WB.16.04.0016 Release Notes

a Hewlett Packard
Enterprise company

Part Number: 5200-5231
Published: July 2018
Edition: 1

Notices

Acknowledgments

Description

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

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

Product series supported by this software:

Aruba 2920 Switch Series

Important information

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

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

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

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

Version history

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

Version number	Release date	Based on	Remarks
WB.16.04.0016	2018-06-22	WB.16.04.0015	Released, fully supported, and posted on the web.
WB.16.04.0015	2018-06-05	WB.16.04.0014	Released, fully supported, and posted on the web.
WB.16.04.0014	n/a	WB.16.04.0013	Never released.
WB.16.04.0013	2018-03-28	WB.16.04.0012	Released, fully supported, and posted on the web.
WB.16.04.0012	n/a	WB.16.04.0011	Never released.
WB.16.04.0011	2017-12-22	WB.16.04.0010	Released, fully supported, and posted on the web.
WB.16.04.0010	n/a	WB.16.04.0009	Never released.
WB.16.04.0009	2017-10-16	WB.16.04.0008	Released, fully supported, and posted on the web.

Table Continued

Version number	Release date	Based on	Remarks
WB.16.04.0008	2017-07-27	WB.16.03.0003	Initial release of the WB.16.04 branch. Released, fully supported, and posted on the web.
WB.16.03.0005	2017-07-07	WB.16.03.0004	Released, fully supported, and posted on the web.
WB.16.03.0004	2017-04-17	WB.16.03.0003	Released, fully supported, and posted on the web.
WB.16.03.0003	2016-12-20	WB.16.02.0008	Initial release of the WB.16.03 branch. Released, fully supported, and posted on the web.
WB.16.02.0014	2016-10-28	WB.16.02.0013	Please see the WB.16.02.0114 release notes for detailed information on the WB.16.02 branch. Released, fully supported, and posted on the web.
WB.16.02.0013	n/a	WB.16.02.0012	Never released.
WB.16.02.0012	2016-08-31	WB.16.02.0011	Released, fully supported, and posted on the web.
WB.16.02.0011	2016-08-24	WB.16.02.0010	Released, fully supported, and posted on the web.
WB.16.02.0010	2016-08-11	WB.16.02.0009	Released, fully supported, and posted on the web.
WB.16.02.0009	n/a	WB.16.02.0008	Never released.
WB.16.02.0008	2016-07-08	WB.16.01.0004	Initial release of the WB.16.02 branch. Released, fully supported, and posted on the web.

Products supported

This release applies to the following product models:

Product number	Description
J9726A	Aruba 2920 24G Switch
J9728A	Aruba 2920 48G Switch
J9727A	Aruba 2920 24G PoE+ Switch
J9729A	Aruba 2920 48G PoE+ Switch
J9836A	Aruba 2920 48G PoE+ 740W 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

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

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 16.04.0016

No enhancements were included in version 16.04.0016.

Version 16.04.0015

No enhancements were included in version 16.04.0015.

Version 16.04.0014

No enhancements were included in version 16.04.0014.

Version 16.04.0013

Connected Devices Reporting (CDR)

Added support for Connected Devices Reporting (CDR) details about the connected devices to the Aruba switch into Aruba Central using subscription based (both event based and periodic based) mechanism. This feature reports remotely authenticated devices, locally authenticated devices as well as devices onboarding on switch ports that are not configured with any authentication mechanism.

CDR is using additional options added to the IP Client Tracker CLI command. Trusted option enables tracking of trusted clients and untrusted option enables tracking of untrusted clients only.

```
ip client-tracker [trusted | untrusted]
```

When IP client tracker is enabled to track untrusted devices, a new CLI command is added to configure switch ports that are connected to the network infra devices (for example, switch, router, and AP).

```
interface <PORT-LIST> device-type network-device
```

Version 16.04.0012

Version 16.04.0012 was never released.

Version 16.04.0011

No enhancements were included in version 16.04.0011.

Version 16.04.0010

Version 16.04.0010 was never released.

Version 16.04.0009

Authentication

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

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

OpenFlow

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

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

Version 16.04.0008

/31 Subnet Support

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

Batch CLI command execution over REST Interface

REST interface users may now choose to push a subset of the switch configuration in one go via the newly added 'CliBatchCommand' instead of using the individual REST APIs to configure features. If the configuration (in CLI format) of the switch is already known, this command can be leveraged for initial setup by executing the CLI commands in a single batch over the REST API. For more information, see the *ArubaOS-Switch REST API Guide*.

CLI Commands over REST Interface

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

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

Connected Device Reporting

Connected Device Reporting provides visibility to Central customers about wired devices connected to the switch. Central now has visibility into both authenticated as well as unauthenticated devices, helping customers understand the status of their current network. Central 2.3.6 is the minimum version required.

Enhanced Fan Status

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

Increase Subject length for the certificate

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

IPv6 Default Gateway on OOBM port

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

IPv6 Set Router Preference

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

Management of 2920 stacks on Aruba Central

Besides enabling the stacking REST APIs, 16.04 also allows for 2920 stacks to be fully managed by Aruba Central. Please refer to the Aruba Central release notes for information on availability on the feature. For more information, see the *ArubaOS-Switch Management and Configuration Guide* for your switch.

Stacking support with REST APIs

This release enables the management of stacks of switches (both backplane and frontplane) via REST APIs. Backplane stacks (2920, 2930M, 3810M) and front plane or VSF stacks (2930F and 5400R) can now be fully set up and managed using the REST APIs. For more information, see the *ArubaOS-Switch Management and Configuration Guide* for your switch.

Time-Domain Reflectometry for 2920

Cable tests using Time Domain Reflectometry (TDR) can help detect cable faults on copper cables within the resolution of meters and help admins troubleshoot cable faults. This feature has been available on other

ArubaOS-Switch platforms is now supported on the 2920. For more information, see the *ArubaOS-Switch Management and Configuration Guide* for your switch.

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.

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

Version 16.04.0016

Accounting
CR_0000241399

Symptom: The switch sends delayed accounting request packet.

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

Workaround: Disable DHCP snooping on the switch.

ACLs
CR_0000244157

Symptom: The switch experiences a loss in available memory.

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

Classifier
CR_0000244171

Symptom: The switch does not display certain traffic classes.

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

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

Job Scheduler
CR_0000244075

Symptom: The switch fails to execute scheduled jobs.

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

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

Logging
CR_0000242758

Symptom: The switch fails with an error message similar to `Not enough connections in the connectionPtrs[] array`.

Scenario: When the switch is configured to add a hostname to the receiving syslog server, over time the switch may reboot with an error message `Not enough connections in the connectionPtrs[] array`.

Workaround: Avoid using the hostname option for syslog server messages.

CR_0000244348

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

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

Multicast
CR_0000243253

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

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

Workaround: Perform one of the following:

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

OSPF
CR_0000243557

Symptom/Scenario: The word "compatibility" is misspelled "compatability" in the output of the `show ip ospf general` command.

sFlow
CR_0000243278

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

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

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

SSH
CR_0000241598

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

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

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

Switch Module
CR_0000242516

Symptom/Scenario: In rare conditions, the switch may reboot with an error message similar to `Excessive OM FP interrupts`.

Workaround: The switch reboots on its own and resumes normal operations.

Transceivers
CR_0000243304

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

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

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

Version 16.04.0015

Security fixes were applied in version 16.04.0015.

Version 16.04.0014

Enhanced Secure Mode
CR_0000244231

Symptom: Unable to delete switch manager and operator passwords in enhanced secure mode.

Scenario: In enhanced secure mode, the switch manager and operator passwords cannot be deleted using the `no password` command.

Version 16.04.0013

Authentication
CR_0000241206

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

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

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

CLI
CR_0000241599

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

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

Configuration
CR_0000242401

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

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

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

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

Dynamic IP Lockdown
CR_0000240248

Symptom: The switch incorrectly blocks traffic.

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

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

Front Panel Security
CR_0000242467

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

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

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

IP Stacking
CR_0000237504

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

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

LLDP
CR_0000241838

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

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

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

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

OpenFlow
CR_0000236916

Symptom: Communication between hosts fails.

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

Workaround: Use a single OpenFlow vendor.

REST
CR_0000241895

Symptom: The REST incorrectly returns 204 response.

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

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

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

RMON
CR_0000241677

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

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

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

Transceivers
CR_0000237544

Symptom: Switch fails with an error message similar to `Software exception at ppmgr_portInterrupt.c: <...> -- in 'mPmSlvCtrl' <...>`.

Scenario: During the switch boot up with mix of 10M, 100M and 1000M copper port link partners with SFP transceiver 1000SX on dual personality ports, the switch may fail with an error message similar to `Software exception at ppmgr_portInterrupt.c: <...> -- in 'mPmSlvCtrl' <...>`.

Workaround: Insert the SFP 1000SX transceivers in dual personality ports after the switch is fully booted up or disable the ports with these transceivers before the switch reboot and re-enable after the switch is completely rebooted.

Trunking
CR_0000241091

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

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

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

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

CR_0000241138

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

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

Workaround: Remove the missing port from the aggregated link.

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

User Roles
CR_0000240708

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

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

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

Web UI
CR_0000241156

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

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

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

Version 16.04.0012

Version 16.04.0012 was never released.

Version 16.04.0011

Airwave
CR_0000236230

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

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

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

Authentication
CR_0000236646

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

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

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

DHCP Server
CR_0000238265

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

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

DHCP Snooping
CR_0000239864

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

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

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

Key Management
CR_0000237991

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

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

Example:

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

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

Example:

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

Multicast
CR_0000237850

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

MVRP
CR_0000238146

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

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

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

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

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

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

PBR
CR_0000236962

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

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

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

Rogue AP Isolation
CR_0000238207

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

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

```
switch# show rogue-ap-isolation

Rogue AP Isolation
Rogue AP Status : Disabled
Rogue AP Action : Block
```

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

SNMP
CR_0000236648

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

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

Suite-B
CR_0000239841

Symptom: The switch is incorrectly advertising ciphers not compliant with Suite-B Cryptography.

Scenario: When using the `crypto SuiteB-MinLoS <128 | 192> tls strict` command to configure the switch for Suite-B compliance for minimum levels of security for TLS version 1.2 in strict mode, the switch fails to strictly enforce the configured security strength.

NOTE:

A switch running ArubaOS-Switch configured for Suite-B compliance in strict mode will no longer support TLS connections with other ciphers not allowed in strict mode. If other cipher suites are needed, remove strict mode using the `no crypto SuiteB-MinLoS <128 | 192> tls strict` command.

VLAN
CR_0000240169

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

Web UI
CR_0000237484

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

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

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

Version 16.04.0010

Version 16.04.0010 was never released.

Version 16.04.0009

Authentication
CR_0000235976

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

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

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

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

Central
CR_0000236990

Symptom: Incorrect switch IP address is displayed in the Central UI.

Scenario: When the switch is configured with multiple IP addresses on the uplink interface, the DeviceInfo and SystemInfo stats in the Central UI may report incorrect switch IP address info.

DHCP
CR_0000234234

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

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

DHCP Snooping
CR_0000230898

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

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

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

New event messages were added for broadcast client packets:

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

Physical Port
CR_0000234441

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

Scenario: When a switch port link repeatedly toggles and negotiated speeds change between 10G and 1G, the switch may crash with an error message similar to `Health Monitor: Read Error Restr Mem Access <..> Task='mPmSlvCtrl'`.

Workaround: Configure the port's speed and duplex settings to auto-10g or auto-1000 to avoid speed changes and minimize port toggling.

Smart Link
CR_0000235633

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

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

Workaround: Configure Smart Link ports as consecutive ports.

SNMP
CR_0000237141

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

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

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

SSH
CR_0000233725

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

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

Workaround: Do one of the following:

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

CR_0000236513

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

Scenario: When the SSH public-keys are installed without comments using the switch OS version xx.15.17.xxxx or older and the switch is upgraded to a newer OS version, the switch may crash when issuing the CLI command `show crypto client-public-key`.

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

Web UI
CR_0000234086

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

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

Version 16.04.0008

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.

Central
CR_0000233323

Symptom/Scenario: When a switch configuration is pushed via Aruba Central, the configuration may not be entirely pushed to the switch, resulting in an incomplete or truncated switch configuration.

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_0000229987

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

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

CR_0000233449

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

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

Example from a chassis with slots A-L populated:

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

 OpenFlow Instance Flow Table Information

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

Table
 ID    Table Name             Available Free Flow Count
 ----- ---------------------- ------------------------------
 0     Custom L2 Src          Slot A              : 7372
                              Slot B              : 7372
                              Slot C              : 7372
                              Slot D              : 7372
                              Slot E              : 7372
                              Slot F              : 7372
                              Slot G              : 7372
                              Slot H              : 7372
                              Slot I              : 7372
```

```
                              Slot J              : 7
 1      Custom L2 Dst         Slot A              : 6144
                              Slot B              : 6144
                              Slot C              : 6144
                              Slot D              : 6144
                              Slot E              : 6144
                              Slot F              : 6144
                              Slot G              : 6144
                              Slot H              : 6144
                              Slot I              : 6144
                              Slot J              : 6
...
```

OSPF
CR_0000230472

Symptom: OSPF interface authentication may fail.

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

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

Private VLAN
CR_0000233782

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

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

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

Workaround: Disable security on the access port.

CR_0000234099

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

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

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

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

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_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.

Web UI
CR_0000229939

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

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

Workaround: Use the following CLI command to change PoE status for the port:

`[no] interface <PORT-LIST> power-over-ethernet`

CR_0000234086

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

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

Issues and workarounds

The following are known open issues with this branch of the software.

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.

Central

CR_0000237778

Symptom: Login to switch from Central Remote Console System (RCS) may fail.

Scenario: When the switch is configured with local authentication as well as RADIUS/TACACS authentication and the local user credentials are not provisioned in RADIUS/TACACS, Central RCS authentication fails.

Workaround: Add local user credentials to RADIUS/TACACS server.

Upgrade information

Upgrading restrictions and guidelines

WB.16.04.0016 uses BootROM WB.16.03. 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 WB. 16.04*.

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

Firmware downgrade to a version earlier than 16.01 is not allowed if the max-vlans value is greater than 2048.

Unconfigure the max-vlans before attempting to downgrade from WB.16.02.0008 or later to a version earlier than 16.01 of the firmware.

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

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

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

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the *ArubaOS-Switch Basic Operations Guide Version 16.04*.

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

IMPORTANT: 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 information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline 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.