AOS-S K.16.02.0033
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

Description

This release note covers software versions for the K.16.02 branch of the software.

Version K.16.02.0008 was the initial build of Major version K.16.02 software. K.16.02.0008 includes all enhancements and fixes in the K.16.01.0004 software, plus the additional enhancements and fixes in the K. 16.02.0008 enhancements and fixes sections of this release note.

Product series supported by this software:

- HPE 3500 and 3500 yl Switch Series
- HPE 5400 zl Switch Series

Important information

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

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 *HPE ArubaOS-Switch Basic Operations Guide Version 16.02*.

Version history

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

Version number	Release date	Remarks
K.16.02.0033	2021-07-06	Released, fully supported, andposted on the web.
K.16.02.0032	2021-01-29	Released, fully supported, andposted on the web.
K.16.02.0031	2020-08-04	Released, fully supported, andposted on the web.
K.16.02.0030	2020-05-26	Released, fully supported, andposted on the web.
K.16.02.0029	2020-04-16	Released, fully supported, andposted on the web.
K.16.02.0028	2019-11-04	Released, fully supported, andposted on the web.
K.16.02.0027	2019-05-06	Released, fully supported, andposted on the web.
K.16.02.0026	2018-11-27	Released, fully supported, andposted on the web.

Table Continued

Version number	Release date	Remarks
K.16.02.0025	2018-06-22	Released, fully supported, andposted on the web.
K.16.02.0024	n/a	Never released.
K.16.02.0023m	n/a	Never released.
K.16.02.0022m	2017-12-22	Released, fully supported, andposted on the web.
K.16.02.0021	2017-09-15	Released, fully supported, andposted on the web.
K.16.02.0020	2017-07-07	Released, fully supported, andposted on the web.
K.16.02.0019	2017-05-15	Released, fully supported, andposted on the web.
K.16.02.0018	2017-03-31	Released, fully supported, andposted on the web.
K.16.02.0017	2017-03-01	Released, fully supported, andposted on the web.
K.16.02.0016	2017-01-27	Released, fully supported, andposted on the web.
K.16.02.0015	n/a	Never released.
K.16.02.0014	2016-10-28	Released, fully supported, andposted on the web.
K.16.02.0013	n/a	Never released.
K.16.02.0012	2016-08-31	Released, fully supported, andposted on the web.
K.16.02.0011	2016-08-24	Released, fully supported, andposted on the web.
K.16.02.0010	2016-08-11	Released, fully supported, andposted on the web.
K.16.02.0009	2016-08-02	Released, fully supported, but never posted on the web.
K.16.02.0008	2016-07-08	Initial release of the K.16.02 branch. Released, fully supported, and posted on the web.
K.16.01.0008	2016-08-02	Please see the K.16.01.0008 release notes for detailed information on the K.16.01 branch. Released, fully supported, and posted on the web.
K.16.01.0007	2016-05-31	Released, fully supported, andposted on the web.
K.16.01.0006	2016-03-28	Released, fully supported, andposted on the web.

Table Continued

Version number	Release date	Remarks
K.16.01.0005	n/a	Never released.
K.16.01.0004	2016-01-20	Released, fully supported, andposted on the web.
K.15.18.0012	2016-08-02	Please see the K.15.18.0012 release notes for detailed information on the K.15.18 branch. Released, fully supported, and posted on the web.
K.15.18.0011	2016-05-31	Released, fully supported, andposted on the web.
K.15.18.0010	2016-03-28	Released, fully supported, andposted on the web.
K.15.18.0009	n/a	Never released.
K.15.18.0008	2016-01-19	Released, fully supported, andposted on the web.
K.15.18.0007	2015-11-10	Released, fully supported, andposted on the web.
K.15.18.0006	2015-08-15	Initial release of the K.15.18 branch. Released, fully supported, and posted on the web.

Products supported

This release applies to the following product models:

Product number	Description
J9470A	HPE 3500 24 Switch
J9471A	HPE 3500 24 PoE Switch
J9472A	HPE 3500 48 Switch
J9473A	HPE 3500 48 PoE Switch
J8692A	HPE 3500yl 24G PWR Intelligent Edge Switch
J8693A	HPE 3500yl 48G PWR Intelligent Edge Switch
J9310A	HPE 3500yl 24G PoE+ Switch
J9311A	HPE 3500yl 48G PoE+ Switch
J8697A	HPE 5406zl Intelligent Edge Switch
J9642A	HPE 5406zl Switch with Premium SW
J8698A	HPE 5412zl Intelligent Edge Switch
J9643A	HPE 5412 zl Switch with Premium Software
J8699A	HPE 5406zl 48G Intelligent Edge Switch
J8700A	HPE 5412zl 96G Intelligent Edge Switch

Table Continued

Product number	Description
J9447A	HPE 5406zl 48G PoE+ Switch
J9448A	HPE 5412zl 96G PoE+ Switch
J9533A	HPE 5406 44G PoE+/2XG-SFP+ v2 zl Switch
J9532A	HPE 5412 92G PoE+/2XG-SFP+ v2 zl Switch
J9539A	HPE 5406 44G PoE+/4G-SFP v2 zl Switch
J9540A	HPE 5412 92G PoE+/4G-SFP v2 zl Switch
J9866A	HPE 5406 8p 10GBASE-T 8p 10GbE SFP+ v2 zl Switch with Premium Software

Compatibility/interoperability

The switch web agent supports the following web browsers:

Browser	Supported versions
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 thisrelease note.

Minimum supported software versions

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

Product number	Product name	Minimum software version
J9546A	HPE 8-port 10GBase-T v2 zl Module	K.15.04.0002
J9310A	HPE 3500yl 24G PoE+ Switch	K.15.02.0004

Table Continued

Product number	Product name	Minimum software version
J9311A	HPE 3500yl 48 PoE+ Switch	K.15.02.0004
J9312A	HPE 2-Port SFP+/2-Port CX4 10GbE yl Module	K.15.02.0004
J9534A	HPE 24-port 10/100/1000 PoE + v2 zl Module	K.15.02.0004
J9535A	HPE 20-port 10/100/1000 PoE + / 4-port SFP v2 zl Module	K.15.02.0004
J9536A	HPE 20-port 10/100/1000 PoE + / 2-port 10-GbE SFP+ v2 zl	K.15.02.0004
J9537A	HPE 24-port SFP v2 zl Module	K.15.02.0004
J9538A	HPE 8-port 10-GbE SFP+ v2 zl Module	K.15.02.0004
J9547A	HPE 24-port 10/100 PoE+ v2 zl Module	K.15.02.0004
J9548A	HPE 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module	K.15.02.0004
J9549A	HPE 20-port Gig-T / 4-port SFP v2 zl Module	K.15.02.0004
J9550A	HPE 24-port Gig-T v2 zl Module	K.15.02.0004
J9637A	HPE 12-port Gig-T / 12-port SFP v2 zl Module	K.15.02.0004
J9307A	HPE 24-Port 10/100/1000 PoE + zl Module	K.14.34
J9308A	HPE 20-Port 10/100/1000 PoE +/4-port MiniGBIC zl Module	K.14.34
J9478A	HPE 24-port 10/100 PoE+ zl Module	K.14.34
J9447A	HPE 5406zl 48G PoE+ Switch	K.14.34
J9448A	HPE 5412zl 96G PoE+ Switch	K.14.34
J9470A	HPE 3500 24 Switch	K.14.31
J9471A	HPE 3500 24 PoE Switch	K.14.31
J9472A	HPE 3500 48 Switch	K.14.31
J9473A	HPE 3500 48 PoE Switch	K.14.31
J9154A	HPE ONE Services zl Module	K.13.51

Table Continued

Product number	Product name	Minimum software version
J9051A, J9052A	HPE Wireless Edge Services zl Module, HPE Redundant Wireless Services zl Module	K.12.43
J8993A, J8994A	Premium Features on Series 3500yl and 5400zl Switches	K.11.33
J8706A	HPE Switch 5400zl 24p Mini-GBIC Module	K.11.33
J8708A	HPE Switch 5400zl 4p 10-GbE CX4 Module	K.11.33
J8694A	HPE Switch 3500yl 2p 10GbE X2 + 2p CX4 Module	K.11.17

For information on networking application compatibility, see the *HPE ArubaOS-Switch Software FeatureSupport 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.

Version 16.02.0033

No enhancements were included in version 16.02.0033.

Version 16.02.0032

No enhancements were included in version 16.02.0032.

Version 16.02.0031

No enhancements were included in version 16.02.0031.

Version 16.02.0030

No enhancements were included in version 16.02.0030.

Version 16.02.0029

No enhancements were included in version 16.02.0029.

Version 16.02.0028

PoE status

A new `Fault` status has been added to event logs and the output of PoE CLI commands to indicate ahardware failure.

Version 16.02.0027

No enhancements were included in version 16.02.0027.

Version 16.02.0026

No enhancements were included in version 16.02.0026.

Version 16.02.0025

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
```

RMON

Support for system buffers to log an RMON event similar to `buffer allocation has reached xx%`, whenever the buffer usage exceeds a certain threshold.

Version 16.02.0024

Version 16.02.0024 was never released.

Version 16.02.0023m

Version 16.02.0023m was never released.

Version 16.02.0022m

No enhancements were included in version 16.02.0022m.

Version 16.02.0021

No enhancements were included in version 16.02.0021.

Version 16.02.0020

No enhancements were included in version 16.02.0020.

Version 16.02.0019

Local User Roles

When this feature is enabled, every authenticated client is associated with a user role (even when authentication fails), which determines the client's network privileges, frequency of re-authentication, VLAN,captive portal profile, rate-limit, and QoS (Quality of Service).

The feature is globally enabled for all authentication methods and does not impact clients connected toports without port-security.

User Roles are locally created in an ArubaOS-Switch-based switch and applied based on a client's MAC Address for Local-MAC-Authentication or via the HPE-User-Role VSA (Vendor Specific Attribute) returned bythe RADIUS server for MAC-Authentication, Web-Authentication, and 802.1X.

Version 16.02.0018

REST ACL Rules

Support for ICMP and IGMP protocols, ToS, precedence, and log options have been added to the REST APIfor ACL rules.

Version 16.02.0017

No enhancements were included in version 16.02.0017.

Version 16.02.0016

IPv6 Neighbor Discovery

Symptom/Scenario: Added support for configuration of Default Router Preference in IPv6 RouterAdvertisement messages using the following CLI command:

```
[no] ipv6 nd ra router-preference {low|medium|high}
```

OpenFlow

Added restriction warning message for trunk interface modifications when in use by OpenFlow:

```
Trunk in use by an OpenFlow instance may not be modified.
```

VLAN

Switch design does not allow a port to be orphaned when it is removed from the port's last assigned VLAN. The port has to be manually re-assigned to any other existing VLAN to make sure the port is always assigned to a VLAN. If removing a port from its last VLAN, the port is now automatically untagged to the DEFAULT VLAN, eliminating the previous 2-step process - move port to another VLAN prior to removing the port's last assigned VLAN.

Version 16.02.0015

Version 16.02.0015 was never released.

Version 16.02.0014

TCP Push Preserve

Starting with this build, the TCP Push Preserve mode is set to DISABLED by default.

The TCP Push Preserve mode determines the queuing of the TCP packets that have the PUSH flag set. Whenthis mode is enabled and the egress queue is full, TCP packets with the PUSH flag set are queued at the head of the ingress queue for egress queue space. This may delay subsequent incoming packets in the same queue and create a head-of-line blocking situation. When this mode is disabled and the egress queueis full, TCP packets with the PUSH flag set are dropped from the head of the ingress queue.

If the current switch TCP Push Preserve mode has been set to DISABLED, it will be preserved as DISABLEDand the corresponding configuration entries will be suppressed. If the current switch TCP PUSH preserve mode has been set to ENABLED, it will be changed to DISABLED and the change will be noted in system event logs as `The tcp-push-preserve feature was disabled. This is a change to default configuration.`

The CLI command `show tcp-push-preserve` indicates the status of TCP push mode ENABLED/DISABLED.CLI command `[no] tcp-push-preserve` changes the status of TCP push mode.

Version 16.02.0013

Version 16.02.0013 was never released.

Version 16.02.0012

No enhancements were included in version 16.02.0012.

Version 16.02.0011

Add MTU to Device Profile

ArubaOS-Switch-based switches support the jumbo frame attribute in device profile. When an Aruba AP isattached to the port, the configured MTU is applied to the port.

The default size of the MTU is 9K. This value is not configurable through device profile context commands. Ifthe user wants to change this value, they manually configure it in the switch global configuration. Users canenable or disable Jumbo frame support through device profile. By default, jumbo frame support is disabled.

If jumbo frame support is already enabled on a VLAN, but disabled in the device profile for the same VLAN,jumbo frame support will remain enabled even if the device profile is active. Non device-profile configuration takes precedence over device profile configuration.

When the user enables jumbo frame support, all the VLANs configured in the device profile will get jumbo frame enabled. All ports belonging to that VLAN can handle packets up to 9k size (default size). This includesports where an Aruba AP is not connected if that port belongs to a VLAN configured in the device profile.

Add 'no CoS' to Device Profile

Class of service (CoS) is applied on the packets received on the port. The default value is “none”. If a user wants to change the CoS configuration, the user can set any CoS value from 0-7. Whenever the configuredvalue is “none,” the switch honors the CoS value of the packet. If the CoS value is set via the Device Profile,the CoS setting on the Device Profile is used instead.

Please note: In the 16.01 release, the CoS value could be set to any value from 0 to 7. From 16.02 onwards,the CoS value can be configured as "none" also.

The commands to set CoS value to "none" are:

```
(config)#device-profile name abc
(device-profile)#no cos
```

Version 16.02.0010

No enhancements were included in version 16.02.0010.

Version 16.02.0009

No enhancements were included in version 16.02.0009.

Version 16.02.0008

Add 'no CoS' to Device Profile

Class of service (CoS) is applied on the packets received on the port. The default value is “none”. If a user wants to change the CoS configuration, the user can set any CoS value from 0-7. Whenever the configuredvalue is “none,” the switch honors the CoS value of the packet. If the CoS value is set via the Device Profile,the CoS setting on the Device Profile is used instead.

Please note: In the 16.01 release, the CoS value could be set to any value from 0 to 7. From 16.02 onwards,the CoS value can be configured as "none" also.

The commands to set CoS value to "none" are:

```
(config)#device-profile name abc
(device-profile)#no cos
```

Instrumentation Enhancements

Provide additional/enhanced information that can assist in diagnostics, monitoring, and troubleshooting ofvarious switch features.

- DT, STP, and LLDP `show tech` enhancements
- Multicast `show tech` enhancements

MAC Authentication Toggle

Port-based MAC authentication allows an infrastructure device to be authenticated with a port-based policy that dictates the distribution switch to open the authenticator port to all clients from the authenticated device. This is similar to the existing port-based 802.1X authentication available on HPE switches, except thatthe new port-based 802.1X authentication can also be statically configured on an authenticator port to be persistent over port toggling and switch reboot, while the existing port-based mode MAC authentication willbe dynamic, triggered by the dynamic policy an authenticated client will receive.

Username VSA support

This feature enables the 'Client Name' field on the switch to be updated with a value configured via the User-Name VSA (Vendor Specific Attribute) returned by the RADIUS server. This improves the data displayed via the Consolidated Client View output generated by the CLI command `show port-access client`, especially when using MAC-Authentication.

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes arelisted 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.

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

Version 16.02.0033

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 16.02.0032

Chassis Manager
CR_0000252317

Symptom: End-devices fail to connect due to inconsistencies in the MAC addresses learned between theInter Switch-Connect (ISC) link and a trunk member link.

Scenario: This issue occurred when the switches were configured with distributed trunk (DT), and one of theDT member switches was upgraded.

Workaround: Use the `clear mac-address` command to clear the incorrect MAC entries in both the DT switches

Distributed Trunking
CR_0000254354

Symptom: The MAC address of a peer is missing in the MAC table even though a packet is received beforethe expiration of the MAC age-timeout interval.

Scenario: This issue occurred when a packet with the same source MAC address was alternatively sent onboth distributed trunk links at an interval close to the MAC age-timeout time.

Workaround:

- Increase the MAC age of the switch to a higher value.
- Configure static MAC addresses.

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.

OSPFv2
CR_0000254760

Symptom: A delay is observed when removing OSPF routes from the link state database.

Scenario: This issue occurred when the switch received an external Link-State Advertisement (LSA) with anage set to `MaxAge 3600` from an OSPF neighbor.

Version 16.02.0031

PoE
CR_0000253001

Symptom: When there are continuous link flaps on the link-to-monitor ports within a fraction of a second,some link-to-disable ports may not come up once the link-to-monitor port stabilizes.

Scenario: The link-to-monitor port used a transceiver connected by fibre and flapped continuously at a highrate.

Workaround:

Use Fault-Finder to disable the link-to-monitor if it is flapping too often. Disable the link-to-disable port andre-enable it to bring it back up.

Version 16.02.0030

BGP
CR_0000252825

Symptom: A switch crashes and displays the following message: `Software exception at bgp_med.c:629 -- in 'eRouteCtrl' …. Routing Stack: Assert Failed`

Scenario: This issue occurred when the maximum prefix for BGP was configured to limit the number ofroutes BGP learns, in an environment with many route flaps.

Workaround: Eliminate the frequent BGP route flaps.

Version 16.02.0029

OSPF
CR_0000249465

Symptom: A switch crashes and displays the following message: `Software exception at ospf2.c --in 'eRouteCtrl' -> Routing Stack: Assert Failed.`

Scenario: This issue is observed when a switch is configured with OSPF and one of the OSPF neighbors is disconnected.

Version 16.02.0028

Distributed Trunking
CR_0000248556

Symptom: Some end devices are not reachable from one of the DT peers.

Scenario: With Distributed Trunking enabled, MAC addresses are learned from the ISC rather than from the downlink connections, causing some end devices to lose connectivity to one of the DT peers.

Workaround: Clear the MAC address table using the `clear mac-address` command.

OSPF
CR_0000250833

Symptom: After a switch reboot, OSPF is stuck in the INIT state.

Scenario: When a switch that is configured with OSPF, but `ip router-id` has not been configured, isrebooted OSPF remains in the INIT state.

Workaround: Configure the router ID manually.

Version 16.02.0027

ARP
CR_0000248143

Symptom: The switch experiences temporary traffic loss.

Scenario: When the switch has a large number of ARP entries and one of the later entries moves from oneport to another, the switch temporarily loses traffic.

Workaround: Reboot the switch.

SNMP
CR_0000248977

Symptom: The SNMP trap is sent with a wrong value.

Scenario: When there is an authentication error, the SNMP trap is sent with an incorrect value.

Version 16.02.0026

Distributed Trunking
CR_0000244370

Symptom: The MAC entry is learned on the ISC in a distributed trunk (DT) and in DT-trunk/DT-LACP in thepeer DT.

Scenario: When configuring the switch-interconnect with the switch receiving continuous unknown SA traffic through the ISC, the MAC entry is learned on the ISC.

Workaround: Use the `clear mac-address` command to clear MAC entries.

CR_0000247258

Symptom: Some MAC addresses are learned on the ISC link as well as on the DT trunk on the peer DTdevice.

Scenario: When a MAC address is learned through the inter-switch (ISC) link while its DT trunk was disabled,the switch fails to age out and remove the respective MAC address from the switch MAC table.

Workaround: Use the `clear mac-address` CLI command to clear MAC entries.

IPv4
CR_0000244916

Symptom: The switch is unable to communicate with any device outside of the VLANs configured on theswitch.

Scenario: When a default gateway is configured and the switch loses power or undergoes a cold/warm reboot, it cannot communicate with any device outside of the VLANs configured when it powers back up.

Workaround: Delete and re-add the default gateway.

IPv6 RA
CR_0000246423

Symptom: The switch fails to forward IPv6 RA packets.

Scenario: When both IGMP and MLD are enabled on an un-authenticated VLAN (unauth-vid), the switch may randomly fail to forward IPv6 RA packets destined to authenticated users on the authenticated VLAN (auth- vid).

Workaround: Disable MLD on the un-authenticated VLAN (unauth-vid).

Logging
CR_0000246621

Symptom: In certain conditions, the switch fails with an error message similar to `NMI event <...> Task='eDevIdle'`.

Scenario: When issuing the CLI command `show logging`, if the switch event log is over 80% full and theswitch CPU is under high utilization, the switch may randomly fail with an error message similar to `NMI event <...> Task='eDevIdle'`.

NTP
CR_0000244733

Symptom: The switch fails to synchronize its time from the NTP Server.

Scenario: When the switch time is manually updated with an offset value of more than 100 secs (+ve)compared with the NTP server time, the switch fails to re-synchronize its time with the NTP server.

Workaround: Disable and re-enable NTP server using the CLI command `[no] ntp enable`.

SNMP
CR_0000246226

Symptom: The switch fails to correctly report the switch ports of some switch module.

Scenario: When querying the SNMP MIB, the switch incorrectly reports the ports of the switch moduleJ8694A as "ZeodotZero" in the output of the SNMP MIB 1.3.6.1.2.1.47.1.1.1.1.3.

Workaround: Use the CLI command `show interfaces brief` to display the details of the ports on theswitch module J8694A.

TELNET
CR_0000244606

Symptom: Telnet/SSH session cannot be established after a period of time.

Scenario: When connecting via telnet/SSH, the switches may report all sessions are in-use (`TELNET from <...> is rejected because maximum session limit is reached`), even though the `show session-list` command shows connected session under maximum supported.

Version 16.02.0025

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 thestatistics 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.

CLI
CR_0000241070

Symptom: The switch displays an incorrect power supply information.

Scenario: When using the J9306A power supply, the incorrect product number is displayed in the output ofthe `show system power-supply` command.

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 highnumber 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 whenthe destination is unknown.

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

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.

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 theoutput 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>`

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_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`.

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 ofdropping the corrupt packets.

Rate Limiting
CR_0000241892

Symptom: Configured broadcast or multicast rate limit affects unicast traffic.

Scenario: When an inbound, physical port-based broadcast or multicast rate-limit is configured with a valueof 100,000 kbps or less, the rate limiting may affect the unicast packets as well.

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 avalid 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.

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 actuallevel 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 opena session.

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

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 switchincorrectly starts and closes a RADIUS Accounting session..

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

Version 16.02.0024

Version 16.02.0024 was never released.

Version 16.02.0023m

Version 16.02.0023m was never released.

Version 16.02.0022m

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`").

CR_0000236646

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

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 duringreboot with an error message similar to `Software exception in ISR at btmDmaApi.c:445 -> ASSERT: No resources available!`

Multicast
CR_0000237850

Symptom/Scenario: The switch is incorrectly flooding MLD reports received with a Well Known MulticastIPv6 address.

SNMP
CR_0000237141

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

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 targetaddress` to display target configured parameters.

SSH
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 issuingthe CLI command `show crypto client-public-key`.

Workaround: Install all SSH public keys with comments section or remove all SSH public keys installedwithout comments before upgrading the switch to a newer OS version.

Version 16.02.0021

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 credentialswith a slight delay.

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

PIM
CR_0000235741

Symptom: Switch may fail to route multicast traffic and RMON message similar to `Failed to allocatenew SW 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 allocatenew SW IP multicast group, table full FIB entry`.

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

PoE
CR_0000230920

Symptom: Different values are displayed for the PSE's allocated power when comparing the output of `showlldp` and `show power <port>`.

Scenario: The issue will trigger if the port is configured to `poe-allocate-by class` after the attached PD sends an LLDP power request.

Workaround: Disable and re-enable the port or reattach the PD after changing the `poe-allocate-byvalue`.

Smart Link
CR_0000235633

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

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

Workaround: Configure Smart Link ports as consecutive ports.

Transceivers
CR_0000234291

Symptom/Scenario: After hot-swapping a 10GbE X2 transceiver, the transceiver is not properly initialized. Itmay experience a link up delay or fail to link.

Workaround: Reload the module after hot-swapping the 10GbE X2 transceiver.

Version 16.02.0020

BGP
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 onthe BGP peer, 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.

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 forthe 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 messagefor 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 withoutSTATS.

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 defaultpriority queue, instead of the remarked priority queue.

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.

CR_0000233729

Symptom: The output of OSPF related commands, such as `show ip ospf [ external-link-state | link-state | statistics ]`, take an extended amount of time to run or display incomplete data.

Scenario: Any show command which includes `show ip ospf [ external-link-state | link-state | statistics ]`, 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 or datacollected regarding OSPF status may be incomplete.

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 secondaryVLAN 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 thenew 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 themonitored MIB objects.

sFlow
CR_0000227597

Symptom: The switch may not create outbound sFlow samples.

Scenario: When flow-control is enabled on any switch interface, the switch may stop sampling egress sFlowtraffic.

Workaround: Disable flow-control on the switch interfaces using the CLI command `no interface <PORT-LIST> flow-control`.

CR_0000228486

Symptom: sFlow displays invalid levels of dropped samples.

Scenario: When using trunk interfaces, sFlow is incorrectly calculating the levels of dropped samplesdisplayed 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.

Transceivers
CR_0000229877

Symptom: The LED for the link state of the dual personality ports does not turn green (ON).

Scenario: After switch boot up with a transceiver inserted in a dual personality port with an active linkpartner connected, the link state LED does not turn green.

Workaround: Remove and reinsert the transceiver to reset the port status.

Version 16.02.0019

No fixes were included in version 16.02.0019.

Version 16.02.0018

BGP
CR_0000229238

Symptom: Switch may crash with a `Restricted Memory Access` or `Misaligned Memory Access` error message.

Scenario: When using non-default administrative distances for BGP routes (for example, `distance bgp <external-distance> <internal-distance>`), in the event of failing over the WAN link, the switch maycrash with a message similar to:

```
Health Monitor: Invalid Instr Misaligned Mem Access <…> Task='InetServer'<…>
```

or

```
Health Monitor: Restr Mem Access <…> Task='eRouteCtrl'<…>
```

Workaround: Use default administrative distances for BGP routes.Example:

The default distance for external routes is 20.

The default distance for internal routes is 200.

CDP
CR_0000228335

Symptom: Switch reports an error message `Module command missing for port or invalid port <TRUNK-NAME>` when a configuration file is restored from backup.

Scenario: When a backup configuration file contains a CDP setting (for example, `no cdp enable <TRUNK-NAME>`) for a trunk port, the switch fails to restore it and reports an error message similar to:

```
line: 6. Module command missing for port or invalid port <TRUNK-NAME>.
Corrupted download file.
```

Device Profile
CR_0000213606

Symptom: Device profile removed and re-applied after a redundancy switchover event.

Scenario: After failing over to standby in an HA (high availability) configuration, the Device Profile isremoved and reapplied to the port. This may result in service interruption on that port.

DHCP Snooping
CR_0000228042

Symptom: An incorrect RMON message is logged when a DHCP RELEASE message is dropped by DHCPSnooping on the switch.

Scenario: If DHCPv4-Snooping and IPv4 routing are enabled when the switch receives a unicast DHCP client message (RELEASE/DECLINE), the switch logs an incorrect RMON message `Attempt to release address <IPv4 address> leased to port <lport_src> detected on port <lport_src>`. However, this switch does not have the lease entry updated in the DHCPv4-Snooping binding state table (BST).

In environments with multiple DHCP servers reachable through different network paths, the message islogged repeatedly.

Fault Finder
CR_0000223670

Symptom: The switch incorrectly allows ports with fault-finder enabled for broadcast-storm to beconfigured for link aggregation.

Scenario: The switch should prevent a port configured for fault-finder alarms to also be configured for link aggregation (trunk). Similarly, in case a port is already in a link aggregation (trunk), the switch should not allowed to configure it with fault-finder alarms for broadcast storm. For such instances, the switch should deny the requested configuration and prompt an error message similar to:

`Fault-finder broadcast-storm configuration cannot be applied to members of a trunk port(s) <PORT-NUM>.`

`Port <PORT-NUM> with fault-finder broadcast-storm configuration cannot be added to a trunk.`

IGMP
CR_0000227470

Symptom: In certain scenarios, the multicast traffic may not flow towards clients and traffic may not beforwarded to IGMP Querier or PIM routers from a non-Querier.

Scenario: In the event that a port, identified as a router-detect port for more than one IGMP-enabled VLAN,stops being the router-detected port for one of the VLANs, the switch may stop forwarding IGMP Membership Reports from Non Querier to Querier device for all IGMP-enable VLANs for which the port is identified as router-detected port. A port may stop being a router-detected port for a VLAN whenever the querier for that VLAN changes and it is no longer detected via respective port, or due to administratively disabling IGMP or PIM on that VLAN, or in case of a DT topology, distributed trunk port membership configuration changes are made.

Workaround: Enable IGMP isolation for un-joined multicast groups using CLI command `igmp filter-unknown-mcast` on global context. This filter limits multicast traffic flooding only on interfaces that contain queriers that are on the same VLAN as the multicast traffic. Enabling of the `igmp filter-unknown-mcast`will consume one filter per IGMP enabled VLAN, impacting the IGMP Group Capacity (i.e. the number of IGMP groups that can be forwarded without flooding). For more information on using the `igmp filter- unknown-mcast` command, see the *ArubaOS-Switch Multicast and Routing Guide* for your switch.

OSPF
CR_0000225246

Symptom: Intermittent connectivity loss to certain IPv6 destinations after an extended period of switchuptime.

Scenario: It is possible after an extended period of uptime for the switch to incorrectly calculate the OSPFv3Link State Advertisement (LSA) Refresh Age time and fail to refresh its self-originated LSAs. As a result, peer switches may incorrectly delete the routes to the prefixes in these LSAs from their Routing Information Base(RIB) for 30 minutes.

Workaround: On the originator switches, enabling `debug ipv6 ospfv3` and then disabling (`no debugipv6 ospfv3`) will trigger an immediate refresh for LSAs which are over the age of 1800 seconds.

MAC Authentication
CR_0000228130

Symptom: Switch may not correctly forward traffic on a successfully authenticated port with mac-authentication.

Scenario: When a switch port is configured for concurrent mac-authentication and 802.1X in client-mode, if this setting is overridden and changed to port-mode through RADIUS VSA 'HP-Port-Auth-Mode-MA' after a

successful client authentication on the port with this RADIUS attribute, the switch may not correctly forward traffic when configured for ingress traffic control.

Example: `aaa port-access <PORT-LIST> controlled-direction in`

Workaround: Disable 802.1X on the port and reconnect or re-authenticate the client with RADIUS VSA 'HP-Port-Auth-Mode-MA' attribute.

Mirroring
CR_0000227861

Symptom: The switch displays incorrect mirroring policy status.

Scenario: The switch displays incorrect 'inactive' status in the output of CLI command `show monitor` whena mirror policy is applied to a VLAN.

Workaround: Execute CLI command `show monitor <mirror-session>` to check the mirror policy status.

PIM
CR_0000192574

Symptom: In certain scenarios, on a switch module where a multicast source is connected, multicast stream interruptions lasting a few seconds and high CPU utilization may occur.

Scenario: In a PIM routing setup, if there is no ARP entry on the switch for the multicast source and in caseof some events or mechanisms (for example, ARP resolution of a new host entry causes the multicast flowsto be restarted), the multicast streams may experience brief interruptions or distortions and high CPU utilization on the switch module where the multicast source is connected.

Workaround: Prevent the multicast flow from being restarted by ensuring a neighbor host entry already exists when the flow is started. For example, pinging the IP address of the source multicast will add an ARPentry for it on the switch, preventing the issue as long as the ARP entry exists on the switch.

CR_0000223590

Symptom: In certain conditions, the switch may crash with an error message similar to `Softwareexception at vls_xmit.c:<...>...`

Scenario: When PIM-DM (Dense Mode) is enabled on multiple VLANs, the switch may crash during periodsof heavy traffic with an error message similar to `Software exception at vls_xmit.c:<...>...`

PoE
CR_0000226003

Symptom: An invalid config entry is added to the switch for a port where some PDs are connected: `power-over-ethernet 0`.

Scenario: When connected PDs request port priority via LLDP MED, such as Cisco 7910G or similar PDs, and poe-lldp-detect is enabled on the respective switch port, an invalid config entry is added to the switch for therespective port `power-over-ethernet 0`. For switches which support stacking, this may cause the switch to crash with a message similar to:

`Health Monitor: Read Error Restr Mem Access <…> Task='mPoeMgrCtl' <…>`

Workaround: Disable `poe-lldp-detect` on the port where the respective PD is connected to clean up the invalid configuration entry.

QoS
CR_0000227806

Symptom: The switch may crash with an error message similar to `Software exception in ISR at btmDmaApi.c <...> No resources available!`

Scenario: When QoS for IP protocol is enabled and IPv6 traffic such as DHCP requests or IPv6 multicast is running on the network, the switch may crash with an error message similar to `Software exception inISR at btmDmaApi.c <...> No resources available!`

Workaround: Disable QoS for IP protocol.

Routing
CR_0000223965

Symptom: Default route is not listed in the output of CLI command `show ip route`.

Scenario: When a VLAN interface is configured as the next-hop for the default static route, the route entry isnot displayed in the output of the CLI command `show ip route`, while the static route counter is incremented in the output of the CLI command `show ip route summary`.

Spanning Tree
CR_0000227215

Symptom: Incorrect VLAN ID is displayed in the output of CLI command `display stp region-configuration`.

Scenario: A 4-digit VLAN ID number is truncated to 3 digits in the output of CLI command `display stp region-configuration`.

Example: Correct VLAN ID using `show spanning-tree mst-config`:

```
Instance ID Mapped VLANs
  -------------- ---------------------------------------------------------------------------
  1              2,6-8,10-14,20-22,1022,1029,1035
```

Example: Truncated VLAN ID using `display stp region-configuration`:

```
Instance      Vlans Mapped
  1            2, 6 to 8, 10 to 14, 20 to 22, 102, 102, 103
```

Workaround: Use CLI command `show spanning-tree mst-config` to get the correct VLAN IDs mappedto the Spanning Tree instance.

Syslog
CR_0000210928

Symptom: Syslog messages do not contain the configured source IP address.

Scenario: When a source IP address or interface is configured for syslog protocol (`ip source-interface syslog {<IP-ADDR> | vlan <VLAN-ID> | loopback <LOOPBACK-ID>}`), the syslog message always contains the IP address of the VLAN the syslog is sourced from, instead of the configured source IP address,VLAN or loopback interface.

Virus Throttling
CR_0000228950

Symptom: An invalid message is displayed when configuring connection-rate-filter on a static LACP trunkinterface.

Scenario: When a connection-rate-filter is applied to a static LACP trunk interface, although the configuration is supported and applied successfully to the trunk interface, the switch displays a misleading error message similar to `LACP has been disabled on CRF enabled port(s).`

Web UI
CR_0000227777

Symptom: Port mode setting may be incorrectly shown in the VLAN Properties section of the VLANManagement web page.

Scenario: When a port is selected in the VLAN Properties section of the VLAN Management web page, the"Mode for selected ports" may be different from what is displayed in the output of CLI command `show vlan <VLAN-ID>`.

Workaround: Use CLI command `show vlan <VLAN-ID>` to obtain the configured port mode.

Version 16.02.0017

OSPF
CR_0000225246

Symptom: Intermittent connectivity loss to certain IPv6 destinations after an extended period of switchuptime.

Scenario: It is possible after an extended period of uptime for the switch to incorrectly calculate the OSPFv3Link State Advertisement (LSA) Refresh Age time and fail to refresh its self-originated LSAs. As a result, peer switches may incorrectly delete the routes to the prefixes in these LSAs from their Routing Information Base(RIB) for 30 minutes.

Workaround: On the originator switches, enabling `debug ipv6 ospfv3` and then disabling (`no debugipv6 ospfv3`) will trigger an immediate refresh for LSAs which are over the age of 1800 seconds.

PoE
CR_0000228643

Symptom: The switch may randomly start removing and reapplying power to multiple connected PoweredDevices (PDs).

Scenario: While there is still power available in the switch power budget (`show power-over-ethernet`),the switch may fail to allocate sufficient power for multiple PDs connected to v1 zl switch modules (J8702Aand J8705A), 3500 switches (J9471A and J9473A) and 3500yl switches (J8692A and J8693A). This causes connected PDs to repeatedly power cycle. The switch will log a repetitive sequence of event messages similar to:

```
00565 ports: port <port_num> PD Removed.
00560 ports: port <port_num> PD Detected.
00566 ports: port <port_num> PD Denied power due to insufficient power allocation.
00560 ports: port <port_num> PD Detected.
00561 ports: port <port_num> Applying Power to PD.
```

Routing
CR_0000228710

Symptom: In certain scenarios, the switch may have connectivity issues to certain destinations or induce routing loops in the network.

Scenario: The switch may incorrectly process certain routes in the routing table and erroneously chooseless specific routes over more specific ones. These routes will remain in the routing table until they are flushed. This behavior may cause routing loops to occur, inability to reach the default gateway, or other similar routing symptoms that could vary by routing protocol. This condition may be exacerbated by thenumber of routes being learned within a short time.

Version 16.02.0016

Banner
CR_0000225460

Symptom: SNMPv3 get request on the switch login banner SNMP OID fails with `tooBig` error message.

Scenario: When switch post-login banner or MOTD banner is configured with more than 1300 characters,running an SNMPv3 get request on the corresponding banner SNMP OID will fail with the error message `Reason:[tooBig].`

Workaround: Use SNMPv2 get request on SNMP banner OID when the configured login banner size islarger than 1300 characters.

Cable Diagnostic
CR_0000222089

Symptom: Non-support for cable diagnostic tests is not indicated prior to executing the tests.

Scenario: When executing the CLI command `test cable-diagnostics <PORT-LIST>`, on a switch port that does not support this feature, the following execution warning message is displayed for non-supportedports:

```
This command will cause a loss of link on all tested ports and will take several
seconds per port to complete. Use the 'show cable-diagnostics' command to view the
results. Continue (y/n)? Y.
```

The non-support for such test is indicated only when displaying the test results using CLI command `'show cable-diagnostics' command'`, in a report message such as `Port <port-number> does not support cable diagnostics.`

DHCP
CR_0000222120

Symptom: The switch DHCP server may delay honoring IP address renewal requests.

Scenario: When a client which acquired an IP address from the switch DHCP server is roaming to a differentVLAN also managed by the switch DHCP server, a fresh new DHCP client request process is initiated in placeof the DHCP renewal request process, resulting in a longer delay for the DHCP client to acquire the new IP address.

Workaround: Using an external DHCP server may help resolve the delay in DHCP client IP renewal whenroaming from one VLAN to another.

DHCP Server
CR_0000216603

Symptom: DHCP clients are not able to obtain IP addresses from the switch's locally configured DHCPserver address pool.

Scenario: When the default route (0.0.0.0/0) is configured with a VLAN as the next hop, the DHCP requestpackets are being dropped and the DHCP clients are not able to obtain IP address from the switch DHCP server.

Workaround: Configure the default route's next hop value with an IP address instead of a VLAN.

DHCP Snooping
CR_0000218841

Symptom: The DHCP snooping bindings information may not be properly updated.

Scenario: After a boot event in a multi-management configuration, such as redundant management module or stack configuration, the DHCP snooping lease binding from a TFTP/SFTP stored database may fail to be updated.

Workaround: Disable/enable DHCP snooping globally after the config synchronization with standby iscompleted.

Event Log
CR_0000218695

Symptom: Incorrect message and assigned event class of the following error message `Failed toallocate new HW IP multicast address, table full FIB entry`.

Scenario: The following error message `Failed to allocate new HW IP multicast address, table full FIB entry` is incorrectly classified as "warning" class instead of "informational" class.

Workaround: This event message is for informational purposes whenever the switch is retrying to allocateFIB entries.

CR_0000225392

Symptom: The proper event log message is not generated when a port is blocked due to a link failuredetection protocol.

Scenario: When a port is configured for Device Link Detection Protocol (DLDP) or Uni-directional Link Detection (UDLD) and a link failure is detected, the switch fails to log corresponding event log messagessimilar to:

`00435 ports: port <NUM> is Blocked by DLDP`

`00435 ports: port <NUM> is Blocked by UDLD`

OpenFlow
CR_0000219687

Symptom: OpenFlow fails to authenticate a client with a DHCP-assigned IP address.

Scenario: OpenFlow fails to authenticate a client with a DHCP-assigned IP address, when the DHCP clientand the DHCP server are connected on different OpenFlow VLANs with IP routing enabled.

Workaround: Configure DHCP server on a non-OpenFlow VLAN.

PIM
CR_0000215604

Symptom: Distortion or pixelation in multicast video stream or multicast stream continuity errors arereported by multicast monitoring tools.

Scenario: When a PIM enabled topology with multiple join/leave for same group are processed for multiple VLANs, the multicast video stream may experience distortion or pixelation or multicast stream errors may be reported in some multicast monitoring tools.

PoE
CR_0000207335

Symptom: Power-enabled devices may randomly encounter a brief power interruption.

Scenario: When connected to a J8702A or J8705A switch module or to a J9471A or J9473A switch, PDs may experience brief power interruptions. The power is not removed from the PD, but the switch will briefly powercycle the PD.

QinQ
CR_0000225416

Symptom: Switch fails to restore configuration from backup.

Scenario: Switch configuration with Q-in-Q cannot be restored from a backup file. The file transfer will failand the switch will return an error message similar to:

```
line: 15. Cannot configure qinq port-type for cvlan ports.

Corrupted download file.
```

Workaround: Remove Q-in-Q related configuration from the backup file before restoring it, then afterwards apply the respective Q-in-Q configuration from the CLI command.

SNMP
CR_0000217437

Symptom: Switch does not report the information regarding IPv6 loopback interface reported in MIB object ipAddressIfIndex.

Scenario: After an IPv6 link-local address is configured on a VLAN, the switch no longer reports the information regarding IPv6 loopback interface reported in MIB object ipAddressIfIndex when executing CLIcommand `walkMIB ipAddressIfIndex`.

Spanning Tree
CR_0000201299

Symptom: A switch configured with RPVST may crash with an error message similar to `Softwareexception at bttfMsgSysDrv.c <...> -- in 'mPvstSlvCtrl' <...>`.

Scenario: When disabling Spanning Tree on a switch that is part of RPVST topology, an external loop may be created. As a result, a broadcast of RPVST BPDUs may be received by the switch, potentially leading to a crash with an error message similar to `Software exception at bttfMsgSysDrv.c <...> -- in 'mPvstSlvCtrl' <...> ASSERT: No resources available!`

Workaround: Make sure that no external loops are created when disabling Spanning Tree on any switchthat is part of an RPVST topology.

CR_0000217382

Symptom: Switch ports enabled for BPDU protection are not properly flagged as administratively down in `show interface brief` output when BPDU traffic is detected.

Scenario: When BPDU traffic is detected on a BPDU protected port, the port is being operationally broughtdown (logically disabled) due to BPDU detection, although it is still being maintained enabled for administrative purposes in the output of CLI command `show interface brief`. Administrative status of the port is mainly intended to be changed by manually enabling/disabling the port from CLI command `interface <PORT-LIST> enable | disable`.

```
 Port       Type |   Alert     Enabled Status  Mode       Mode     Ctrl
------- ---------- + ---------- --------- -------- ---------- ------ ------
  1     10/100TX |   No          Yes     Down    100FDx                  MDI         off
```

The BPDU protected port is operationally disabled when BPDU traffic is detected and only its administrativestate is enabled.

```
ifAdminStatus.1 = 1     (up)
ifOperStatus.1 = 2      (down)
```

Terminal
CR_0000223941

Symptom: The terminal command line is not working properly after terminating a session to the switch.

Scenario: After a VT100 terminal session to the switch is terminated, the terminal line wrap-around configuration is disabled.

Workaround: Re-enable "line-wrap" mode via SNMP command `setmib hpicfPrivateTermLineWrap.0 -i 6` followed by configuration save and reboot.

Trunking
CR_0000211583

Symptom: In a certain scenario, the switch allows to create a trunk interface with more than a maximum of8 ports.

Scenario: When a fast copy and paste operation with multiple port addition entries to the same trunk interface is used to create a trunk interface, more than the maximum 8 allowed ports can be added to the trunk. Once such invalid trunk interface is created, no other changes to the trunk interface are allowed fromCLI.

Example: Copy & Paste from text file:

trunk 1-4 trk1

trunk 5-9 trk1

Workaround: To avoid triggering, do not use a fast copy and paste function to configure the trunk group. Once triggered, use the Menu interface to remove additional ports exceeding the maximum of 8 from the invalid trunk interface.

Version 16.02.0015

Version 16.02.0015 was never released.

Version 16.02.0014

Authorization
CR_0000221546

Symptom: When executing unauthorized commands, the switch may fail to include a blank line beforeprinting the error message `Not authorized to run this command`.

Scenario: When the switch is configured for TACACS+ command authorization and an unauthorized command is executed, the switch may fail to include a blank line before printing the error message `Not authorized to run this command`. This may cause some applications, such as IMC, to misunderstand the message.

Console
CR_0000206708

Symptom: Management access to the switch through SSH, telnet or console may fail with an error messagesimilar to `Connection closed by remote host`.

Scenario: New sessions may fail to be established after previous sessions are closed due to inactivity timeout when using certain client applications, such as MobaXterm, for management access to the switchthrough SSH, telnet or console.

Workaround: Rebooting the switch will clear the locked sessions. Alternatively, you can disable the inactivitytimer using the CLI command `console inactivity-timer 0`. Once the inactivity timer is disabled, you must log out of each session to properly close the connection.

MAC Authentication
CR_0000210511

Symptom: Switch ports may get into an endless MAC authentication cycle preventing re-authentication.

Scenario: When a switch port is configured for both 802.1X and mac-authentication, during the re-authentication process due to reauth-period expiry, the port may not be able to complete the re- authentication process and get into a MAC authentication loop.

Workaround: Disabling and re-enabling the affected port via CLI command `interface <port-num> enable | disable` should clear the problem.

mDNS
CR_0000216815

Symptom: Switch may run out of memory and crash when receiving many multicast DNS packets.

Scenario: When receiving multicast DNS packets with ACL filter applied to the VLAN, the switch may crash due to running out of heap memory.

OpenFlow
CR_0000202097

Symptom: The OpenFlow rule duration may show invalid values.

Scenario: The OpenFlow rule duration may show invalid values in the output of CLI command `show openflow instance <instance-name-str> flows`, after the system time is updated following a switch boot.

Workaround: Toggle OpenFlow state on the switch (Disable/Enable).

CR_0000219033

Symptom: OpenFlow match on destination mac-groups does not work.

Scenario: OpenFlow instances with destination mac-grouping enabled are not correctly matched todestination mac-groups.

OSPF
CR_0000204189

Symptom: Unable to establish OSPF adjacency when jumbo frames are enabled on a VLAN.

Scenario: When jumbo frames are enabled, the switch is unable to form OSPF adjacencies on link connections between v1 switch modules or 3500yl switches and v2/v3 switch modules or 3800/3810 switches.

Workaround: Disable jumbo frames support on such links. Alternatively, avoid using v1 switch module or3500yl switch links when OSPF is needed with jumbo frames enabled.

PBR
CR_0000216797

Symptom: PBR policies counters are not cleared.

Scenario: CLI command `clear statistics policy <policy-id>` does not clear the counters for PBR policies.

SSH

CR_0000201108

Symptom: Switch configured with DSA key refuses SSH connections.

Scenario: When the switch is configured with host DSA public key, SSH connection from client using thegenerated public-key in switch cannot be established.

Workaround: Configure switch with host RSA public-key for SSH connections.

CR_0000217201

Symptom: The SSH server cannot be bound to well-known port numbers ranging from 0 to 1023.

Scenario: When using the CLI command `ip ssh port <port-num>`, the switch does not allow the SSH server to be configured to listen to well-known or system ports ranging from 0 to 1023. The switch displaysthe error message `Cannot bind reserved TCP port <port-num>`, except when using `"default"` and `22` as the *<port-num>*.

Workaround: Configure the SSH server to listen for SSH connections on ports `"default"`, `22`, or portsgreater than 1023.

Switch Module

CR_0000202463

Symptom: Switch Module may crash with an error message similar to `Too Many MAC [6] Interrupts`.

Scenario: Rarely, environment issues (for example, low power rails) might trigger a v2 switch module crashwith an error message similar to `Too Many MAC [6] Interrupts`.

CR_0000213653

Symptom: Incorrect event log warning message is displayed while replacing a switch module with adifferent type of module.

Scenario: When a v1 or v2 switch module is replaced/hot-swapped with a different module type, the switch might log an event message similar to `Module not supported by this software version` instead of `Module/Configuration mismatch`.

Workaround: Before inserting a different type of module, remove the previous module's configuration viaCLI command `no module <module-num>`. This is the recommended method to replace a module with a different type and will avoid the switch warning message.

CR_0000216853

Symptom: Lower chassis switch modules may not power up when additional PSU is added to the switchchassis.

Scenario: When 8212 or 5412 switch chassis is powered up with 1 PSU providing power and if a second or more PSU power is subsequently added past boot sequence, the lower switch modules in slots G through Ldo not power up, show up in switch logs or are listed in the output of CLI command `show modules`.

Workaround: Reboot the switch with at least 2 PSU's providing power when switch modules are present inslots G through L.

CR_0000216989

Symptom: Switch performance degrades when using ports 4, 5, or 6 on the J9538A switch module (HPE 8-port 10GbE SFP+ v2 zl Module).

Scenario: When data traffic with the TCP push flag is passed through ports 4, 5, or 6 of the J9538A switch module and the switch TCP Push Preserve feature is enabled, a head-of-line blocking situation may occureleading to switch performance degradation, latency, or connectivity issues.

Workaround: Disabling the TCP push function using the CLI command `no tcp-push-preserve` may improve the situation. To verify the TCP Push Preserve feature status on the switch, use the CLI command `show tcp-push-preserve`. If the TCP Push Preserve feature is needed, avoid sending the traffic with TCP push flag through ports 4, 5, or 6 of the J9538A switch module.

Version 16.02.0013

Version 16.02.0013 was never released.

Version 16.02.0012

IGMP
CR_0000216285

Symptom: Losing management access to the switch.

Scenario: When the switch receives IGMPv3 query packets with the source IP address 0.0.0.0 or IGMPv3 query packet without Router Alert option, it may deem the switch unable to resolve the MAC address for thedefault gateway.

Workaround: Rebooting the switch or failing over to standby (where applicable) can temporarily restoreconnectivity to the switch.

Version 16.02.0011

CLI
CR_0000201228

Symptom: Management module status timestamp is incorrectly displayed in the output of CLI command `show redundancy detail`.

Scenario: On a switch chassis with support for management module, the "Module Up Since" and "State Since" timestamp values displayed in the output of CLI command `show redundancy detail` are incorrectfor the corresponding reported module state change.

Distributed Trunking
CR_0000200355

Symptom: In a distributed trunking (DT) topology, a DT switch might start flooding VLAN traffic destined toits peer DT switch.

Scenario: In a distributed trunking topology, if the peer DT mac-address is not learned on a DT switch and ifit receives VLAN traffic, it may flood that traffic.

Workaround: Sending a ping from DT to its peer DT on that VLAN, forces mac-address learning and VLANtraffic will be forwarded until the MAC entry expires.

CR_0000211345

Symptom: A switch configured as a Distributed Trunking Device may start flooding traffic.

Scenario: When the forward traffic and the return traffic follows a different path in a DT setup, the pairedDT switches may get out of sync and start flooding traffic until the switches are re-synchronized.

Workaround: Traffic flooding is intermittent and resolves on its own once paired DT switches are re-synchronized.

GVRP
CR_0000204332

Symptom: The detailed information about mac-addresses dynamically learned by the switch is not correctly displayed in the output of the CLI command `show mac-address <mac-address>`.

Scenario: When mac-addresses are learned from a VLAN that was dynamically configured using GVRP, theCLI command `show mac-address <mac-address>` does not display any detailed information.

Workaround: Use the CLI command `show mac-address`.

IP Tunnels
CR_0000212791

Symptom: In certain conditions, tunnel interface activation may fail.

Scenario: When the switch IP address configuration is modified after a tunnel interface was alreadyconfigured on the switch, the tunnel activation may fail.

Workaround: Delete then re-create the tunnel interface after modifying the switch IP address.

LEDs
CR_0000197148

Symptom: Port status LED lights up even after disabling the port administratively.

Scenario: On a 3500 switch with no other devices connected, when a port is administratively disabled usingthe CLI command `interface <PORT-LIST> disable` or from the menu interface, the LED status stays turned on even after a switch reboot.

Workaround: After the switch reboot, disable the port once again to turn off the port status LED.

MAC Authentication
CR_0000201029

Symptom: Switch may crash with a message similar to `Health Monitor: Misaligned Mem Access <...> Task='eDrvPoll' <...>`, when data cable is plugged into a port.

Scenario: Switch may crash with a message similar to `Health Monitor: Misaligned Mem Access <...> Task='eDrvPoll' <...>`, when data cable is plugged into a port configured with mac-authentication and spanning-tree is enabled on the switch.

Workaround: Administratively disable the port and re-enable after the data cable is plugged into the port,disable the port using CLI command `interface <port-num> disable | enable`.

OpenFlow
CR_0000193376

Symptom: Switch may not be able to connect to the SDN controller.

Scenario: After a reboot of another switch upstream on the path to the SDN controller, the switch may beunable to connect to the SDN controller.

Workaround: Reboot the switch.

Packet Buffers
CR_0000213551

Symptom: Switch intermittently drops multicast and broadcast traffic passed through the J9538A switchmodule.

Scenario: Using 1G SFP transceivers in ports 4, 5, or 6 of a J9538A switch module might cause intermittentpacket loss.

Workaround: Use 10G SFP+ transceivers on ports 4, 5, or 6 on the J9538A switch module or use the otherports (1, 2, 3, 7, or 8).

Stacking
CR_0000213756

Symptom: IP Switch Stack Management may not work properly.

Scenario: When the configured primary VLAN is different than the factory-default VLAN (DEFAULT_VLAN), IPStack Management may not work properly.

Workaround: Configure the factory-default VLAN DEFAULT_VLAN as the primary VLAN and add allcandidate switches on the same stack to DEFAULT_VLAN.

Temperature
CR_0000211349

Symptom/Scenario: Switch intermittently displays `hpSystemAirCurrentTemp.0` as zero degrees Celsius.

Transceivers
CR_0000210703

Symptom: The OID entLastChangeTime value is not correctly updated.

Scenario: When a transceiver is inserted, moved or hotswapped, the switch does not correctly update thevalue reported in entLastChangeTime OID.

Version 16.02.0010

No fixes were included in version 16.02.0010.

Version 16.02.0009

Trunking
CR_0000214638

Symptom: LACP link failure recovery might result in traffic outage.

Scenario: A connection outage to the peer device might be observed during the recovery from a link failureon a port member of an LACP trunk, when the switch's LACP links are connected to a non-ArubaOS-Switch- based switch on which LACP links are configured in Active/Standby mode.

Version 16.02.0008

Authentication
CR_0000193385

Symptom: RADIUS authenticated users might have switch authentication issues.

Scenario: When RADIUS users are authenticated using user profiles with HP-Privilege-Level VSA configuredwith values other than HP predefined privilege levels, switch authentication might fail.

Workaround: Use one of the following workarounds:

- Configure RADIUS user profile with HP-Privilege-Level = 35 for Manager privilege level, or HP-Privilege-Level = 21 for Operator privilege level.
- Configure RADIUS user profile with HP-Command-String and HP-Command-Exception attributes to definethe privilege level.
- Use RBAC group ID configuration on the switch to define authentication privilege level - group ID 21(Operator) and group ID 35(Manager).

Banner
CR_0000190968

Symptom: Copying a configuration file with a banner text containing the quote (") character could cause acrash.

Scenario: Copying a configuration file with a banner message containing the quote (") character spanning across multiple lines, might cause a crash with an error message similar to `Health Monitor: Restr MemAccess <...>`.

Workaround: Use short banner text or replace quote (") characters in the banner text message.

Captive portal using Aruba CPPM
CR_0000192066

Symptom: When working with Captive Portal feature with URL hash key enabled, if the Captive-Portal-URL attribute in CPPM includes any uppercase letter in the URL and the client attempts to browse, the redirection to the Captive Portal Login page works but an error is displayed preventing the user from entering credentials in the web page.

Scenario: Enter any uppercase letter on the Captive-Portal-URL attribute in CPPM.

Workaround: In CPPM, when configuring the Captive Portal profile attribute to redirect traffic to ClearPass,enter the value for the Captive-Portal-URL attribute in lowercase only.

CLI
CR_0000157943

Symptom: When copy command-output `show tech all tftp <server addr> <file name>` command is executed, the switch might crash.

Scenario: The switch might crash when IPv6 route entries in the system grows to a huge value.

Counters
CR_0000189924

Symptom: Incorrect values are displayed for transmit and receive counters of an interface.

Scenario: The Broadcast and Multicast transmit and receive counter values from the CLI output of the `showint <ports>` command are incorrect.

DHCP
CR_0000191729

Symptom: A switch acting as a DHCP Relay agent drops any DHCPINFORM packets with a TTL value set to 1.

Scenario: DHCPINFORM packets received with a TTL value of 1 are dropped by the DHCP Relay agent, so theDHCP client cannot acquire an IP address from the DHCP server.

Workaround: Configure the DHCP client network interface to use TTL values greater than 1.

DNS
CR_0000190533

Symptom: IPv6 Router Advertisements do not always announce the DNSSL properly.

Scenario: Updates or changes to the domain name are not dynamically updated in RA advertisements.

Workaround: Execute `write mem` and reboot after updating the domain name in the switch config file.

Event Log
CR_0000192766

Symptom: When MAC Tracker table reaches 10,000 allocated entries, the following message is logged to the event log system: `IpAddrMgr: Failed to allocate new L2 MAC tracker, L3 FIB may ignore L2 MAC moves FIB entry`.

Scenario: When MAC Tracker table allocated entries reaches 10,000, the aged or stale entries are overwritten, so there is no operational issue. For informational purposes, the switch logs an event message,which is flagged as warning rather than a debug message.

File Transfer
CR_0000192894

Symptom: Setting the session idle-timeout to lower settings can cause a file transfer to hang indefinitely.

Scenario: When session idle-timeout is configured to lower values, a file transfer exceeding the configuredidle-timeout may hang indefinitely when executed from a remote session to the switch.

Workaround: Configure session idle-timeout value to a higher value to allow file transfers to completebefore the idle timer expires.

IGMP
CR_0000189793

Symptom: Deleting and reconfiguring an IGMP or PIM VLAN interface might not forward multicast trafficcorrectly.

Scenario: Enable IGMP or PIM on a VLAN. Delete VLAN from the configuration and re-configure the VLAN.

Workaround: Disable IGMP or PIM before deleting and reconfiguring VLAN interface.

IPv6 ND
CR_0000191216

Symptom: Non-human readable characters might appear in the output of CLI command `show running-config`.

Scenario: In a VFS stacking configuration, when LED savepower is turned on for all modules using the CLIcommand `savepower led all`, non-human readable characters might appear in the output of the CLI command `show running-config`.

Workaround: Use CLI command `save power led <slot-list>` with SLOT-ID or range options.

MAC-Based VLANs
CR_0000183936

Symptom: If a MAC is configured as a static-mac address on the switch, the same MAC might be detected asrogue and may not be blocked by the rogue-ap-isolation feature.

Scenario: After configuring a static mac with the command `static-mac <mac-address> vlan <y> interface <z>` and enabling the rogue-ap-isolation feature using the `rogue-ap-isolation enable`

command, the MAC is not blocked by the rogue-ap-isolation feature due to conflict and the following RMON message is displayed:

`Blocking rogue device <mac-address> failed as it conflicts with either lockout MAC or static MAC configuration.`

Workaround: There are two workarounds for this issue:

1. Enable rogue-ap-isolation feature before configuring the static-mac address for that MAC to ensure that itis blocked.
2. Remove the static-mac configuration for the *<mac-address>* to ensure that it is blocked by rogue-ap-isolation.

Menu
CR_0000198649

Symptom: An incorrect maximum number of supported authorized managers is specified in the help textmessage of the Menu interface.

Scenario: The message text of the IP Authorized Managers Help Screen Menu interface states `A maximum of 10 addresses is supported`. The switch allows the configuration of up to 100 authorized managers.

Workaround: Use the CLI command `ip authorized-managers help` to determine the maximum number of authorized managers that can be configured on the switch.

NTP
CR_0000193443

Symptom: NTP debug configuration is incorrectly displayed in the output of the CLI command `show debug`.

Scenario: The NTP debug options enabled using the CLI command `debug NTP <packet | event>` arenot correctly displayed in the output of the CLI command `show debug`.

OOBM
CR_0000194019

Symptom: A switch with OOBM port may experience an NMI crash and reboot.

Scenario: When there is a broadcast storm on the OOBM network, the switch might encounter a crash withan error message similar to `NMI event <...> Task='tDevPollRx' <...>`.

Workaround: Avoid broadcast storms on the OOBM network.

OSPF
CR_0000189794

Symptom: Configuring a VLAN with IPv6 OSPF3 passive mode, incorrectly applies the configuration to allVLANs.

Scenario: Enable a VLAN with IPv6 OSPF3 passive mode and observe the output of CLI command `show run vlan` shows IPv6 OSPF3 passive mode applied to all VLAN interfaces.

Workaround: If passive mode is set after creating all VLANs, then all VLANs will be set as passive. To avoid this, create passive VLANs first, then create remaining VLANs.

PIM
CR_0000200178

Symptom: Switch might crash with an error message similar to `Health Monitor: Invalid Instr Misaligned Mem Access <...> Task='mSnmpCtrl' <...>` while displaying learned multicast routes.

Scenario: When PIM is enabled on a VLAN and a large number of routes exist in the routing table (4000+), the switch might crash with an error message similar to `Health Monitor: Invalid Instr MisalignedMem Access <...> Task='mSnmpCtrl' <...>` while displaying IP multicast routing table content using the CLI command `show ip mroute`.

PoE
CR_0000175016

Symptom: Power-enabled devices may randomly encounter a brief power interruption.

Scenario: Power-enabled devices may randomly encounter a brief power interruption when connected toV1 switch modules, such as J8702A, J8705A and an event message similar to `PD Removed` is registered.

Workaround: The power-enabled device reboots and comes back up on its own.

SNMP
CR_0000192914

Symptom: SNMP community access violation warning messages are not always reported in the switch eventlog.

Scenario: When Authorized IP Managers are configured on the switch, SNMP access from unauthorized management stations with correct community names are not reported in the switch event log.

Spanning Tree
CR_0000194044

Symptom: Traffic may be disrupted in an RPVST topology when VLAN configuration changes.

Scenario: In an RPVST topology, when there are ports configured for BPDU filter, PVST filter, and root guard, removing any VLAN from the switch configuration might cause traffic disruption in the network.

Workaround: Reapply all the configurations related to the root-guard, tcn-guard, bpdu-filter, and pvst-filter after removing VLAN.

Supportability
CR_0000183389

Symptom: CLI command `show tech all` may fail to run properly.

Scenario: CLI command `show tech all` may not complete or execute properly.

CR_0000200816

Symptom: In some cases, the switch might halt or crash when executing the CLI command `show techall`.

Scenario: A switch hang or crash might be encountered during execution of the CLI command `show tech all` while the switch is configured with policies applied to interfaces with the CLI command `policy {qos|pbr|mirror|zone} <policy-name>...`. The issue is intermittent and not every execution of `show techall` causes a crash.

Workaround: Avoid executing `show tech all` if policies are applied to switch interfaces, or remove thepolicies from interfaces before executing `show tech all`.

Switch Module
CR_0000192470

Symptom: After a period of uptime, switch blades might reset with an error message similar to `Software exception in ISR at interrupts_mac.c <...> -> Excessive MAC Interrupts at chipPort <...>`.

Scenario: When there is an excessive amount of received packets with shorter preamble than the industrystandard, HPE switch blades might reset due to excessive interrupt handling.

Workaround: Reconfigure the peer device to use a long preamble.

Time
CR_0000197232

Symptom: In a rare condition, the switch might crash with an error message similar to `NMI event <...> Task='mCronDaemon' <...>`.

Scenario: In a rare condition, when the switch time is updated from remote time servers, the switch mightcrash with an error message similar to `NMI event <...> Task='mCronDaemon' <...>`.

VRRP
CR_0000192567

Symptom: When a VLAN is configured with multiple VRRP virtual IP addresses, ping to VRRP virtual IPaddress might fail.

Scenario: When the virtual IP address of a VLAN is multi-network configured, the virtual-ip-ping commandfails when sent from one subnet to another.

Workaround: Configure the VLAN designated for VRRP virtual ping with only one IP address.

CR_0000197506

Symptom: VRRPv3 traps are not correctly generated for new master change events.

Scenario: When VRRP traps are enabled using the CLI command `router vrrp traps` and VRRPv3 is configured, the router switch sends the wrong trap. 'vrrpTrapNewMaster,' instead of 'vrrpv3NewMaster'.

Upgrade information

Upgrading restrictions and guidelines

K.16.02.0032 uses BootROM K.15.30. If your switch has an older version of BootROM, the BootROM will be 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. Afterthe 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.

Table 1: *BootROM updates*

If your software version is:	Your next step should be:
K.11.11 through K.12.29 (BootROM K.11.00 - K.11.03)	Update and reload into software version K.12.31 or K.12.62
K.12.31 through K.13.55 (BootROM K.12.12 - K.12.14)	Update and reload into software version K.13.58 or K.13.68
K.13.58 or newer (BootROM K.12.17 or newer; use `show flash` command)	Update directly into software version K.16.02.0032 (BootROM K.15.30)

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 *ArubaOS-Switch Basic Operations Guide Version 16.02*.

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/**.

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 viaemail.