AOS-S Switch 16.11.0004 Release Notes

aruba

a Hewlett Packard
Enterprise company

Copyright Information

Open Source Code

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Contents

Chapter 1
Release Overview

These release notes include the following topics:

- Important Information
- Terminology Change
- Version History
- Security Bulletin Subscription Service
- Compatibility/Interoperability

Important Information

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Switch Security	Master	Main
Switch Routing	Master	Main Router
Smart Link	Master-Slave	Primary-Secondary
Chassis Events, IPv6 Configuration, and Troubleshooting	Master-Slave	Management-Slot
Switch Stack	Master-Slave	Conductor-Member
Switch Security, Configuration and Routing	Blacklist, Whitelist	Denylist, Allowlist
Route Type	Blackhole Route	Null Route
Type of Hackers	Black Hat, White Hat	Unethical, Ethical

Version History

NOTE

All released versions are fully supported by Hewlett Packard Enterprise, unless noted in the table.

Table 1: *Version History*

Version number	Software	Release Date	Remarks
16.11.0004	KB, WC, YC, and YA/YB	2022-03-16	Released, fully supported, and posted on the web.
16.11.0003	KB, WC, YC, and YA/YB	2021-12-13	Released, fully supported, and posted on the web.
16.11.0002	KB, WC, YC, and YA/YB	2021-09-30	Released, fully supported, and posted on the web.
16.11.0001	KB, WC, YC, and YA/YB	2021-09-13	Initial release of the 16.11 branch. Released, fully supported, and posted on the web.

Security Bulletin Subscription Service

You can sign up at https://sirt.arubanetworks.com/mailman/listinfo/security-alerts_sirt.arubanetworks.com to initiate a subscription to receive future Aruba Security Bulletin alerts via email.

Compatibility/Interoperability

The switch web agent supports the following web browsers:

- Internet Explorer- Edge, 11
- Chrome- 53, 52
- Firefox- 49, 48
- Safari (MacOS only)- 10, 9

NOTE

HPE recommends using the most recent version of each browser as of the date of this release note.

Chapter 2
KB.16.11

This release note covers software versions for the KB.16.11 branch of the software.

Version KB.16.11.0001 is the initial build of Major version KB.16.11 software. KB.16.11.0003 includes all enhancements and fixes in the KB.16.11.0002 software, plus the additional enhancements and fixes in the KB.16.11.0003 enhancements and fixes sections of this release note.

This release applies to the following Aruba 5400R Switch Series and Aruba 3810M Switch Series:

Table 2: *Products Supported*

Product number	Description
J9821A	Aruba 5406R zl2 Switch
J9823A	Aruba 5406R 44G PoE+/2SFP+ (No PSU) v2 zl2 Switch
J9824A	Aruba 5406R 44G PoE+/4SFP (No PSU) v2 zl2 Switch
J9822A	Aruba 5412R zl2 Switch
J9825A	Aruba 5412R 92G PoE+/2SFP+ (No PSU) v2 zl2 Switch
J9826A	Aruba 5412R 92G PoE+/4SFP (No PSU) v2 zl2 Switch
J9868A	Aruba 5406R 8XGT/8SFP+ (No PSU) v2 zl2 Switch
JL001A	Aruba 5412R 92GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch
JL002A	Aruba 5406R 8 port 1/2.5/5/10GBASE T PoE+ / 8 port SFP+ (No PSU) v3 zl2 Switch
JL095A	Aruba 5406R 16 port SFP+ (No PSU) v3 zl2 Switch
JL003A	Aruba 5406R 44GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch
JL071A	Aruba 3810M 24G 1 slot Switch
JL072A	Aruba 3810M 48G 1 slot Switch
JL073A	Aruba 3810M 24G PoE+ 1 slot Switch
JL074A	Aruba 3810M 48G PoE+ 1 slot Switch
JL075A	Aruba 3810M 16SFP+ 2 slot Switch
JL076A	Aruba 3810M 40G 8 HPE Smart Rate PoE+ 1 slot Switch

Minimum Supported Software Versions

NOTE

If your switch or module is not listed in the below table, it runs on all versions of the software.

Table 3: *Minimum Supported Software Versions*

Product number	Product name	Minimum software version
J9986A	HPE 24-port 10/100/1000BASE-T PoE+ MACsec v3 zl2 Module	KB.15.17.0003
J9987A	HPE 24-port 10/100/1000BASE-T MACsec v3 zl2 Module	KB.15.17.0003
J9988A	HPE 24-port 1GbE SFP MACsec v3 zl2 Module	KB.15.17.0003
J9989A	HPE 12-port 10/100/1000BASE-T PoE+ / 12-port 1GbE SFP MACsec v3 zl2 Module	KB.15.17.0003
J9990A	HPE 20-port 10/100/1000BASE-T PoE+ / 4-port 1G/10GbE SFP+ MACsec v3 zl2 Module	KB.15.17.0003
J9991A	HPE 20-port 10/100/1000BASE-T PoE+ / 4p 1/2.5/5/10GBASE-T PoE+ MACsec v3 zl2 Module	KB.15.17.0003
J9992A	HPE 20-port 10/100/1000BASE-T PoE+ MACsec / 1-port 40GbE QSFP+ v3 zl2 Module	KB.15.17.0003
J9993A	HPE 8-port 1G/10GbE SFP+ MACsec v3 zl2 Module	KB.15.17.0003
J9995A	HPE 8-port 1/2.5/5/10GBASE-T PoE+ MACsec v3 zl2 Module	KB.15.17.0003
J9996A	HPE 2-port 40GbE QSFP+ v3 zl2 Module	KB.15.17.0003
JH231A	HPE X142 40G QSFP+ MPO SR4 Transceiver	KB.15.17.0003
JH232A	HPE X142 40G QSFP+ LC LR4 SM Transceiver	KB.15.17.0003
JH233A	HPE X142 40G QSFP+ MPO eSR4 300M XCVR	KB.15.17.0003
JH234A	HPE X242 40G QSFP+ to QSFP+ 1m DAC Cable	KB.15.17.0003
JH235A	HPE X242 40G QSFP+ to QSFP+ 3m DAC Cable	KB.15.17.0003
JH236A	HPE X242 40G QSFP+ to QSFP+ 5m DAC Cable	KB.15.17.0003
JL001A	Aruba 5412R 92GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch	KB.15.17.0003
JL002A	Aruba 5406R 8-port 1/2.5/5/10GBASE-T PoE+ / 8-port SFP+ (No PSU) v3 zl2 Switch	KB.15.17.0003
JL003A	Aruba 5406R 44GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch	KB.15.17.0003
JL095A	Aruba 5406R 16-port SFP+ (No PSU) v3 zl2 Switch	KB.15.17.0003
JL075A	Aruba 3810M 16SFP+ 2-slot Switch	KB.16.01.0004
JL071A	Aruba 3810M 24G 1-slot Switch	KB.16.01.0004

Product number	Product name	Minimum software version
JL073A	Aruba 3810M 24G PoE+ 1-slot Switch	KB.16.01.0004
JL076A	Aruba 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch	KB.16.01.0004
JL072A	Aruba 3810M 48G 1-slot Switch	KB.16.01.0004
JL074A	Aruba 3810M 48G PoE+ 1-slot Switch	KB.16.01.0004
JL081A	Aruba 3810M/2930M 4 1/2.5/5/10 GbE HPE Smart Rate Module	KB.16.04.0008
JL308A	Aruba 40G QSFP+ LC Bidirectional 150m MMF 2-strand Transceiver	KB.16.04.0008
JL745A	Aruba 1G SFP LC SX 500m MMF TAA XCVR	KB.16.10.0007
JL746A	Aruba 1G SFP LC LX 10km SMF TAA XCVR	KB.16.10.0007
JL747A	Aruba 1G SFP RJ45 T 100m Cat5e TAA XCVR	KB.16.10.0007
JL748A	Aruba 10G SFP+ LC SR 300m MMF TAA XCVR	KB.16.10.0007
JL749A	Aruba 10G SFP+ LC LR 10km SMF TAA XCVR	KB.16.10.0007

NOTE

For information on networking application compatibility, see the Software Feature Support Matrix.

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

Table 4: *Enhancements*

Version	Software	Description	Category
16.11.0004	KB	OSPF Route Filtering feature provides an option to filter the intra-area routes from installing into local FIB table. By using this, operator can create `distribute-list` with one or more network addresses which will be used to filter the intra area routes in OSPFv2/OSPFv3. **Syntax:** OSPFv2: `distribute-list <IP-ADDR>/<Prefix-Len>` OSPFv3: `distribute-list <IPV6-ADDR>/<Prefix-Len>`	OSPF/OSPFv3

Version	Software	Description	Category
		Refer to the *Aruba 3810/5400R Multicasting and Routing Guide for AOS-S Switch 16.11* and *Aruba 3810/5400R IPv6 Configuration Guide for AOS-S Switch 16.11* for more information.	
16.11.0004	KB	Added support in Device fingerprinting (DFP) module to send protocol data to Aruba Central for telemetry. Added `options-list` parameter to device-fingerprinting CLI. Switch software is enhanced to collect DHCP options list and up to three instances of HTTP user agent headers. **Syntax:** `device-fingerprinting [policy]<PROFILE_NAME> dhcp [option-num <NUM> | options-list].` Refer to the *Aruba 3810/5400R Access Security Guide for AOS-S Switch 16.11* for more information.	Device Finger Printing
16.11.0003	KB	The Enrollment over Secured Transport (EST) client feature is updated to download and renew the CA certificates from an EST server independent of application certificate enrollment. A new command `est-server <profile-name> cacerts-download` is added to enable independent CA certificate download from the EST server. This enhancement initiates automatic CA certificate download and renewal when the existing TA profile is about to expire. The switch will use the existing `est-server <profile-name> re-enrollment-prior-expiry` command to determine how many days in advance the renewal is to be done. A MIB has also been added to enable automatic download and renew of the CA certificates from the EST server. Refer to the *Aruba 3810/5400R Access Security Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	EST
16.11.0002	KB	TCP timestamps are an extension to the original TCP stack, that was introduced to identify and reject old duplicate packets (PAWS) and to improve round-trip-time measurement. Using a scanner or other tool, an attacker can observe the TCP timestamp and determine the system uptime to gain information about the operational state of the system. To avoid such risks, a new command `ip tcp randomize-timestamp` has been introduced to randomize the TCP timestamp offsets per connection. Once the command is issued, all the newly established TCP sessions will a use random offset along with the timestamp. A MIB has also been added to enable or disable the randomization of TCP timestamp offsets. Refer to the *Aruba 3810/5400R Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Security

Version	Software	Description	Category
16.11.0002	KB	This is an enhancement to an existing User-Based Tunneling `vlan-extend-enable` (VLAN-aware) mode. Silent devices like Programmable Logic Controller (PLC) devices do not initiate any traffic until they receive a message from the uplink server. Thus, such devices cannot leverage the benefits of colorless ports, which include being authenticated through a RADIUS server and being dynamically placed in a VLAN or being tunneled to a controller. To support such silent devices, a new command `tunneled-node-server ubt-wol-enable vlan <VLAN-ID-LIST>` has been introduced. This command configures the silent client so that the controller allows the first packet from the silent server to reach the silent client without a user tunnel. This will initiate user authentication and tunnel formation. A MIB has also been added to enable User-Based Tunneling Wake-on-LAN (WoL) on the specified VLANs. Refer to the *Aruba 3810/5400R Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Support for Silent Device
16.11.0001	KB	Updated all non-inclusive terminologies. Refer to Terminology Change for more information.	-

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

Table 5: *Fixed Issues*

Version	Bug ID	Software	Description	Category
16.11.0004	256274	KB	**Symptom/Scenario**: VSF Stack Member crashed with a message similar to the following: `Software exception at lava_chassis_slot_sm.c:3626 – in 'eChassMgr', task ID = 0x37b07bc0.`	VSF
16.11.0004	256257	KB	**Symptom/Scenario**: Certain transceivers had link issues in unsupported transceiver mode.	Transceivers
16.11.0004	256234	KB	**Symptom**: The `show rmon statistics <port no>` command returns the wrong counter values.	CLI

Version	Bug ID	Software	Description	Category
			Scenario: This issue occurred when the `clear statistics global` or `clear statistics <port no>` was executed first and then `show rmon statistics <port no>`.	
16.11.0004	256233	KB	**Symptom**: Client ports may encounter packet drops when multicast sources stream video over 500 Mbps. **Scenario**: This issue can occur when multiple clients from different ports subscribed to the same group, which streams using HD channels requiring high bandwidth. TX drops can occur when several clients change channels simultaneously. **Workaround**: Lower the bandwidth of the video streams to below 500 Mbps in order to avoid over-subscription of ports.	IGMP-NG
16.11.0004	256220	KB	**Symptom**: Missing OSPF routes. **Scenario**: This issue occurred when both userbased tunneling and OSPF are configured and either of the uplinks to the controller is down. **NOTE:** `source-interface` to be configured for tunneled node when the switch has more than one vlan to the reach the controller.	OSPFv2
16.11.0004	256205	KB	**Symptom**: A configuration template push from Aruba Central fails. **Scenario**: This issue occurred when the end devices are connected to ports that are configured with `port-security learn-mode static`.	Central Integration
16.11.0004	256121	KB	**Symptom**: Web authentication fails when the switch is managed by Aruba Central (aruba-central support-mode disable). **Scenario**: This issue occurred when the switch connects to Aruba Central and `aruba-central support-mode` is disabled. **Workaround**: Execute `aruba-central support-mode enable` command so the switch is no longer managed by Aruba Central.	Web Authentication
16.11.0004	256140	KB	**Symptom**: The switch crashes with an error message: `NMI event`. **Scenario**: This issue occurred when the HP MSM 775 wireless controller was connected to the switch and `snmpwalk` was executed.	SNMPV2
16.11.0004	256167	KB	**Symptom**: Ports with per-port tunneled node (PPTN) configured may be disabled after a switch reboot. **Scenario**: This issue occurred when a device profile was configured with tunneled-node.	Tunneled Node

Version	Bug ID	Software	Description	Category
			Workaround: Disable and enable the problematic PPTN enabled port manually.	
16.11.004	256144	KB	**Symptom**: The switch is unable to establish a connection with Aruba Activate. **Scenario**: This issue occurred when the switch was first onboarded, but it can also happen after the switch is visible on Aruba Central.	Activate
16.11.0004	255916	KB	**Symptom/Scenario**: Slot crashes with signatures `OMFP LPTR Err Status = 0x00000310 (DEC_ERR_CNT)` and `FR Error = 0x18000020 (ALLOC_CHIP_PORT_UNDERFLOW).`	Basic Layer2
16.11.0004	256115	KB	**Symptom**: Although the switch does not react to pings or SSH commands, it continues to transit traffic. The event log contains a crash message. **Scenario**: This issue occurred when device fingerprinting was configured with DHCP protocol.	CPPM
16.11.0003	256037	KB	**Symptom**: Clients are not authenticated on a switch port. **Scenario**: This issue occurred when multiple clients were connected to a single port (for example, a Personal Computer (PC) was connected to a phone), both MAC authentication and 802.1X authentication methods were attempted at the same time on the PC, and both the authentication methods used the same user role attribute. **Workaround**: Configure the `auth-order` parameter first with `authenticator`, and then with `mac-based`.	802.1X

16.11.0003	255940	KB	**Symptom**: A switch crashes with a message similar to the following:
			`Software exception at svc_misc.c:1088 - in 'mDHCPClint'`
			`-> Failed to malloc 9202 bytes`
			Scenario: This issue occurred when the switch attempted to reconnect to Aruba Central.
				Aruba Central

16.11.0003	255928	KB	**Symptom/Scenario**: A switch is unable to connect to Aruba Central.	Aruba Central

16.11.0003	255978	KB	**Symptom**: A switch crashes with a message similar to the following:
			`Software exception in ISR at pvDmaV1Rx.c`
			`-> ASSERT: No resources available!`
			Scenario: This issue occurred when 802.1X and
				Authentication

Version	Bug ID	Software	Description	Category
			MAC authentication were enabled on the same port with auth-order, and the client was initially authenticated through MAC authentication with a user role having the `port mode` attribute.	
16.11.0003	255995	KB	**Symptom**: A switch crashes when the `show port-access clients` command is issued or when an `SNMP GET` operation is performed to get the MIB object `hpicfUsrAuthMacAuthSessionStatsEntry`. **Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters.	Authentication
16.11.0003	255896	KB	**Symptom**: A stack member loses connection to the stack and gets stuck in a boot loop. **Scenario**: This issue occurred when the stacking links were configured as a full mesh, and two links went down leaving the stacking links in a chain configuration.	Back Plan Stacking
16.11.0003	254566	KB	**Symptom**: Traffic fails to pass through an IEEE 802.1ad tunnel. **Scenario**: This issue occurred because of the following reasons: 1. A Small Form-factor Pluggable+ (SFP+) port was configured as an uplink. 2. IEEE 802.1ad was configured on the same port. 3. The switch was rebooted without a transceiver in the slot. 4. A 1G SFP transceiver was inserted during the runtime. **Workaround**: Insert the 1G SFP transceiver, and then reboot the switch.	IEEE 802.1ad
16.11.0003	256123	KB	**Symptom**: Received packet drops are observed on a port. **Scenario**: This issue occurred when the TCP traffic, with the push flag set, consumed 100% bandwidth on a 1G port of a V3 module.	Interfaces
16.11.0003	256016	KB	**Symptom**: When a private VLAN is configured on a switch, the traffic from the secondary VLAN does not reach the primary VLAN. **Scenario**: This issue occurred when the switch was rebooted, and the secondary VLAN contained a tagged trunk or Link Aggregation Control Protocol (LACP) port. **Workaround**: Remove and add the tagged trunk or LACP configuration to the secondary VLAN.	Private VLAN

Version	Bug ID	Software	Description	Category
16.11.0003	256034	KB	**Symptom**: SNMP MIB files are not reachable, and the MIB file returns some errors. **Scenario**: This issue occurred when the customer used an SNMP monitoring tool to read or parse the MIB files.	SNMP
16.11.0003	256050	KB	**Symptom**: A switch crashes when the **WebUI Security > Clientspage** is accessed. **Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters.	Web UI
16.11.0002	255888	KB	**Symptom/Scenario**: When a proxy server is configured on the switch, the switch does not onboard into Aruba Central or Activate.	Aruba Central
16.11.0002	255799	KB	**Symptom**: The user is unable to copy a configuration file to the switch using Secure File Transfer Protocol (SFTP) and the following error message is displayed. `Invalid input: grep usage error` **Scenario**: This issue occurred when the pipe character (|) was used as a part of the command input for some configuration commands, such as the `banner motd` and `snmpv3 user` commands. **Workaround**: Do not use the pipe character (|) in the command input for the configuration commands.	Configuration
16.11.0002	255825	KB	**Symptom/Scenario**: When a switch is rebooted through an SSH session, the `show boot-history`, `show logging`, and `boot` command outputs include the `Operator cold reboot from TELNET session` message instead of the `Operator cold reboot from SSH session` message.	SSH
16.11.0001	-	KB	No fixes were included in version 16.11.0001.	-

Upgrade Information

Upgrading Restrictions and Guidelines

KB.16.10.0009 uses BootROM KB.16.01.0006 when running on 5400R switches and BootROM KB.16.01.0008 when running on 3810M switches. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.01 is not allowed if MSTP instances configured are greater than 16; or the max-vlans value is greater than 2048, or this system is part of a VSF stack.

Unconfigure these features before attempting to downgrade from KB.16.01.0004 or later to a version earlier than 16.01 of the firmware.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the Basic Operation Guide.

Aruba Security Policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/ sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/ security-bulletins/.

Chapter 3
WC.16.11

This release note covers software versions for the WC.16.11 branch of the software.

Version WC.16.11.0001 is the initial build of Major version WC.16.11 software. WC.16.11.0003 includes all enhancements and fixes in the WC.16.11.0002 software, plus the additional enhancements and fixes in the WC.16.11.0003 enhancements and fixes sections of this release note.

This release applies to the following Aruba 2930F Switch Series and Aruba 2930M Switch Series:

Table 6: *Products Supported*

Product number	Description
JL253A	Aruba 2930F 24G 4SFP+ Switch
JL254A	Aruba 2930F 48G 4SFP+ Switch
JL255A	Aruba 2930F 24G PoE+ 4SFP+ Switch
JL256A	Aruba 2930F 48G PoE+ 4SFP+ Switch
JL258A	Aruba 2930F 8G PoE+ 2SFP+ Switch
JL259A	Aruba 2930F 24G 4SFP Switch
JL260A	Aruba 2930F 48G 4SFP Switch
JL261A	Aruba 2930F 24G PoE+ 4SFP Switch
JL262A	Aruba 2930F 48G PoE+ 4SFP Switch
JL263A	Aruba 2930F 24G PoE+ 4SFP+ TAA-compliant Switch
JL264A	Aruba 2930F 48G PoE+ 4SFP+ TAA-compliant Switch
JL319A	Aruba 2930M 24G 1-slot Switch
JL320A	Aruba 2930M 24G PoE+ 1-slot Switch
JL321A	Aruba 2930M 48G 1-slot Switch
JL322A	Aruba 2930M 48G PoE+ 1-slot Switch
JL323A	Aruba 2930M 40G 8SR PoE+ 1-slot Switch
JL324A	Aruba 2930M 24SR PoE+ 1-slot Switch
JL557A	Aruba 2930F 48G PoE+ 4SFP 740W Switch
JL558A	Aruba 2930F 48G PoE+ 4SFP+ 740W Switch

Product number	Description
JL559A	Aruba 2930F 48G PoE+ 4SFP+ 740W TAA-compliant Switch
JL692A	Aruba 2930F 8G PoE+ 2SFP+ TAA Switch
JL693A	Aruba 2930F 12G PoE+ 2G/2SFP+ Switch
R0M67A	Aruba 2930M 40G 8 HPE Smart Rate PoE Class 6 1-slot Switch
R0M68A	Aruba 2930M 24 HPE Smart Rate PoE Class 6 1-slot Switch

Minimum Supported Software Versions

If your switch or module is not listed in the below table, it runs on all versions of the software.

Table 7: *Minimum Supported Software Versions*

Product number	Product name	Minimum software version
JL078A	Aruba 3810M/2930M 1-port QSFP+ 40GbE Module	WC.16.04.0004
JL083A	Aruba 3810M/2930M 4-port 100M/1G/10G SFP+ MACsec Module	WC.16.04.0004
JL308A	Aruba 40G QSFP+ LC Bidirectional 150m MMF 2-strand Transceiver	WC.16.04.0008
JL323A	Aruba 2930M 40G 8SR PoE+ 1-slot Switch	WC.16.04.0008
JL324A	Aruba 2930M 24SR PoE+ 1-slot Switch	WC.16.04.0008
JL557A	Aruba 2930F 48G PoE+ 4SFP 740W Switch	WC.16.05.0003
JL558A	Aruba 2930F 48G PoE+ 4SFP+ 740W Switch	WC.16.05.0003
JL559A	Aruba 2930F 48G PoE+ 4SFP+ 740W TAA-compliant Switch	WC.16.05.0003
R0M67A	Aruba 2930M 40G 8 HPE Smart Rate PoE Class 6 1-slot Switch	WC.16.07.0002
R0M68A	Aruba 2930M 24 HPE Smart Rate PoE Class 6 1-slot Switch	WC.16.07.0002
J9142B	HPE X122 1G SFP LC BX-D Transceiver	WC.16.07.0003
J9143B	HPE X122 1G SFP LC BX-U Transceiver	WC.16.07.0003
JL692A	Aruba 2930F 8G PoE+ 2SFP+ TAA Switch	WC.16.08.0005
JL693A	Aruba 2930F 12G PoE+ 2G/2SFP+ Switch	WC.16.10.0001

Product number	Product name	Minimum software version
JL745A	Aruba 1G SFP LC SX 500m MMF TAA XCVR	WC.16.10.0007
JL746A	Aruba 1G SFP LC LX 10km SMF TAA XCVR	WC.16.10.0007
JL747A	Aruba 1G SFP RJ45 T 100m Cat5e TAA XCVR	WC.16.10.0007
JL748A	Aruba 10G SFP+ LC SR 300m MMF TAA XCVR	WC.16.10.0007
JL749A	Aruba 10G SFP+ LC LR 10km SMF TAA XCVR	WC.16.10.0007

NOTE

For information on networking application compatibility, see the Software Feature Support Matrix.

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions

Table 8: *Enhancements*

Version	Software	Description	Category
16.11.0004	WC	OSPF Route Filtering feature provides an option to filter the intra-area routes from installing into local FIB table. By using this, operator can create `distribute-list` with one or more network addresses which will be used to filter the intra area routes in OSPFv2/OSPFv3. **Syntax:** OSPFv2: `distribute-list <IP-ADDR>/<Prefix-Len>` OSPFv3: `distribute-list <IPV6-ADDR>/<Prefix-Len>` Refer to the *Aruba 3810/5400R Multicasting and Routing Guide for AOS-S Switch 16.11* and *Aruba 3810/5400R IPv6 Configuration Guide for AOS-S Switch 16.11* for more information.	OSPF/OSPFv3
16.11.0004	WC	Added support in Device fingerprinting (DFP) module to send protocol data to Aruba Central for telemetry. Added `options-list` parameter to device-fingerprinting CLI. Switch software is enhanced to collect DHCP options list and up to three instances of HTTP user agent headers. **Syntax:** `device-fingerprinting [policy]<PROFILE_NAME> dhcp [option-num <NUM> | options-list].` Refer to the *Aruba 3810/5400R Access Security Guide for AOS-S Switch 16.11* for more information.	Device Finger Printing

Version	Software	Description	Category
16.11.0003	WC	The Enrollment over Secured Transport (EST) client feature is updated to download and renew the CA certificates from an EST server independent of application certificate enrollment. A new command `est-server <profile-name> cacerts-download` is added to enable independent CA certificate download from the EST server. This enhancement initiates automatic CA certificate download and renewal when the existing TA profile is about to expire. The switch will use the existing `est-server <profile-name> re-enrollment-prior-expiry` command to determine how many days in advance the renewal is to be done. A MIB has also been added to enable automatic download and renew of the CA certificates from the EST server. Refer to the *Aruba 2930M/2930F Access Security Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	EST
16.11.0002	WC	TCP timestamps are an extension to the original TCP stack, that was introduced to identify and reject old duplicate packets (PAWS) and to improve round-trip-time measurement. Using a scanner or other tool, an attacker can observe the TCP timestamp and determine the system uptime to gain information about the operational state of the system. To avoid such risks, a new command `ip tcp randomize-timestamp` has been introduced to randomize the TCP timestamp offsets per connection. Once the command is issued, all the newly established TCP sessions will a use random offset along with the timestamp. A MIB has also been added to enable or disable the randomization of TCP timestamp offsets. Refer to the *Aruba 2930F/2930M Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Security
16.11.0002	WC	This is an enhancement to an existing User-Based Tunneling `vlan-extend-enable` (VLAN-aware) mode. Silent devices like Programmable Logic Controller (PLC) devices do not initiate any traffic until they receive a message from the uplink server. Thus, such devices cannot leverage the benefits of colorless ports, which include being authenticated through a RADIUS server and being dynamically placed in a VLAN or being tunneled to a controller. To support such silent devices, a new command `tunneled-node-server ubt-wol-enable vlan <VLAN-ID-LIST>` has been introduced. This command configures the silent client so that the controller allows the first packet from the silent server to reach the silent client without a user tunnel. This will initiate user authentication and tunnel formation. A MIB has also been added to enable User-Based Tunneling Wake-on-LAN (WoL) on the specified VLANs. Refer to the *Aruba 2930F/2930M Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Support for Silent Device

Version	Software	Description	Category
16.11.0001	WC	Updated all non-inclusive terminologies. Refer to Terminology Change for more information.	-

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

Table 9: *Fixed Issues*

Version	Bug ID	Software	Description	Category
16.11.0004	256274	WC	**Symptom/Scenario**: VSF Stack Member crashed with a message similar to the following: `Software exception at lava_chassis_slot_sm.c:3626 – in 'eChassMgr', task ID = 0x37b07bc0.`	VSF
16.11.0004	256257	WC	**Symptom/Scenario**: Certain transceivers had link issues in unsupported transceiver mode.	Transceivers
16.11.0004	256234	WC	**Symptom**: The `show rmon statistics <port no>` command returns the wrong counter values. **Scenario**: This issue occurred when the `clear statistics global` or `clear statistics <port no>` was executed first and then `show rmon statistics <port no>`.	CLI
16.11.0004	256233	WC	**Symptom**: Client ports may encounter packet drops when multicast sources stream video over 500 Mbps. **Scenario**: This issue can occur when multiple clients from different ports subscribed to the same group, which streams using HD channels requiring high bandwidth. TX drops can occur when several clients change channels simultaneously. **Workaround**: Lower the bandwidth of the video streams to below 500 Mbps in order to avoid over-subscription of ports.	IGMP-NG
16.11.0004	256220	WC	**Symptom**: Missing OSPF routes. **Scenario**: This issue occurred when both userbased tunneling and OSPF are configured and either of the uplinks to the controller is down.	OSPFv2

Version	Bug ID	Software	Description	Category
			NOTE: `source-interface` to be configured for tunneled node when the switch has more than one vlan to the reach the controller.	
16.11.0004	256205	WC	**Symptom**: A configuration template push from Aruba Central fails. **Scenario**: This issue occurred when the end devices are connected to ports that are configured with `port-security learn-mode static`.	Central Integration
16.11.0004	256121	WC	**Symptom**: Web authentication fails when the switch is managed by Aruba Central (`aruba-central support-mode disable`). **Scenario**: This issue occurred when the switch connects to Aruba Central and `aruba-central support-mode` is disabled. **Workaround**: Execute `aruba-central support-mode enable` command so the switch is no longer managed by Aruba Central.	Web Authentication
16.11.0004	256167	WC	**Symptom**: Ports with per-port tunneled node (PPTN) configured may be disabled after a switch reboot. **Scenario**: This issue occurred when a device profile was configured with tunneled-node. **Workaround**: Disable and enable the problematic PPTN enabled port manually.	Tunneled Node
16.11.0004	256115	WC	**Symptom**: Although the switch does not react to pings or SSH commands, it continues to transit traffic. The event log contains a crash message. **Scenario**: This issue occurred when device fingerprinting was configured with DHCP protocol.	CPPM
16.11.0003	256037	WC	**Symptom**: Clients are not authenticated on a switch port. **Scenario**: This issue occurred when multiple clients were connected to a single port (for example, a Personal Computer (PC) was connected to a phone), both MAC authentication and 802.1X authentication methods were attempted at the same time on the PC, and both the authentication methods used the same user role attribute. **Workaround**: Configure the `auth-order` parameter first with `authenticator`, and then with `mac-based`.	802.1X
16.11.0003	255940	WC	**Symptom**: A switch crashes with a message similar to the following: `Software exception at svc_misc.c:1088 - in 'mDHCPClint'`	Aruba Central

Version	Bug ID	Software	Description	Category
			`-> Failed to malloc 9202 bytes` **Scenario**: This issue occurred when the switch attempted to reconnect to Aruba Central.	
16.11.0003	255928	WC	**Symptom/Scenario**: A switch is unable to connect to Aruba Central.	Aruba Central

16.11.0003	255978	WC	**Symptom**: A switch crashes with a message similar to the following:
			`Software exception in ISR at`
			`pvDmaV1Rx.c`
			`-> ASSERT: No resources available!`
			Scenario: This issue occurred when 802.1X and MAC authentication were enabled on the same port with auth-order, and the client was initially authenticated through MAC authentication with a user role having the `port mode` attribute.
				Authentication

16.11.0003	255995	WC	**Symptom**: A switch crashes when the `show port-access clients` command is issued or when an `SNMP GET` operation is performed to get the MIB object `hpicfUsrAuthMacAuthSessionStatsEntry`. **Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters.	Authentication
16.11.0003	254566	WC	**Symptom**: Traffic fails to pass through an IEEE 802.1ad tunnel. **Scenario**: This issue occurred because of the following reasons: 1. A Small Form-factor Pluggable+ (SFP+) port was configured as an uplink. 2. IEEE 802.1ad was configured on the same port. 3. The switch was rebooted without a transceiver in the slot. 4. A 1G SFP transceiver was inserted during the runtime. **Workaround**: Insert the 1G SFP transceiver, and then reboot the switch.	IEEE 802.1ad
16.11.0003	256016	WC	**Symptom**: When a private VLAN is configured on a switch, the traffic from the secondary VLAN does not reach the primary VLAN. **Scenario**: This issue occurred when the switch was rebooted, and the secondary VLAN contained a tagged trunk or Link Aggregation Control Protocol (LACP) port.	Private VLAN

Version	Bug ID	Software	Description	Category
			Workaround: Remove and add the tagged trunk or LACP configuration to the secondary VLAN.	
16.11.0003	256034	WC	**Symptom**: SNMP MIB files are not reachable, and the MIB file returns some errors. **Scenario**: This issue occurred when the customer used an SNMP monitoring tool to read or parse the MIB files.	SNMP
16.11.0003	256050	WC	**Symptom**: A switch crashes when the **WebUI Security > Clientspage** is accessed. **Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters.	Web UI
16.11.0002	255888	WC	**Symptom/Scenario**: When a proxy server is configured on the switch, the switch does not onboard into Aruba Central or Activate.	Aruba Central
16.11.0002	255799	WC	**Symptom**: The user is unable to copy a configuration file to the switch using Secure File Transfer Protocol (SFTP) and the following error message is displayed. `Invalid input: grep usage error` **Scenario**: This issue occurred when the pipe character (|) was used as a part of the command input for some configuration commands, such as the `banner motd` and `snmpv3 user` commands. **Workaround**: Do not use the pipe character (|) in the command input for the configuration commands.	Configuration
16.11.0002	255825	WC	**Symptom/Scenario**: When a switch is rebooted through an SSH session, the `show boot-history`, `show logging`, and `boot` command outputs include the `Operator cold reboot from TELNET session` message instead of the `Operator cold reboot from SSH session` message.	SSH
16.11.0001	-	WC	No fixes were included in version 16.11.0001.	-

Upgrade Information

Upgrading Restrictions and Guidelines

WC.16.10.0009 uses BootROM WC.16.01.0006 or WC.16.01.0007 (JL692A only) when running on 2930F switches and BootROM WC.17.02.0006 when running on 2930M switches. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.
IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of theBasic Operation Guide.

Aruba Security Policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/ sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/ security-bulletins/.

Chapter 4
YA/YB.16.11

This release note covers software versions for the YA/YB.16.11 branch of the software.

Version YA/YB.16.11.0001 is the initial build of Major version YA/YB.16.11 software. YA/YB.16.11.0003 includes all enhancements and fixes in the YA/YB.16.11.0002 software, plus the additional enhancements and fixes in the YA/YB.16.11.0003 enhancements and fixes sections of this release note.

This release applies to the following Aruba 2530 Switch Series:

Table 10: *Products Supported*

Product number	Description
J9783A	Aruba 2530 8 Switch
J9782A	Aruba 2530 24 Switch
J9781A	Aruba 2530 48 Switch
J9777A	Aruba 2530 8G Switch
J9776A	Aruba 2530 24G Switch
J9775A	Aruba 2530 48G Switch
J9780A	Aruba 2530 8 PoE+ Switch
J9779A	Aruba 2530 24 PoE+ Switch
J9778A	Aruba 2530 48 PoE+ Switch
J9774A	Aruba 2530 8G PoE+ Switch
J9773A	Aruba 2530 24G PoE+ Switch
J9772A	Aruba 2530 48G PoE+ Switch
JL070A	Aruba 2530 8 PoE+ Internal Power Supply Switch
J9856A	Aruba 2530 24G 2SFP+ Switch
J9855A	2530 48G 2SFP+ Switch
J9854A	2530 24G PoE+ 2SFP+ Switch
J9853A	2530 48G PoE+ 2SFP+ Switch

Minimum Supported Software Versions

NOTE

If your switch or module is not listed in the below table, it runs on all versions of the software.

Table 11: *Minimum Supported Software Versions*

Product number	Product name	Minimum software version
J9856A	Aruba 2530 24G 2SFP+ Switch	YA.15.15.0006
J9855A	Aruba 2530 48G 2SFP+ Switch	YA.15.15.0006
J9854A	Aruba 2530 24G PoE+ 2SFP+ Switch	YA.15.15.0006
J9853A	Aruba 2530 48G PoE+ 2SFP+ Switch	YA.15.15.0006
J9783A	Aruba 2530 8 Switch	YB.15.12.0006
J9782A	Aruba 2530 24 Switch	YB.15.12.0006
J9780A	Aruba 2530 8 PoE+ Switch	YB.15.12.0006
J9779A	Aruba 2530 24 PoE+ Switch	YB.15.12.0006
J9781A	Aruba 2530 48 Switch	YA.15.12.0006
J9778A	Aruba 2530 48 PoE+ Switch	YA.15.12.0006
J9777A	Aruba 2530 8G Switch	YA.15.12.0006
J9774A	Aruba 2530 8G PoE+ Switch	YA.15.12.0006
J9776A	Aruba 2530 24G Switch	YA.15.10.0003
J9775A	Aruba 2530 48G Switch	YA.15.10.0003
J9773A	Aruba 2530 24G PoE+ Switch	YA.15.10.0003
J9772A	Aruba 2530 48G PoE+ Switch	YA.15.10.0003

NOTE

For information on networking application compatibility, see the Software Feature Support Matrix.

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

Table 12: *Enhancements*

Version	Software	Description	Category
16.11.0004	YA/YB	No enhancements were included in version 16.11.0004.	NA
16.11.0003	YA/YB	No enhancements were included in version 16.11.0003.	NA

Version	Software	Description	Category
16.11.0002	YA/YB	TCP timestamps are an extension to the original TCP stack, that was introduced to identify and reject old duplicate packets (PAWS) and to improve round-trip-time measurement. Using a scanner or other tool, an attacker can observe the TCP timestamp and determine the system uptime to gain information about the operational state of the system. To avoid such risks, a new command `ip tcp randomize-timestamp` has been introduced to randomize the TCP timestamp offsets per connection. Once the command is issued, all the newly established TCP sessions will a use random offset along with the timestamp. A MIB has also been added to enable or disable the randomization of TCP timestamp offsets. Refer to the *Aruba 2530 Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	Security
16.11.0001	YA/YB	Updated all non-inclusive terminologies. Refer to Terminology Change for more information.	-

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

Table 13: *Fixed Issues*

Version	Bug ID	Software	Description	Category
16.11.0004	256234	YA/YB	**Symptom**: The `show rmon statistics <port no>` command returns the wrong counter values. **Scenario**: This issue occurred when the `clear statistics global` or `clear statistics <port no>` was executed first and then `show rmon statistics <port no>`.	CLI
16.11.0004	256257	YA/YB	**Symptom/Scenario**: Certain transceivers had link issues in unsupported transceiver mode.	Transceivers
16.11.0004	256233	YA/YB	**Symptom**: Client ports may encounter packet drops when multicast sources stream video over 500 Mbps.	IGMP-NG

Version	Bug ID	Software	Description	Category
			Scenario: This issue can occur when multiple clients from different ports subscribed to the same group, which streams using HD channels requiring high bandwidth. TX drops can occur when several clients change channels simultaneously. **Workaround**: Lower the bandwidth of the video streams to below 500 Mbps in order to avoid over-subscription of ports.	
16.11.0004	256205	YA/YB	**Symptom**: A configuration template push from Aruba Central fails. **Scenario**: This issue occurred when the end devices are connected to ports that are configured with `port-security learn-mode static`.	Central Integration
16.11.0004	256202	YA/YB	**Symptom**: Unable to provision the switch from Aruba Activate and records an EST enrollment failure. **Scenario**: This issue occurred when the hostname for the EST enrollment server is not resolved during zero-touch provisioning (ZTP). **Workaround**: Ensure that the DHCP server provides a DNS server IP address.	CertManager
16.11.0004	256121	YA/YB	**Symptom**: Web authentication fails when the switch is managed by Aruba Central (aruba-central support-mode disable). **Scenario**: This issue occurred when the switch connects to Aruba Central and `aruba-central support-mode` is disabled. **Workaround**: Execute `aruba-central support-mode enable` command so the switch is no longer managed by Aruba Central.	Web Authentication

16.11.0003	255819	YA/YB	**Symptom**: A switch crashes with a message similar to the following:
			`SubSystem 100 went down:`
			`Health Monitor: Read Error Restr Mem Access`
			Scenario: This issue occurred because of the following actions:
			1. An AP was authenticated with 802.1X `port mode`.
			2. The AP was rebooted, and the 802.1X authentication configuration was removed from the port.
				802.1X

16.11.0003	255940	YA/YB	**Symptom**: A switch crashes with a message similar to the following: `Software exception at svc_misc.c:1088 - in 'mDHCPClint'`	Aruba Central

Version	Bug ID	Software	Description	Category
			`-> Failed to malloc 9202 bytes` **Scenario**: This issue occurred when the switch attempted to reconnect to Aruba Central.	
16.11.0003	255995	YA/YB	**Symptom**: A switch crashes when the `show port-access clients` command is issued or when an `SNMP GET` operation is performed to get the MIB object `hpicfUsrAuthMacAuthSessionStatsEntry`. **Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters.	Authentication
16.11.0003	255120	YA/YB	**Symptom/Scenario**: The Key Expansion Module of a Cisco 8851 phone does not power up. **Workaround**: Configure `poe-allocate-by` command with `class` parameter on the ports, and reduce the number of powered devices connected to the switch.	PoE
16.11.0003	256034	YA/YB	**Symptom**: SNMP MIB files are not reachable, and the MIB file returns some errors. **Scenario**: This issue occurred when the customer used an SNMP monitoring tool to read or parse the MIB files.	SNMP
16.11.0003	256050	YA/YB	**Symptom**: A switch crashes when the **WebUI Security > Clientspage** is accessed. **Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters.	Web UI
16.11.0002	255888	YA/YB	**Symptom/Scenario**: When a proxy server is configured on the switch, the switch does not onboard into Aruba Central or Activate.	Aruba Central
16.11.0002	255799	YA/YB	**Symptom**: The user is unable to copy a configuration file to the switch using Secure File Transfer Protocol (SFTP) and the following error message is displayed. `Invalid input: grep usage error` **Scenario**: This issue occurred when the pipe character (|) was used as a part of the command input for some configuration commands, such as the `banner motd` and `snmpv3 user` commands. **Workaround**: Do not use the pipe character (|) in the command input for the configuration commands.	Configuration

Version	Bug ID	Software	Description	Category
16.11.0002	255825	YA/YB	**Symptom/Scenario**: When a switch is rebooted through an SSH session, the `show boot-history`, `show logging`, and `boot` command outputs include the `Operator cold reboot from TELNET session` message instead of the `Operator cold reboot from SSH session` message.	SSH
16.11.0001	-	YA/YB	No fixes were included in version 16.11.0001.	-

Upgrade Information

Upgrading Restrictions and Guidelines

YA/YB.16.10.0009 uses BootROM YA.15.20 or YB.15.10. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the **Basic Operation Guide**.

Aruba Security Policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/ sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/ security-bulletins/.

Chapter 5
YC.16.11

This release note covers software versions for the YC.16.11 branch of the software.

Version YC.16.11.0001 is the initial build of Major version YC.16.11 software. YC.16.11.0003 includes all enhancements and fixes in the YC.16.11.0002 software, plus the additional enhancements and fixes in the YC.16.11.0003 enhancements and fixes sections of this release note.

This release applies to the following Aruba 2540 Switch Series:

Table 14: *Products Supported*

Product number	Description
JL354A	Aruba 2540 24G 4SFP+ Switch
JL356A	Aruba 2540 24G PoE+ 4SFP+ Switch
JL355A	Aruba 2540 48G 4SFP+ Switch
JL357A	Aruba 2540 48G PoE+ 4SFP+ Switch

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

Table 15: *Enhancements*

Version	Software	Description	Category
16.11.0004	YC	No enhancements were included in version 16.11.0004.	NA
16.11.0003	YC	No enhancements were included in version 16.11.0003.	NA
16.11.0002	YC	TCP timestamps are an extension to the original TCP stack, that was introduced to identify and reject old duplicate packets (PAWS) and to improve round-trip-time measurement. Using a scanner or other tool, an attacker can observe the TCP timestamp and determine the system uptime to gain information about the operational state of the system. To avoid such risks, a new command `ip tcp randomize-timestamp` has been introduced to randomize the TCP timestamp offsets per connection. Once the command is issued, all the newly established TCP sessions will a use random offset along with the timestamp.	Security

Version	Software	Description	Category
		A MIB has also been added to enable or disable the randomization of TCP timestamp offsets. Refer to the *Aruba 2540 Management and Configuration Guide for AOS-S 16.11* and *Aruba MIB and Trap Support Matrix for AOS-S 16.11* for more information.	
16.11.0001	YC	Updated all non-inclusive terminologies. Refer to Terminology Change for more information.	-

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

Table 16: *Fixed Issues*

Version	Bug ID	Software	Description	Category
16.11.0004	256274	YC	**Symptom/Scenario**: VSF Stack Member crashed with a message similar to the following: `Software exception at lava_chassis_slot_sm.c:3626 – in 'eChassMgr', task ID = 0x37b07bc0.`	VSF
16.11.0004	256257	YC	**Symptom/Scenario**: Certain transceivers had link issues in unsupported transceiver mode.	Transceivers
16.11.0004	256234	YC	**Symptom**: The `show rmon statistics <port no>` command returns the wrong counter values. **Scenario**: This issue occurred when the `clear statistics global` or `clear statistics <port no>` was executed first and then `show rmon statistics <port no>`.	CLI
16.11.0004	256233	YC	**Symptom**: Client ports may encounter packet drops when multicast sources stream video over 500 Mbps. **Scenario**: This issue can occur when multiple clients from different ports subscribed to the same group, which streams using HD channels requiring high bandwidth. TX drops can occur when several clients change channels simultaneously. **Workaround**: Lower the bandwidth of the video streams to below 500 Mbps in order to avoid over-subscription of ports.	IGMP-NG

Version	Bug ID	Software	Description	Category
16.11.0004	256205	YC	**Symptom**: A configuration template push from Aruba Central fails. **Scenario**: This issue occurred when the end devices are connected to ports that are configured with `port-security learn-mode static`.	Central Integration
16.11.0004	256121	YC	**Symptom**: Web authentication fails when the switch is managed by Aruba Central (aruba-central support-mode disable). **Scenario**: This issue occurred when the switch connects to Aruba Central and `aruba-central support-mode` is disabled. **Workaround**: Execute `aruba-central support-mode enable` command so the switch is no longer managed by Aruba Central.	Web Authentication
16.11.0003	256037	YC	**Symptom**: Clients are not authenticated on a switch port. **Scenario**: This issue occurred when multiple clients were connected to a single port (for example, a Personal Computer (PC) was connected to a phone), both MAC authentication and 802.1X authentication methods were attempted at the same time on the PC, and both the authentication methods used the same user role attribute. **Workaround**: Configure the `auth-order` parameter first with `authenticator`, and then with `mac-based`.	802.1X

16.11.0003	255940	YC	**Symptom**: A switch crashes with a message similar to the following:
			`Software exception at svc_misc.c:1088`
			`- in 'mDHCPClint'`
			`-> Failed to malloc 9202 bytes`
			Scenario: This issue occurred when the switch attempted to reconnect to Aruba Central.
				Aruba Central

16.11.0003	255928	YC	**Symptom/Scenario**: A switch is unable to connect to Aruba Central.	Aruba Central
16.11.0003	255995	YC	**Symptom**: A switch crashes when the `show port-access clients` command is issued or when an `SNMP GET` operation is performed to get the MIB object `hpicfUsrAuthMacAuthSessionStatsEntry`. **Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters.	Authentication
16.11.0003	256016	YC	**Symptom**: When a private VLAN is configured on a switch, the traffic from the secondary VLAN does not reach the primary VLAN.	Private VLAN

Version	Bug ID	Software	Description	Category
			Scenario: This issue occurred when the switch was rebooted, and the secondary VLAN contained a tagged trunk or Link Aggregation Control Protocol (LACP) port. **Workaround**: Remove and add the tagged trunk or LACP configuration to the secondary VLAN.	
16.11.0003	256034	YC	**Symptom**: SNMP MIB files are not reachable, and the MIB file returns some errors. **Scenario**: This issue occurred when the customer used an SNMP monitoring tool to read or parse the MIB files.	SNMP
16.11.0003	256050	YC	**Symptom**: A switch crashes when the **WebUI Security > Clientspage** is accessed. **Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters.	Web UI
16.11.0002	255888	YC	**Symptom/Scenario**: When a proxy server is configured on the switch, the switch does not onboard into Aruba Central or Activate.	Aruba Central
16.11.0002	255799	YC	**Symptom**: The user is unable to copy a configuration file to the switch using Secure File Transfer Protocol (SFTP) and the following error message is displayed. `Invalid input: grep usage error` **Scenario**: This issue occurred when the pipe character (|) was used as a part of the command input for some configuration commands, such as the `banner motd` and `snmpv3 user` commands. **Workaround**: Do not use the pipe character (|) in the command input for the configuration commands.	Configuration
16.11.0002	255825	YC	**Symptom/Scenario**: When a switch is rebooted through an SSH session, the `show boot-history`, `show logging`, and `boot` command outputs include the `Operator cold reboot from TELNET session` message instead of the `Operator cold reboot from SSH session` message.	SSH
16.11.0001	-	YC	No fixes were included in version 16.11.0001.	-

Upgrade Information

Upgrading Restrictions and Guidelines

YC.16.10.0009 uses BootROM YC.16.01.0002. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the Basic Operation Guide.

Aruba Security Policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/ sirt/.
Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/ security-bulletins/.