AOS-S Switch RA.16.04.0025 Release Notes

a Hewlett Packard Enterprise company

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

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

This release note covers software versions for the RA.16.04 branch of the software.

Version RA.16.04.0008 is the initial build of Major version RA.16.04 software. RA.16.04.0008 includes all enhancements and fixes in the RA.16.03.0003 software, plus the additional enhancements and fixes in the RA.16.04.0008 enhancements and fixes sections of this release note.

Product series supported by this software: Aruba 2620 Switch Series

This release note includes the following topics:

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

Usage	Old Language	New Language
Route Type	Blackhole Route	Null Route
Type of Hackers	Black Hat, White Hat	Unethical, Ethical

Version History

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

Table 1: *Version History*

Version number	Release date	Based on	Remarks
RA.16.04.0025	2022-06-13	RA.16.04.0024	Released, fully supported, and posted on the web.
RA.16.04.0024	2022-01-14	RA.16.04.0023	Released, fully supported, and posted on the web.
RA.16.04.0023	2021-07-06	RA.16.04.0022	Released, fully supported, and posted on the web.
RA.16.04.0022	2021-01-29	RA.16.04.0020	Released, fully supported, and posted on the web.
RA.16.04.0020	2020-08-04	RA.16.04.0016	Released, fully supported, and posted on the web.
RA.16.04.0016	2018-06-22	RA.16.04.0015	Released, fully supported, and posted on the web.
RA.16.04.0015	n/a	RA.16.04.0014	Never released.
RA.16.04.0014	n/a	RA.16.04.0013	Never released.
RA.16.04.0013	2018-03-28	RA.16.04.0012	Released, fully supported, and posted on the web.
RA.16.04.0012	n/a	RA.16.04.0011	Never released.
RA.16.04.0011	2017-12-22	RA.16.04.0010	Released, fully supported, and posted on the web.
RA.16.04.0010	n/a	RA.16.04.0009	Never released.
RA.16.04.0009	2017-10-16	RA.16.04.0008	Released, fully supported, and posted on the web.
RA.16.04.0008	2017-07-27	RA.16.03.0003	Initial release of the RA.16.04 branch. Released, fully supported, and posted on the web.
RA.16.03.0005	2017-07-07	RA.16.03.0004	Released, fully supported, and posted on the web.
RA.16.03.0004	2017-04-17	RA.16.03.0003	Released, fully supported, and posted on the web.
RA.16.03.0003	2016-12-20	RA.16.02.0008	Initial release of the RA.16.03 branch. Released, fully supported, and posted on the web.
RA.16.02.0014	2016-10-28	RA.16.02.0013	Please see the RA.16.02.0014 release note for detailed information on the RA.16.02 branch. Released, fully supported, and posted on the web.

Version number	Release date	Based on	Remarks
RA.16.02.0013	n/a	RA.16.02.0012	Never released.
RA.16.02.0012	2016-08-31	RA.16.02.0011	Released, fully supported, and posted on the web.
RA.16.02.0011	2016-08-24	RA.16.02.0010	Released, fully supported, and posted on the web.
RA.16.02.0010	2016-08-11	RA.16.02.0009	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

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

Products supported

This release applies to the following product models:

Product number	Description
J9623A	Aruba 2620 24 Switch
J9626A	Aruba 2620 48 Switch
J9625A	Aruba 2620 24 PoE+ Switch
J9627A	Aruba 2620 48 PoE+ Switch
J9624A	Aruba 2620 24 PPoE+Switch

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.

Version 16.04.0025

No enhancements were included in version 16.04.0025.

Version 16.04.0024

No enhancements were included in version 16.04.0024.

Version 16.04.0023

No enhancements were included in version 16.04.0023.

Version 16.04.0022

No enhancements were included in version 16.04.0022.

Version 16.04.0021

No enhancements were included in version 16.04.0021.

Version 16.04.0020

No enhancements were included in version 16.04.0020.

Version 16.04.0016

No enhancements were included in version 16.04.0016.

Version 16.04.0015

Version 16.04.0015 was never released.

Version 16.04.0014

Version 16.04.0014 was never released.

Version 16.04.0013

Multicast Listener Discovery (MLD)

Added new "link-local" option for MLD `show` commands to display well-known multicast group addresses.

```
show ipv6 mld link-local
```

Version 16.04.0012

Version 16.04.0012 was never released.

Version 16.04.0011

No enhancements were included in version 16.04.0011.

Version 16.04.0010

Version 16.04.0010 was never released.

Version 16.04.0009

No enhancements were included in version 16.04.0009.

Version 16.04.0008

Device Profiles for custom device types

This feature is an extension of the Device Profile feature which automatically applies a configuration from a set of pre-defined configurations to a port upon connection of a known device (like, an Aruba AP). The extension allows the automatic detection of new device types based on information in the LLDP TLV and allows configuration of new OUIs on the switch to recognize new types of devices. Administrators can use this feature for automatic assignment of configuration for devices that are not pre-defined on the switch.

For more information, see the *ArubaOS-Switch Management and Configuration Guide* for your switch.

Increase Subject length for the certificate

In the self-signed certificates, or in certificate signing requests created by the switch, the length of the subject name has been increased to accommodate the maximum values of the individual maximums of each of the attributes in the subject (Distinguished Name). For more information, see the *ArubaOS-Switch Access Security Guide* for your switch.

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.

Version 16.04.0025

Security fixes applied.

Version 16.04.0024

PIM Dense Mode

CR_0000256023

Symptom: When a Policy-Based Routing (PBR) policy is hit, multicast or Protocol-Independent Multicast (PIM) traffic is blocked.

Scenario: This issue occurred when a PBR policy rule was configured with any destination IP and a trunk as the next hop, and multicast traffic was transmitted.

Version 16.04.0023

RADIUS

CR_0000255171

Symptom: The switch CPU spikes and the ClearPass Remote Authentication Dial-In User Service (RADIUS) server shuts down.

Scenario: This issue occurred when MAC authentication used the peap-mschapv2 authentication method. As a result, the Access-Request message from the switch and the Access-Challenge message from the RADIUS server were exchanged in a loop.

SNMPv3

CR_0000255067

Symptom: Switch does not respond to Simple Network Management Protocol version 3 (SNMPv3) queries.

Scenario: This issue occurred when there was a wrong value in the boot counter.

ACL

CR_0000255581

Symptom: Access Control List (ACL) logging does not log the permitted and denied packets correctly.

Scenario: This issue occurred when routed ACL was applied in the out direction on a VLAN and ACL logging was enabled.

CR_0000255582

Symptom: The `show statistics aclv4 <acl-name-str> vlan <VLAN-ID> in` command displays other ACLs incorrectly.

Scenario: This issue occurred when two IP access-lists were configured and mapped to a VLAN.

Version 16.04.0022

SSH

CR_0000254278

Symptom: The switch crashes when the `show crypto client-public-key` command is issued.

Scenario: This issue occurred when the `show crypto client-public-key` was issued when the `\t:` symbol was present in the client public key file.

Workaround: Remove `\t:` symbol from the client public key file.

CR_0000254786

Symptom: SSH connections to the switch fail.

Scenario: This issue occurred when more than one RADIUS server was configured, and `aaa authentication ssh enable` was configured to use a RADIUS server other than the first one in the configuration.

Version 16.04.0020

Security fixes were applied in version 16.04.0020.

Version 16.04.0016

Accounting

CR_0000241399

Symptom: The switch sends delayed accounting request packet.

Scenario: After a successful 802.1x authentication with DHCP snooping enabled, the switch sends the accounting request packet delayed by ~45 seconds.

Workaround: Disable DHCP snooping on the switch.

ACL

CR_0000244157

Symptom: The switch experiences a loss in available memory.

Scenario: When removing and re-applying IPv6 ACLs repeatedly, the switch free memory decreases.

DHCP Snooping

CR_0000244260

Symptom: The switch drops certain DHCPv6 advertisements.

Scenario: When the switch is configured for DHCPv6 Snooping, the switch drops DHCPv6 advertisements with the IAID value (option 3) set to 0.

Workaround: Disable DHCPv6 Snooping where there are clients requesting IPv6 address send DHCPv6 solicit requests with an IAID value 0 (option 3).

Job Scheduler

CR_0000244075

Symptom: The switch fails to execute scheduled jobs.

Scenario: When Daylight Savings rule (DST) is configured on the switch close to the DST begin time and the switch time shifts by one hour, the switch fails to execute already configured jobs.

Workaround: Remove previously configured jobs and re-configure them after the DST rule is configured and the switch clock shifts by one hour.

Logging

CR_0000244348

Symptom: The switch is sending incorrect notification regarding configuration changes to the syslog server.

Scenario: If the switch is configured to send notifications about changes in running configuration (`logging notify running-config-change`), when it receives client LLDP-MED information with priority, the switch incorrectly sends a notification regarding switch configuration changes to the syslog sever.

Multicast

CR_0000243253

Symptom: The switch fails to deliver multicast traffic destined to clients managed by an AP.

Scenario: When using device profile for clients managed by an AP, the switch fails to direct multicast IGMP if enabled on the VLAN after the device-profile is applied.

Workaround: Perform one of the following:

1. Enable IGMP on the VLAN before connecting the AP device with the device-profile that dynamically adds ports in the respective VLAN.
2. If IGMP is enabled on the VLAN after device-profile is activated, disable and enable device-profile on the switch.

sFlow

CR_0000243278

Symptom: In certain sFlow polling and sampling ratios, the switch fails with a software exception error.

Scenario: When the sFlow is configured for a large number of ports with a low sampling rate for the actual level of network utilization, the switch may fail with a software exception error.

Workaround: Increase the sFlow sampling rate based on the network traffic burst.

SSH

CR_0000241598

Symptom: SSH connections to the switch management fail to be established.

Scenario: If an SSH connection has been removed by an asynchronous network error, when established using switch data ports, the subsequent sessions to the switch gets immediately closed, unable to fully open a session.

Workaround: Use the switch OOBM IP address to establish SSH connections or use Telnet.

Version 16.04.0015

Version 16.04.0015 was never released.

Version 16.04.0014

Scenario: When switch console access is configured for PEAP-MSCHAPv2 as primary and LOCAL authentication as secondary method for management access, if the default VLAN is not configured with an IP address, the switch does not failover to LOCAL secondary authentication method.

Workaround: Configure an IP address for the default VLAN when PEAP-MSCHAPv2 is the primary authentication method.

Version 16.04.0013

Authentication

CR_0000241206

Symptom: In certain conditions, the switch fails to authenticate switch console access with local credentials.

Configuration

CR_0000242401

Symptom: Port speed-duplex configuration is reset to default.

Scenario: The port-speed configuration is reset to default value after a switch reboot or after re-seating a GigT transceiver in a port configured with non-default speed-duplex.

Workaround: Reconfigure the desired speed-duplex setting using the CLI command:

```
interface <PORT-LIST> speed-duplex <SPEED>
```

Front Panel Security

CR_0000242467

Symptom: The switch fails to disable password recovery through front panel button functions.

Scenario: When the Clear Password function is disabled for the front panel buttons using the CLI command `no front-panel-security password-clear`, the switch fails to disable Password recovery function for front panel buttons with the CLI command `no front-panel-security password-recovery`.

Workaround: Enable Clear Password function before disabling Password Recovery function for front panel buttons.

IP Stacking

CR_0000237504

Symptom: Unable to initiate a new management session to the switch.

Scenario: If IP stacking is enabled, when multiple Telnet/SSH sessions exceeding the maximum configured limit (>6) are opened and closed to the switch, the switch rejects a new session even if the number of used sessions are less than the configured limit. An event message similar to "`rejected because maximum user session limit is reached`" is logged.

LLDP

CR_0000241838

Symptom: The switch displays incorrect "Device ID" in the CDP output.

Scenario: When the Chassis ID TLV contains an IPv4 address, the "Device ID" is not correctly displayed in the output of CLI commands `show cdp neighbor detail` and `walk ciscoCdpMib`.

Workaround: Use LLDP Chassis ID TLV to retrieve the "Device ID" information of the peer device.

`show lldp info remote-device <PORT-LIST>`

REST

CR_0000241895

Symptom: The REST incorrectly returns 204 response.

Scenario: When REST makes a DELETE request with double slash ("/") characters in the request URI and a valid session ID as cookie, the switch incorrectly returns 204 response.

`DELETE http://<hostname>/rest/v1//login-sessions`

Version 16.04.0013

Authentication

CR_0000241206

Symptom: In certain conditions, the switch fails to authenticate switch console access with local credentials.

Workaround: Remove the extra slash ("/") characters from the URI.

RMON

CR_0000241677

Symptom: The switch event log is flooded with unexpected warning messages.

Scenario: The RMON logs are flooded with a warning message similar to `Failed to find FIB entry slaveIpProcessArpUpdate: NULL arpOnMacVid.`

Workaround: This is an internal event message not intended for RMON.

Trunking

CR_0000241091

Symptom: In certain conditions, the switch fails to correctly unblock LACP status of a port.

Scenario: When a switch port, which is a member of an LACP trunk connected to different partners, failover and failback from one partner to another and changes state from ACTIVE to BLOCKED then changes back to ACTIVE, the switch may fail to unblock the port from a previously blocked state.

Workaround: Disable and re-enable the affected port using the following CLI commands:

```
interface <PORT-LIST> disable
interface <PORT-LIST> enable
```

Web UI

CR_0000241156

Symptom: The switch displays an incorrect value for the Unicast PPS counter.

Scenario: The switch may show incorrect values for interface unicast counters in the legacy web GUI.

Workaround: Use CLI command `show interface <PORT-LIST>` to get the correct interface unicast counters.

Version 16.04.0012

Version 16.04.0012 was never released.

Version 16.04.0011

Authentication

CR_0000236646

Symptom: An authenticated port configured with controlled traffic direction may fail to egress packets to the port.

Scenario: When an authenticated port is configured as a spanning-tree edge port using CLI command `spanning-tree <PORT> admin-edge-port`, the port's operational controlled direction does not change correctly from "BOTH" to "IN" state.

Workaround: Disable and re-enable the interface using CLI command `interface <PORT> disable | enable.`

DHCP Server

CR_0000238265

Symptom: The switch event log is flooded with incorrect "Unsolicited Echo Reply" ICMP messages.

Scenario: When DHCP clients request IP renewal, the switch event log is flooded with incorrect "Unsolicited Echo Reply" ICMP messages.

DHCP Snooping

CR_0000239864

Symptom: Some DHCP clients do not receive a DHCP IP address.

Scenario: When the switch is enable for DHCP snooping, it may generate a malformed DHCP OFFER packet when processing the DHCP options of a DHCP packet received from the DHCP server.

Workaround: Configure the port where these DHCP packets are received as trusted using the `dhcp-snooping trust` command.

Key Management

CR_0000237991

Symptom: The key-chain encrypted string may not be displayed in the switch configuration file.

Scenario: When the "key-string" option value for the protocol using the key is configured in two steps to a key configuration (added after the key ID configuration), if the "include credentials" and "encrypted credentials" are enabled, the encrypted key-string is not displayed in the switch configuration file.

Example:

```
key-chain <chain_name>
key-chain <chain_name> key <key_id>
key-chain <chain_name> key <key_id> key-string <key_str>
```

Workaround: Configure the "key-string" option at the same time as key configuration using the following CLI command:

Example:

```
key-chain <chain_name>
key-chain <chain_name> key <key_id> key-string <key_str>
```

Multicast

CR_0000237850

Symptom/Scenario: The switch is incorrectly flooding MLD reports received with a Well Known Multicast IPv6 address.

MVRP

CR_0000238146

Symptom: The switch fails to display the correct warning message.

Scenario: When the switch is configured with MVRP and IGMP/MLD, MVRP's dynamic port membership may affect IGMP/MLD's forwarding behavior. Similarly, MVRP dynamic port membership assignment may also affect IGMP forwarding behavior.

When MVRP is enabled on the switch, if IGMP/MLD is already enabled on any VLAN, the following warning messages are displayed and RMON logs are generated:

```
MVRP's dynamic port membership may affect IGMP's forwarding behavior.
MVRP's dynamic port membership may affect MLD's forwarding behavior.
```

When IGMP is enabled on any VLAN, if MVRP is already enabled on the switch, the following warning message is displayed and RMON log is generated.

`IGMP's forwarding behavior may be affected by MVRP's dynamic port membership.`

Rogue AP Isolation

CR_0000238207

Symptom: The switch incorrectly logs Rogue AP detection event messages.

Scenario: The switch incorrectly logs the isolation of rogue APs, although the Rogue IP Isolation is disabled. Example:

```
switch# show rogue-ap-isolation
Rogue AP Isolation
Rogue AP Status : Disabled
Rogue AP Action : Block
```

Workaround: Add the known APs which have been reported as rogue-APs to the switch white-list using the `rogue-ap-isolation whitelist` command.

SNMP

CR_0000236648

Symptom: Switch may fail with an error message similar to `Health Monitor: Restr Mem Access <...> Task='mSnmpEvt' <...>.`

Scenario: When the security log is almost full, if a new security event is triggered while the SNMP traps such as fault-finder, connection-rate are generated, the switch may fail.

VLAN

CR_0000240169

Symptom/Scenario: When issuing the CLI command `no interface <port> forbid vlan <vlan_id>`, if the respective port is not on the VLAN forbidden port map, the switch becomes unresponsive.

Web UI

CR_0000237484

Symptom: The switch may crash with a Health Monitor signature on its console.

Scenario: When there are attached devices that return LLDP system name string value greater than 64 characters in length, the switch may crash while accessing the NextGen web GUI.

Workaround: Configure the information returned by LLDP on the attached device to be shorter than 64 characters in length or disable LLDP on the attached device.

CR_0000237911

Symptom: IP Stacking page is missing from NextGen GUI.

Scenario: When reverting from the NextGen Web UI to the legacy Web GUI, the IP Stacking page is missing the member selection menu.

Version 16.04.0010

Version 16.04.0010 was never released.

Version 16.04.0009

Authentication

CR_0000235976

Symptom: Clients in guest VLAN (`unauth-vid`) are not reauthenticated.

Scenario: When RADIUS server is not available for authentication, if the client is placed in guest VLAN (`unauth-vid`) and the port is not configured for reauthentication, the switch does not re-authenticate the client after the RADIUS server connectivity becomes available.

Workaround: Do one of the following to resolve the issue:

1. Disable and re-enable the authentication port.
2. Configure re-authentication on the port ("`reauth-period`").

DHCP

CR_0000234234

Symptom: The switch may fail to obtain the IP address assigned from a DHCP Server.

Scenario: When a DHCP Server sends the DHCP OFFER messages with destination IP address set to 0.0.0.0 destined to the switch's DHCP client, the switch drops the DHCP packet and fails to assign the IP address to its VLAN.

DHCP Snooping

CR_0000229137

Symptom: Clients connected to the switch may fail to obtain an IP address from the DHCP server.

Scenario: When DHCP Snooping is enabled on the switch and the number of L2 multicast and unicast MAC addresses to be learned reaches or exceeds the switch capacity, the switch may sporadically drop DHCP OFFER and DHCP ACK packets with a debug error message containing `outbound port unknown`.

Workaround: Disable DHCP Snooping on the switch.

CR_0000230898

Symptom: DHCP Snooping RMON messages intended for unicast client packets are incorrectly displayed for broadcast client packets.

Scenario: When DHCP Snooping is enabled globally and on a VLAN, if there is no trusted port or IP helper address configured on the VLAN, the switch logs incorrect event messages:

```
dhcp-snoop: backplane: Client packet destined to untrusted port dropped
dhcp-snoop: backplane: Ceasing untrusted port destination logs for 5m
```

New event messages were added for broadcast client packets:

```
dhcp-snoop: backplane: Client broadcast packet on <PORT-NUM> dropped, as neither trusted port nor DHCP Relay configured on <VLAN-ID>
dhcp-snoop: backplane: Ceasing client broadcast packet drop logs for 5m.
```

Menu

CR_0000235670

Symptom: The VLAN Address Table in the switch's menu interface does not display all MAC addresses.

Scenario: When viewing the MAC address table via **Menu** > **Status and Counters** > **VLAN Address Table**, only addresses associated with the Default VLAN and VLAN 2 are displayed.

Workaround: View the MAC address table from the CLI using the output of the `show mac-address` command.

Smart Link

CR_0000235633

Symptom: Standby Smart Link ports do not become active even if the active port goes down when one member is powered off.

Scenario: In a switch stack with non-consecutive Smart Link ports, if one member is powered off, the other non-consecutive ports also go down.

Workaround: Configure Smart Link ports as consecutive ports.

SNMP

CR_0000237141

Symptom: SNMPv3 target address configured parameters are not displayed in the switch running configuration.

Scenario: When SNMPv3 is configured with target parameters using the CLI command `snmpv3 targetaddress <ASCII-STR> params <ASCII-STR>`, the parameters are not displayed in the output of CLI command `show running-config`.

Workaround: Use the CLI command `show snmpv3 target address` to display target configured parameters.

SSH

CR_0000236513

Symptom: Switch may crash with an error message similar to `Health Monitor: Invalid Instr Misaligned Mem Access <...> Task='tWatchD'`.

Scenario: When the SSH public-keys are installed without comments using the switch OS version xx.

15.17.xxxx or older and the switch is upgraded to a newer OS version, the switch may crash when issuing the CLI command `show crypto client-public-key`.

Workaround: Install all SSH public keys with comments section or remove all SSH public keys installed without comments before upgrading the switch to a newer OS version.

Web UI

CR_0000234086

Symptom/Scenario: The Save button for Port Security configuration modifications is missing in the NextGen WebUI.

Workaround: Use CLI command to make changes to an existing Port Security configuration.

Version 16.04.0008

RMON

CR_0000230643

Symptom: The switch may generate false RMON alarm traps.

Scenario: After an uptime of over 500 days, the switch may generate false RMON alarm traps for the monitored MIB objects.

Upgrading restrictions and guidelines

RA.16.04.0025 uses BootROM RA.15.13. If your switch has an older version of BootROM, the BootROM willbe updated with this version of software.

For more information about BootROM, see the ArubaOS-Switch Management and Configuration Guide for your switch. 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.

Unconfigure these features before attempting to downgrade from RA.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/.