WB.16.06.0006 Release Notes

a Hewlett Packard
Enterprise company

Part Number: 5200-5222
Published: June 2018
Edition: 1

© Copyright 2018 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.16.06 branch of the software.

Version WB.16.06.0006 is the initial build of Major version WB.16.06 software. WB.16.06.0006 includes all enhancements and fixes in the WB.16.05.0003 software, plus the additional enhancements and fixes in the WB.16.06.0006 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	Based on	Remarks
WB.16.06.0006	2018-06-26	WB.16.05.0003	Initial release of the WB.16.06 branch. Released, fully supported, and posted on the web.
WB.16.05.0009	2018-06-08	WB.16.05.0008	Released, fully supported, and posted on the web.
WB.16.05.0008	n/a	WB.16.05.0007	Never released.
WB.16.05.0007	2018-03-28	WB.16.05.0006	Released, fully supported, and posted on the web.
WB.16.05.0006	n/a	WB.16.05.0005	Never released.
WB.16.05.0005	n/a	WB.16.05.0004	Never released.
WB.16.05.0004	2017-12-22	WB.16.05.0003	Released, fully supported, and posted on the web.
WB.16.05.0003	2017-12-12	WB.16.04.0008	Initial release of the WB.16.05 branch. Released, fully supported, and posted on the web.
WB.16.04.0010	2017-10-16	WB.16.04.0008	Released, fully supported, and posted on the web.
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.

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 16.06.0006

HTTP Proxy support with ZTP

The Aruba switch connects through Public Cloud to access Aruba Activate and Aruba Central. The switch uses a combination of the Public and Private networks to access Aruba Airwave, and Aruba ClearPass Policy Manager (CPPM). This features provides support for an HTTP Proxy during the Zero Touch Provisioning (ZTP) process.

For more information see the *Management and Configuration Guide* for your switch.

IPSec tunnel to secondary controller

ArubaOS-Switch provides support for IPSec tunnel between the switch and the Aruba Controller as VPN concentrator to carry switch-generated traffic to multiple services behind the Aruba Controller. The services include Airwave, ClearPass, DNS, and Syslog. IPsec tunnel needs a backup support for IPsec session failure. With this feature, if the existing IPsec session is lost, the switch is able to establish a new IPsec tunnel session with a backup controller (secondary controller).

For more information, see the *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 16.06.0006

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 <POLIY-ID>` command.

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

CLI
CR_0000243117

Symptom: The switch fails while collecting support information.

Scenario: When the switch is configured to allow mac-moves on ports, the switch may fail with an error message similar to `Invalid Instr Misaligned Mem Access <...> Task='mAdMgrCtrl'`, when dumping multiple switch support information using the `show tech` *`<OPTION>`* or `copy command-output 'show tech` *`<OPTION>`*`' ...` commands in a middle of a mac-move action.

Workaround: Avoid collecting support files from multiple concurrent sessions.

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.

DHCP Snooping
CR_0000244260

Symptom: The switch drops certain DHCPv6 advertisements.

Scenario: When the switch is configured for DHCPv6 Snooping, the switch drops DHCPv6 advertisements with the IAID value (option 3) set to 0.

Workaround: Disable DHCPv6 Snooping where there are clients requesting IPv6 address send DHCPv6 solicit requests with an IAID value 0 (option 3).

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.

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.

CR_0000244262

Symptom: The switch is incorrectly assuming the default priority value 5 for DSCP codepoint 46 instead of value 7.

Scenario: When the default value of DSCP codepoint 46 is changed to 5 using the `qos dscp-map 46 priority 5` command, the switch does not display the configuration in the output of the `show running-config` or `show config` commands.

Workaround: There is no functional impact to QoS DSCP. Verify the DSCP configuration using the `show qos dscp-map` 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.

CR_0000242387

Symptom: Unable to establish SSH connections to the switch.

Scenario: Over time, the switch may become unable to accept SSH connections. When attempting to access the switch console interface, it may crash with an error message similar to `Unable to get semaphore for Server`.

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.

Web UI
CR_0000243453

Symptom: The port statistic counters in the **Interfaces / Ports** section are not properly updated.

Scenario: When the Ports Status page of the NextGen web interface is accessed, the ports counters are not immediately updated. Once an individual port is selected, the counter is updated appropriately.

Workaround: There is no functional impact. This is a display issue with populating the counters on the first access of the **Ports Status** page.

CR_0000243765

Symptom: The switch is not accessible via secured connection to the web management interface.

Scenario: In a redundant configuration, the switch cannot be accessed through its secured web interface after a redundancy failover event to the standby switch or management module.

Workaround: Reconfigure secured access for web management using the `web-management ssl` command after the failover event.

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.16.06.0006 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.

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.