WB.16.07.0004 Release Notes

a Hewlett Packard
Enterprise company

Part Number: 5200-5600
Published: March 2019
Edition: 1

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.16.07 branch of the software.

Version WB.16.07.0002 is the initial build of Major version WB.16.07 software. WB.16.07.0002 includes all enhancements and fixes in the WB.16.06.0006 software, plus the additional enhancements and fixes in the WB.16.07.0002 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.16.07.0004	2019-03-04	Released, fully supported, and posted on the web.
WB.16.07.0003	2018-11-21	Released, fully supported, and posted on the web.
WB.16.07.0002	2018-09-13	Initial release of the WB.16.07 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 16.07.0004

No enhancements were included in version 16.07.0004.

Version 16.07.0003

No enhancements were included in version 16.07.0003.

Version 16.07.0002

No enhancements were included in version 16.07.0002.

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 16.07.0004

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`.

Config restore

CR_0000247332

Symptom: The switch fails to restore some previously backed up configuration files.

Scenario: When the backup configuration file contains QoS dscp-map statements, such as `qos dscp-map <code-point> priority <priority>` or `action dscp <code-point>`, the switch fails to restore configuration using the CLI command `cfg-restore`.

Workaround: Use CLI command `copy` to restore such configuration files. Note that this will require a switch reboot.

CR_0000247374

Symptom/Scenario: When "encrypt-credential" is enabled and the switch tries to run the command `cfg-restore tftp` triggered by AirWave, the configured NTP authentication key cannot be configured and displays the following error message:

```
Encrypted key expected for command 'ntp authentication key-id'
```

CR_0000247435

Symptom: When loading a configuration file to the switch using the command `cfg-restore tftp`, the configuration file fails to load.

Scenario: The configuration file fails to load using the `cfg-restore tftp` command in the following cases:

- The configuration file contains `encrypt-credentials`, `include-credentials`, and `hide-sensitive-data` commands.
- The configuration file contains `encrypt-credentials` and `include-credentials` commands and the switch is configured with NTP using the `ntp authentication key-id 5 authentication-mode md5 encrypted-key trusted` command.

CR_0000248007

Symptom: When restoring a config file, the output of the `cfg-restore` command displays the error message `Failed to send authorization REQUEST packet to the TACACS+ server` along with the `Out of memory` error.

Scenario: When a config file is created on a TFTP server with 'encrypt-credentials' and other changes, if the `cfg-restore` command is run, the cfg-restore operation fails with the following error message:

```
Failed to send authorization REQUEST packet to the TACACS+ server
```

Workaround: Remove 'encrypt-credentials' from the config file on the TFTP server.

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`.

MAC Authentication

CR_0000247997

Symptom: The end devices disconnect after successfully being authenticated (MAC) using ClearPass.

Scenario: When the end devices are connected to ports with MAC authentication, authenticated successfully using ClearPass, and assigned to the correct VLAN, they are unable to receive the IP address assigned by DHCP.

Per-user Tunneled Node

CR_0000247797

Symptom: The switch is unable to establish a PUTN tunnel connection.

Scenario: When both MAC and 802.1X authentication are enabled on a port, if there are two responses (one for MAC authentication and the other for 802.1X authentication) with different VLAN IDs, the switch is unable to establish a PUTN tunnel connection.

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.

SSH
CR_0000248171

Symptom/Scenario: When using SSH to connect to a switch through ConsoleWorks, the last few characters entered are not displayed until another character is entered. When using the menu interface through ConsoleWorks, the incorrect option is selected while moving rapidly through the menu and pressing the 'Enter' key.

Workaround: Use an SSH client other than ConsoleWorks.

Stacking
CR_0000247715

Symptom/Scenario: On a two-member 2920 switch stack, the standby member keeps rebooting randomly causing the switch to fail with the following error message:

```
Software exception in ISR at interrupts_om.c:1625 -> OMFP Err Status = 0x00200001
```

Switch Hang
CR_0000247266

Symptom/Scenario: The switch fails with the following error message:

```
NMI event SW:IP=0x0e4471c4 MSR:0x02029200 LR:0x0e3df7a8
               cr: 0x48000400 sp:0x1f39cf28 xer:0x20000000
               Task='mlldpCtrl' Task ID=0x1f3ede68
```

Workaround: Port-access or port-security should not be configured on an interface where mac-notify learn traps are configured.

Transceivers
CR_0000241915

Symptom: Switch port status counters do not increment correctly.

Scenario: When inserting certain 100FX transceivers, such as J9045C, into the switch port without the fiber cable attached, the port status counter may incorrectly increment.

Workaround: There is no functional impact, though there is a false report for port state changes.

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.

CR_0000248790

Symptom: The end client IP address is not displayed in the **Security** > **Clients** page of the switch web interface.

Scenario: When the end client is authenticated using MAC-based authentication with Downloadable User Roles (DUR) and obtains an IP address successfully, if the output of `show port-access client` shows the details of the IP address for the client, the details of the IP address are not displayed on the **Security** > **Clients** page of the switch web interface.

Version 16.07.0003

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.

IPsec
CR_0000244975

Symptom: A VPN tunnel to Airwave fails and does not recover.

Scenario: A VPN tunnel to Airwave is established but is brought down and the switch is not able to re-establish the tunnel to Airwave.

Workaround: Reboot the switch or set the IP address to none and then back to DHCP (no ip address, ip address dhcp) for VLAN 1.

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.

CR_0000246715

Symptom: The switch fails to properly send traffic over the forwarding switch interfaces.

Scenario: In a stacking configuration running spanning tree in PVST mode, after a redundancy switchover to the standby switch, the switch fails to forward traffic after the switch ports transition from Blocking to Forwarding.

Workaround: Disable and re-enable the affected switch ports.

User Roles
CR_0000245072

Symptom: The switch fails to place authenticated users in the critical authentication role.

Scenario: When RADIUS server tracking is enabled and the RADIUS server is unresponsive, the switch fails to place the authenticated clients in the critical authentication role.

Workaround: Disable RADIUS tracking or configure the initial role with the same privileges as the critical authentication role.

VLAN
CR_0000245933

Symptom: Unable to enter the VLAN context using the name of the VLAN.

Scenario: When using the `vlan <vlan-name>` CLI command to enter the VLAN context, an `Invalid input: <vlan-name>` error is displayed.

Workaround: Use the `vlan <vlan-id>` CLI command to enter the VLAN context.

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.

CR_0000245750

Symptom/Scenario: After switch upgrade, when the self-signed certificate is generated, the connection to the switch cannot be established via web server using HTTPS.

Workaround: Downgrade to the lower version, generate the self-signed certificate from that build and use this generated certificate in the upgraded build.

Version 16.07.0002

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_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.

Certificates
CR_0000245750

Symptom/Scenario: After switch upgrade, when the self-signed certificate is generated, the connection to the switch cannot be established via web server using HTTPS.

Workaround: Downgrade to the lower version, generate the self-signed certificate from that build and use this generated certificate in the upgraded build.

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.

Transceivers
CR_0000245596

Symptom/Scenario: When `allow-unsupported-transceiver` is enabled on a switch, the supported transceiver is shown as unsupported or excluded. However, when the `allow-unsupported-transceiver` is disabled, the same transceiver works.

Workaround: Disable unsupported transceiver mode config.

VLAN
CR_0000245933

Symptom: Unable to enter the VLAN context using the name of the VLAN.

Scenario: When using the `vlan <vlan-name>` CLI command to enter the VLAN context, an `Invalid input: <vlan-name>` error is displayed.

Workaround: Use the `vlan <vlan-id>` CLI command to enter the VLAN context.

Upgrade information

Upgrading restrictions and guidelines

WB.16.07.0004 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**.
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.