

# WB.16.05.0013 Release Notes

**aruba**

a Hewlett Packard  
Enterprise company

Part Number: 5200-5590  
Published: March 2019  
Edition: 1

© Copyright 2019 Hewlett Packard Enterprise Development LP

## Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

## Acknowledgments

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

## Description

This release note covers software versions for the WB.16.05 branch of the software.

Version WB.16.05.0003 is the initial build of Major version WB.16.05 software. WB.16.05.0003 includes all enhancements and fixes in the WB.16.04.0008 software, plus the additional enhancements and fixes in the WB.16.05.0003 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.

## Version history

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

Version number	Release date	Remarks
WB.16.05.0013	2019-03-04	Released, fully supported, and posted on the web.
WB.16.05.0012	2018-11-21	Released, fully supported, and posted on the web.
WB.16.05.0011	2018-09-05	Released, fully supported, and posted on the web.
WB.16.05.0010	n/a	Never released.
WB.16.05.0009	2018-06-22	Released, fully supported, and posted on the web.
WB.16.05.0008	n/a	Never released.
WB.16.05.0007	2018-03-28	Released, fully supported, and posted on the web.
WB.16.05.0006	n/a	Never released.
WB.16.05.0005	n/a	Never released.
WB.16.05.0004	2017-12-22	Released, fully supported, and posted on the web.
WB.16.05.0003	2017-12-12	Initial release of the WB.16.05 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	<ul style="list-style-type: none"> <li>Edge</li> <li>11</li> </ul>
Chrome	<ul style="list-style-type: none"> <li>53</li> <li>52</li> </ul>
Firefox	<ul style="list-style-type: none"> <li>49</li> <li>48</li> </ul>
Safari (MacOS only)	<ul style="list-style-type: none"> <li>10</li> <li>9</li> </ul>



**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 16.05.0013

No enhancements were included in version 16.05.0013.

### Version 16.05.0012

No enhancements were included in version 16.05.0012.

### Version 16.05.0011

No enhancements were included in version 16.05.0011.

## Version 16.05.0010

Version 16.05.0010 was never released.

## Version 16.05.0009

### CDP

Support for cdpCachedCapabilities information in HEX value.

### Spanning Tree

Support for interoperability with Cisco switches when running spanning-tree in RPVST+ mode.

## Version 16.05.0008

Version 16.05.0008 was never released.

## Version 16.05.0007

### Central

Added support into Aruba Central for fault finder switch events.

### Cisco Discovery Protocol (CDP) support

Added support for PHONE, REMOTE\_DEVICE, CVTA, and TWO\_PORT\_MAC\_RELAY capabilities displayed in the output of the CDP CLI command:

```
show cdp neighbor details <PORT-LIST>
```

### 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
```

### Multicast Listener Discovery (MLD)

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

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

## Version 16.05.0006

Version 16.05.0006 was never released.

## Version 16.05.0005

Version 16.05.0005 was never released.

## Version 16.05.0004

No enhancements were included in version 16.05.0004.

## Version 16.05.0003

### Advanced Threat Detection

By enhancing syslog information to include details of the clients (MAC and IP) and sharing this with ClearPass and IntroSpect, switches across the enterprise act as a network of sensors to detect and alert admins about potential threats to the network. Admins can monitor as well as take actions, such as quarantine, in ClearPass in response to the security events. Refer to the "Configuring Advanced Threat Protection" chapter of the *Access Security Guide* for details.

### Aruba APs on Tunneled Node

Customers that use tunneled node for uniform policy management of wired and wireless traffic can now connect Aruba APs to tunneled node ports without having to undo tunneled node configuration on those ports. A configuration knob in the device profile feature avoids double-tunneling and results in improved performance. Refer to the "Tunneled node" chapter of the *Management and Configuration Guide* for details.

### Config Backup and Restore without Reboot

Admins can now go from one stable configuration to another without necessarily rebooting the switch as long as the new configuration does not involve reprogramming the hardware or the ASIC. This feature results in improved workflows with Aruba Central and AirWave as well as helping admins recover lost connectivity to remote switches when used in conjunction with the Job Scheduler feature. Refer to the "Configuration backup and restore without reboot" chapter of the *Management Configuration Guide* for details.

### Global OSPF Cost Setting

Admins can now set a default OSPF v2 and v3 cost which can be inherited by a VLAN associated with an OSPF area if the cost is not explicitly specified. Refer to the "Open Shortest Path First Protocol (OSPF)" chapter in the *Multicast and Routing Guide*.

### Improved ZTP with Central

The Zero Touch Provisioning process involves the switch being able to get the correct time to generate certificates to contact Activate/Central. In cases where local NTP servers and public NTP servers are unavailable, the switch will use the HTTP Time Protocol with Activate and update the system clock. This results in a more reliable outcome during NTP outage scenarios. Refer to the "ZTP with AirWave Network Management" chapter of the *Management and Configuration Guide* for information on how the new process works.

### MAC Pinning

Devices connected via MAC Authentication or Local MAC Authentication are automatically de-authenticated after a default logoff period but this can be an issue for some legacy devices and for those that are non-chatty (IP Cameras for example). To prevent this from happening, ArubaOS-Switch provides a configuration knob for MAC Auth and LMA clients to stay pinned to the particular port until they explicitly de-authenticate. Refer to the "Web-based and MAC authentication" chapter of the *Access Security Guide* for information on using this features for non-chatty devices.

## Show MAC age

Lists the MAC age of clients as part of the `show mac-address detail` command.

## Specify FQDN for NTP server configuration

The NTP client takes a fully qualified domain name as input and cycles through the list of IP addresses resulting from the DNS resolution until a reachable NTP server is found. Please refer to the "Time synchronization" chapter in the *Management and Configuration Guide* for details.

## Specify source IP to reach OpenFlow Controller

If multiple routes are available to reach the OpenFlow controller, admins can now use this option to specify the source interface through which the switch reaches out to the OpenFlow Controller. Refer the "Configuring OpenFlow" chapter of the *OpenFlow Administrator's Guide* for details.

## 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 16.05.0013

### ACLs

#### CR\_0000247659

**Symptom/Scenario:** When a routed ACL is applied in the "out" direction on a VLAN, if the traffic is permitted or denied by the switch, it is not reported to the syslog server and no event is recorded in the event log.

### Config

#### CR\_0000247316

**Symptom:** The switch fails to set the default startup configuration file from files stored in index 4 or 5 on the switch.

**Scenario:** When using the CLI command `startup-default config` to set the default startup configuration file from files stored in index 4 or 5 on the switch, the switch displays an error message similar to Configuration file <...> stored in config index X is not supported in lower image versions.

**Example:**

```
# show config files
```

```
Configuration files:
```

```
id | act pri sec | name
---+-----+-----
 1 | *   *   *   | config
 2 |     |   | file1
 3 |     |   | file2
 4 |     |   | file3
 5 |     |   | file4
```

```
# startup-default config file4
```

Configuration file file4 stored in config index 5 is not supported in lower image versions.

**Workaround:** Set the default startup configuration from a file stored in index 1-3 on the switch.

## CR\_0000247335

**Symptom:** The output of the command `show config files` displays the incorrect config file as active.

**Scenario:** When the output of CLI command `show config files` displays one config file (config\_1) as active, primary, and secondary, if the `boot system flash primary config config_2` command is used to boot the switch and to mark the second config (config\_2) as active, primary, and secondary, the output of the CLI command `show run` displays config\_1 is still in use.

**Workaround:** Once the config file config\_2 is active, reboot the switch with the previously loaded active configuration file using the command `boot system flash primary config config_1`.

## IP Client Tracker

### CR\_0000246816

**Symptom:** In certain conditions, the switch may experience some packet loss on uplink ports.

**Scenario:** When IP client-tracker is enabled on an L2 switch where clients are connected on different VLANs that have dhcp-relay configured, if the VLANs communicate with each other using a router on the uplink port, some packet loss occurs.

**Workaround:** Enable IP client-tracker with the trusted option, using the CLI command `ip client-tracker trusted`.

## REST

### CR\_0000247259

**Symptom:** The switch returns partial system configuration requested via API calls.

**Scenario:** When responding to bulk API calls requesting port details or running-configuration sent via HTTPS, the switch may return incomplete system configuration results.

**Workaround:** Send the bulk API calls for port details or running configuration via HTTP.

### CR\_0000247734

**Symptom/Scenario:** When a REST GET request for "rest/v3/ports" is created to get the list of ports in the switch, the REST query is unable to get the results for port 52.

## SNMP

### CR\_0000247769

**Symptom/Scenario:** When `hpicfBridgeRstpPortPathCost` (1.3.6.1.4.1.11.2.14.11.5.1.12.1.4.5.1.6) is used to set the value of the path-cost of the spanning-tree port (STP) through SNMP to 'Auto', the user is unable to find the OID to set the STP path-cost.

**Workaround:** Configure spanning-tree port path-cost to "auto" using the CLI.

## Web UI

### CR\_0000245830

**Symptom:** The switch fails to list the switch ports in the Ports web management page.

**Scenario:** When a peer device that advertises information in LLDP has a sysName string with special characters, the switch fails to display the port list table on the Ports web management page.



**Workaround:** Remove the special characters from the peer device sysName or use CLI commands to get specific port information.

## Version 16.05.0012

### Authentication CR\_0000245450

**Symptom:** The switch fails to display the correct expected username in the Endpoint Username attribute.

**Scenario:** When the username attribute of the mac-based authenticated client is changed in the authenticating server before the next reauth-period, the switch fails to update the username of the authenticated client in the output of the CLI command `show port-access client`.

**Workaround:** Disable and re-enable the interface to force all the new authentication attributes to be reapplied.

### Central CR\_0000246091

**Symptom/Scenario:** The switch fails to close TCP port 8900 (jmb-cds1) after completing the connection to the Aruba Central application.

### IPv4 CR\_0000244916

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

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

**Workaround:** Delete and re-add the default gateway.

### IPv6 RA CR\_0000246423

**Symptom:** The switch fails to forward IPv6 RA packets.

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

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

### Logging CR\_0000246621

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

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

### PoE CR\_0000244889

**Symptom:** Unable to configure the PoE allocate by value on dual personality ports.

**Scenario:** While provisioning a new member to the 2-member stack the poe-allocate-by value on the dual personality ports cannot be configured.

**Workaround:** After connecting the physical switch, configure the poe-allocate-by value.

## RADIUS Accounting

### CR\_0000244813

**Symptom:** The switch delays the accounting request packet by 50-60 seconds after the client authentication is accepted.

**Scenario:** When the port access is configured for MAC address and 802.1x authentication and the switch is enabled for DHCP snooping, if the authenticated port is concurrently untagged and tagged in different VLAN IDs, the accounting request packet may be delayed by 50-60 seconds.

## SNMP

### CR\_0000246595

**Symptom:** The switch fails to report some stacking ports' details.

**Scenario:** In a stacking configuration, after a switch reboot or redundancy switchover, the switch may fail to report the port status for the standby switch in the SNMP MIB 1.3.6.1.2.1.47.1.1.1.1.7.

**Workaround:** Use the CLI command `show stacking stack-ports` to get the stacking ports' details.

## Spanning Tree

### CR\_0000245603

**Symptom:** The switch CPU utilization increases leading to a switch failure with an error message similar to `NMI event <...> Task='mMstpCtrl' <...>`.

**Scenario:** When root-guard is enabled on multiple switch interfaces, if there are frequent root-guard inconsistencies due to spanning tree instance priority changes, the switch CPU utilization may get high and lead to a switch failure with an error message similar to `NMI event <...> Task='mMstpCtrl' <...>`.

**Workaround:** Adjust the switch spanning tree priority to eliminate the root-guard inconsistencies.

## Web UI

### CR\_0000243495

**Symptom:** On the Web UI, the switch fails to display the port list under the Ports status web page.

**Scenario:** When the LLDP information is updated for a neighbor device, if the SysName contains a colon (":") character, the switch fails to display the port list under the Ports status web page.

**Workaround:** Avoid using the colon (":") character in SysName on peer devices.

## Version 16.05.0011

## ACLs

### CR\_0000245015

**Symptom:** When an IP access-list is configured with a name containing a dot character, the access-list cannot be modified or deleted.

**Scenario:** In the VLAN context, when an IP access-group is configured with a name containing a dot character, the access-list cannot be modified or deleted.

**Workaround:** Configure access-groups with names that do not contain dot characters.

## Central

### CR\_0000244754

**Symptom:** Switch crashes with the following message:

```
Software exception in ISR at pvDmaV1Rx.c:2302  
-> ASSERT: No resources available!
```

**Scenario:** When running XcvtDiag via REST or executing the `show interfaces` command from the CLI at regular intervals, the switch crashes.

**Workaround:** Reload the switch module or the switch.

## mDNS

### CR\_0000244624

**Symptom:** mDNS rule to permit/deny "any" traffic does not work as expected, instead the global default rule to deny all traffic is applied.

**Scenario:** When the following mDNS rules are created, the "any" keyword will be treated as any other service name and the rule will not allow "any" mDNS traffic through the specified VLANs. Instead, the default rule to deny all traffic is applied.

```
mdns profile "mDNS_Profile1"  
  rule 1 service "any" action permit  
  vlan 10,20  
  exit  
mdns profile "mDNS_Profile2"  
  rule 1 service "any" action deny  
  vlan 30,40  
  exit
```

**Workaround:** Apply permit/deny rule by specifying the exact service name.

## RMON

### CR\_0000244685

**Symptom:** The switch fails to record some user logout RMON events in the switch event log.

**Scenario:** When the operator user is configured using the `password operator` command without configuring any manager users, if the user connects to the switching using SSH and logs in as the operator user then moves to manager mode using the `enable` command and logs out from the SSH session, the RMON log-out event of SSH is not displayed in the event logs.

**Workaround:** Configure both operator and manager usernames and passwords on the switch.

## SNMP

### CR\_0000245461

**Symptom/Scenario:** When IPv4 addresses and subnet masks are configured in both ACEs and class entries using SNMP, if the GPPCv2 SNMP code does not contain proper byte-order conversions (NTOHL) for the source and destination IPv4 addresses and their subnet masks, the IP address and subnet mask values are displayed in reverse.

## Spanning Tree

### CR\_0000211478

**Symptom:** The switch displays the port ID as a + symbol in the output of the `show spanning-tree topo-change-history <...>` command.

**Scenario:** When the switch is configured with aggregated ports using a trunk ID greater than 4 characters (for example, trk11, trk111), the switch displays the Port ID as a + symbol in the output of the `show spanning-tree topo-change-history <...>` for those trunk IDs. For example:

Port	Mac Address	Date	Time
+	40a8f0-0e75db	08/18/2016	16:08:18

## CR\_0000244858

**Symptom/Scenario:** When the `show spanning-tree detail` command is executed, the output does not list the counters of the 802.1w and 802.1s topology change packets.

**Workaround:** Execute the `show spanning-tree debug-counters` command to display the counters of the 802.1w and 802.1s topology change packets.

## Syslog

### CR\_0000244622

**Symptom:** When `logging origin-id hostname` is configured and the hostname length is more than 16 characters, the hostname in the syslog message is truncated.

**Scenario:** When the hostname is configured with a length of more than 16 characters and the syslog server is configured over UDP, if the origin-id is set to hostname, the hostname in the syslog message is truncated.

**Workaround:** Configure a shorter hostname where the length is less than or equal to 16 or configure using `logging origin-id ip-address`.

## Telnet/SSH

### CR\_0000244606

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

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

## Version 16.05.0010

Version 16.05.0010 was never released.

## Version 16.05.0009

## 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.

## Authentication

### CR\_0000244438

**Symptom:** An authenticated client loses connectivity to the switch.

**Scenario:** If a switch port is configured for multiple authentication methods (MAC-based and 802.1x) clients already authenticated with one method, for example 802.1x, lose connectivity when any change is made to an authentication parameter for the other authentication method, such as logoff-period, mac-pin, etc.

**Workaround:** Disable and enable the 802.1x and MAC authentication on the port to restore client connectivity.

## 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.

## Config restore CR\_0000243650

**Symptom:** The switch incorrectly displays keys in clear text.

**Scenario:** When using ZTP or the `cfg-restore` to push a switch configuration with encrypted keys included in the switch configuration (`include-credentials` and `encrypt-credentials`), the switch displays the keys and credentials in clear text.

**Workaround:** Disable and re-enable the encryption after the configuration is restored using the `[no]encrypt-credentials` command.

## 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.

## NTP

### CR\_0000244068

**Symptom:** The switch does not allow NTP configuration updates.

**Scenario:** When the switch is configured for encrypted credentials in the configuration (`encrypt-credentials`), the switch fails to update or remove the NTP authentication key when using the `[no] ntp authentication key-id <KEY-ID> command`.

**Workaround:** Disable credentials encryption on the switch (`no encrypt-credentials`) before updating or removing the NTP authentication key and re-enable credentials encryption afterwards (`encrypt-credentials`).

## OSPF

### CR\_0000243557

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

## QoS

### CR\_0000243738

**Symptom:** CLI command `show qos resources` does not display correct information.

**Scenario:** The sum of QoS rules does not add up to the total of rules available on the switch in the results of the `show qos resources` command.

## REST

### CR\_0000244084

**Symptom:** The switch fails to get all the port details in the REST GET call.

**Scenario:** The switch fails to GET the full details for mac-authenticated ports if the REST call is not in the switch port sequence.

## 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.

## Supportability

### CR\_0000237219

**Symptom/Scenario:** In certain conditions, when the switch may suddenly reset due to hardware issues, it fails to generate crash files and there is no reported reason for the reboot in the event logs:

```
00061 system: ST2-STBY: -----
```

## 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 16.05.0008

Version 16.05.0008 was never released.

## Version 16.05.0007

## 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\_0000236784

**Symptom:** Incorrect VLAN assignment is displayed in the output of CLI command `show port-access clients`.

**Scenario:** When an authenticated port is configured with tagged and untagged VLANs during authentication, incorrect VLAN assignment is displayed in the output of CLI command `show port-access clients`.

**Workaround:** Use CLI command `show port-access clients detailed` to display all VLAN assignments to the authenticated port.

### CR\_0000240913

**Symptom:** Switch fails with a `Restr Mem Access` error message.

**Scenario:** In a stacked configuration, in certain conditions, when there is a high surge of 802.1x concurrent client authentication requests with applied ACLs or downloadable user roles received from the RADIUS server, the switch may fail with an error message similar to `Health Monitor: Restr Mem Access <...> Task='rngCtrl'`.

### 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.

## 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>
```

## 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.

## 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.

## 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\_0000240133

**Symptom:** The switch hangs at 'Initializing...' during reboot.

**Scenario:** After a successful client authentication and its associated user-role with downloaded and applied policy configuration ID, if a local user-role is configured with the same policies as the previously downloaded user-role and saved in the switch configuration, the switch may not be able to complete a reboot cycle and may hang during the initialization process.

### 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 16.05.0006

Version 16.05.0006 was never released.

## Version 16.05.0005

Version 16.05.0005 was never released.

## Version 16.05.0004

### REST

#### CR\_0000241465

**Symptom:** The switch may fail to update VLAN configuration changes through the REST API.

**Scenario:** When using REST calls similar to `DELETE /rest/vlans-ports/<vlan_id>-<port_id>`, the switch returns `HTTP/1.1 400 Bad Request` and the switch fails to apply port changes to an existing VLAN.

**Workaround:** Use the REST AnyCli mode or the switch CLI interface to modify the port configuration for an existing VLAN.

## Version 16.05.0003

### 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`.

### 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.
```

### 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.

## Tunneled Node CR\_0000237797

**Symptom:** In certain cases, the traffic may not be properly tunneled.

**Scenario:** When the uplink is configured as LAG, if there is any change in the client VLAN, the switch may fail to properly tunnel the client traffic.

## 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.

## 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.16.05.0013 uses BootROM WB.16.03. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.



**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*.

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](http://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](http://www.hpe.com/support/Subscriber_Choice) to initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email.