WB.16.03.0003 Release Notes

Part Number: 5200-2945
Published: December, 2016
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.

Chapter 1 WB.16.03.0003 Release Notes 5
Description 5
Important information 5
Version history 5
Products supported 6
Compatibility/interoperability 6
Enhancements 6
Version WB.16.03.0003 7
DHCP Snooping 7
Federal Government certifications 7
Hiding sensitive information 7
IPsec 7
Job Scheduler 7
LLDP 8
Netdestinations and Netservices 8
Next Gen Web UI 8
Warning message for configuring PoE allocate-by-value 8
Power allocation algorithm based on usage power for allocate-by-usage mode 8
REST 8
show interface Command 8
show power-over-ethernet Display 8
show system Commands 8
Static IP visibility 9
TCP Push Preserve 9
VLAN range addition 9
Fixes 9
Version WB.16.03.0003 9
ARP 9
Cable Diagnostic 10
DHCP 10
DHCP Server 10
Job Scheduler 10
OpenFlow 11
SNMP 11
Upgrade information 11

Chapter 2 Hewlett Packard Enterprise security policy 12
Finding Security Bulletins 12
Security Bulletin subscription service 12

Chapter 3 Websites 13

Chapter 4 Support and other resources 14
Accessing Hewlett Packard Enterprise Support 14
Accessing updates 14
Customer self repair 14
Remote support 15

Warranty information....15
Regulatory information....15
Documentation feedback....16

Description

This release note covers software versions for the WB.16.03 branch of the software.

Version WB.16.03.0003 is the initial build of Major version WB.16.03 software. WB.16.03.0003 includes all enhancements and fixes in the WB.16.02.0008 software, plus the additional enhancements and fixes in the WB.16.03.0003 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.16.03.0003	2016-12-20	WB.16.02.0008	Initial release of the WB.16.03 branch. Released, fully supported, and posted on the web.
WB.16.02.0014	2016-10-28	WB.16.02.0013	Please see the WB.16.02.0114 release notes for detailed information on the WB.16.02 branch. Released, fully supported, and posted on the web.
WB.16.02.0013	n/a	WB.16.02.0012	Never released.
WB.16.02.0012	2016-08-31	WB.16.02.0011	Released, fully supported, and posted on the web.
WB.16.02.0011	2016-08-24	WB.16.02.0010	Released, fully supported, and posted on the web.
WB.16.02.0010	2016-08-11	WB.16.02.0009	Released, fully supported, and posted on the web.
WB.16.02.0009	n/a	WB.16.02.0008	Never released.
WB.16.02.0008	2016-07-08	WB.16.01.0004	Initial release of the WB.16.02 branch. Released, fully supported, and posted on the web.
WB.16.01.0008	2016-08-02	WB.16.01.0007	Please see the WB.16.01.0008 release notes for detailed information on the WB.16.01 branch. Released, fully supported, and posted on the web.

Table Continued

Version number	Release date	Based on	Remarks
WB.16.01.0007	2016-05-31	WB.16.01.0006	Released, fully supported, and posted on the web.
WB.16.01.0006	2016-03-28	WB.16.01.0005	Released, fully supported, and posted on the web.
WB.16.01.0005	n/a	WB.16.01.0004	Never released.
WB.16.01.0004	2016-01-20	WB.15.18.0007	Initial release of the WB.16.01 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

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.16.03.0003

DHCP Snooping

The binding table built by the DHCP Snooping feature might need to be cleared by an administrator in case:

- If there is a change of the DHCPv4 Server or change in the configuration of the server
- If there are changes in the network topology causing the clients movement to a different VLAN or port
- If the administrator wants to clear the entries for clients that are not actively using the lease

The `clear dhcp-snooping binding` command has been added to cater to the above use cases.

Federal Government certifications

In order to meet security requirements under NDcPP (Network Device Collaborative Protection Profile) additional security features have been delivered as part of this release. The following features have been implemented:

IPSec support for OSPFv3: Provides support for authentication for OSPFv3 routing traffic on switches running ArubaOS-Switch. The authentication support for OSPFv3 will be provided in compliance to RFC 4552 (partially, covering the portions required by NDcPP).

SHA-256 support for management user passwords: Provides a CLI to store administrative passwords as uniquely sorted SHA-256 hashes.

Validation of Extended Key Usage Extension in X509 certificates: This feature validates the EKU field of X509v3 for the Client and Server authentication OIDs.

RSA-1024 deprecation: Provides a CLI to remove support for RSA-1024 key generation.

TLS1.2 Enforcement: Forces the Zero Touch Provisioning applications on the switch to use TLS1.2.

Local Audit Command Logging: Supports local storage of log files of all administrative actions done on the switch.

Re-Key Support for Secure Shell Protocol: This feature enables the support for SSH Re-Keying for SSH Server and SSH Client.

Support for X509v3 Certificate Authentication for Secure Shell Protocol: Enables the support for X509v3 certificate based server and user authentication for SSH protocol.

Hiding sensitive information

The newly added `hide-sensitive-data` command prevents sensitive information like keys and passwords from being visible in plain text during the configuration in standard secure mode of the switch.

IPsec

To create a secure channel for communication between the switch and certain services such as Airwave, ClearPass, Syslog, DNS, and others, support has been added for creating an IPSec tunnel between the switch and the Aruba mobility controller acting as VPN concentrator. The feature can be used by customers who are looking for a secure way to communicate with certain services. There is also the ability to set routes to multiple destinations through the IPSec tunnel as well as a default gateway route from the switch to controller for non-IPSec traffic.

Job Scheduler

Minor enhancements to the job scheduler feature to:

1. show the last run time in the `show job <job_name>` command
2. not to display the job as disabled in `show running` if it has run and will never run anymore
3. show the status in `show job <job_name>` as expired/executed.

LLDP

This a security feature to prevent the LLDP packets from sending out the management IP address of the switch as part of the TLV. Since this information is not relevant to client devices and PoE devices, we provide an additional CLI command to disable sending out the management IP addresses as part of LLDP TLVs.

Netdestinations and Netservices

This feature simplifies CLI configuration of ACL rules and reduces the tediousness of configuring ACL rules for multiple hosts and services . `net-destination` is a list of hosts, networks or subnets and 'net-service' is a list of names for UDP or TCP port numbers. Using a combination of the `net-service` and `net-destination` commands users can configure complex ACL rules in a few lines of configuration.

Next Gen Web UI

The Next Gen Web GUI, which was experimental and available only on the 2930F, is now available on all ArubaOS-Switch platforms and includes additional troubleshooting and visualization capabilities. NextGenWebUI is the default WebUI from 16.03 release onwards. There is an option to set the newer GUI as the default if desired.

Warning message for configuring PoE allocate-by-value

Since `poe-alloc-by value` and `poe-value` are existing commands but are not standard PoE features, a warning message has been added to proceed with caution.

Power allocation algorithm based on usage power for allocate-by-usage mode

When the switch is configured in poe-alloc-by-usage mode and PoE LLDP is enabled (which is the default switch configuration), even when an AP is only drawing 5-7w per port, the power reserved on the port is as per LLDP requested power. This limits the total number of such APs that will be powered by the switch. This feature allows the power reservation on the port to be as per the actual used power and not LLDP requested power. This allows more APs/devices to be powered on than before.

REST

Additional REST APIs have been added to enhance the programmability of switches running ArubaOS-Switch.

show interface Command

Enhanced the `show interface [ethernet] <port_list>` and the `show interface queues` commands to indicate which ports are link down versus administratively down.

show power-over-ethernet Display

Enhancements to the `show power-over-ethernet br` and `show power-over-ethernet <port | all>` CLI commands to provide more information on the various power allocation models, LLDP configuration and associated power reporting.

show system Commands

The `show system power-supply` command was modified to include details on all system power usage including fan, management modules and line cards. This details include available system power, actual real-time demand and available budget. It also distinguishes between 100V and 220V power supplies.

The `show system temperature` has also been modified to include the temperature of the power supply.

Static IP visibility

This feature allows ClearPass to perform accounting for clients with static IP address. Using the `ip client-tracker` command allows the switch to learn the client's IP address by snooping the initial data packets. The benefit of this feature is that the RADIUS server will have visibility to clients with DHCP as well as static IP addresses.

TCP Push Preserve

Starting with this build, the TCP Push Preserve mode is set to DISABLED by default.

The TCP Push Preserve mode determines the queuing of the TCP packets that have the PUSH flag set. When this mode is enabled and the egress queue is full, TCP packets with the PUSH flag set are queued at the head of the ingress queue for egress queue space. This may delay subsequent incoming packets in the same queue and create a head-of-line blocking situation. When this mode is disabled and the egress queue is full, TCP packets with the PUSH flag set are dropped from the head of the ingress queue.

If the current switch TCP Push Preserve mode has been set to DISABLED, it will be preserved as DISABLED and the corresponding configuration entries will be suppressed. If the current switch TCP PUSH preserve mode has been set to ENABLED, it will be changed to DISABLED and the change will be noted in system event logs as `The tcp-push-preserve feature was disabled. This is a change to default configuration.`

The CLI command `show tcp-push-preserve` indicates the status of TCP push mode ENABLED/DISABLED. CLI command `[no] tcp-push-preserve` changes the status of TCP push mode.

VLAN range addition

A new feature that allows creation and management of multiple VLANs and assigns multiple ports to them at the time of creation. Only tagged ports are supported in this command while creating a list of VLANs. This feature simplifies bulk creation and management of VLANs.

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.16.03.0003

ARP
CR_0000200474

Symptom: The switch may intermittently drop traffic when receiving high level of ARP requests for unresolved ARP entries.

Scenario: If the switch is configured with subnet size that allows for more than 16K host entries (example: CIDR /18 (netmask 255.255.192.0) or greater), when receiving bursts of ARP request for unknown ARP entries, the switch may temporary lose connectivity on active connections.

Workaround: Configure the switch with smaller sized subnets than CIDR /18 (netmask 255.255.192.0).

Cable Diagnostic
CR_0000222089

Symptom: Non-support for cable diagnostic tests is not indicated prior to executing the tests.

Scenario: When executing the CLI command `test cable-diagnostics <PORT-LIST>`, on a switch port that does not support this feature, the following execution warning message is displayed for non-supported ports:

```
This command will cause a loss of link on all tested ports and will take several
seconds per port to complete. Use the 'show cable-diagnostics' command to view the
results. Continue (y/n)? Y.
```

The non-support for such test is indicated only when displaying the test results using CLI command `'show cable-diagnostics' command'`, in a report message such as `Port <port-number> does not support cable diagnostics.`.

A new check is added to identify the non-supported ports before executing the cable diagnostic test.

DHCP
CR_0000222120

Symptom: The switch DHCP server may delay honoring IP address renewal requests.

Scenario: When a client which acquired an IP address from the switch DHCP server is roaming to a different VLAN also managed by the switch DHCP server, a fresh new DHCP client request process is initiated in place of the DHCP renewal request process, resulting in a longer delay for the DHCP client to acquire the new IP address.

Workaround: Using an external DHCP server may help resolve the delay in DHCP client IP renewal when roaming from one VLAN to another.

DHCP Server
CR_0000216603

Symptom: DHCP clients are not able to obtain IP addresses from the switch's locally configured DHCP server address pool.

Scenario: When the default route (0.0.0.0/0) is configured with a VLAN as the next hop, the DHCP request packets are being dropped and the DHCP clients are not able to obtain IP address from the switch DHCP server.

Workaround: Configure the default route's next hop value with an IP address instead of a VLAN.

Job Scheduler
CR_0000221236

Symptom: The switch does not execute scheduled jobs at expected scheduled time.

Scenario: When the switch time settings are adjusted for time protocol, time zone or daylight savings time rule (daylight-time-rule), the Job Scheduler fails to execute scheduled jobs at the configured time. This is triggered when switch time is (re-)adjusted, following a time settings change. For example, adding a daylight-time-rule would trigger a time re-adjustment, but the job scheduler time is not re-adjusted with the new switch time settings and it will not trigger job execution at the expected time.

Workaround: Remove and re-configure the jobs after making configuration changes to the switch time settings.

CR_0000222032

Symptom: When executing a scheduled job involving the copy command with a server hostname, the switch may crash with a message similar to: `Health Monitor: Read Error Restr Mem Access <...> Task='tCron000001' <...>`.

Scenario: If a job is scheduled to copy data files to/from a remote server configured with a HOSTNAME in the COMMAND-STR of the CLI command `job`, the switch may crash with an error message similar to `Health`

`Monitor: Read Error Restr Mem Access <...> Task='tCron000001' <...>` when executing the job at scheduled time.

Example: `job <name> at [HH:]MM "copy running-config tftp mytftpserver.com FILENAME-STR"`.

Workaround: Configure the job to copy data files using IP address instead of hostname.

Example: `job <name> at [HH:]MM "copy running-config tftp 192.168.0.1 FILENAME-STR"`.

OpenFlow
CR_0000219687

Symptom: OpenFlow fails to authenticate a client with a DHCP-assigned IP address.

Scenario: OpenFlow fails to authenticate a client with a DHCP-assigned IP address, when the DHCP client and the DHCP server are connected on different OpenFlow VLANs with IP routing enabled.

Workaround: Configure DHCP server on a non-OpenFlow VLAN.

SNMP
CR_0000217437

Symptom: Switch does not report the information regarding IPv6 loopback interface reported in MIB object ipAddressIfIndex.

Scenario: After an IPv6 link-local address is configured on a VLAN, the switch no longer reports the information regarding IPv6 loopback interface reported in MIB object ipAddressIfIndex when executing CLI command `walkMIB ipAddressIfIndex`.

Upgrade information

Upgrading restrictions and guidelines

WB.16.03.0003 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 *HPE ArubaOS-Switch Management and Configuration Guide WB.16.03*.

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.

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 *HPE ArubaOS-Switch Basic Operations Guide Version 16.03*.

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 **www4.hpe.com/signup_alerts** 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 HP 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, see the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* document, available at the Hewlett Packard Enterprise Support Center:

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.