Hewlett Packard Enterprise

WB.16.01.0006 Release Notes

Abstract

This document contains supplemental information for the WB.16.01.0006 release.

Part Number: 5200-0960
Published: March 2016
Edition: 1

Acknowledgments

Contents

1 WB.16.01.0006 Release Notes

Description

This release note covers software versions for the WB.16.01 branch of the software.

Version WB.16.01.0004 was the initial build of Major version WB.16.01 software. WB.16.01.0004 includes all enhancements and fixes in the WB.15.18.0007 software, plus the additional enhancements and fixes in the WB.16.01.0004 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.

Firmware downgrade is not allowed if the max-vlans value is greater than 2048. Unconfigure the max-vlans before attempting to downgrade from WB.16.01 to an earlier version 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 16.01*.

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.16.01.0006	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	Released, fully supported, and posted on the web.
WB.15.18.0007	2015-11-10	WB.15.18.0006	Released, fully supported, and posted on the web.
WB.15.18.0006	2015-08-15	WB.15.17.0003	Initial release of the WB.15.17 branch. Released, fully supported, and posted on the web.
WB.15.17.0009	2015-11-10	WB.15.17.0008	Please see the WB.15.17.0009 release note for detailed information on the WB.15.17 branch. Released, fully supported, and posted on the web.
WB.15.17.0008	2015-08-29	WB.15.17.0007	Released, fully supported, and posted on the web.
WB.15.17.0007	2015-06-22	WB.15.17.0006	Released, fully supported, and posted on the web.
WB.15.17.0006	n/a	WB.15.17.0005	Never released.
WB.15.17.0005	2015-05-11	WB.15.17.0004	Released, fully supported, but not posted on the web.

Version number	Release date	Based on	Remarks
WB.15.17.0004	2015-04-23	WB.15.17.0003	Released, fully supported, but not posted on the web.
WB.15.17.0003	n/a	WB.15.16.0004	Initial release of the WB.15.17 branch. Never released.

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 operating system and web browser combinations:

Operating System	Supported Web Browsers
Windows XP SP3	Internet Explorer 7, 8 Firefox 12
Windows 7	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows 8	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows Server 2008 SP2	Internet Explorer 8, 9 Firefox 24
Windows Server 2012	Internet Explorer 9, 10 Firefox 24
Macintosh OS	Firefox 24

Minimum supported software versions

NOTE: If your switch or module is not listed in the below table, it runs on all versions of the software.

Product number	Product name	Minimum software version
J9805A	HPE 640 Redundant/External PS Shelf	WB.15.13.0003

For information on networking application compatibility, see the *HPE ArubaOS-Switch Software Feature Support Matrix*.

Enhancements

This section lists enhancements added to the WB.16.01 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.

NOTE: The number preceding the enhancement description is used for tracking purposes.

Version WB.16.01.0006

Authentication

CR_0000181093 Increase maximum password length for local user from 16 to 64 characters.

Event Log

CR_0000189525 Added audit log message to the system logging for the following events:

- termination of a secure session
- failure to negotiate the cipher suite due to cipher mismatch for SSL and SSH sessions

CR_0000190131 Added RMON audit log messages when SNTP is disabled using CLI command `no sntp`.

CR_0000190134 Added an audit log message regarding the console inactivity timer when the `console idle-timeout` command is used.

CR_0000190141 Added audit log messages when default gateway IP address is configured or modified.

RADIUS

CR_0000183521 New options added to CLI command to configure replay protection for dynamic authorization messages "positive-time-window" and "plus-or-minus-time-window". Example:

Usage: `[no] radius-server host <IP-ADDR> time-window <Seconds>`

`radius-server host <IP-ADDR> time-window positive-time-window`

`radius-server host <IP-ADDR> time-window plus-or-minus-time-window`

When replay protection is enabled and positive-time-window is set, messages from the server must contain an Event-Timestamp attribute that differs from the current time by no more than the specified number of seconds. When replay protection is enabled and plus-or-minus-time-window is set, messages from the server must contain an Event-Timestamp attribute that differs from the current time by no more than the (+/-) specified number of seconds. The positive-time-window option is default with 300 seconds as its default value.

Zeroization

CR_0000183856 Added CLI command `erase all [zeroize]` to enable zeroization of the switch file storage.

Example:

```
HP Switch(config)# erase all zeroize
The system will be rebooted and all management module files except
software images will be erased and zeroized. This will take up to 60
minutes and the switch will not be usable during that time. Continue
(y/n)? y
```

The zeroization feature will remove and “zeroize” all the files from flash storage except software images. Information removed includes the following:

- switch configurations
- system generated private keys
- user installed private keys
- legacy manager/operator password files
- crypto-key files
- fdr logs
- core dumps

It is recommended that zeroization be performed from the serial console so that the status information can be viewed during the zeroization process.

Version WB.16.01.0005

Never released.

Version WB.16.01.0004

ACL Grouping

In general, for each of the “x” ACEs configured on the switch will consume x*n hardware resources. If the ACEs are shared under a common group the hardware resource consumption can be reduced to “n”. Hence share/group ACL reduces the hardware resource usage when the same ACL is applied to multiple ports/VLANs, hence making maximum hardware resource usage. For more information, see the *HPE ArubaOS-Switch Access Security Guide* and the *HPE ArubaOS-Switch Advanced Traffic Management Guide* for your switch.

Platform support: 2920, 3800, 3810, 5400R

AirWave

AirWave is a Network Management Solution (NMS) tool. Once connected to AirWave, the user can

- Configure Aruba switches using Zero Touch Provisioning (ZTP)
- Configure Aruba switches using the CLI
- Troubleshoot Aruba switches
- Monitor Aruba switches
- Upgrade Aruba firmware for your switches

For more information, see the *HPE ArubaOS-Switch Management and Configuration Guide* for your switch.

Platform: 2530, 2620, 2920, 3800, 3810, 5400R

ARP Attack Detection

Source-MAC based ARP attack detection protects the switch CPU from ARP attacks by enabling restriction of the overall number of ARP packets the CPU receives from a given client. An ARP attack occurs when the switch receives more ARP packets from the same source MAC address than allowed by the configured threshold setting. IP ARP-throttle uses a “remediation mode” to determine whether IP ARP-throttle simply monitors the frequency of ARP packets or actually restricts the ARP-packet traffic from a given client. In cases where normal operation of a device in your network exceeds the configured IP ARP-throttle threshold, and you do not want to blacklist

the device, you can configure IP ARP throttling to exclude that device from being monitored. For more information, see the *HPE ArubaOS-Switch Multicast and Routing Guide* for your switch.

Platform: 2530, 2620, 2920, 3500, 3810, 5400, 5400R

Aruba Rebranding for Web UI

The 2530, 2920, and 5400R switches have taken on the Aruba sub-brand. The products are now called the Aruba 2530 Switch Series, the Aruba 2920 Switch Series, and the Aruba 5400R zl2 Switch Series.

Auto Configuration with Aruba AP

Auto device detection and configuration

The auto device detection and configuration detects a directly connected Aruba AP dynamically and applies predefined configurations to ports on which the Aruba AP is detected. The following parameters are supported:

- `untagged-vlan`
- `tagged-vlan`
- `ingress-bandwidth`
- `egress-bandwidth`
- `cos`
- `speed-duplex`
- `poe-max-power`
- `poe-priority`

Auto VLAN configuration

VLAN configuration on Aruba APs are learned automatically using GVRP protocol.

Rogue AP isolation

The Rogue AP Isolation feature detects and blocks any unauthorized APs in the network. You can either log or block the rogue device. If the action requested is to log the rogue device, the MAC address of the rogue device is logged in the system logs (RMON). If the action is to block the rogue device, the traffic to and from the MAC address of the rogue device is blocked. The MAC is also logged in the system log.

Platform: 2530, 2620, 2920, 3800, 3810, 5400R

Bonjour Gateway

Hewlett Packard Enterprise's mDNS Gateway solution supports Apple's Bonjour protocol to the switch.

The mDNS gateway, running on a switch, will listen for Bonjour responses and Bonjour queries and forward them to different subnets. Its main function is to forward Bonjour traffic between different subnets (reflector). For more information, see the *HPE ArubaOS-Switch Multicast and Routing Guide* for your switch.

Platform: 2530, 2620, 2920, 3500, 3800, 3810, 5400, 5400R

Captive portal for ClearPass

The Captive Portal feature allows the support of the ClearPass Policy Manager (CCPM) into the ArubaOS-Switch product line. The switch provides configuration to allow you to enable or disable the Captive Portal feature.

By default, Captive Portal is disabled to avoid impacting existing installations as this feature is mutually exclusive with the following web-based authentication mechanisms:

- Web Authentication
- EWA
- MAFR
- BYOD Redirect

Platform: 5400 (V2 only), 2620, 2920, 3800, 5400R, 3810
5400 (V1), and 3500: only CoA Port Bounce not Captive Portal Redirect

Chromecast Gateway

Chromecast is a line of digital media players developed by Google. Designed as small dongles, the devices play audio/video content on a high-definition television or home audio system by directly streaming it via Wi-Fi from the Internet or a local network. Users select the media to play using mobile apps and web apps that support the Google Cast technology.

Chromecast uses a simple multicast protocol for mDNS discovery and launch that enables users to mirror their devices on a second screen.

Hewlett Packard Enterprise supports mDNS protocol, implemented as a server. mDNS is the primary method of discovering a Chromecast that supports the v2 API. For more information, see the *HPE ArubaOS-Switch Multicast and Routing Guide* for your switch.

Platform: 2530, 2620, 2920, 3500, 3800, 3810, 5400, 5400R

IGMPv3

The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group membership to any neighboring multicast routers. Version 1, specified in [RFC-1112], was the first widely-deployed version. Version 2, specified in [RFC-2236], added support for “low leave latency”, that is, a reduction in the time it takes for a multicast router to learn that there are no longer any members of a particular group present on an attached network.

Version 3 adds support for “source filtering”, that is, the ability for a system to report interest in receiving packets only from specified source addresses, or from all but specified source addresses, sent to a particular multicast address.

Version 3 is designed to be interoperable with Versions 1 and 2. For more information, see the *HPE ArubaOS-Switch Multicast and Routing Guide* for your switch.

Platform support: 2920, 3800, 3810, 5400R

Instrumentation Enhancements

Supportability Infrastructure: User Initiated Diagnostic Reset via Clear button

This feature allows the switch’s front panel button (Clear) to manually initiate a diagnostic reset. User can perform reliable diagnostic reset via the front panel button (Clear) which will capture information needed to debug application hang. Diagnostic reset is controlled via the Front Panel Security (FPS) options.

Supportability infrastructure: User Initiated Diagnostic Reset via Serial Console

This supportability feature remotely triggers a diagnostic reset via serial console to reboot the switch and collect diagnostic data to debug switch application hang or system hang or any other rare occurrences (which is seen rarely in the lab, field, or customer setups). This feature improves the service availability of the switch by providing remote diagnostic reset option via serial console attached to the accessible console server and provide the diagnostic data to quickly analyze the issue and debug. Diagnostic reset is controlled via FPS options.

The serial sequence to initiate User Initiated Diagnostic Reset via Serial console is Ctrl+S, Ctrl+T, Ctrl+Q, Ctrl+T, Ctrl+S. For more information, see the *HPE ArubaOS-Switch Management and Configuration Guide* for your switch.

Platform: 2530, 2620, 2920, 3500, 3800, 3810, 5400, 5400R

Job Scheduler

The Job Scheduler feature enables the user to schedule commands or jobs on the switch for one time or multiple times. This is similar in concept to the UNIX ‘cron’ utility. The user can schedule any CLI command that the user would otherwise enter interactively. This includes commands to enable or disable ports, LEDs, and Power-Over-Ethernet. Jobs can also be scheduled to be triggered by certain pre-defined events such as switch reboot. The only major restriction on commands is the user cannot prompt for user input. For more information, see the *HPE ArubaOS-Switch Management and Configuration Guide* for your switch.

Platform support: 2530, 2620, 2920, 3800, 3810, 5400R

LLDP over OOBM

The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling the switch to advertise itself to adjacent devices and to learn about adjacent LLDP devices.

Standard LLDP frames are sent over regular Ethernet ports on the switch. LLDP over OOBM is an extension that allows LLDP frames to be sent over an OOBM port. For more information, see the *HPE ArubaOS-Switch Management and Configuration Guide* for your switch.

Platform support: 2920, 3800, 3810, 5400R

Max VLANs

A maximum of 4K VLANs can be configured on supported switches. This support is for 5400R, 3800 and 3810 platforms. For 2920 the support is limited to 1022. The existing scale numbers for IP VLAN and Static route has been changed. For more information, see the *HPE ArubaOS-Switch Advanced Traffic Management Guide* for your switch.

Platform	Attribute	15.18	16.01
5400R, 3800, 3810	VLAN	2048	4094
	IP VLAN	512	1024 total with up to: • 1024 IPv4 • 512 IPv6
	Static Route	256	1024 total with up to: • 256 interface-based • 1024 gateway-based
2920	VLAN	256	1022
	IP VLAN	256	512 total with up to: • 512 IPv4 • 256 IPv6
	Static Route	256	256 Total

Platform support: 2920, 3800, 3810, 5400R

MVRP

The Multiple VLAN Registration protocol (MVRP) provides a mechanism of dynamically propagating VLAN information from a source switch to other switches in the LAN.

MVRP is similar to GVRP where by which it helps administrators to maintain the VLAN topology in an efficient way. GVRP by itself is not optimized for VLAN propagation when the scale of VLAN grows. To address this IEEE has come up with MVRP, the new multi registration protocol to propagate VLANs. For more information, see the *HPE ArubaOS-Switch Advanced Traffic Management Guide* for your switch.

Platform support: 2530, 2620, 2920, 3800, 3810, 5400R

ND Snooping

Neighbor Discovery Protocol uses the Internet Control Message Protocol version 6 (ICMPv6) for the purpose of router solicitation, router advertisement, neighbor solicitation, neighbor advertisement, and network redirects.

The Neighbor Discovery Protocol packets can be easily exploited by the spoofers/attackers in the ipv6 network if there are no security mechanisms. ND snooping provides security against different kind of attacks. For more information, see the *HPE ArubaOS-Switch IPv6 Configuration Guide* for your switch.

Platform support: 2920, 3800, 3810, 5400, 5400R

NTP

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers in order to correlate events when system logs and other time-specific events from multiple network devices received.

NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communications use Coordinated Universal Time (UTC). For more information, see the *HPE ArubaOS-Switch Management and Configuration Guide* for your switch.

Platform support: 2530, 2620, 2920, 3500, 3800, 3810, 5400, 5400R

Password Complexity

In current provision software, the user is not enforced to configure a complex password. As per UCR 2008 requirements there are few checks that are to be performed while configuring the password. Also, to provide some alert mechanisms to the user based on the configuration at the expiry of the password.

The password configuration and password complexity check will be implemented as per Section 5.4.6.2.1.2 of UCR- 2008. The password expiry helps as a proactive security measure to protect the user credentials. The introduction of password history, complex check and minimum length ensures that the password is complex enough so that it cannot be easily cracked. The user will be mandated to configure the password consisting of alpha numeric characters along with the supported special characters.

The authentication requirement (entry of old password) while configuration of the password increases the security level. For more information, see the *HPE ArubaOS-Switch Access Security Guide* for your switch.

Platform support: 2530, 2620, 2920, 3800, 3810, 5400R

PVLAN

Private VLANs feature partitions a VLAN by grouping multiple sets of ports that need traffic isolation from one another into independent broadcast sub domains. The VLAN that is being partitioned is referred to as the Primary VLAN and the sub domains carved out of this primary VLAN are referred to as Secondary VLANs.

These Secondary VLANs are also regular VLANs, constituted by a subgroup of ports of the original VLAN and identified by a unique VLAN ID. However, they are usually local to a switch whose Primary VLAN is being partitioned or in cases where it needs to be extended to multiple switches, it is restricted to the downstream (access) layers. Upstream switches need not have

to be aware of these Secondary VLAN IDs. For more information, see the *HPE ArubaOS-Switch Advanced Traffic Management Guide* for your switch.

Platform support: 2920, 3800, 3810, 5400, 5400R

RADIUS Service Tracking

This feature helps to track the availability of radius servers configured on the switch. If the primary server is not available, it will move to the next available server that minimizes the delay in authentication.

Note that this feature is disabled by default. For more information, see the *HPE ArubaOS-Switch Access Security Guide* for your switch.

Platform support: 2530, 2620, 2920, 3500, 3800, 3810, 5400, 5400R

RBAC

The Role Based Access Control (RBAC) is a runtime database that consists of roles and rules that are mapped to users. RBAC lets you secure the management of your network infrastructure by defining the roles for each network administrator for their specific function. The resource access permissions ensure that the network administrator of one department cannot modify the configuration of another department. The feature access permission allows creation of roles based on the function of the user. For more information, see the *HPE ArubaOS-Switch Access Security Guide* for your switch.

Platform support: 2920, 3800, 3810, 5400R

REST

Representational State Transfer (REST) is a software architecture style consisting of guidelines and best practices for creating scalable web services. RESTful systems typically, but not always, communicate over the Hypertext Transfer Protocol with the same HTTP verbs (GET, POST, UT, DELETE, etc.) used by web browsers to retrieve web pages and send data to remote servers.

The REST Interface will be enabled by default in Aruba switches and user is provided with an option to disable it if required. HTTP/HTTPS server should be running in the switch to process rest requests.

Platform support: 2530, 2620, 2920, 3500, 3800, 3810, 5400, 5400R

RIPng

RIP is a distance vector Interior Gateway Protocol (IGP) which is used in small-size IPv4 networks. To route IPv6 packets, IETF developed RIPng based on RIP. Hence RIPng is the Routing Information Protocol for IPv6. The fundamental mechanisms of RIP remain unchanged. However, differences between RIP and RIPng include support for IPv6 addresses and prefixes, different packet formats and lengths, no authentication in RIPng, etc. RIPng is specified by RFC 2080 and RFC 2081. For more information, see the *HPE ArubaOS-Switch Multicast and Routing Guide* for your switch.

Platform support: 2920, 3800, 3810, 5400, 5400R

Fixes

This section lists released builds that include fixes found in the WB.16.01 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.

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

Version WB.16.01.0006

Airwave

CR_0000190886 Symptom: The switch does not properly advertise its factory settings status.

Scenario: Airwave UI does not properly detect the factory settings status change to non-default, until a switch reboot occurs.

Workaround: After configuring Airwave and other details, save the config (`write memory`) and reboot the switch.

Authentication

CR_0000193385 Symptom: RADIUS authenticated users might have switch authentication issues.

Scenario: When RADIUS users are authenticated using user profiles with HP-Privilege-Level VSA configured with values other than HP predefined privilege levels, switch authentication might fail.

Workaround: Use one of the following workarounds:

1. Configure RADIUS user profile with `HP-Privilege-Level = 35` for Manager privilege level or `HP-Privilege-Level = 21` for Operator privilege level.
2. Configure RADIUS user profile with `HP-Command-String` and `HP-Command-Exception` attributes to define the privilege level.
3. Use RBAC group ID configuration on the switch to define authentication privilege level - group ID 21 (Operator) and group ID 35 (Manager).

Authorization

CR_0000197468 Symptom: User may experience authorization issues with pre-defined local commands in the authorization rules.

Scenario: When an invalid command string (*<COMMAND-STR>*) is defined in the local commands authorization rules using the command `aaa authorization group` *<GROUPNAME>* *<SEQ-NUM>* `match-command` *<COMMAND-STR>* `{deny|permit} [log]`, user authentication may fail.

Workaround: Remove invalid local command authorization rules from the switch configuration.

Banner

CR_0000190968 Symptom: Copying a configuration file with a banner text containing the quote (") character could cause a crash.

Scenario: Copying a configuration file with a banner message containing the quote (") character, where the message spans across multiple lines, might cause a crash with an error message similar to `Health Monitor: Restr Mem Access <...>`.

Workaround: Use short banner text or replace quote (") characters in the banner text message.

CLI

CR_0000192212 Symptom: The output of CLI command `show CPU` is not consistent.

Scenario: When the CPU goes to Idle state, the line for 1 minute average CPU usage is not displayed.

CR_0000193389 Symptom/Scenario: CLI command `show interfaces queues <port-list>` fails with error message: `Module not present for port or invalid port: queues.`

Workaround: Upgrade to the most recent switch software revision.

Console

CR_0000179094 Symptom: Sending special keys to a console switch configured in stacking mode may cause the switch to crash.

Scenario: Sending the **ESC** or **~** key to the console of a standby or member switch connected in a stack configuration may cause the switch to crash with an error message similar to `Software exception at multMgmtUtil.c <…>`.

Counters

CR_0000189924 Symptom: Incorrect values are displayed for transmit and receive counters of an interface.

Scenario: The Broadcast (Bcast) and Multicast (Mcast) transmit (Tx) and receive (Rx) counter values displayed in the output of the CLI command `show interfaces <PORT-LIST>` are inaccurate.

DHCP

CR_0000191729 Symptom: A switch acting as a DHCP Relay agent drops any DHCPINFORM packets with a TTL value set to 1.

Scenario: DHCPINFORM packets received with a TTL value of 1 are dropped by the DHCP Relay agent, so the DHCP client cannot acquire and IP address from the DHCP server.

Workaround: Configure the DHCP client network interface to used TTL values greater than 1.

DHCP Snooping

CR_0000183894 Symptom: DHCP Snooping may prevent DHCP clients from getting an IP address from a trusted server.

Scenario: When there are multiple DHCP servers configured for the same IP address scope and a DHCP server failover is triggered, new DHCP clients might not be able to obtain an IP address that is already registered in the switch DHCP Snooping binding database before the existing lease expires.

Workaround: Use one of these options:

1. Have the multiple DHCP servers configured with the same scope synchronized.
2. Delete the existing binding from the DHCP Snooping binding table using CLI command `no ip source-binding <…>`.

IGMP

CR_0000189793 Symptom: Deleting and reconfiguring an IGMP or PIM VLAN interface may not forward multicast traffic correctly.

Scenario: Enable IGMP or PIM on a VLAN. Delete VLAN from the configuration and re-configure the VLAN.

Workaround: Disable IGMP or PIM before deleting and reconfiguring VLAN interface.

IPv6

CR_0000189760 Symptom: An MLD-enabled switch may not properly interoperate with other third-party devices.

Scenario: When IPv6 is configured with the Router Alert option set for MLD, the switch may not properly interoperate with some third-party devices (such as CISCO).

IPv6 ND

CR_0000191543 Symptom: In certain conditions, the switch is unable to discover an IPv6 neighbor.

Scenario: The switch is unable to discover an IPv6 neighbor when the point-to-point inter-router link is configured with /127 IPv6 prefix length.

Workaround: Do not use /127 IPv6 prefix length for the point-to-point inter-router link.

MAC Authentication

CR_0000189021 Symptom: Authorized VLAN for MAC authenticated clients cannot be set to 0 when using the CLI command `no aaa port-access mac-based <port-list> auth-vid`.

Scenario: Using the `no` form of the CLI command to reset the already configured `auth-vid` back to `0`, for MAC authenticated clients, returns an error message similar to `Error setting value auth-vid for port <port-list>`.

Workaround: Remove the VLAN by executing `no vlan <vlan-id>`. This deletes all the configurations related to MAC authentication `auth-vid`. Then create the VLAN again and restore the mac-authentication configuration with the default `auth-vid`.

MAC-Based VLANs

CR_0000183936 Symptom: If a MAC is configured as a static-mac address on the switch, the same MAC might be detected as rogue and may not be blocked by the rogue-ap-isolation feature.

Scenario: After configuring a static mac with the command `static-mac <MAC-ADDRESS> vlan <y> interface <z>` and enabling the rogue-ap-isolation feature using the `rogue-ap-isolation enable` command, the MAC is not blocked by the rogue-ap-isolation feature due to conflict and the following RMON message is displayed: `Blocking rogue device <MAC-ADDRESS> failed as it conflicts with either lockout MAC or static MAC configuration`.

Workaround: There are two workarounds for this issue:

1. Enable rogue-ap-isolation feature before configuring the static-mac address for that MAC to ensure that it is blocked.
2. Remove the static-mac configuration for the `<MAC-ADDRESS>` to ensure that it is blocked by rogue-ap-isolation.

PoE

CR_0000175786 Symptom: PoE devices that are power class 3 may experience random PoE power toggling.

Scenario: The switch may randomly report overcurrent indications on the system logs for the ports where connected PoE devices of power class 3 are drawing power via LLDP. When this event occurs, the connected PoE devices are losing power.

Workaround: Reduce the number of PoE devices of power class 3 connected on the switch at system boot.

CR_0000177617 Some vendor powered devices (PDs) supporting the POE+ standard can issue non-standard POE+ packets or packets with invalid TLVs while negotiating for power from the switch (PSE). Strict interpretation of the standard forces power to be cut off to such devices and could cause the PD to reboot continuously.

Workaround: Configure the associated port to be `poe- allocated-by value` and `poe-value <required-watts>` on the switch to avoid reboot.

CR_0000191040 Symptom: Connecting both E0 & E1 ports on an Aruba AP325 to a POE ports on a HPE Aruba Switch results in a POE failure, loss of power on one of the switch ports, lighted switch fault LED and a `bad FET` message in the switch logs.

Workaround: Power can be restored to the affected port by unplugging the cable from it and perform a poe-reset. Alternately, unplugging the affected port and rebooting the switch will also restore power to the faulted ports. HPE recommends only E0 port of the AP plugs into the switch.

Policies

CR_0000189858 Symptom: When service policy configuration is applied to a range of interfaces, the configuration is not properly displayed in the output of show CLI command.

Scenario: Apply a configured service policy to a range of ports using the CLI command `interface <port-list> service-policy <policy-name> in`. Only the first applied interface is displayed in the running configuration or the output of CLI command `show policy ports <port-list>`.

Workaround: Apply the policy to a single port at a time using the same CLI command.

Spanning Tree

CR_0000198794 Symptom: The switch may suffer occasional or chronic BPDU starvation, with log messages similar to `CIST starved for a BPDU Rx on port`.

Scenario: When the BPDU Throttling feature is enabled, it can trigger occasional or chronic BPDU starvation episodes. Spanning tree BPDU throttle configuration status can be confirmed by running the CLI command `show spanning-tree bpdu-throttle`.

Workaround: Disabling BPDU Throttling should stop the BPDU starvation symptoms. To disable BPDU Throttling feature, run the CLI command `no spanning-tree bpdu-throttle`.

Stacking

CR_0000193017 Symptom: Stacking might crash during stack activation.

Scenario: When a stack transitions from inactive fragment to active fragment while stack member switches are booted one-by-one, the commander switch might crash with an error message similar to `Software exception at hwBp.c <...> mStackingCtrl <...>`.

Workaround: Upgrade to the software that has the fix.

Supportability

CR_0000183389 Symptom: CLI command `show tech all` may fail to run properly.

Scenario: CLI command `show tech all` may not complete or execute properly.

Syslog

CR_0000189320 Symptom: The switch might crash when enabling debug destination to syslog using the CLI command `debug destination logging`.

Scenario: When the switch is configured for logging to a remote syslog server with IPv6 address using temporary debug facility to system logging destination using the CLI command `debug destination logging`, the switch might crash.

Workaround: Configure the remote syslog server with an IPv4 address or redirect temporary debug to the local console or buffer facility using the CLI command `debug destination console | buffer`.

Time

CR_0000197232 Symptom: In a rare condition, the switch may crash with an error message similar to `NMI event <…> Task='mCronDaemon' <…>`.

Scenario: In a rare condition, when the switch time is updated from remote time servers, the switch may crash with an error message similar to `NMI event <…> Task='mCronDaemon' <…>`.

Version WB.16.01.0005

Never released.

Version WB.16.01.0004

CLI

CR_0000157943 When the CLI command `copy command-output 'show tech all'` is executed, the switch might run out of free memory and trigger an unexpected reboot (crash) when memory allocation fails. The risk of this problem occurring is higher when other switch tasks have consumed a large portion of free memory.

Note that the first task or process to fail to allocate memory is the one displayed in the crash message, so the event log and crash messaging may vary. An example message is: `Software exception at svc_misc.c:858 -- in 'mCnfTrMgr', task ID = 0xa9f7c40 -> Failed to malloc 3032 bytes`

When insufficient resources are available to copy the requested output to a file, the process is terminated automatically. When this happens, the following message is displayed to the CLI and logged: `The command was terminated prematurely because the output exceeded the maximum memory limit`.

Config

CR_0000170324 When a change is made from the CLI in the **Switch Configuration – Port/Trunk Settings** Menu, the change is not saved, resulting in an `Unable to save field` error.

DHCP

CR_0000180195 A fix applied to make the DHCPACK packet being sent by the DHCP Server in response to a DHCPINFROM uses the MAC Address of the client as destination instead of a broadcast address.

DHCP Snooping

CR_0000177144 There is a discrepancy between the DHCP-snooping binding database and the value reported by the dynamic binding counter.

IPv6

CR_0000172573 Configuring a port for IPv6 ra-guard and adding the port to a new or existing trunk results in the generic error message `Operation failed on Port X##: General error`.

MAC Authentication

CR_0000157903 With mac-auth failure-redirect feature configured as FQDN, loss of connectivity could be experienced at end points if DNS query is unable to resolve.

Menu Interface

CR_0000179336 While using the **IP Configuration Menu** interface to switch from **DHCP/Bootp** to **Manual** IP address configuration without first editing the switch's currently configured IP address for the respective VLAN interface, an `Invalid value` error message is received.

PoE

CR_0000169265 After an electrical surge or ESD charge on a PoE port, the switch might exhibit BAD FET messages, which indicate a failure to deliver PoE on those ports. Event log messages appear similar to the following:

```
W 04/02/15 07:58:49 02562 ports: Port 1/1: Possible bad FET/PSE supplying PoE
   power - suggest configuring other end of link with "no power"
W 04/02/15 07:58:49 00567 ports: port 1/1 PD Other Fault indication.
```

CR_0000177617 Some vendor powered devices (PDs) supporting the POE+ standard can issue non-standard POE+ packets or packets with invalid TLVs while negotiating for power from the switch (PSE). Strict interpretation of the standard forces power to be cut off to such devices and could cause the PD to reboot continuously.

Workaround: Configure the associated port to be `poe-allocated-by value` and `poe-value <required-watts>` on the switch to avoid reboot.

Policy Based Routing

CR_0000173164 After a loss and restoration of connectivity between the switch and the PBR specified next-hop, the switch routes traffic conforming to match rules, as well as traffic conforming to the ignoring of rules to the PBR next-hop.

Port Counters

CR_0000183662 Symptom: When the flow mod statistics are queried from the controller, incorrect values are received from the controller for the packet and byte count on a switch.

Scenario: When querying the flow statistics from the controller, incorrect multi-part reply packets are sent for flow stats with unknown message types. This happens when the flow table includes over 400 entries. If the flow tables exceed 400 entries, the controller fails to pull more flows from the switch. This causes multipart reply packets to be sent to the controller with an unknown message type.

Routing

CR_0000174012 Applying BPG route-map with `set weight` while there is more than one path could result in a switch crash with a message similar to `Software exception at bgp_med.c:597 -- in 'eRouteCtrl'`.

Workaround: The failure may be avoided by applying BPG route-map with `set local-pref` instead of using `set weight`.

Security Vulnerability

CR_0000166717 Login is permitted with the default username manager, even when the manager username has been changed to a custom username.

SNMP

CR_0000177848 Restoring backup configuration files with SNMPv3 enabled or QinQ SVLAN set, triggers an unexpected switch reboot even if the backup config is identical to the current config.

CR_0000181295 Running SNMP on dot3StatsDuplexStatus OID using an index of 0 causes the switch to crash.

CR_0000182311 Symptom: If a switch is reconfigured from MSTP to RPVST, while spanning-tree traps are already enabled on the switch, none of the RPVST SNMP traps are sent.

Scenario: When the switch is configured for MSTP, Spanning Tree mode, and SNMP notifications, changing the mode to RPVST also disables the configured Spanning Tree traps. Although the traps are displayed in the configuration as ‘enabled’ and the value of the object ‘hpSwitchStpCntl’ (.1.3.6.1.4.1.11.2.14.11.5.1.7.1.14.3) indicates that the traps are properly enabled, none of the

configured notifications are sent to a trap receiver. When the traps are reconfigured or the switch is rebooted, the SNMP traps are transmitted again as expected.
Workaround: Re-enable SNMP Spanning Tree traps using CLI command `spanning-tree traps` or reboot the switch to restart the Spanning Tree SNMP traps transmission.

Spanning Tree

CR_0000175721 When setting the RPVST mode for spanning tree, the switch continuously displays the erroneous error message: `WARNING: Reboot switch and use CLI commands to configure MSTP parameters`.
Workaround: The error message can be ignored.

Stacking

CR_0000173162 The J number of stacked devices is not properly reported in `entPhysicalVendorType OID`.

CR_0000181025 Symptom: When a stack is running 16.01 (or later) image and provisions a new member that has 15.xx image loaded, it will not join the stack.

Scenario: 1. Member having newer software version (16.01 (or later), trying to join a stack running old version (15.xx image) of stacking protocol.

2. Member having older software and trying to join a stack running newer version of stacking protocol.

3. Booting whole stack with members running different (old and new) software versions.

Workaround: Upgrade the members to the latest software (16.01) and connect to the stack that is running new software version (16.01).

Switch Initialization

CR_0000171369 When communicating with the switch (for example, via SCP, SSH, Telnet) over a connection with IP fragments, where some IP fragments are getting dropped, transfers stall or take an excessive amount of time.

TACACS

CR_0000177904 If more than one TACACS server is configured as authentication method and all TACACS servers become unreachable, failover to secondary authentication does not occur. When this happens, you will not be able to login to the switch using the same access method.

TFTP

CR_0000180230 TFTP transfer does not work with packet sizes other than 1416 bytes.
Workaround: Configure TFTP client to use a packet size of 1416 bytes.

VLAN

CR_0000169998 A port becomes an untagged member in more than one VLAN when the changes to the port's tagged/untagged VLAN membership are made in the CLI Menu.
Workaround: Reset the switch, reset the module, or power cycle the switch.

Issues and workarounds

The following are known issues in the WB.16.01.0006 release.

CPPM

CR_0000192066 Symptom: When working with Captive Portal feature with URL hash key enabled, if the Captive-Portal-URL attribute in CPPM includes any uppercase letter in the URL and the client attempts to browse, the redirection to the Captive Portal Login page works but an error is displayed preventing the user from entering credentials in the web page.

Scenario: Enter any uppercase letter on the Captive-Portal-URL attribute in CPPM.

Workaround: In CPPM, when configuring the Captive Portal profile attribute to redirect traffic to ClearPass, enter the value for the Captive-Portal-URL attribute in lowercase only.

GVRP

CR_0000184015 Symptom: When an Aruba AP is connected to a switch port that has a device profile applied, a GVRP VLAN advertised from the Aruba AP gets created on the switch but VLAN membership of the switch port does not get modified to include the advertised GVRP VLAN.

Scenario: (1) Connect an Aruba AP to the switch and enable device profile.

(2) Configure AP to send GVRP PDUs with some VLANs.

(3) Check VLAN status on the switch port connected to Aruba AP, GVRP VLANs advertised by AP would not be seen for the AP connected port.

Workaround: Add the GVRP VLAN advertised from AP as part of device profile. The switch port connected to that AP would then be added as a member of that GVRP VLAN.

PoE

CR_0000189058 Symptom: Rarely, AP does not power up. The power LED on the AP remains unlit.

Scenario: Having dual Ethernet port Aruba APs connected to HPE Aruba Switches. Problem is commonly seen on 5400 V1 blades, but might rarely be seen on other HPE Aruba switches.

Workaround: Power can be restored by toggling PoE power to the connected port on the switch: `no int <portnums> power` and `int <portnums> power`.

CR_0000192808 Symptom: Dual-port Aruba APs, such as AP325, AP225, AP135, may occasionally power up with reduced power (802.3af mode) and AP's system status LED will lit up amber.

Scenario: Occasionally, when both Ethernet ports of dual-port Aruba APs, such as AP325, AP225, AP135 are connected to a PoE+ switch, AP's LED status may indicate a fault condition (amber) and only one of AP's ports E0 or E1 is on and will be receiving power.

Workaround: Disable LLDP dot3TLV on the switch whenever both ports of dual-port Aruba APs are plugged into the switch.

RADIUS

CR_0000184382 Symptom: ClearPass does not allow the user to be created with password that includes a " " (blank). If so, you will see failed authentication attempts for the radius-tracking-user in ClearPass.

Scenario: Use ClearPass as the RADIUS server and have "radius-tracking-user" configured on the switch.

Workaround: None, but RADIUS tracking will maintain the keep alive with a RADIUS accept or reject response.

SNMP

CR_0000190877 Symptom: SNMP communities default configuration values are not consistently displayed between the output of CLI command `show running-config` and `show snmp-server`.

Scenario: When executing CLI command `show running-config`, only non-default configuration parameters for SNMP communities are displayed, such as read/write MIB access mode, and operator/manager MIB access level.

Workaround: Use the CLI command `show snmp-server` to display SNMP communities' complete configuration.

Upgrade information

Upgrading restrictions and guidelines

WB.16.01.0006 uses BootROM WB.15.05. 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.16.01*.

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 is not allowed if the max-vlans value is greater than 2048.

Unconfigure the max-vlans before attempting to downgrade from WB.16.01 to an earlier version 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 16.01*.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  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, go to either of the following:
  - Hewlett Packard Enterprise Support Center Get **connected with updates** page:

    www.hpe.com/support/e-updates
  - HPE Networking Software:

    www.hpe.com/networking/software
  - 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.

Hewlett Packard Enterprise security policy

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.

To find security bulletins:

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.

To initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email, sign up at:

www4.hpe.com/signup_alerts

Documents

To find related documents, see the Hewlett Packard Enterprise Support Center website: **www.hpe.com/support/hpesc**. Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.

Related documents

The following documents provide related information:

- HPE ArubaOS-Switch Access Security Guide WB.16.01
- HPE ArubaOS-Switch Advanced Traffic Management Guide WB.16.01
- HPE ArubaOS-Switch Basic Operation Guide Version 16.01
- HPE ArubaOS-Switch Event Log Message Reference Guide Version 16.01
- HPE ArubaOS-Switch Feature and Commands Index Version 16.01
- HPE ArubaOS-Switch IPv6 Configuration Guide WB.16.01
- HPE ArubaOS-Switch Management and Configuration Guide WB.16.01
- HPE ArubaOS-Switch Multicast and Routing Guide WB.16.01
- HPE ArubaOS-Switch Troubleshooting Guide Version 16.01
- HPE OpenFlow 1.3 Administrator Guide K/KA/KB/WB.16.01

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Networking Information Library	**www.hpe.com/networking/resourcefinder**
Hewlett Packard Enterprise Networking website	**www.hpe.com/info/networking**
Hewlett Packard Enterprise Networking My Support	**www.hpe.com/networking/support**
General websites	
Hewlett Packard Enterprise Information Library	**www.hpe.com/info/enterprise/docs**
Hewlett Packard Enterprise Support Center	**www.hpe.com/support/hpesc**
Contact Hewlett Packard Enterprise Worldwide	**www.hpe.com/assistance**
Subscription Service/Support Alerts	**www.hpe.com/support/e-updates**
HPE Networking Software	**www.hpe.com/networking/software**
Customer Self Repair (not applicable to all devices)	**www.hpe.com/support/selfrepair**
Insight Remote Support (not applicable to all devices)	**www.hpe.com/info/insightremotesupport/docs**

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: **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.

For more information and device support details, go to the following website:
www.hpe.com/info/insightremotesupport/docs

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.