KA.16.02.0021 Release Notes

aruba

a Hewlett Packard
Enterprise company

Description

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

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

Product series supported by this software:

Aruba 3800 Switch Series

Important information

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

To enable ZTP for Activate in switches that are updated to 16.02.0010 or later from previous versions, the switches have to be reset to factory default (see the *Installation and Getting Started Guide* for your switch for details on resetting the switch). For switches that come from the factory with 16.02.0012 or later installed, ZTP for Activate is enabled by default. To disable ZTP for Activate, see the *Management and Configuration Guide* for your switch.

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.16.02.0008 or later to a version earlier than 16.01 of the firmware.

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	Based on	Remarks
KA.16.02.0021	2017-09-15	KA.16.02.0020	Released, fully supported, and posted on the web.
KA.16.02.0020	2017-07-07	KA.16.02.0019	Released, fully supported, and posted on the web.
KA.16.02.0019	n/a	KA.16.02.0018	Never released.
KA.16.02.0018	2017-03-31	KA.16.02.0017	Released, fully supported, and posted on the web.
KA.16.02.0017	n/a	KA.16.02.0016	Never released.
KA.16.02.0016	2017-01-27	KA.16.02.0015	Released, fully supported, and posted on the web.

Table Continued

Version number	Release date	Based on	Remarks
KA.16.02.0015	n/a	KA.16.02.0014	Never released.
KA.16.02.0014	2016-10-28	KA.16.02.0013	Released, fully supported, and posted on the web.
KA.16.02.0013	n/a	KA.16.02.0012	Never released.
KA.16.02.0012	2016-08-31	KA.16.02.0011	Released, fully supported, and posted on the web.
KA.16.02.0011	2016-08-24	KA.16.02.0010	Released, fully supported, and posted on the web.
KA.16.02.0010	2016-08-11	KA.16.02.0009	Released, fully supported, and posted on the web.
KA.16.02.0009	2016-08-02	KA.16.02.0008	Released, fully supported, but never posted on the web.
KA.16.02.0008	2016-07-08	KA.16.01.0004	Initial release of the KA.16.02 branch. Released, fully supported, and posted on the web.
KA.16.01.0008	2016-08-02	KA.16.01.0007	Please see the KA.16.01.0008 release notes for detailed information on the KA.16.01 branch. Released, fully supported, and posted on the web.
KA.16.01.0007	2016-05-31	KA.16.01.0006	Released, fully supported, and posted on the web.
KA.16.01.0006	2016-03-28	KA.16.01.0005	Released, fully supported, and posted on the web.
KA.16.01.0005	n/a	KA.16.01.0004	Never released.
KA.16.01.0004	2016-01-20	KA.15.18.0007	Released, fully supported, and posted on the web.
KA.15.18.0012	2016-08-02	KA.15.18.0011	Please see the KA.15.18.0012 release notes for detailed information on the KA.15.18 branch. Released, fully supported, and posted on the web.
KA.15.18.0011	2016-05-31	KA.15.18.0010	Released, fully supported, and posted on the web.
KA.15.18.0010	2016-03-28	KA.15.18.0009	Released, fully supported, and posted on the web.
KA.15.18.0009	n/a	KA.15.18.0008	Never released.
KA.15.18.0008	2016-01-19	KA.15.18.0007	Released, fully supported, and posted on the web.
KA.15.18.0007	2015-11-10	KA.15.18.0006	Released, fully supported, and posted on the web.
KA.15.18.0006	2015-08-15	KA.15.17.0003	Initial release of the KA.15.18 branch. Released, fully supported, and posted on the web.

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
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

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

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 KA.16.02.0021

No enhancements were included in version KA.16.02.0021.

Version KA.16.02.0020

No enhancements were included in version KA.16.02.0020.

Version KA.16.02.0019

Version KA.16.02.0019 was never released.

Version KA.16.02.0018

IPsec Tunnel

Support for creating an IPsec tunnel between the switch and the Aruba mobility controller acting as a VPN concentrator has been added. This functionality allows the creation of a secure channel for communication between the switch and certain services such as Airwave, ClearPass, Syslog, and DNS. The ability to set routes to multiple destinations through the IPsec tunnel, as well as a default gateway route from the switch to the controller for non-IPsec traffic, is now possible.

The CLI command `aruba <vpn-type> peer-ip` initiates the IPsec session with the controller. The `<vpn-type>` can be either `amp` or `any`. If type `amp` is used, the switch will perform ZTP by triggering check-in (to Airwave) through the IPsec channel. If type `any` is used, the switch will not automatically add a route to Airwave IP through the tunnel.

To configure Routes (to services behind the Aruba VPN Controller, such as CPPM, Syslog, DNS, etc.) through the IPsec channel use the CLI command `ip route /mask interface tunnel aruba-vpn`. Before adding/ deleting a route to service network through the IPsec tunnel, it is recommended to execute the following CLI commands in case the controller IP also belongs to service network. These commands add/delete a static route to reach the controller IP through the default gateway:

```
aruba-vpn default-gateway enable
aruba-vpn default-gateway disable
```

IPsec VPN Type

Added a new aruba-vpn type "any" to enable control plane traffic protection for a Remote Access VPN session.

Example: `aruba-vpn type any`

When deleting an existing aruba-vpn configuration and before configuring with a new aruba-vpn type, a warning message is prompted: `Remove the existing aruba-vpn configuration before configuring with a new aruba vpn type.`

Switch software downgrade to a previous version is not allowed with Aruba VPN type "any" configured. An error message is displayed: `Firmware downgrade is not allowed if aruba vpn is configured with type any. Please unconfigure it before attempting to downgrade.`

REST ACL Rules

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

REST System Details

Removed version dependency on displaying VLAN ID and IP address in REST interface for System Details. VLAN ID and assigned IP address of Aruba Central connection is now supported with REST v2.

Version KA.16.02.0017

Version KA.16.02.0017 was never released.

Version KA.16.02.0016

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 KA.16.02.0015

Version KA.16.02.0015 was never released.

Version KA.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. When this 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 queue is 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 DISABLED and 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 KA.16.02.0013

Version KA.16.02.0013 was never released.

Version KA.16.02.0012

No enhancements were included in version KA.16.02.0012.

Version KA.16.02.0011

MAS feature: LLDP Authentication bypass with AP

This feature by-passes authentication for an AP that sends LLDP TLV.

Trap generation with hardware removal/insertion

To generate SNMP traps for physical insertion/removal (of a slot/transceiver/stacking-module) events by default without manual intervention.

Tunneled Node enhancement: fallback to switching and CoA

When tunneled node is enabled on a port and controller is not reachable, an option is added to continue to do local switching on the port traffic.

Once the tunnel is established to the controller, the port traffic is tunneled to the controller.

Version KA.16.02.0010

No enhancements were included in version KA.16.02.0010.

Version KA.16.02.0009

No enhancements were included in version KA.16.02.0009.

Version KA.16.02.0008

ACL Logging Match

ACL Logging provides persistent configuration of the log packets that match ACEs (Access Control Entry) with logging enabled. Make these configurations persistent using the write memory command as with other configuration CLIs.

To provide more granularity for logging, the ACL Logging timer value is reduced from 30 seconds to 5 seconds. Performance might be impacted because of the above mentioned configuration.

Add MTU to Device Profile

ArubaOS-Switch-based switches support the jumbo frame attribute in device profile. When an Aruba AP is attached 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. If the user wants to change this value, they manually configure it in the switch global configuration. Users can enable 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 includes ports 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 configured value 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
```

AirWave Management Platform (AMP) Server MIB Changes

SNMP MIB support for AMP-Server and IPSec tunnel for AMP management traffic are available in 16.02.

Connection via Management VLAN

When the Management VLAN is configured and enabled (active), connection to the AMP Server will be allowed only via Management VLAN.

Instrumentation Enhancements

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

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

IP Service Level Agreement

IP Service Level Agreement (IP SLA) is a feature that helps administrators collect information about network performance in real time. With increasing pressure on maintaining agreed-upon Service Level Agreements on Enterprises and ISPs alike, the IP SLA serves as a useful tool.

The IP SLA feature provides:

- Application-aware monitoring that simulates actual protocol packets.
- Predictable measures that aid in ease of deployment and help with assessment of existing network performance.
- Measures of delay and packet loss for time-sensitive applications.
- End-to-end measurements to represent actual user experience.

The following SLA types are supported:

- UDP Echo, including connectivity testing of transport layer (UDP) services, Round-Trip-Time (RTT) measurement, one-way delay, and packet loss details.
- ICMP Echo, including connectivity testing, RTT measurement, and packet loss details.
- TCP Connect, including connectivity testing of transport layer (TCP) services, and handshake time measurement.

IPsec for AirWave Connection

Support for secure communication between ArubaOS-Switches and an Aruba mobility controller (VPN concentrator) for the management traffic sent to or received from the AirWave Management Platform (AMP) server.

This feature provides necessary support for Zero Touch Provisioning (ZTP) by establishing a secure channel between an ArubaOS-Switch-based switch and the Network Management Server (AirWave). ZTP is a feature by which switches discover their respective management system (AirWave or Aruba Central) during initial boot up using DHCP or Activate. This enables switches to be configured and managed automatically without admin intervention.

In a deployment scenario where a switch at a remote branch and an AirWave server located at corporate headquarters or datacenter are connected via an un-trusted public network (Internet), communication between the switch and the AirWave server must be protected. This feature ensures that communication between ArubaOS-Switch-based switches and an AirWave Server (management traffic) is protected by establishing a secure channel between the switches and an Aruba VPN Controller (connected to an AirWave server) using an IPsec tunnel for the management traffic between the AMP server and the switch.

Please note: This feature only works with the following ArubaOS-Switch-based switches as these switches fully support TPM certificates: 2920, 2930F, 3800, 3810, and 5400R. This feature is restricted to work only with an Aruba Controller (as VPN concentrator) for the IPsec tunnel between the switch and the AMP server.

This feature is currently supported only with Aruba Controller running ArubaOS 6.5.0.0.

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 to ports 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 by the RADIUS server for MAC-Authentication, Web-Authentication, and 802.1X.

Log Blackhole/NULL Route

This feature provides the capability to log received packets that are destined to the static Blackhole route. Blackhole logging can be configured for both IPv4 and IPv6 routes. Because all the packets destined to the blackhole route are logged, there is performance impact, and a warning message is displayed to alert the user.

Information like Source IP, Destination IP, VLAN ID and logical port are logged in the syslog server or in the debug buffer per the configured logging destination. The following sys-debug commands enable debug logging persistent across reload:

```
sys-debug ip fib blackhole
sys-debug ipv6 fib blackhole
```

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 that the 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 will be dynamic, triggered by the dynamic policy an authenticated client will receive.

Per Port Trust

The per-port Trust QoS feature allows customers to select which packet fields are used to determine inbound service-priority:

Packet fields	Description
Default	Use the VLAN cos (Priority Code Point, or PCP) value and preserve any IP-ToS values.
dot1p	Same as default mode.
ip-prec	Use the QoS value corresponding to the IP-Precedence priority-mapping for the IP-ToS field.
Dscp	Use the QoS value corresponding to the Differentiated Services priority-mapping for the IP-ToS field.
None	Use none of the inbound packet-priority information.

For details about the QoS Type-of-Service IP-Precedence or Differentiated-Services priority mappings, please refer to the *Advanced Traffic Management Guide* for your switch.

Please note: QoS trust modes other than "default" or "none" are **mutually exclusive** with the QoS port-priority feature.

Per Port Tunneled Node

Tunneled node, also known as a wired tunneled node, provides access and security using an overlay architecture.

The tunneled node connects to one or more client devices at the edge of the network and then establishes an L2 GRE tunnel to the controlling concentrator server. This approach allows the controller to support all the centralized security features, such as 802.1X authentication, captive-portal authentication, and stateful firewall.

The Tunneled Node feature is enabled on a per-port basis. Any traffic coming from non-tunneled node interfaces will be forwarded "normally" without being tunneled to a Mobility Controller.

User Policies

User Policies are new QoS (Quality of Service) Policies that are used in conjunction with User-Roles to provide control over ingress traffic originating from User-Role assigned clients. This feature supports IPv4 and IPv6 traffic. Classified user traffic is matched and shaped by user policy actions. User Policy actions allow traffic to be rate-limited, permitted, and denied. It also allows VLAN priority, DSCP, and IP-Precedence (DSCP & IP-precedence are mutually exclusive) to be assigned to matching traffic. User Policies are assigned to User-Roles.

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.

ZTP for Activate

The Aruba Activate service is part of the larger Mobility as a Service (MaaS) cloud initiative from Aruba. The Aruba Activate service consists of many services like Tracking, Provisioning, Upgrade and Inventory. Due to a limitation in the Activate server, this feature is only available for switch units manufactured after February 1, 2016 (the 3rd and 4th letters in the serial number have to be 62 or higher).

Zero Touch Provisioning (ZTP) enables auto-configuration of an ArubaOS-Switch-based switch without requiring any admin intervention on the switch. When a Cloud-enabled ArubaOS-Switch-based switch with factory default configuration becomes active on the network, it first contacts the NTP server, then contacts the Activate server, where it gets validated and forwarded to a Central or AirWave server to start further communications for auto provisioning.

The Activate ZTP process:

*   Redirects the switch to AirWave or Central. Activate is not responsible for the actual switch configuration.
*   If Activate returns an Aruba Mobility Controller IP address (in addition to AirWave parameters), the switch establishes an IPSec tunnel with the Controller and sends traffic over this tunnel.

Fixes

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

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

Version KA.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 credentials with 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 allocate new 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 allocate new 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 `show lldp` 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-by value`.

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.

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.

Stacking
CR_0000230530

Symptom: The switch stack may show incorrect global uptime.

Scenario: If the stack members have different timestamps prior to stack formation, when the stack is formed and a redundancy switchover event occurs, the global uptime may not be reported accurately.

Workaround: Synchronize the timestamp across switches prior to configuring them in a stack.

CR_0000222585

Symptom: When applying a source-port filter to the uplink ports of every stack member, the source-port configuration is not applied to one or more stack members.

Scenario: The issue occurs in a backplane or VSF stack if the members initially have source-port filters configured, then are removed from the stack and subsequently re-added prior to re-applying the source-port filter.

Workaround: Remove source-port filter configurations manually by using the command `no filter source-port` before removing the stack member.

Version KA.16.02.0020

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 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.

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.

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 data collected regarding OSPF status may be incomplete.

PoE
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
```

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 Smart Link 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.

Version KA.16.02.0019

Version KA.16.02.0019 was never released.

Version KA.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 may crash 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.`

CLI
CR_0000210794

Symptom: Stack member uptime information is incorrect in the output of the CLI command `show redundancy detail`.

Scenario: The timestamp is incorrectly calculated for "Module Up Since" and "State Since" values displayed in the output of the CLI command `show redundancy detail`.

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 is removed 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 DHCP Snooping 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 is logged repeatedly.

Fault Finder
CR_0000223670

Symptom: The switch incorrectly allows ports with fault-finder enabled for broadcast-storm to be configured 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 be forwarded 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.

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` when a mirror policy is applied to a VLAN.

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

OOBM
CR_0000170024

Symptom: Communication through the OOBM port may fail.

Scenario: When the OOBM Port is disabled in the switch configuration (`oobm interface disable`), after a redundancy switchover event occurs, the OOBM Ports status remains "down" when the OOBM interface is re-enabled from the CLI command `oobm interface enable`.

Workaround: Disable and enable the OOBM interface once more to bring it up.

```
oobm interface disable
oobm interface enable
```

OSPF
CR_0000225246

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

Scenario: It is possible after an extended period of uptime for the switch to incorrectly calculate the OSPFv3 Link 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 debug ipv6 ospfv3`) will trigger an immediate refresh for LSAs which are over the age of 1800 seconds.

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 case of some events or mechanisms (for example, ARP resolution of a new host entry causes the multicast flows to 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 ARP entry 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 `Software exception at vls_xmit.c:<...>...`

Scenario: When PIM-DM (Dense Mode) is enabled on multiple VLANs, the switch may crash during periods of 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 the respective 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 in ISR 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 is not 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`.

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 choose less 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 the number of routes being learned within a short time.

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 mapped to 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 trunk interface.

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 VLAN Management 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 KA.16.02.0017

Version KA.16.02.0017 was never released.

Version KA.16.02.0016

Authentication
CR_0000226106

Symptom: The switch does not transmit LLDP packets.

Scenario: The switch no longer transmits LLDP packets on the port after it is configured for AAA port-access authentication.

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 is larger 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-supported ports:

```
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 different VLAN also managed by the switch DHCP server, a fresh new DHCP client request process is initiated in place of 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 when roaming 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 DHCP server address pool.

Scenario: When the default route (0.0.0.0/0) is configured with a VLAN as the next hop, the DHCP request packets 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 is completed.

Event Log
CR_0000218695

Symptom: Incorrect message and assigned event class of the following error message `Failed to allocate 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 allocate FIB entries.

CR_0000225392

Symptom: The proper event log message is not generated when a port is blocked due to a link failure detection 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 messages similar to:

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

Job Scheduler
CR_0000221236

Symptom: The switch does not execute scheduled jobs at expected scheduled time.

Scenario: When the switch time settings are adjusted for time protocol, time zone or daylight savings time rule (daylight-time-rule), the Job Scheduler fails to execute scheduled jobs at the configured time. This is triggered when switch time is (re-)adjusted, following a time settings change. For example, adding a daylight-time-rule would trigger a time re-adjustment, but the job scheduler time is not re-adjusted with the new switch time settings and it will not trigger job execution at the expected time.

Workaround: Remove and re-configure the jobs after making configuration changes to the switch time settings.

CR_0000222032

Symptom: The switch may crash with an error message similar to `Health Monitor: Read Error Restr Mem Access <...> Task='tCron000001' <...>` when executing a scheduled job.

Scenario: If a job is scheduled to copy data files to/from a remote server configured via hostname, the switch may crash with an error message similar to `Health Monitor: Read Error Restr Mem Access <...> Task='tCron000001' <...>` when executing the job at scheduled time.

Example: `job <name> at [HH:]MM "copy running-config tftp mytftpserver.com FILENAME-STR"`.

Workaround: Configure the job to copy data files using IP address instead of hostname.

Example: `job <name> at [HH:]MM "copy running-config tftp 192.168.0.1 FILENAME-STR"`.

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 client and 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 are reported 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.

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 fail and 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 CLI command `walkMIB ipAddressIfIndex`.

Spanning Tree
CR_0000201299

Symptom: A switch configured with RPVST may crash with an error message similar to `Software exception 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 switch that 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 brought down (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 administrative state is enabled.

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

Stacking
CR_0000197626

Symptom: A stack might fail to split according to the configured split policy.

Scenario: In a 2-member stack configuration, when the OOBM interface is configured for dynamic DHCP IP address, a stack might fail to split according to the configured split policy.

Workaround: Configure any of the OOBM interfaces with static assigned IP address.

CR_0000211777

Symptom: The standby member ID is not properly updated.

Scenario: When the standby member of a stack is rebooted or lost, the standby member ID is not properly updated with the new standby ID. This condition potentially impacts subsequent stacking events, failover, and stack member role mitigation.

Workaround: No known workaround. Rebooting the stack will clear stale standby member ID information.

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 of 8 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 from CLI.

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.

Tunneling
CR_0000197220

Symptom: Unexpected broadcast traffic is received on ports not enabled for tunnel-node.

Scenario: In a switch where ports configured for tunnel-mode support and ports not configured for tunnel-node belong to the same VLAN, the broadcast traffic destined only to ports enabled for tunnel-node is observed on ports without tunnel-node enabled.

Workaround: Configure source port filter to filter traffic from tunnel-node ports to non-tunnel-node ports.

Example: `filter source-port <non-TN-port> drop <TN portlist>`

Version KA.16.02.0015

Version KA.16.02.0015 was never released.

Version KA.16.02.0014

Authorization
CR_0000216097

Symptom: In certain conditions, the User Roles feature may be unintentionally disabled.

Scenario: If the User Role feature is already enabled on the switch and an unsuccessful switch configuration restore using a file transfer occurs, the User Role may become disabled.

Workaround: Manually disable and then re-enable the User Role feature using the CLI command `aaa authorization user [disable | enable]`.

CR_0000221546

Symptom: When executing unauthorized commands, the switch may fail to include a blank line before printing 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 message similar 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 switch through SSH, telnet or console.

Workaround: Rebooting the switch will clear the locked sessions. Alternatively, you can disable the inactivity timer 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.

IPsec
CR_0000221636

Symptom: IPSec tunnel may break in case of Layer-2 topology change.

Scenario: When the connection to the Controller is switched from one port to another (for example when a layer-2 topology change occurs), the IPSec tunnel will not be re-established due to the port UP notification being received on a different port.

Workaround: Re-start the IPSec session manually using CLI command `aruba-vpn type <vpn-type>`.

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.

OOBM
CR_0000214640

Symptom: Communication through OOBM IP address may be lost after a failover.

Scenario: After a failover event in a VSF or backplane stacking configuration, a gratuitous ARP may fail to be sent. The global OOBM IP address becomes unreachable because the new commander's MAC address is not associated with the OOBM IP address in the neighbor devices' ARP table.

Workaround: Issue a ping from the switch to any destination through the OOBM interface to update the ARP entry in the neighbor devices.

CR_0000216669

Symptom: OOBM port remains active after being administratively disabled.

Scenario: When in a VSF or hardware backplane stack, the global OOBM interface may not be turned off after being administratively disabled using the CLI command `oobm disable`.

Workaround: In addition to disabling the global OOBM, disable the OOBM interfaces for all stack members with the CLI command `oobm member <member-id> interface disable`.

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 to destination mac-groups.

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.

SNMP
CR_0000214384

Symptom: SNMP ifTable reports invalid OID values for OOBM loopback interface.

Scenario: When a switch is configured in a stack, SNMP ifTable reports OID value '0" for 'ifType' (. 1.3.6.1.2.1.2.2.1.3), 'ifAdminStatus' (.1.3.6.1.2.1.2.2.1.7), and 'ifOperStatus' (.1.3.6.1.2.1.2.2.1.8) corresponding to the OOBM loopback interface.

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 the generated 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 displays the 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 ports greater 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 crash with an error message similar to `Too Many MAC [6] Interrupts`.

Trunking
CR_0000212455

Symptom: When trying to re-create a trunk, the switch may prompt the error message `Ambiguous input: trk...`

Scenario: When configured in a stacking mode, the switch may not be able to re-create a trunk after the last port of last stacking member was already configured as a member to another trunk.

Workaround: Do not configure last port of last stacking member as trunk port.

Web UI
CR_0000216915

Symptom: Switch web UI may become unresponsive or encounter a script error.

Scenario: When a stackable switch is configured for stacking mode but no other stack member has joined the stack, the switch web UI may become unresponsive or return a script error.

Workaround: Disable stacking when only one stack member is needed or wait for another member to join before using web UI.

Version KA.16.02.0013

Version KA.16.02.0013 was never released.

Version KA.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 the default gateway.

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

Version KA.16.02.0011

Distributed Trunking
CR_0000200355

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

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

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 already configured on the switch, the tunnel activation may fail.

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

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 be unable to connect to the SDN controller.

Workaround: Reboot the switch.

Redundancy
CR_0000212756

Symptom: Interface configuration of stack member might be lost from the global configuration.

Scenario: When a stack member switch is replaced with a new MAC address in an existing stack, the interface configuration corresponding to the replaced member switch is lost in the event of redundancy. This causes the current standby switch to switchover to the commander role.

Workaround: Perform another redundancy using CLI command `redundancy switchover`.

Spanning Tree
CR_0000202511

Symptom: Incorrect Spanning Tree hello time is reported as a MIB value.

Scenario: In a Spanning Tree topology, the switch reports the value of OID dot1dStpHelloTime on a root switch in seconds instead of centiseconds as reported in non-root switches.

Workaround: There is no impact on Spanning Tree functionality as this is merely a value conversion from seconds to centiseconds.

Version KA.16.02.0010

Stacking
CR_0000214504

Symptom/Scenario: After a stack failover to standby, the switch may fail to forward traffic.

Workaround: Toggling the affected links using CLI command `interface <port-num> disable | enable` can clear the issue.

Version KA.16.02.0009

Aruba Management Software
CR_0000214536

Symptom/Scenario: The ArubaOS-Switch-based switch fails to connect to the Aruba Activate server, potentially impacting Aruba Central connectivity and ZTP (zero-touch provisioning) using Activate for the AirWave and IPsec (connection with Aruba Controller for AirWave management traffic) solution. The switch logs an event message similar to `Activate: Received failure "response from the Activate server with status code: None"`.

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 failure on 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 KA.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 configured with 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 define the 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 a crash.

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 Mem Access <...>`.

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.

Console
CR_0000179094

Symptom: Sending special keys to a console switch configured in stacking mode may cause the switch to crash.

Scenario: Sending the **ESC** or **~** key to the console of a standby or member switch connected in a stack configuration may cause the switch to crash with an error message similar to `Software exception at multMgmtUtil.c <…>`.

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 the DHCP 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 configured idle-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 complete before the idle timer expires.

IGMP
CR_0000189793

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

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_0000191543

Symptom: In certain conditions, the switch is unable to discover an IPv6 neighbor.

Scenario: The switch is unable to discover an IPv6 neighbor when the point-to-point inter-router link is configured with /127 IPv6 prefix length.

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 with an 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 all VLANs.

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 Misaligned Mem Access <...> Task='mSnmpCtrl' <...>` while displaying IP multicast routing table content using the CLI command `show ip mroute`.

PoE
CR_0000189058

Symptom: Rarely, a directly connected AP does not power up. The power LED on the AP remains unlit.

Scenario: Having dual Ethernet port Aruba APs connected to HPE Aruba Switches. Problem is commonly seen on 5400 V1 blades, but might rarely be seen on other HPE Aruba switches.

Workaround: Power can be restored by toggling PoE power to the connected port on the switch: `no int <port-nums> power` and `int <port-nums> power`.

CR_0000191040

Symptom/Scenario: Connecting both E0 & E1 ports on an Aruba AP325 to a POE ports on an HPE Aruba Switch results in a POE failure, loss of power on one of the switch ports, lighted switch fault LED and a `bad FET` message in the switch logs.

Workaround: Power can be restored to the affected port by unplugging the cable from it and perform a poe-reset. Alternately, unplugging the affected port and rebooting the switch will also restore power to the faulted ports. HPE recommends only E0 port of the AP plugs into the switch.

SNMP
CR_0000192914

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

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.

VRRP
CR_0000192567

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

Scenario: When the virtual IP address of a VLAN is multi-network configured, the virtual-ip-ping command fails 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

KA.16.02.0021 uses BootROM KA.15.10. 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.

ⓘ 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.

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.

Finding Security Bulletins

Procedure

1. Go to the HPE Support Center - Hewlett Packard Enterprise at **www.hpe.com/support/hpesc**.
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

Security Bulletin subscription service

You can sign up at **http://www.hpe.com/support/Subscriber_Choice** to initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email.

Networking Websites

> **Hewlett Packard Enterprise Networking Information Library**
>
> > **www.hpe.com/networking/resourcefinder**
>
> **Hewlett Packard Enterprise Networking Software**
>
> > **www.hpe.com/networking/software**
>
> **Hewlett Packard Enterprise Networking website**
>
> > **www.hpe.com/info/networking**
>
> **Hewlett Packard Enterprise My Networking website**
>
> > **www.hpe.com/networking/support**
>
> **Hewlett Packard Enterprise My Networking Portal**
>
> > **www.hpe.com/networking/mynetworking**
>
> **Hewlett Packard Enterprise Networking Warranty**
>
> > **www.hpe.com/networking/warranty**

General websites

> **Hewlett Packard Enterprise Information Library**
>
> > **www.hpe.com/info/EIL**
>
> For additional websites, see **Support and other resources**.

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center
      www.hpe.com/support/hpesc
  Hewlett Packard Enterprise Support Center: Software downloads
      www.hpe.com/support/downloads
  Software Depot
      www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

ⓘ   Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information
   HPE Get Connected
      www.hpe.com/services/getconnected
   HPE Proactive Care services
      www.hpe.com/services/proactivecare
   HPE Proactive Care service: Supported products list
      www.hpe.com/services/proactivecaresupportedproducts
   HPE Proactive Care advanced service: Supported products list
      www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information
   Proactive Care central
      www.hpe.com/services/proactivecarecentral
   Proactive Care service activation
      www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information
   HPE ProLiant and x86 Servers and Options
      www.hpe.com/support/ProLiantServers-Warranties
   HPE Enterprise Servers
      www.hpe.com/support/EnterpriseServers-Warranties
   HPE Storage Products
      www.hpe.com/support/Storage-Warranties
   HPE Networking Products
      www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.