AOS-S Switch KA.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 KA.16.04 branch of the software.

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

Product series supported by this software: Aruba 3800 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.

Version Number	Release Date	Remarks
KA.16.04.0025	2022-06-13	Released, fully supported, and posted on the web.
KA.16.04.0024	2022-01-14	Released, fully supported, and posted on the web.
KA.16.04.0023	2021-07-06	Released, fully supported, and posted on the web.
KA.16.04.0022	2021-01-29	Released, fully supported, and posted on the web.
KA.16.04.0021	2020-10-01	Released, fully supported, and posted on the web.
KA.16.04.0020	2020-08-04	Released, fully supported, and posted on the web.
KA.16.04.0019	2019-05-20	Released, fully supported, and posted on the web.
KA.16.04.0018	n/a	Never released.
KA.16.04.0017	n/a	Never released.
KA.16.04.0016	2018-06-22	Released, fully supported, and posted on the web.
KA.16.04.0015	n/a	Never released.
KA.16.04.0014	n/a	Never released.
KA.16.04.0013	2018-03-28	Released, fully supported, and posted on the web.
KA.16.04.0012	n/a	Never released.
KA.16.04.0011	2017-12-22	Released, fully supported, and posted on the web.
KA.16.04.0010	n/a	Never released.
KA.16.04.0009	2017-10-16	Released, fully supported, and posted on the web.
KA.16.04.0008	2017-07-27	Initial release of the KA.16.04 branch. Released, fully supported, and posted on the web.
KA.16.03.0005	2017-07-07	Released, fully supported, and posted on the web.
KA.16.03.0004	2017-04-17	Released, fully supported, and posted on the web.
KA.16.03.0003	2016-12-20	Initial release of the KA.16.03 branch. Released, fully supported, and posted on the web.

Version Number	Release Date	Remarks
KA.16.02.0014	2016-10-28	Please see the KA.16.02.0014 release notes for detailed information on the KA.16.02 branch. Released, fully supported, and posted on the web.
KA.16.02.0013	n/a	Never released.
KA.16.02.0012	2016-08-31	Released, fully supported, and posted on the web.
KA.16.02.0011	2016-08-24	Released, fully supported, and posted on the web.
KA.16.02.0010	2016-08-11	Released, fully supported, and posted on the web.
KA.16.02.0009	2016-08-02	Released, fully supported, but never posted on the web.
KA.16.02.0008	2016-07-08	Initial release of the KA.16.02 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

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
J9575A	Aruba 3800 24G 2SFP+ Switch
J9576A	Aruba 3800 48G 4SFP+ Switch
J9573A	Aruba 3800 24G PoE+ 2SFP+ Switch
J9574A	Aruba 3800 48G PoE+ 4SFP+ Switch
J9584A	Aruba 3800 24SFP 2SFP+ Switch

Product number	Description
J9585A	Aruba 3800 24G 2XG Switch
J9586A	Aruba 3800 48G 4XG Switch
J9587A	Aruba 3800 24G PoE+ 2XG Switch
J9588A	Aruba 3800 48G PoE+ 4XG 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 16.04.0019

No enhancements were included in version 16.04.0019.

Version 16.04.0018

Version 16.04.0018 was never released.

Version 16.04.0017

Version 16.04.0017 was never released.

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

Authentication

Added a new authentication option to pin Local-MAC and MAC-based authenticated clients and to allow them to remain authenticated when they become inactive, after the expiration of authentication log-off period. When mac pinning option is enabled on a port, it overrides the regular log-off period for authenticated clients. The option can be enabled using the following CLI command:

```
aaa port-access local-mac <PORT-LIST> mac-pin
aaa port-access mac-based <PORT-LIST> mac-pin
```

OpenFlow

Added a configuration option allowing you to specify the controller interface's source IP address used to establish a connection with the OpenFlow controller.

```
controller-id <ID> ip <IPV4-ADDR> [port <PORT-NUM>]
controller-interface vlan <VLAN-ID> source-ip <IPV4-ADDR>
```

Version 16.04.0008

/31 Subnet Support

On a point-to-point link, where there is no need for a broadcast address, this enhancement allows configuration of an IP address with prefix length of /31. This feature allows users to set the subnet mask to 255.255.255.254 and accepts a broadcast address as a valid IP address for a host on the network. For more information, see the `AOS- Switch Management and Configuration Guide` and the `AOS-Switch Access Security Guide` for your switch.

CLI Commands over REST Interface

As the AOS-Switch software continues to add richer REST interface for programmatically managing the switch, there is a desire to execute configuration and show commands that are not currently supported by the REST interface for troubleshooting purposes.

AOS-Switch 16.04 introduces the 'CliCommand' interface that allows execution of most configuration commands, action commands, and show commands to help existing REST interface users expand the set of tools in their arsenal. For more information, see the *AOS-Switch REST API Guide*.

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 *AOS-Switch Management and Configuration Guide* for your switch.

Enhanced Fan Status

The show system fans command shows the status of power supply fans, fans in the fan trays, and fans on the individual members of stacks depending on the context from which the command is issued. For more information, see the *AOS-Switch Management and Configuration Guide* for your switch.

IPv6 Default Gateway on OOBM port

The option to allow setting of the default gateway for IPv6 on OOBM ports obviates the need to turn on neighbor discovery and helps simplify IPv6 rollouts in Campus Networks. For more information, see the *AOS-Switch Management and Configuration Guide* for your switch.

IPv6 Set Router Preference

This feature extends the IPv6 Router Advertisement message to include router preference to help hosts choose the best default router for off-link destinations. For more information, see the *AOS-Switch Management and Configuration 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

Back Plane Stacking

CR_0000256404

Symptom: The switch reboots or fails over from the commander to standby in the case of a stack. The reason for the reboot may not be recorded in the event log.

Scenario: This issue occurred when the IP directed-broadcast was configured and Wake On LAN traffic type was sent to a directly connected subnet.

Workaround: Disable the IP directed-broadcast.

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.

ACL

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 16.04.0021

Security fixes were applied in version 16.04.0021.

Version 16.04.0020

Security fixes were applied in version 16.04.0020.

Version 16.04.0019

User Roles CR_0000248185

Symptom/Scenario: When the switch is unable to contact the RADIUS server and the client device is assigned the default initial role "deny all", if the RADIUS server is reachable and reauthentication occurs again, the client moves to a user-role with no policy attribute.

Workaround: Disable and enable the port or bounce the port using a RADIUS CoA message after the RADIUS server is reachable.

Version 16.04.0018

Version 16.04.0018 was never released.

Version 16.04.0017

Version 16.04.0017 was never released.

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.

ACLs

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.

Classifier

CR_0000244171

Symptom: The switch does not display certain traffic classes.

Scenario: If a traffic class name includes reserved words, such as "remark", the switch does not display the statistics for the respective class name in the output of the `show statistics policy <POLICY-ID>` command.

Workaround: Avoid using reserved words when configuring traffic class names.

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.

OSPF

CR_0000243557

Symptom/**Scenario:** The word "compatibility" is misspelled "compatability" in the output of the show ipospf general command.

PIM

CR_0000244151

Symptom: The switch fails with an NMI event message in the "nPim" task.

Scenario: If receiving certain corrupted PIM packets, the switch may fail with an NMI event instead of dropping the corrupt packets.

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.

Transceivers

CR_0000243304

Symptom: The switch fails with an error message similar to `Software exception at ppmgr_portInterrupt.c during boot up`.

Scenario: When there is a mix of 10M, 100M, and 1000M copper ports with active linked partners and there are 1000SX SPF transceivers present in dual-personality ports, the switch may fail during boot up.

Workaround: Disable dual-personality ports with SFP transceivers present before rebooting the switch, then re-enable the dual-personality ports after the switch is completely rebooted. Or remove the SFP transceivers and re-insert after the reboot.

Web UI

CR_0000243765

Symptom: The switch is not accessible via secured connection to the web management interface.

Scenario: In a redundant configuration, the switch cannot be accessed through its secured web interface after a redundancy failover event to the standby switch or management module.

Workaround: Reconfigure secured access for web management using the `web-management ssl` command after the failover event.

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

Authentication

CR_0000241206

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

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.

CLI

CR_0000241599

Symptom: The SS management session to the switch hangs during CLI execution.

Scenario: When executing the show tech all command from a session to the switch multiple times, the session may enter into a hang state and will eventually disconnect from the switch with a message similar to `The SSH connection closed: Connection closed by hos`t.

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>`

Distributed Trunking

CR_0000240640

Symptom: Switch module fails with an error message similar to `Slot A crash - Software exceptionin ISR at pvDmaV1Rx.c: -> ASSERT: No resources available!`

Scenario: The ISC (switch-interconnect) link state is frequently changing on/off, the switch generates a high number of ISC synchronization traffic and a high number of "ISC protocol hello receive time is elapsed" messages, which may lead to a failure of the switch module hosting the ISC link.

Workaround: Resolve the reason for frequent ISC (switch-interconnect) link state changes on/off.

CR_0000241657

Symptom: The switch fails to correctly flood packets with unknown destination.

Scenario: In a back-to-back distributed trunking topology, the switches do not flood packets correctly when the destination is unknown.

Workaround: Attempt to access the destination address multiple times to allow all the switches to learn the source MAC address.

Dynamic IP Lockdown

CR_0000240248

Symptom: The switch incorrectly blocks traffic.

Scenario: When the switch is configured with dynamic IP lockdown on a switch interface, it may incorrectly block traffic on that interface after a switch reboot.

Workaround: Clearing switch ARP cache resolves the issue until the next switch reboot.

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>
```

Meshing

CR_0000241632

Symptom: The switch fails to establish link with a mesh peer.

Scenario: When switches with redundancy capabilities, such as dual management modules present to stacked switches are configured in a mesh topology, they fail to establish meshed link after a redundancy switchover event. The CLI command show mesh displays the port state as "disabled" on the switch where the redundancy failover occurred and "Not Established" on the peer switch.

Workaround: Reboot the switch to restore the mesh link state.

OpenFlow CR_0000236916

Symptom: Communication between hosts fails.

Scenario: In a topology with mixed OpenFlow vendors (for example, Ryu, OpenDaylight), the communication between two hosts may fail.

Workaround: Use a single OpenFlow vendor.

OSPF

CR_0000240127

Symptom: The switch generates a misleading OSPF authentication RMON event log.

Scenario: When the switch is configured with OSPFv2 authentication mechanism, the switch may generate incorrect RMON events similar to `OSPF: RECV: Discarding packet on interface vl3011: Invalid authentication key`.

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
```

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
```

CR_0000241138

Symptom: Spanning tree blocks a port without a loop present.

Scenario: In a stacking topology with aggregated links and port members connected to each stack member, if the lowest port number in the aggregated link goes down when it is connected to the lowest member-id of the stack, the entire aggregated link may be incorrectly blocked by spanning tree.

Workaround: Remove the missing port from the aggregated link.

```
no trunk <PORT-LIST>
```

User Roles

CR_0000240708

Symptom: The switch incorrectly starts and closes a RADIUS Accounting session.

Scenario: When there is no user role returned in HP-User-Role VSA from the RADIUS server for the authenticated user or the user role does not exist and the user is placed in the initial user role, the switch incorrectly starts and closes a RADIUS Accounting session.

Workaround: There is no functional impact as the switch is sending unnecessary back-to-back start and stop accounting requests.

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

AirWave

CR_0000236230

Symptom: The switch is not able to recreate the VPN tunnel for Aruba Airwave device management.

Scenario: When the NAT device is changing the dynamically-assigned WAN IP address or there is a failover of the WAN link to the secondary link, the switch may not be able to recreate the VPN tunnel to the Aruba Airwave device management for an extended period of time.

Workaround: Remove and recreate the VPN tunnel for Aruba Airwave device management using the `[no] aruba-vpn type amp peer-ip` command.

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 "UnsolicitedEcho 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`.

Distributed Trunking

CR_0000240374

Symptom: The switch may fail with the error message No resources available.

Scenario: In rare cases, when the switch is configured for distributed trunking, the switch may fail during reboot with an error message similar to `Software exception in ISR at btmDmaApi.c:445 -> ASSERT: No resources available!`

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 MulticastIPv6 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 mayaffect 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.`

PBR

CR_0000236962

Symptom: Switch may fail to forward policy based routed traffic.

Scenario: When a redundancy switchover takes place with policy based routing next hop configured, the switchmay fail to correctly forward the traffic until ARP cache is updated.

Workaround: Remove all non-permanent entries in the ARP cache using CLI command `clear arp`.

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 64characters 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 64characters in length or disable LLDP on the attached device.

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_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.
```

PIM

CR_0000235741

Symptom: Switch may fail to route multicast traffic and RMON message similar to `Failed to allocate newSW IP multicast group, table full FIB entry is generated.`

Scenario: If a new set of multicast flows is sent to the PIM router and the multicast FIB table becomes full, the switch may fail to route the multicast traffic and log an RMON event similar to `Failed to allocate new SWIP multicast group, table full FIB entry.`

Workaround: Disable and re-enable the PIM routing feature on the switch to clear the problem.

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 target address`

`<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_0000233725

Symptom: A delay is observed with ping response between the switch and the RADIUS server. Slow CLI response from SSH sessions are also observed.

Scenario: Symptoms occur when RADIUS Accounting is configured for Network and the interim-update is configured with MAC-based or 802.1X clients for a duration of 1 minute.

Workaround: Do one of the following:

1. Remove the RADIUS Network Accounting interim-update configuration.
2. Increase the interim-update interval to more than 5 minutes.

CR_0000236513

Symptom: Switch may crash with an error message similar to `Health Monitor: Invalid InstrMisaligned 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

Authentication CR_0000232197

Symptom: The switch may delay the request for authentication credentials.

Scenario: When accessing telnet and console session, the switch prompts for authentication credentials with a slight delay.

Workaround: Use SSH to access the switch to get the prompt for authentication credentials immediately.

BGP

CR_0000229326

Symptom: The output of BGP related commands, such as `show ip bgp [<ip-prefix> [longer-prefix]] [route {as-path | community}]`, take an extended amount of time to run.

Scenario: Any show command which includes `show ip bgp [<ip-prefix> [longer-prefix]] [route {as-path | community}]`, takes an extended amount of time to run. Commands such as show tech contain multiple iterations which further exacerbate the amount of time needed to run the commands.

CR_0000229755

Symptom: The statistical session counters are not properly reset.

Scenario: When a BGP link to peer is lost due to either a disconnected link to the BGP peer or BGP reset on the BGPpeer, Prefix Activity counters and Local Policy Denied Prefixes displayed in the output of the CLI command `show ip bgp neighbor` are not cleared once the BGP session is re-established with the peer.

Workaround: Use CLI command `clear ip bgp stats` to reset the BGP peering sessions statistics.

Console

CR_0000230819

Symptom: The switch console may become unresponsive.

Scenario: When disconnecting the console session, connected to a standby or member switch of a stack, using ESC + ~, the console may not disconnect properly and become unresponsive causing the respective stack member to crash with an error message similar to `Software exception at multMgmtUtil.c:141--in 'mLoopPTx' <...>`.

LLDP

CR_0000232922

Symptom: The switch reports an incorrect error message when it fails to configure the loopback interface IP address for LLDP advertisements.

Scenario: When attempting to configure the loopback interface IP address for LLDP advertisements, the switch displays an incorrect error message:

```
This IP address is not configured or is a DHCP address
```

Instead, the following error message should be displayed:

```
This IP address is not configured or is a DHCP/Loopback address
```

Workaround: Configure a statically assigned VLAN IP address for LLDP advertisements.

OpenFlow

CR_0000229081

Symptom: OpenFlow flow statistics counters may reset to zero and fail to increment after that.

Scenario: Packet count in the flow statistics reported in the CLI command `show openflow instance <name> flows` may stop incrementing. OpenFlow flows may fail to age out and the hard/idle timeout for the affected flows may not expire.

Workaround: Disable and re-enable OpenFlow instance state.

CR_0000229141

Added support for 'stats' flag in OpenFlow meter. The switch advertises OFPMF_STATS as a configurable flag when creating/modifying a meter. You are now able to get the meter statistics using the multipart message for any configured meter.

With the added support of STATS, the users will be able to query the statistics only if the STATS flag is configured along with the KBPS/PKTPS flags. Users will no longer be able to query the statistics without STATS.

CR_0000229248

Symptom: OpenFlow traffic may not be sent to the correct priority queue.

Scenario: OpenFlow traffic with DSCP priority remarked by the configured traffic meter is sent to the default priority queue, instead of the remarked priority queue.

CR_0000229987

Symptom: OpenFlow may not be forwarding LLDP and CDP traffic to the specified port.

Scenario: LLDP and CDP traffic on OpenFlow enabled VLANs may not be properly redirected to the OpenFlow port.

CR_0000233449

Symptom: The output of CLI command `show openflow instance <inst_name> flow-table` may be incomplete.

Scenario: When using OpenFlow instance with custom pipeline model on a stack commander with morethan 4 members or on a switch chassis with more than 10 slots, the output of the CLI command `show openflow instance <inst_name> flow-table` may be incomplete.

Example from a chassis with slots A-L populated:

```
HP-Switch-5412Rzl2# show openflow instance a flow-table
```

OpenFlow Instance Flow Table Information

Table ID	Table Name	Flow Count	Miss Count	Go to Table
0	Custom L2 Src	1	688	1, 2, 3
1	Custom L2 Dst	1	0	2, 3
2	Custom L3 Table	1	0	3
3	Custom TCAM Table	1	0	*

Tabe ID	Table Name	Available	Free Flow Count
0	Custom L2 Src	Slot A	: 7372
		Slot B	: 7372
		Slot C	: 7372
		Slot D	: 7372
		Slot E	: 7372
		Slot F	: 7372
		Slot G	: 7372
		Slot H	: 7372
		Slot I	: 7372
		Slot J	: 7
1	Custom L2 Dst	Slot A	: 6144
		Slot B	: 6144
		Slot C	: 6144
		Slot D	: 6144
		Slot E	: 6144
		Slot F	: 6144
		Slot G	: 6144
		Slot H	: 6144
		Slot I	: 6144
		Slot J	: 6

OSPF

CR_0000230472

Symptom: OSPF interface authentication may fail.

Scenario: After a switch reboot, the OSPF authentication may fail when it is set to `md5-auth-key-chain` and `encrypt-credentials` is enabled on only one peer.

Workaround: Enable encrypt-credentials on both OSPF peers and reboot.

Private VLAN

CR_0000233782

Symptom: The switch may not properly forward traffic to the promiscuous port in the private VLAN.

When there is a client connected on a security enabled port and the port is an access port of the secondary VLAN, the client is not able to reach the router connected on the promiscuous port.

Scenario: In a private VLAN configuration, when using security enabled VLAN (for example, radius assigned attributes) on the secondary VLAN, the switch may fail to forward traffic from authenticated client to the promiscuous port.

Workaround: Disable security on the access port.

CR_0000234099

Symptom: The switch may not properly move a client's MAC address from one port to another.

Scenario: In a private VLAN, when a client moves from one access port to another on the same secondary VLAN across the ISL, the switch may not correctly move the client's MAC address to the new access port.

The MAC will clear when MAC age time expires, allowing the MAC address to be re-learned on the new port.

Workaround: Manually clear the MAC address from CLI to allow immediate MAC address re-learning on the new port.

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.

sFlow

CR_0000228486

Symptom: sFlow displays invalid levels of dropped samples.

Scenario: When using trunk interfaces, sFlow is incorrectly calculating the levels of dropped samples displayed in the output of the CLI command `show sflow <INSTANCE> sampling-polling`.

Smart Link

CR_0000229453

Symptom: The switch may fail to forward traffic on ports with Smart Link enabled.

Scenario: When changing the Spanning Tree mode or the port status of the Spanning Tree enabled ports, the Smart Link enabled ports may stop forwarding the traffic.

Workaround: Disable and re-enable the affected Smart Link enabled ports.

CR_0000233339

Symptom: The Smart Link port might flood VLAN traffic even though it is not a member of that VLAN.

Scenario: When the switch is configured with Smart Links and multiple VLANs, VLAN traffic is sent on SmartLink ports that are not a member of those VLANs.

Workaround: No workaround. Remove the Smart Link port configuration to avoid this issue.

SSH

CR_0000229176

Symptom: Unable to access switch via SSH.

Scenario: When using raw console terminal (console terminal none) with message of the day banner configured (banner motd) and SSH session to the switch may fail with the error message `Session terminated, unable to login.`

Workaround: Configure console ANSI or VT100 console terminal or disable message of the day banner.

CR_0000232500

Symptom: Switch fails to authenticate an SSH client using keyboard-interactive method.

Scenario: When the switch access is enabled for SSH public key authentication (for example, `aaa authentication ssh login public-key`), if the SSH client fails to authenticate using client private key for N-1 configured number of authentication attempts (for example, `aaa authentication num- attempts N`), the switch does not failover to authenticate the client using keyboard-interactive method. The switch causes the client authentication to fail with an error message similar to `Too many authentication failures, even when one more attempt is available.`

UDLD

CR_0000229788

Symptom: In a redundant configuration, the switch may stop forwarding traffic on LACP aggregated ports.

Scenario: In a redundant configuration with Spanning Tree enabled, when multiple redundancy switchover events occur, the switch may fail to forward traffic over an LACP trunk which has UDLD enabled in "verify-then- forward" mode.

Workaround: Disable and re-enable Spanning Tree. Alternatively, disable and re-enable the affected port.

Web UI

CR_0000229939

Symptom: Switch port PoE status cannot be changed from the Web UI.

Scenario: In a stacked switch environment, the Web UI does not allow you to change the PoE status of a port belonging to a stack member other than commander switch. It reports an error message: Not a valid PoE port.

Workaround: Use the following CLI command to change PoE status for the port: `[no] interface <PORT-LIST> power-over-ethernet`

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.

Upgrading restrictions and guidelines

KA.16.04.0022 uses BootROM KA.15.10. 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 KA.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/.