing the default VLAN command, all IGMP parameters are now correctly set to their default values.
wi00863415	**IPFIX:** A template packet is now correctly sent to the IPFIX collector when enabling IPFIX globally.
wi00869476, wi00928619	**MAC MAC Security:** MAC addresses are now correctly deleted when the no mac-security mac-address-table command is issued.
wi00875002	**Management VLAN:** Irrespective of the state of IP routing on the switch, as soon as a port in the Management VLAN is active the ifOperStatus and ipAdEntIfIndex will now correctly respond as UP.
wi00664779	**Management VLAN:** The ifAdminStatus and ifOperStatus MIB objects now provide the correct operational status of the management VLAN if the Management VLAN is operating in Layer 2 mode only.
wi00882779	**Memory Leak, ADAC:** A memory leak which could occur when running ADAC in certain scenarios where IP Phones are repeatedly power cycled through disabling and then re-enabling PoE is now addressed.
wi00483626	**MLT/DMLT:** It is now possible to change the VLAN membership of MLT/DMLT & LAG ports while in-service. If you change the VLAN assignment on administratively disabled MLT/DMLT ports, the system prevents them from being added back into the MLT/DMLT group because the VLAN assignments of the links within the groups are inconsistent.
wi00863190	**NEAP, Interim Updates:** When Interim updates are enabled for non-EAP (NEAP) clients, duplicate interim-update with all values set to null are no longer produced.
wi00907963	**Non-Base Unit Reset, ARP:** When the Non-Base Unit in a stack is reset, the ARP entries for end devices are now correctly refreshed and connectivity reestablished without manual intervention.
wi00862952	**OSPF:** In some configurations with multiple devices running OSPF over multiple OSPF Areas routes now correctly recover after link failure and re-establishment.
wi00872828	**OSPF:** When issuing the show ip ospf stats command, the LSDB Table size is now correctly displayed.
wi00872224	**PoE Traps:** The pethPsePortOnOffNotification trap is now correctly not able to be configured on a non-PoE switch if that unit is the base unit.
wi00877870	**PoE, ESD:** In certain situations when the Power over Ethernet (PoE) was reset due to excessive Electrostatic Discharge (ESD) power is now correctly reapplied to end devices.
wi00862300	**QoS, ADAC:** When ADAC and Auto QoS are both enabled, the QoS marking of the traffic destined for the ADAC Call Server or Uplink ports is now correctly marked.
wi00882592	**Secure Software Upgrade, Very Large Configurations:** When performing an upgrade to a stack running the Secure software image with a very large configuration, the configuration will no longer become corrupted during the upgrade process.
wi00934144, wi00491271	**SFP, Shared port:** New shared port functionality using the sharedport auto-select command is now supported on the 4526GTX, 4526GTX-PWR, 4548GT, and 4548GT-PWR which allows customers to force the selection of either the copper 10/100/1000 port or the SFP port.

Reference Number	Description
wi00832588	**SFP, Shared Ports, EDM:** If a SFP is inserted into a shared port, the port now shows correctly in Enterprise Device Manager (EDM) and the associated MIB entries display as being active.
wi00866308	**SFP:** A third party Encryption SFP (EG1) from Infoguard now correctly works and performs auto-negotiation with an ERS 4500 switch.
wi00850218	**Software Exception, RPSU:** In a simulation environment the resetting of the PSU15 supplying power to a non-base unit will no longer cause a software exception on that unit.
wi00840871	**Unified Authentication:** An improved error message is displayed when deleting an IP address and Radius or TACACS+ Authentication is enabled.
wi00907462	**VLAN, CPU Utilization:** In some configurations with over 740 VLANs configured, the CPU utilization of the switch now no longer maintains 100% while performing a show running-config command.

8. Outstanding Issues

Issues of Special Note

Reference Number	Description
wi00856869	**IP Phone Reset, 802.1AB, ADAC**: When some models of Avaya IP Phones are set-up to receive their Voice VLAN through DHCP option 242 they will perform a reset when connected to an ERS stackable switch operating in default configuration. This is due to the switch advertising 802.1AB Network Policy with a value of 0, which is incorrectly processed by some models or firmware releases of Avaya IP Phones. **Workaround:** disable 802.1AB Network policy on the switch or create an 802.1AB-MED network policy which corresponds to the VLAN supplied through DHCP.

Reference Number	Description
Known Issues for Release 5.6.2	
wi01046652	**802.1X, EAP, NEAP, RAV, Different Spanning Tree Group:** When the RADIUS Assigned VLAN (RAV) for a port is in a different Spanning Tree Group to the previous VLAN assigned to the port, the RAV will not be applied. **Workaround:** It is recommended to use same Spanning Tree Group for all EAP related VLANs: Guest, FailOpen, EAP voice vlan, initial VLAN and RADIUS Assigned VLAN (RAV).
wi01035799	**802.1X, EAP, NEAP, RAV, Spanning Tree:** When a port is moved to a different VLAN as a result of receiving a RADIUS Assigned VLANs (RAV), then the spanning tree status of the port may be updated if spanning tree mode is set to auto.
wi01048962	**802.1X, Fail_Open Continuity Mode:** You can configure Fail_Open Continuity Mode when the Fail_Open VLAN is disabled. **Workaround:** It is recommended to enable Fail_Open Continuity Mode only when Fail Open VLAN is enabled.
wi01042215	**802.1X, MHSA, Multi-VLAN**: If you attempt to configure Multi-VLAN when MHSA is also configured on the switch, the show command ”show eapol multihost status” may take a long time to display output. **Workaround:** Customers are advised that Multi-VLAN operation should not be configured in conjunction with MHSA.
wi01048958	**802.1X, NEAP, Multi-VLAN, Fail_Open Continuity Mode:** NEAP clients may incorrectly remain authenticated after the re-authentication-period expires if the switch is setup to use NEAP RADIUS Server and Multi-VLAN is disabled on the port. **Workaround:** It is recommended to unable Multi-VLAN if Fail_Open Continuity Mode Is enabled in conjunction with NEAP clients and RADIUS assigned VLANs.
wi01046091	**802.1X, NEAP, Multi-VLAN, Fail_Open Continuity Mode:** When a switch transitions from standalone operation to stack mode and switch is setup to use NEAP RADIUS Server and Multi-VLAN is disabled on the port. Client authentication on the port may be lost during this transition. **Workaround:** After transition, force client re-authentication.
wi01047064	**802.1X, User Based Policies, EPM:** User Based Policies (UBP) must be defined locally on the switch/stack, as this implementation does not support the dynamic download of policies from Enterprise Policy Manager (EPM).

Reference Number	Description
wi01060151	**802.1X, User Based Policies, EDM:** EDM does not provide the ability to set User Based Policies or User Based Policies for NEAP with this release. **Workaround:** The CLI can be used to configure these settings.
wi01035352	**802.1X, User Based Policies, Filter on MAC, MHSA:** If the switch port is setup for MHSA, a NEAP client authenticated after EAP device will not have the User Based Policies (UBP) filter on MAC applied to the port.
wi01037828	**802.1X, User Based Policy, Change Security Level:** If you change the User Based Policy (UBP) security level from high to low while clients are authorised, the high security filter will remain in place until clients are reauthorized. **Workaround:** To enable connected users policy to be updated, set the port to reauthorize after changing UBP security mode to low.
wi01048480	**EAP, Unable to Change Port Authorization State:** In a situation where all QoS precedences are used on the switch, it may be impossible to change the EAP port authorisation status from auto to unauthorized. **Workaround:** Change EAP port state from auto to authorized and then to unauthorized.
wi01025961	**ERS4000, QoS, IP Element & Source MAC:** When configuring qos ip-element Layer4 in combination with Source MAC address, you now need to specify an Ethernet type on the ERS 4500 platform.
Known Issues for Release 5.6.1	
wi01003809	**802.1X/EAP, Syslog**: The following error message may be incorrectly generated for EAP "EAP Error Radius - ifIndex not found port 0".
wi00978985	**ASCII Script Table:** A General failure message may occur when configuring an ASCII script entry with filename of greater than 30 characters. **Workaround:** Switch operation is otherwise not affected, specify filename of 30 characters or less when using ASCII script table.
wi00987130	**EAP Trace:** Trace configurations are dynamic and not saved across switch resets. Thus if you have Trace enabled in a stack and you reset one of the units within the stack, then after reset, the unit will no longer be performing trace function. **Workaround:** Reconfigure trace level setting after the unit is reset.
wi00989636	**ERS 4500-PWR+, 4800, 4800-PWR+, Minimum Software Revision:** The minimum software revision for 4500-PWR+, 4800, 4800-PWR+ with hardware revision less than 10 is 5.6.0. The minimum software revision for 4500-PWR+, 4800, 4800-PWR+ with hardware revision 10 or later is 5.6.1. **Warning:** Attempting to downgrade the software to release 5.6.0 or earlier on an Ethernet Routing Switch 4500-PWR+ or 4800 (hardware revision 10 or later) will render the unit inoperable.
wi01000089	**MAC Filtering, Maximum VLANs:** If a configuration consisting of multiple MAC DA filter entries per VLAN with maximum number of VLANs, it is possible that the MAC FDB may be filled resulting in no space for additional MAC entries. **Workaround:** Ensure that the number of MAC DA filter entries multiplied by the number of VLAN configured on switch/stack is less than 8,192 entries.
wi01002073	**NTP, Statistics:** When NTP authentication is enabled**,** NTP statistics are incorrectly displayed.
wi01009029	**Protocol VLAN, Tagged Ports, Changed Operation:** In previous software release, if the ingress port was tagged, classification would be based on the PVID and not on the ingress packets Ethertype. The operation for Protocol VLANs has been updated to operate correctly for tagged port, such that VLAN membership will be determined first by the Ethertype on tagged ports.

Reference Number	Description
wi01009381	**QoS, Classifier Name Display:** When track statistics aggregate option is specified for a QoS rule, the “show qos statistics” command may not display classifier name.
wi01004766	**QoS, Traffic Profile, IP Source Guard (IPSG):** If IP Source Guard (IPSG) was enabled on a port which has QoS Traffic Profiles also configured then the resource used by IPSG will not be released if that consumed the last free precedence on the port.
wi00978033	**Running Configuration, Shared-ports:** The shared port commands are not output by the show running-config command or in the ASCII configuration.
wi00980989	**Shared-port s, Speed/Duplex:** Setting the speed/duplex parameter on a port with shared-port force is not supported.
wi00995946	**Software Downgrade, Configuration Reset:** When downgrading 5.6.1 image to 5.4 or earlier, both configuration NVRAM blocks will be defaulted. This is operation. **Workaround:** If the configuration is required on downgrade, the customer should save the configuration to ASCII and then restore this once the downgrade to 5.4. or earlier software has been completed.
wi01005690	**SSH client, SNMP:** If querying the switch SSH Client parameters via SNMP, the value returned by rcSshcGlobalRsaAuthentication is incorrect, you should use the SNMP object rcSshcGlobalRsaAuthenthication.
wi00991539	**USB:** The Ethernet Routing Switch 4000 does not support USB sticks/drives formatted as NTFS. **Workaround:** Use USB sticks/drives formatted as FAT32 or FAT.
Known Issues for Release 5.6.0	
wi00897222	**802.1AB (LLDP)**: If displaying the status for LLDP dot1 transmission flags in a stack which have 1024 VLANs configured, this will take considerably longer if you use the console port of a Non-Base Unit in the stack. **Workaround:** Avaya recommends that you perform all configuration and display using the console port on the Base Unit of a stack.
wi00909985	**AUR, QoS**: When AUR performs an update of a replacement unit if all ports are set to QoS trusted mode and all QoS precedences are used, it may be possible that the QoS parameters will not be correctly restored to the replacement unit. **Workaround:** Save QoS configurations of the stack offline and if this situation occurs, then re-apply the configuration file directly to the affected unit.
wi00887780	**Brouter Ports**: If when you create a brouter ports the maximum number of IP interfaces is reached, the following message will be displayed in ACLI: %Maximum IP interfaces are already configured. In which case the system will not create the brouter port, however the port may be removed from the initial VLAN if VLAN configcontrol is set to automatic and that port will then be without VLAN membership. **Workaround:** To reactivate the port, add the port to the desired VLAN and re-enable STP participation for that port as appropriate.
wi00888620	**Brouter Ports**: Avaya recommends that you do not renumber units if brouter ports are used. This may result in routes being improperly deactivated and in loss of connectivity. **Workaround:** If it is necessary to renumber the stack, you should remove brouter ports, renumber the stack and then re-create brouter ports.
wi00944306	**Brouter Port, MSTP**: If you attempt to configure a brouter port on a port which is assigned to a VLAN configured in MSTI when running in MSTP mode, then the operation will not be applied. **Workaround:** If using MSTP mode, move the port to a VLAN which is a member of CIST then perform the brouter port assignment.

Reference Number	Description
wi00949343	**Brouter Port, STP**: By design, STP participation is disabled when a brouter port is configured. If you then delete the brouter port, STP participation remains disabled on that port. **Workaround:** Re-enable spanning tree on the port if required after a brouter port instance is deleted.
wi00946493	**DHCP Snooping Option 82**: When DHCP Snooping is configured with Option 82 support and both the DHCP server (trusted port) and the DHCP client are on the base unit of a stack, then the option 82 information will not be added to the DHCP release packet or the DHCP unicast requests that the client generates. **Workaround:** Locate the DHCP server or trusted uplink ports on a port which is not on the based unit.
wi00939421	**EDM, IP Phone Automatic PoE Changes**: When IP Phone Automatic PoE Changes is enabled, the dynamic power limit or dynamic power priority is not displayed in EDM. **Workaround:** Use ACLI to query PoE priority and limits when IP Phone Automatic PoE is configured.
wi00928161	**EDM, PoE Status:** In EDM PoE ports may display an incorrect status of “otherFault” instead of “Deny Low Priority”. **Workaround:** Use ACLI to display the correct PoE status information.
wi00939773	**EDM, SFTP**: If you use SFTP with password authentication enabled and you do not configure a password no warning message will be generated by EDM and the SFTP operation will fail. **Workaround:** Ensure that you configure a password in EDM for SFTP if the SFTP authentication type is set to password.
wi00896456	**ERS 4800, 4500-PWR+**: When you add an ERS 4800 or 4500-PWR+ unit to an existing stack, that stack must be running 5.6.0 or later release software. If the stack is running an earlier software release, the switch will not be allowed to join the stack as the software on these new models cannot be downgraded to releases prior to 5.6.0. **Workaround:** First upgrade the existing stack to the 5.6.0 or later software. Then add the ERS 4800 or 4500-PWR+ unit to the stack. Alternatively you could add the ERS 4800 or 4500-PWR+ unit as the new base unit to the stack; remembering only one unit in the stack can have the Base Unit switch set to on.
wi00960581	**ERS 4800, RADIUS Management Logging**: When a telnet connection is made to ERS 4800 switch operating in standalone mode, the RADIUS accounting packets sent by the switch will have the NAS-Type-Port attribute incorrectly set to Async rather than Ethernet.
wi00928249, wi00928260	**ERS 4800, Stack Statistics**: On ERS 4800 models the multicast or broadcast packet statistics are not incremented for the “show stack port-statistics” command output.
wi00945097	**ERS 4800, TDR**: When performing the TDR function on an ERS 4800 switch, the switch will incorrectly report swapped pairs for a straight through cable.
wi00945147	**ERS 4800, TDR**: When performing the TDR function on an ERS 4800 switch, if the switch is connected to an ERS 4500, then the switch will incorrectly report that pairs 1 and 4 are inverted.
wi00936995	**IGMPv3**: If the size of the IGMPv3 membership report is greater than 1600 bytes, the membership report will not be processed by the switch. IGMPv3 membership reports may contain join requests for multiple groups in one request. **Workaround:** Limit the maximum number of multicast groups per join request to less than 195 groups.

Reference Number	Description
wi00959759	**IGMPv3, Maximum Entries**: The maximum number of IGMP groups learned by IGMP Snooping on the switch is 512. However, this depends on the hardware table usage. With IGMPv1/v2 there is a direct correlation between the number of groups and entries. IGMPv3 on the other hand may use more than one hardware entry per group. An IGMPv3 group with N source addresses will typically consume N+1 hardware entries. As an example an IGMPv3 group with 2 specified source will use 3 hardware entries.
wi00861551	**IGMP, Mrouter ports**: With this release IGMPv3 support has been added to the ERS 4000 product. Multicast Router (Mrouter) ports should now be configured under the ip igmp context. Following are some example ACLI commands: ERS4000 (config)# interface vlan 1 ERS4000 (config-if)# ip igmp router 1/4 ERS4000 # show ip igmp snooping
wi00894579	**IGMP, Multicast Flood, OSPF**: If you configure IGMP Snooping with the unknown multicast no flood option, the system drops control traffic for protocols that use multicasting (example, OSPF). **Workaround:** Configure unknown multicast allow flood specifically for the required multicast group.
wi00934434	**IP Phone Automatic PoE Changes, Energy Saver**: If Energy Saver has been configured for PoE power savings mode, then it will not take into account the dynamic PoE priority of a port which is allocated through the IP Phone Automatic PoE function. Thus if the if the underlying static PoE priority is low but even though the IP Phone Automatic PoE has set a port to high or critical PoE priority, energy saver will powered down the port if poe-saver is enabled when energy saver activates. **Workaround:** Avaya recommends to not use poe-savings mode in combination with IP Phone Automatic PoE changes.
wi00929526	**IP Routing, Route Summary Display**: When performing the "show ip route summary" command, the number of connected routes is incorrectly displayed as 0. **Workaround:** Use the command "show ip route" and if necessary perform a count of the directly connected routes.
wi00894103	**NTP**: You can enable NTP without configuring an NTP server, which will result in no time synchronization. **Workaround:** You should configure at least one NTP server.
wi00895539	**NTP, IPv6**: NTP does not support the configuration of servers using IPv6 addressing with this release.
wi00934809	**MAC Address Table, Layer2 FDB**: With the introduction of new features such as static MAC addresses with this release, the MAC addresses of each of the units in the stack will now be shown in the MAC Address table or Layer 2 Forwarding Database (FDB). This is an expected operation and no action is required on your part.
wi00954477, wi00955665	**MAC Address Table, Layer2 FDB**: With the introduction of new features such as static MAC addresses with this release, the MAC addresses associated with VLAN IDs used by STGs (4001–4008) will now be shown in the MAC Address table or Layer 2 Forwarding Database (FDB). This is an expected operation and no action is required on your part.
wi00961473	**Multicast Traffic, Stack of Two**: When you fail one of the stack cables between a stack of two units, then the multicast traffic matching the rule installed by the “vlan igmp unknown-mcast-allow-flood” command (for example to match OSPF hello packets) will be doubled if the egress port is on the other unit in the stack of two. This only occurs on ERS 4800 units and ERS 4500 units with a single ASIC when operating in a stack of 2 units.

Reference Number	Description
wi00933497	**Port Mirroring, Ingress & Egress Mirroring:** When you use port mirroring, if a packet is both ingress and egress mirrored, two copies of the packet will be sent to the MTP ports. If the egress port is operating in tagged mode, then one copy of the packet will be untagged and another copy of the packet tagged from the egress port. This is expected operation.
wi00955218	**Port Mirroring, XrxYtx, IP Routing**: When performing port mirroring in XrxYtx mode on an ERS 4500 switch, traffic which is to be routed will not be mirrored; this is a hardware limitation. When performing port mirroring in XrxYtx mode on an ERS 4800 switch, traffic which is to be routed will be correctly mirrored to the mirror to port.
wi00950622	**QoS, Queue Shaping**: If queue shaping min rate is configured on the highest queue number, then in an oversubscription scenario this rate may not be fully respected if it exceeds 98% from egress bandwidth.
wi00958103	**QoS, Strict Priority, WRR Algorithm**: The ERS 4800 will process traffic differently to ERS 4500 switches when egress queues are congested. On an ERS 4800 switch, during periods of congestion, low drop precedence traffic will be buffered, while high drop precedence traffic could be dropped if there is insufficient egress buffers available.
wi00927762	**SFTP, Download**: If you use specify an incorrect IP address when you download files from a SFTP server, the system displays an incorrect warning message as follows: % Tftp server IP address invalid.
wi00859047	**SSH:** The CLI command “show ssh download-auth-key” does not display the last transfer result when you download the key from USB. **Workaround:** If the download of the SSH key was successful, then when you display the ssh or sshc status you will see the key has been loaded by the switch. Alternatively loading the SSH key from a TFTP server will display correct result.
wi00959582	**SSH, DSA/RSA Key Length**: When you upload the DSA/RSA key to a TFTP server or USB device from a switch/stack you can generate a filename with up to 128 characters. When you attempt to download the DSA/RSA keys, the switch supports a maximum of only 30 character filenames. **Workaround:** Avaya recommends you use filenames with a maximum of 30 characters for DSA/RSA keys.
wi00891090	**SSH Client, Break Sequence, Syslog**: When you use the SSH client from the switch or stack, if you terminate a server connection with the “~.” break sequence, the system does not generate a SSH disconnected syslog message.
wi00961795	**Upgrade to 5.6, IGMP, Unknown Multicast Allow**: When upgrading to Release 5.6 or later, any previously configured Unknown Multicast Allow flood addresses will be lost. This is a result of the change to multicast support in the 5.6 Release. **Workaround:** In previous software releases, the list of addresses was a global setting. Following an upgrade, you must configure the allow flood addresses on a per VLAN basis.
wi00894057	**Voice VLAN, 802.1AB (LLDP)**: When you can create a LLDP MED network policy there is no check performed to ensure that the VLAN type is set to Voice. **Workaround:** Ensure that you configure the VLAN appropriately as a Voice VLAN before setting the LLDP MED network policy.
wi00893827	**Voice VLAN, ADAC, EAP**: Avaya recommends you do not use the same VLAN ID for ADAC Voice VLAN and EAP Voice VLAN.
wi00930645	**Voice VLAN, 802.1AB (LLDP) MED Policy**: When you configure a VLAN as type Voice, you will still need to explicitly configure 802.1AB (LLDP) MED Network policy to advertise that VLAN via LLDP to end devices.

Reference Number	Description
Known Issues prior to Release 5.6.0	
wi00863027	**802.1AB Default Values**: When you upgrade to 5.5 or later software, any old 802.1AB values will be maintained. The new default 802.1AB values are only applied if you reset the configuration (for example, use the boot default command).
wi00856869	**IP Phone Reset, 802.1AB, ADAC**: When some models of Avaya IP Phones are set-up to receive their Voice VLAN through DHCP option 242 they will perform a reset when connected to an ERS stackable switch operating in default configuration. This is due to the switch advertising 802.1AB Network Policy with a value of 0, which is incorrectly processed by some models or firmware releases of Avaya IP Phones. **Workaround:** disable 802.1AB Network policy on the switch or create a 802.1AB-MED network policy which corresponds to the VLAN supplied through DHCP.
wi00857043	**802.1AB Integration / Avaya 1100**: Avaya 1100E IP Phones using firmware SIP1120e04.00.04.00 will not be recognized by the 802.1AB integration capabilities of the switch, as these phones use the manufacturer name in the TIA-Tx-TLV of "Avaya-01" which is different from the expected value of "Avaya". **Workaround:** Avaya 1100 IP Phones can be configured via alternative means such as DHCP.
wi00858022	**802.1AB Integration / Avaya IP Phone**: When the switch detects an Avaya IP Phone, it sends four LLDP packets (according to MedFastStartRepeatCount). With some models of Avaya IP Phone, this process is repeated 60 seconds after device detection. **Workaround:** None required.
wi00861373	**802.1AB Integration / Call Server TLV**: An IP Phone may incorrectly report the Call Server in-use IP address to the switch if different call-servers were previously configured and cached by the IP Phone. **Workaround:** If it is found that there is a mis-match of in-use call-server addresses cached by the IP Phone, performing two consecutive resets of the IP Phone will clear the incorrect data from the IP Phone cache and result in correct information being returned to the switch.
wi00861372	**802.1AB Integration / Call Server TLV**: You can configure up to 8 Call Server IP Addresses on the switch for maximum resiliency. When some of the Call Servers are unreachable, the Avaya IP Phone may incorrectly indicate to the switch that it is using one of the unreachable Call Servers. **Workaround:** Information on call server use can be obtained from the phone or the call server.
wi00849008	**802.1AB Integration / dot1q-framing TLV**: When Avaya proprietary TLV dot1q-framing is set to auto, the IP Phone will always use untagged mode, irrespective of MED Network Policy or other setting being present. **Workaround:** It is recommended not to use the dot1q-framing TLV set to auto, but instead to set the mode to tagged or untagged.
wi00859649, wi00859648	**802.1AB Integration / File Server TLV**: The File Server IP Address which the IP Phone is using is not advertised by some Avaya IP Handsets (9630, 9620L, 9630G, 9640, 9620C) back to the switch. This can result in the switch displaying null information as the configured file server for these IP phones. **Workaround:** Information on fileserver use can be obtained from the phone or call server.
wi00862047	**802.1AB Integration / Phone IP TLV**: If the Avaya IP Phone receives its IP Address from a DHCP sever then the 802.1AB TLV message from the IP Phone to the switch will not contain the IP Address of the phone, but will only contain the gateway address and netmask.

Reference Number	Description
wi00855665	**802.1AB Integration / Phone IP TLV**: The gateway address returned by an Avaya IP Phone in the IP Phone TLV will be null until the IP Phone is able to reach the configured File Server. Once the IP Phone has reached the File Server, then the correct gateway address will be advertised in this TLV and displayed by the switch. **Workaround:** this does not result in any operational issues which require a workaround.
wi00850597, wi00850033, wi00850936, wi00850590, wi00850935	**802.1AB Integration / Power Conservation**: If the switch sets the power conservation TLV to zero (indicating that no power conservation should be used by the IP Phone), Avaya 9600 IP Phones will always return a value of 1. **Workaround:** this does not result in any operational issues which require a workaround.
wi00855650	**802.1AB Integration / SIP Configuration**: The currently defined Avaya Proprietary TLVs, do not support the direct provisioning of SIP parameters (transport protocol, port number, and domain name) from the switch to the IP Handset. **Workaround:** The SIP information can be supplied to the IP Phone through the configuration fileserver, ensure that the File Server TLV is appropriately configured.
wi00862943	**802.1AB Integration / VLAN Name TLV**: Avaya IP Phone does not use information from 802.1AB VLAN Name TLV to configure Voice VLAN. Other devices will correctly set the Voice VLAN if the VLAN name is set to “voice”.
wi00865086, wi00954114	**Avaya IP Phone DHCP Option 242, 802.1AB (LLDP) Default Parameters**: If you have configured Avaya IP Phones with DHCP Option 242 to specify the Voice VLAN (L2QVLAN) the IP Phone will not use the correct VLAN if the switch is using the 802.1AB (LLDP) Default Parameters. Also refer to wi00868382, wi00554875 **Workaround**: If Avaya IP Phones with DHCP Option 242 are to be used, then it is recommended that the default 802.1AB/LLDP MED policies are deleted. Use the interface command no lldp med-network-policies on telephony ports.
wi00841065	**802.1AB MED Network Policy**: When upgrading to 5.5 or later software and the previous configuration contained no network policies, the new default network policies will be applied.
wi00841955	**802.1AB MED, Auto QoS**: Having a custom LLDP MED policy and enabling Auto QoS will result in the LLDP MED network policy being saved with a DSCP value of 47.
wi00862054	**802.1AB VLAN Name TLV**: When the command lldp tx-tlv dot1 port-protocol-VLAN-id VLAN-name is issued on an interface, an incorrect error message “Port(s) not members of all VLANs configured” may appear. This does not affect functionality of VLAN-name or port-protocol TLV.
wi00484050	**ACG, SNMPv3, Secure Image**: When you run the secure software image, an ASCII configuration file generated by the switch has the SNMPv3 user commands ’snmp-server user’ commented out. This is expected behavior as the associated passwords cannot be output in clear text in the ASCII generated file due to security requirements. As a result when the configuration is loaded onto a switch with default configuration, the SNMPv3 users are not recreated. **Workaround:** Manually re-create the SNMPv3 users after loading the ASCII configuration.
wi00491471	**ADAC, EAP, Guest VLAN**: If you configure both Guest VLAN (GVLAN) and ADAC untagged frames advanced mode on a port, then when a device is discovered by ADAC the port is moved from the GVLAN into the ADAC Voice VLAN. This results in lost connectivity for the GVLAN. If you disable ADAC globally, the client is removed from the ADAC Voice VLAN and placed in the initial port based VLAN with the PVID set to 1 (the default VLAN). **Workaround:** Avaya recommends you do not use ADAC untagged frames advanced mode in combination with EAP MHMA and Guest VLAN.

Reference Number	Description
wi00491178	**CPU utilization**: The CPU utilization reported for the 'last 10 minute interval' may be higher than actual if the CPU was loaded at 100% for the first 5 minutes then returns to an idle state for the next 5 minutes. All other values are correctly calculated. The value will be properly displayed after 30 minutes if the CPU load returns to normal activity levels.
wi00484170	**EAP, 384 ports, Intruder MAC**: If you enable or activate EAP on 384 ports simultaneously, while all clients are sending large volumes of traffic, then some intruder (unauthorized) MAC addresses may not appear in the MAC address table. This applies only to intruder addresses which are blocked and not allowed to forward traffic and it is not a security or connectivity problem.
wi00490753	**EAP, Fail Open VLAN**: When a device is moved into or out of the Fail Open VLAN, there is no notification to the end client that the VLAN has been changed. **Workaround:** It is recommended that if Fail Open VLAN is used, you should set the DHCP lease time to a short period so that clients regularly refresh their IP address leases. Alternatively, if a client has been moved to the Fail Open VLAN, then issuing a DHCP release and renew on the client obtains a new IP address appropriate for the Fail Open VLAN.
wi00491652	**EAP, Guest VLAN**: If you disable Guest VLAN (GVLAN) globally or per interface while authenticated clients are present, the system does not remove the port from the GVLAN. **Workaround:** It is recommended that you shut down the switch port before you disable GVLAN, either globally or per interface. Shutting down the port clears the authenticated clients so that the ports are correctly removed from the GVLAN.
wi00484217	**EAP, MHMA MultiVLAN, Guest VLAN**: Switch ports are not moved into the Guest VLAN (GVLAN) if you enable the GVLAN option after EAP clients have authenticated on the port. **Workaround:** It is recommended that you enable Guest VLAN (global or per port option) before EAP clients are authenticated. Alternative: you can globally disable EAP, configure GVLAN, and then re-enable EAP globally.
wi00878611	**EAP, NEAP, Fail Open VLAN**: After the RADIUS server becomes unreachable, then reachable again, not all 384 NEAP clients may be re-authenticated in some circumstances. **Workaround:** After the RADIUS server becomes reachable, you can either reboot the stack or manually clear the mac address table on the EAP enabled ports using the interface configuration command clear mac-address-table interface fastEthernet <portlist>.
wi00491727	**EAP, QoS Traffic Profiles**: If you configure both QoS Traffic Profiles and EAP, in some circumstances after a switch reboot the QoS Traffic Profile may be set to a higher precedence than before the switch reboot. EAP packets could then be blocked by rules defined in the traffic profile. **Workaround:** To prevent EAP packet blocking in this situation, you can define a QoS policy instead of using a Traffic Profile. The same filtering capabilities are supported, but user defined policies use the same QoS precedence correctly before and after a reset.
wi00483818	**EAP, RADIUS Last Assigned VLAN**: When a port is configured for RADIUS Last Assigned VLAN, if the last RADIUS authentication for that port does not contain QoS priority, then the port priority will be either the one manually configured for that port or the one received for the previous authenticated client.
wi00483930	**EAP**: When EAP performs authentication through TTLS, the first authentication between the supplicant and the switch may fail but subsequent authentications will succeed. **Workaround:** If authentication fails when using EAP-TTLS, do one of the following: ● Wait 30 seconds for the client to re-authenticate successfully. ● Use an alternative EAP authentication mechanism for the client.

Reference Number	Description
wi00489861	**EDM, ASCII Configuration**: When loading an ASCII configuration file using EDM it is recommended that the switch has minimal configuration changes from default. Otherwise existing switch/stack configuration might cause warning or error messages that force the ASCII configuration to exit with a FAIL status. **Workaround:** Apply ASCII configuration from EDM to a switch or stack that has a basic configuration. Alternatively, a currently-configured switch/stack can be reconfigured using an ASCII configuration via CLI (console, telnet, SSH) since the system ignores warning and error messages and configuration continues until the last ASCII file line executes.
wi00491403	**EDM, Multiport configuration**: When you use EDM to apply an operation to all ports, the system may generate a misleading error message if the change could not be applied to all ports (for example if applying a PoE setting to PoE and non-PoE ports). EDM provides only an error message indicating the first port for which it was unable to apply the configuration change.
wi00876311, wi00897706	**EDM, Script Busy**: When connecting to EDM the following message may appear: A script on this page may be busy, or it may have stopped responding. You can stop the script now, or you can continue to see if the script will complete. **Workaround:** Check the remember option and click the continue button from the browser and the message will no longer be displayed.
wi00841212. wi00483820	**EDM, TACACS+**: You cannot use EDM to enable TACACS+ because, when you enable TACACS+, the system disables Web access to the switch. If you used EDM to enable TACACS+ you would lose EDM access for any subsequent operations.
wi00846698	**EDM**: EDM multiport select does not work on interfaces with SFPs/XFPs inserted. Please use per port configuration for interfaces with optics installed.
wi00554891	**EDM**: If the browser device has multiple active IP addresses, EDM will only support multiple sessions from the same source IP address on the device. If different IP source addresses are used, the second or subsequent browsers will display the error message 503 Server Busy. **Workaround:** If you require multiple EDM sessions from the same client device which has multiple IP interfaces, ensure the Web browser on the device uses the same source IP address.
wi00483987, wi00484314, wi00484346, wi00491683	**Energy Saver**: When energy saver is activated or deactivated, the link on a port transitions briefly. This brief transition can cause some devices to re-acquire connectivity, but, in most situations, end users do not notice the port transition. On the switch, the system clears the MAC address for the port and then re-learns it. If EAP or NEAP is enabled, EAP authentication restarts. **Workaround:** Avaya recommends that you disable energy saver on copper uplink ports because activating or deactivating energy saver on copper ports triggers a link down followed rapidly by a link up event. Alternative: Use fiber ports for uplinks because energy saver does not change fiber port status when energy saver is activated or deactivated.
wi00490844	**IP Source Guard (IPSG), Traps**: If the maximum IP entries have been learnt on a MLT/LACP enabled port, then if that trunk is disabled additional log messages are generated.
wi00489936	**Jumbo Frames**: As the Avaya Ethernet Routing Switch 4000 supports jumbo frames (up to 9216), the Jabber counter will always be displayed as zero (0). **Workaround:** You can find information about framing errors in the etherStatsCRCAlignErrors counter.
wi00483597	**Management VLAN**: When operating in Layer 3 mode, using the Management VLAN for normal routing may result in lost connectivity to the Management IP address. **Workaround:** If connectivity problems occur to the management IP address, clear the ARP cache.

Reference Number	Description
wi00848300	**NEAP, IP Phone, Multi-VLAN, ADAC:** If EAP Voice VLAN is used in combination with non-eap-phone option and ADAC is configured for tagged frames and EAP multi-vlan is enabled; then if EAP is disabled after IP Phone is detected and authenticated the PVID of the port is reset to initial value instead of remain equal to the value set by ADAC. **Workaround:** Perform a poe shutdown and then no poe shutdown on the IP Phone port so that the Phone is rediscovered and the PVID is set accordingly.
wi00863853	**NEAP, Multiple Requests**: If the switch is operating with more than 1 NEAP client per port and you issue the clear mac-address-table or clear eapol non-eap command, then the switch sends multiple consecutive access-request for the same NEAP client, during the same authentication session.
wi00483323	**NSNA**: After rebooting a switch or stack with NSNA MAC based clients connected, the switch may incorrectly report that the devices are in the RED VLAN even though they are actually in the Green VLAN. **Workaround:** Execute the CLI commands shutdown , then no shutdown on the corresponding ports.
wi00490890	**NSNA**: After units are rebooted in an operational stack, some static MAC authentication clients may be incorrectly displayed as a 0.0.0.0 IP address instead of the correct IP address. This is a display issue only and does not affect functionality. **Workaround:** Use the SNAS to show the correct IP associations.
wi00483205	**NSNA**: For a MAC authenticated client, if the MAC address is deleted from the SNAS database, the SNAS does not send a reset event to the switch, so the client will remain in its currently assigned VLAN. **Workaround:** Execute ACLI commands shutdown, then no shutdown on the corresponding ports.
wi00483629	**NSNA**: If you add a new classifier to the NSNA yellow QoS set (exceeding the resources), the yellow filters may not be applied.
wi00491369	**NSNA, DHCP Snooping, Dynamic ARP Inspection (DAI)**: If NSNA trusted port is set in combination with DHCP Snooping and Dynamic ARP Inspection (DAI), then, occasionally, after a switch reboot, some PCs connected to the switch may be unable to correctly re-acquire an IP address and will appear in the show nsna client command with an IP address of 0.0.0.0. **Workaround:** Disconnect and reconnect the PC, or if using Windows, issue an ipconfig /release and then ipconfig /renew command and the PC will correctly reacquire an IP address.
wi00483355	**Port Mirroring, Bootp**: Due to a hardware limitation, the BOOTP packets cannot be mirrored if the mirror port is on the first ASIC (port 1-24).
wi00491450	**Port Mirroring, XrxYtx, XrxYtxOrYrxXtx:** If you use port 1 as a mirror port in XrxYtx or port mirroring modes, then broadcast or multicast traffic mirrored to the port is doubled on the monitor port. **Workaround:** Use another port on the switch as the mirrored port.
wi00860958	**RADIUS Accounting**: If RADIUS accounting is enabled and the switch/stack is reset, then the accounting messages sent to the RADIUS server will only include a “RADIUS Accounting Off” message (no “RADIUS Accounting Stop” messages will be sent for authenticated clients).

Reference Number	Description
wi00878635	**RADIUS, EAP Server, NEAP Server, Fail Open VLAN**: While servers are unreachable and ports are in Fail_Open VLAN deletion of all of the RADIUS servers of a given type (e.g. all EAP Servers, all NEAP Servers) may result in clients not being properly re-authenticated or assigned to the appropriate RADIUS VLAN. **Workaround:** Do not delete all RADIUS server types when RADIUS servers are unreachable. Alternatively after the RADIUS servers are again reachable, manually clear the MAC address table on the EAP enabled ports using the interface configuration command clear mac-address- table interface fastEthernet <portlist> .
wi00864589	**RADIUS, Interim Updates**: After RADIUS accounting is disabled for a RADIUS server, interim updates will still be sent to that server, if they were previously enabled. It is recommended to turn off interim updates also, if it is not desired receiving them.
wi00490762, wi00483513	**RSTP**: When operating as an RSTP root bridge and the base unit in a stack is reset, or the stack transitions to standalone mode, the system may not always generate the SNMP trap message indicating a change in RSTP root. **Workaround:** A local log message for nnRstNewRoot is always generated.
wi00484096	**Show running-config**: When you execute the show running-config or show running-config module commands the system may take a longer time than expected to display the output. In systems with very large and complex configurations of 8 units in a stack it can take up to 4 minutes to complete the display of the command. This is considered normal behavior.
wi00484079	**SNMP Traps, Temporary Base Unit**: If you create new SNMP Trap notification filters while the stack is operating in Temporary Base Unit (TBU) mode (that is the Base Unit has failed) then the new filters are not saved and are lost upon stack reboot. **Workaround:** If the stack is operating in TBU mode, reset the stack and then create the required SNMP Trap notification filters.
wi00496736	**SNMPv3, ACG**: SNMPv3 user commands (for example, snmp-server user) are commented in the text configuration file generated by the switch or stack if running the SSH version of the switch software. This happens because the associated passwords cannot be put in clear text in the generated configuration file. Please note that when the configuration is loaded the SNMPv3 users are not recreated.
wi00489857	**SONMP**: A change in the operation of the SONMP-based auto topology means that directly connected BayStack 450 switches report a physical auto topology change every 70 seconds to the Avaya ERS 4000 switch. You can ignore this auto topology change message where there is a direct connection from the Avaya ERS 4000 to a BayStack 450 switch.
wi00862444	**TACACS+, Layer3**: In a layer3 environment if the management VLAN is not operational (no link is up on that VLAN), the switch does not generate TACACS+ packets, therefore no authentication can be performed against the TACACS+ server. **Workaround:** Ensure that management VLAN is up.
wi00491296	**Telnet, ASCII Config** : If you configure a very short telnet timeout value and then you connect to the switch using telnet to execute the CLI command copy config , to save the ASCII configuration to USB or TFTP, the configuration file may be incomplete for large or complex stack configurations. **Workaround:** It is recommended to set the minimum telnet timeout value to 5 minutes.
wi00491518	**VLACP**: When you disable VLACP globally or on a per interface basis, the system forwards the following incorrect message to the syslog server: Port X re-enabled by VLACP.
wi00863879	**VRRP**: VRRP may become unstable when multiple VRRP instances with Fast Advertisement are enabled. **Workaround:** If a large number of VRRP instances are to be configured, it is recommended that the minimum Fast Advertisement Interval (FAI) is set to no less than 600ms.

9. Known Limitations

The following table lists supported software and hardware scaling capabilities in Avaya Ethernet Routing Switch 4000 Series Software Release 5.6.1. The information in this table supersedes information contained in any other document in the suite.

Feature	Maximum Number Supported
Egress queues	Configurable 1–8
MAC addresses	8,192
Stacking bandwidth (full stack of 8 units)	Up to 384 Gbps
QoS precedence	8 per ASIC
QoS rules per ASIC	128 rules per precedence
Maximum number of units in a stack	8
Maximum number of Port Mirroring Instances	4
Layer 2	
Concurrent VLANs	1,024
Supported VLAN IDs	1 - 4094 (0 and 4095 reserved; 4001 reserved by STP; 4002-2008 reserved by multiple STP groups)
Protocol VLAN types	7
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	32
Maximum MAC Learning rate on an MLT trunk	500 new MAC addresses per second
Links or ports for MLT, DMLT or LAG	8
Static MAC Addresses	1,024
Spanning Tree Group instances (802.1s)	8
Avaya Spanning Tree Groups	8
DHCP Snooping table entries	1,024
Layer 3	
IP Interfaces (VLANs or Brouter ports)	256
ARP Entries total (local, static & dynamic)	1,792
ARP Entries - local (IP interfaces per switch/stack)	256
ARP Entries - static	256
ARP Entries - dynamic	1,280
IPv4 Routes total (local, static & dynamic)	512
IPv4 Static Routes	32 (configurable 0-256)
IPv4 Local Routes	64 (configurable up to 2-256)
IPv4 Dynamic Routes (RIP & OSPF)	416 (configurable up to 510)
Dynamic Routing Interfaces (RIP & OSPF)	64
OSPF Areas	4 (3 areas plus area 0)
OSPF Adjacencies (devices per OSPF Area)	16

Feature	Maximum Number Supported
OSPF Link State Advertisements (LSA)	10,000
OSPF Virtual Links	4
ECMP (Max concurrent equal cost paths)	4
ECMP (Max next hop entries)	128
VRRP Instances	256
Management Routes	4
UDP Forwarding Entries	128
DHCP Relay Entries	256
DHCP Relay Forward Paths	512
Miscellaneous	
IGMP v1/v2 multicast groups	512
IGMP v3 multicast groups	512
IGMP Enabled VLANs	256
802.1x (EAP) clients per port, running in MHMA	32
802.1x (NEAP) clients per switch/stack	384
802.1x (EAP & NEAP) clients per switch/stack	768
Maximum RADIUS Servers	2
Maximum 802.1X EAP Servers	2
Maximum 802.1X NEAP Servers	2
Maximum RADIUS/EAP/NEAP Servers	6
IPFiX number of sampled flows	100,000
LLDP Neighbors per port	16
LLDP Neighbors	800
RMON alarms	800
RMON events	800
RMON Ethernet statistics	110
RMON Ethernet history	249

10. Documentation Corrections

wi00969142, wi00925480 - Telnet user credentials were lost (defaulted) after upgrading to 5.5 or 5.6

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“

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 .