WB.16.05.0003 Release Notes

Part Number: 5200-4703a
Published: December 2017
Edition: 2

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	Based on	Remarks
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.
WB.16.03.0005	2017-07-07	WB.16.03.0004	Released, fully supported, and posted on the web.
WB.16.03.0004	2017-04-17	WB.16.03.0003	Released, fully supported, and posted on the web.
WB.16.03.0003	2016-12-20	WB.16.02.0008	Initial release of the WB.16.03 branch. Released, fully supported, and posted on the web.
WB.16.02.0014	2016-10-28	WB.16.02.0013	Please see the WB.16.02.0114 release notes for detailed information on the WB.16.02 branch. Released, fully supported, and posted on the web.
WB.16.02.0013	n/a	WB.16.02.0012	Never released.

Table Continued

Version number	Release date	Based on	Remarks
WB.16.02.0012	2016-08-31	WB.16.02.0011	Released, fully supported, and posted on the web.
WB.16.02.0011	2016-08-24	WB.16.02.0010	Released, fully supported, and posted on the web.
WB.16.02.0010	2016-08-11	WB.16.02.0009	Released, fully supported, and posted on the web.
WB.16.02.0009	n/a	WB.16.02.0008	Never released.
WB.16.02.0008	2016-07-08	WB.16.01.0004	Initial release of the WB.16.02 branch. Released, fully supported, and posted on the web.

Products supported

This release applies to the following product models:

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

Compatibility/interoperability

The switch web agent supports the following web browsers:

Browser	Supported versions
Internet Explorer	• Edge • 11
Chrome	• 53 • 52

Table Continued

Browser	Supported versions
Firefox	• 49 • 48
Safari (MacOS only)	• 10 • 9

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 WB.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.

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

Version WB.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.

REST

CR_0000241465

Symptom: The switch may fail to update VLAN configuration changes though 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.

Upgrade information

Upgrading restrictions and guidelines

WB.16.05.0003 uses BootROM WB.16.03. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

For more information about BootROM, see the *ArubaOS-Switch Management and Configuration Guide WB. 16.04*.

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

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

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

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

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

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

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

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

Finding Security Bulletins

Procedure

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

Security Bulletin subscription service

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

Networking Websites

Hewlett Packard Enterprise Networking Information Library

www.hpe.com/networking/resourcefinder

Hewlett Packard Enterprise Networking Software

www.hpe.com/networking/software

Hewlett Packard Enterprise Networking website

www.hpe.com/info/networking

Hewlett Packard Enterprise My Networking website

www.hpe.com/networking/support

Hewlett Packard Enterprise My Networking Portal

www.hpe.com/networking/mynetworking

Hewlett Packard Enterprise Networking Warranty

www.hpe.com/networking/warranty

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

For additional websites, see **Support and other resources**.

Accessing Hewlett Packard Enterprise Support

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

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

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

Information to collect

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

Accessing updates

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

  Hewlett Packard Enterprise Support Center
  www.hpe.com/support/hpesc
  Hewlett Packard Enterprise Support Center: Software downloads
  www.hpe.com/support/downloads
  Software Depot
  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

www.hpe.com/support/AccessToSupportMaterials

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

Customer self repair

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

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

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

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

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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