Hewlett Packard Enterprise

WB.16.01.0012 Release Notes

Abstract

This document contains supplemental information for the WB.16.01.0012 release.

Part Number: 5200-2953
Published: January 2017
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.

Contents

WB.16.01.0012 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.16.01.0012	2017-01-27	WB.16.01.0011	Released, fully supported, and posted on the web.
WB.16.01.0011	2016-11-15	WB.16.01.0010	Released, fully supported, and posted on the web.
WB.16.01.0010	2016-09-13	WB.16.01.0009	Released, fully supported, and posted on the web.
WB.16.01.0009	n/a	WB.16.01.0008	Never released.
WB.16.01.0008	2016-08-02	WB.16.01.0007	Released, fully supported, and posted on the web.
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	Released, fully supported, and posted on the web.

Table Continued

Version number	Release date	Based on	Remarks
WB.15.18.0013	2016-09-13	WB.15.18.0012	Please see the WB.15.18.0013 release note for detailed information on the WB.15.18 branch. Released, fully supported, and posted on the web.
WB.15.18.0012	2016-08-02	WB.15.18.0011	Released, fully supported, and posted on the web.
WB.15.18.0011	2016-05-31	WB.15.18.0010	Released, fully supported, and posted on the web.
WB.15.18.0010	2016-03-28	WB.15.18.0009	Released, fully supported, and posted on the web.
WB.15.18.0009	n/a	WB.15.18.0008	Never released.
WB.15.18.0008	2016-01-19	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.15.17.0013	2016-05-25	WB.15.17.0012	Please see the WB.15.17.0013 release note for detailed information on the WB.15.17 branch. Released, fully supported, and posted on the web.
WB.15.17.0012	2016-03-28	WB.15.17.0011	Released, fully supported, and posted on the web.
WB.15.17.0011	n/a	WB.15.17.0010	Never released.
WB.15.17.00010	2016-01-19	WB.15.17.0009	Released, fully supported, and posted on the web.
WB.15.17.0009	2015-11-10	WB.15.17.0008	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.

Table Continued

Version number	Release date	Based on	Remarks
WB.15.17.0005	2015-05-11	WB.15.17.0004	Released, fully supported, but not posted on the web.
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 web browsers:

Browser	Supported versions
Internet Explorer	• Edge • 11
Chrome	• 53 • 52
Firefox	• 49 • 48
Safari (MacOS only)	• 10 • 9

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 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.16.01.0012

VLAN

Switch design does not allow a port to be orphaned when it is removed from the port's last assigned VLAN. The port has to be manually re-assigned to any other existing VLAN to make sure the port is always assigned to a VLAN. If removing a port from its last VLAN, the port is now automatically untagged to the DEFAULT VLAN, eliminating the previous 2-step process - move port to another VLAN prior to removing the port's last assigned VLAN.

Version WB.16.01.0011

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.

Version WB.16.01.0010

BootROM

The BootROM version was updated to WB.16.03.

Version WB.16.01.0009

Version WB.16.01.0009 was never released.

Version WB.16.01.0008

No enhancements were included in version WB.16.01.0008.

Version WB.16.01.0007

Authentication

CR_0000200562

Symptom: Added 802.1x-2010 compliance support for HPE 2920 Switch Series. 802.1X-2010 mode can be enabled for authenticator and supplicant using the CLI command `[no] aaa port-access dot1x2010 [authenticator|supplicant]`.

BootROM

CR_0000200859

The BootROM has been updated to version WB.16.01.

Enhanced Secure Mode

CR_0000199914

Symptom: Added Enhanced Secure Mode functionality. To transition from one security mode to the other. Enter the following command from a serial terminal connected to the switch: `secure-mode <standard | enhanced>`.

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".

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

Version WB.16.01.0005 was 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 this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

NOTE:

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

Version WB.16.01.0012

Banner

CR_0000225460

Symptom: SNMPv3 get request on the switch login banner SNMP OID fails with `tooBig` error message.

Scenario: When switch post-login banner or MOTD banner is configured with more than 1300 characters, running an SNMPv3 get request on the corresponding banner SNMP OID will fail with the error message `Reason:[tooBig].`

Workaround: Use SNMPv2 get request on SNMP banner OID when the configured login banner size is larger than 1300 characters.

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..`

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.

DHCP Snooping

CR_0000218841

Symptom: The dhcp snooping bindings information may not be properly updated.

Scenario: After a boot event in a multi-management configuration, such as redundant management module or stack configuration, the dhcp snooping lease binding from a TFTP/SFTP stored database may fail to be updated.

Workaround: Disable/enable dhcp snooping globally after the config synchronization with standby is completed.

Event Log

CR_0000225392

Symptom: The proper event log message is not generated when a port is blocked due to a link failure detection protocol.

Scenario: When a port is configured for Device Link Detection Protocol (DLDP) or Uni-directional Link Detection (UDLD) and a link failure is detected, the switch fails to log corresponding event log messages similar to:

```
00435 ports: port <NUM> is Blocked by DLDP
```

```
00435 ports: port <NUM> is Blocked by UDLD
```

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: The switch may crash with an error message similar to `Health Monitor: Read Error Restr Mem Access <...> Task='tCron000001' <...>` when executing a scheduled job.

Scenario: If a job is scheduled to copy data files to/from a remote server configured via hostname, 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"`.

Loop Protection

CR_0000224518

Symptom: Port disable is delayed when loop protection detects a loop.

Scenario: When an IP enabled VLAN comes up, the switch sends a gratuitous ARP looking for a duplicate IP on the network. This ARP request loops and switch detects it as a duplicate IP. The detected duplicate IP, in turn, floods the event logs with messages similar to the following.

```
W 01/01/90 00:05:39 02581 ip: IPv4: Duplicate IPv4 address 5.1.1.1 is
detected on VLAN 10 with a MAC address of 009c02-63a080
```

The resulting CPU consumption leads to a delay in loop protection detecting the loop and disabling the port.

Workaround: The affected switch port is disabled, but not at expected detection time.

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`.

Spanning Tree

CR_0000217382

Symptom: Switch ports enabled for BPDU protection are not properly flagged as administratively down in `show interface brief` output when BPDU traffic is detected.

Scenario: When BPDU traffic is detected on a BPDU protected port, the port is being operationally brought down (logically disabled) due to BPDU detection, although it is still being maintained enabled for administrative purposes in the output of CLI command `show interface brief`. Administrative status of the port is mainly intended to be changed by manually enabling/disabling the port from CLI command `interface <PORT-LIST> enable | disable`.

```
Port      Type |   Alert    Enabled Status  Mode      Mode    Ctrl
```

```
  ----- ---------- + --------- ------- ------ ---------- ---- ----
   1    10/100TX |   No         Yes    Down   100FDx
MDI        off
```

The BPDU protected port is operationally disabled when BPDU traffic is detected and only its administrative state is enabled.

```
ifAdminStatus.1 = 1     (up)
ifOperStatus.1 = 2      (down)
```

Stacking

CR_0000197626

Symptom: A stack might fail to split according to the configured split policy.

Scenario: In a 2-member stack configuration, when the OOBM interface is configured for dynamic DHCP IP address, a stack might fail to split according to the configured split policy.

Workaround: Configure any of the OOBM interfaces with static assigned IP address.

Terminal

CR_0000223941

Symptom: The terminal command line is not working properly after terminating a session to the switch.

Scenario: After a VT100 terminal session to the switch is terminated, the terminal line wrap-around configuration is disabled.

Workaround: Re-enable "line-wrap" mode via SNMP command `setmib hpicfPrivateTermLineWrap.0 -i 6` followed by configuration save and reboot.

TFTP

CR_0000183103

Symptom: The switch is not retaining TFTP server status in configuration after a switch software upgrade or downgrade.

Scenario: When an operator or manager password is set on the switch, the TFTP server is automatically disabled in the switch configuration (`no tftp server`). When the switch is upgraded or downgraded to this major software version (xx.16.01.xxxx), the disabled TFTP server configuration is not retained, hence TFTP server configuration is restored to its default enabled status.

Workaround: Manually disable TFTP server after the switch software upgrade or downgrade, using CLI command `no tftp server`.

Trunking

CR_0000211583

Symptom: In a certain scenario, the switch allows to create a trunk interface with more than a maximum of 8 ports.

Scenario: When a fast copy and paste operation with multiple port addition entries to the same trunk interface is used to create a trunk interface, more than the maximum 8 allowed ports can be added to the trunk. Once such invalid trunk interface is created, no other changes to the trunk interface are allowed from CLI.

Example: Copy & Paste from text file:

trunk 1-4 trk1

trunk 5-9 trk1

Workaround: To avoid triggering, do not use a fast copy and paste function to configure the trunk group. Once triggered, use the Menu interface to remove additional ports exceeding the maximum of 8 from the invalid trunk interface.

Version WB.16.01.0011

Console

CR_0000206708

Symptom: Management access to the switch through SSH, telnet or console may fail with an error message similar to `Connection closed by remote host`.

Scenario: New sessions may fail to be established after previous sessions are closed due to inactivity timeout when using certain client applications, such as MobaXterm, for management access to the switch through SSH, telnet or console.

Workaround: Rebooting the switch will clear the locked sessions. Alternatively, you can disable the inactivity timer using the CLI command `console inactivity-timer 0`. Once the inactivity timer is disabled, you must log out of each session to properly close the connection.

MAC Authentication

CR_0000210511

Symptom: Switch ports may get into an endless MAC authentication cycle preventing re-authentication.

Scenario: When a switch port is configured for both 802.1X and mac-authentication, during the re-authentication process due to reauth-period expiry, the port may not be able to complete the re-authentication process and get into a MAC authentication loop.

Workaround: Disabling and re-enabling the affected port via CLI command `interface <port-num> enable | disable` should clear the problem.

mDNS

CR_0000216815

Symptom: Switch may run out of memory and crash when receiving many multicast DNS packets.

Scenario: When receiving multicast DNS packets with ACL filter applied to the VLAN, the switch may crash due to running out of heap memory.

OOBM

CR_0000214640

Symptom: Communication through OOBM IP address may be lost after a failover.

Scenario: After a failover event in a VSF or backplane stacking configuration, a gratuitous ARP may fail to be sent. The global OOBM IP address becomes unreachable because the new commander's MAC address is not associated with the OOBM IP address in the neighbor devices' ARP table.

Workaround: Issue a ping from the switch to any destination through the OOBM interface to update the ARP entry in the neighbor devices.

OpenFlow

CR_0000193376

Symptom: Switch may not be able to connect to the SDN controller.

Scenario: After a reboot of another switch upstream on the path to the SDN controller, the switch may be unable to connect to the SDN controller.

Workaround: Reboot the switch.

SNMP

CR_0000214384

Symptom: SNMP ifTable reports invalid OID values for OOBM loopback interface.

Scenario: When a switch is configured in a stack, SNMP ifTable reports OID value '0" for ‘ifType’ (. 1.3.6.1.2.1.2.2.1.3), ‘ifAdminStatus’ (.1.3.6.1.2.1.2.2.1.7), and ‘ifOperStatus’ (.1.3.6.1.2.1.2.2.1.8) corresponding to the OOBM loopback interface.

Version WB.16.01.0010

IGMP

CR_0000200038

Symptom: Loss of management access to the switch.

Scenario: When IGMP version 3 is enabled in a VLAN and the switch receives IGMPv2 membership reports with well-known multicast group address, the switch might be unable to resolve the MAC address for the default gateway while passing the traffic.

Workaround: Rebooting the switch or failing over to standby (where applicable) can temporarily restore connectivity to the switch.

CR_0000216285

Symptom: Losing management access to the switch.

Scenario: When the switch receives IGMPv3 query packets with the source IP address 0.0.0.0 or IGMPv3 query packet without Router Alert option, it may deem the switch unable to resolve the MAC address for the default gateway.

Workaround: Rebooting the switch or failing over to standby (where applicable) can temporarily restore connectivity to the switch.

GVRP

CR_0000213176

Symptom: In a GVRP configuration, if a link is disabled and re-enabled, the switch may lose port VLAN assignment.

Scenario: In a daisy-chain topology configured with GVRP on all switches and the downstream switch configured with radius assigned VLANs on authenticated ports, if an upstream link is toggled disabled/ enabled, the downstream link loses its GVRP VLAN assignment.

Workaround: Disable and re-enable GVRP on downstream switch to clear the issue.

Redundancy

CR_0000212756

Symptom: Interface configuration of stack member might be lost from the global configuration.

Scenario: When a stack member switch is replaced with a new MAC address in an existing stack, the interface configuration corresponding to the replaced member switch is lost in the event of redundancy. This causes the current standby switch to switchover to the commander role.

Workaround: Perform another redundancy using CLI command `redundancy switchover`.

REST

CR_0000214629

Symptom/Scenario: REST POST commands fail when operator and manager passwords are set but usernames are disabled.

Workaround: Remove the password for operator or manager or disable-usernames configuration to allow the REST POST commands execution.

SSH

CR_0000201108

Symptom: Switch configured with DSA key refuses SSH connections.

Scenario: When the switch is configured with host DSA public key, SSH connection from client using the generated public-key in switch cannot be established.

Workaround: Configure switch with host RSA public-key for SSH connections.

Stacking

CR_0000214504

Symptom/Scenario: After a stack failover to standby, the switch may fail to forward traffic.

Workaround: Toggling the affected links using CLI command `interface <port-num> disable | enable` can clear the issue.

CR_0000215067

Symptom: Switch may stop forwarding traffic over an LACP trunk.

Scenario: After a stacking switchover, the switch may stop forwarding traffic over an LACP trunk configured on flex ports.

Workaround: Toggle the non-forwarding LACP ports using CLI command `interface <port-num> disable | enable`.

Trunking

CR_0000212455

Symptom: When trying to re-create a trunk, the switch may prompt the error message `Ambiguous input: trk...`

Scenario: When configured in a stacking mode, the switch may not be able to re-create a trunk after the last port of last stacking member was already configured as a member to another trunk.

Workaround: Do not configure last port of last stacking member as trunk port.

CR_0000214638

Symptom: LACP link failure recovery might result in traffic outage.

Scenario: A connection outage to the peer device might be observed during the recovery from a link failure on a port member of an LACP trunk, when the switch's LACP links are connected to a non-ArubaOS-Switch-based switch on which LACP links are configured in Active/Standby mode.

Version WB.16.01.0009

Version WB.16.01.0009 was never released.

Version WB.16.01.0008

GVRP

CR_0000204332

Symptom: The detailed information about mac-addresses dynamically learned by the switch is not correctly displayed in the output of the CLI command `show mac-address <mac-address>`.

Scenario: When mac-addresses are learned from a VLAN that was dynamically configured using GVRP, the CLI command `show mac-address <mac-address>` does not display any detailed information.

Workaround: Use the CLI command `show mac-address`.

MAC Authentication

CR_0000201029

Symptom: Switch may crash with a message similar to `Health Monitor: Misaligned Mem Access <...> Task='eDrvPoll' <...>`, when data cable is plugged into a port.

Scenario: Switch may crash with a message similar to `Health Monitor: Misaligned Mem Access <...> Task='eDrvPoll' <...>`, when data cable is plugged into a port configured with mac-authentication and spanning-tree is enabled on the switch.

Workaround: Administratively disable the port and re-enable after the data cable is plugged into the port, disable the port using CLI command `interface <port-num> disable | enable`.

PoE

CR_0000189058

Symptom: Rarely, a directly connected 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 <port-nums> power` and `int <port-nums> power`.

Spanning Tree

CR_0000202511

Symptom: Incorrect spanning tree hello time is reported as a MIB value.

Scenario: In a spanning-tree topology, the switch reports the value of OID dot1dStpHelloTime on a root switch in seconds instead of centiseconds as reported in non-root switches.

Workaround: There is no impact on spanning tree functionality as this is merely a value conversion from seconds to centiseconds.

TACACS

CR_0000201235

Symptom: Authentication and authorization requests may be delayed up to 1 second.

Scenario: The switch may delay sending TACACS authentication and authorization requests for up to 1 second.

Transceivers

CR_0000210703

Symptom: The OID entLastChangeTime value is not correctly updated.

Scenario: When a transceiver is inserted, moved or hotswapped, the switch does not correctly update the value reported in entLastChangeTime OID.

USB

CR_0000202216

Symptom: The switch might crash with an error message similar to `MemWatch Trigger: Offending task 'mSess1' <...>`.

Scenario: When executing the `dir` command without any other parameters on a USB device connected and mounted into the switch while accounting is enabled, the switch might crash with an error message similar to `MemWatch Trigger: Offending task 'mSess1' <...>`.

Workaround: Execute the `dir` command with a specified path parameter. For example, `dir/ <dir_path>`.

Version WB.16.01.0007

Display Issue

CR_0000190925

Symptom/Scenario: A 100% CPU usage spike occurs every 10 minutes, caused by the HTTP task calling the Entropy function.

Event Log

CR_0000192892

Symptom: Audit event message is not logged when an invalid configuration fails to be downloaded onto the switch.

Scenario: When an identical, incorrect or invalid configuration file is rejected when downloaded on the switch, the audit event log message indicating the reason for file rejection is not recorded in the system event log.

Workaround: The error message rejecting the configuration file is displayed on the switch console though no RMON event is recorded in the switch event log.

NTP

CR_0000193443

Symptom: NTP debug configuration is incorrectly displayed in the output of the CLI command `show debug`.

Scenario: The NTP debug options enabled using the CLI command `debug NTP <packet | event>` are not correctly displayed in the output of the CLI command `show debug`.

OOBM

CR_0000194019

Symptom: A switch with OOBM port may experience an NMI crash and reboot.

Scenario: When there is a broadcast storm on the OOBM network, the switch might encounter a crash with an error message similar to `NMI event <...> Task='tDevPollRx' <...>`.

Workaround: Avoid broadcast storms on the OOBM network.

OpenFlow

CR_0000171815

Symptom: In rare circumstances, OpenFlow traffic might incorrectly be looped back to the switch.

Scenario: Repetitive enabling and disabling of OpenFlow while Service Insertion tunnels are removed and created, might lead to a condition where OpenFlow traffic could end up being looped back to the switch instead of being forwarded to its destination.

Workaround: Reboot the switch.

SNMP

CR_0000192914

Symptom: SNMP community access violation warning messages are not always reported in the switch event log.

Scenario: When Authorized IP Managers are configured on the switch, SNMP access from unauthorized management stations with correct community names are not reported in the switch event log.

Spanning Tree

CR_0000194044

Symptom: Traffic may be disrupted in an RPVST topology when VLAN configuration changes.

Scenario: In an RPVST topology, when there are ports configured for BPDU filter, PVST filter, and root guard, removing any VLAN from the switch configuration might cause traffic disruption in the network.

Workaround: Reapply all the configurations related to the root-guard, tcn-guard, bpdu-filter, and pvst-filter after removing VLAN.

Supportability

CR_0000200816

Symptom: In some cases, the switch might halt or crash when executing the CLI command `show tech all`.

Scenario: A switch hang or crash might be encountered during execution of the CLI command `show tech all` while the switch is configured with policies applied to interfaces with the CLI command `policy {qos|pbr|mirror|zone} <policy-name>....` The issue is intermittent and not every execution of `show tech all` causes a crash.

Workaround: Avoid executing `show tech all` if policies are applied to switch interfaces, or remove the policies from interfaces before executing `show tech all`.

Switch Module

CR_0000192470

Symptom: After a period of uptime, switch blades might reset with an error message similar to `Software exception in ISR at interrupts_mac.c <...> -> Excessive MAC Interrupts at chipPort <...>`.

Scenario: When there is an excessive amount of received packets with shorter preamble than the industry standard, HPE switch blades might reset due to excessive interrupt handling.

Workaround: Reconfigure the peer device to use a long preamble.

Trunking

CR_0000198822

Symptom: The switch does not accept the LACP key option to configure an LACP trunk.

Scenario: When executing CLI command `lacp key <0-65535>`, the switch returns the error message `Invalid input: key`.

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:

- Configure RADIUS user profile with HP-Privilege-Level = 35 for Manager privilege level, or HP-Privilege-Level = 21 for Operator privilege level.
- Configure RADIUS user profile with HP-Command-String and HP-Command-Exception attributes to define the privilege level.
- 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 spanning 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.

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 and Multicast transmit and receive counter values from the CLI output of the `show int <ports>` command are incorrect.

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 an IP address from the DHCP server.

Workaround: Configure the DHCP client network interface to use 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 might 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

Symptom/Scenario: 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/Scenario: Connecting both E0 & E1 ports on an Aruba AP325 to a POE ports on an 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 might 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 might crash with an error message similar to `NMI event <…> Task='mCronDaemon' <…>`.

Version WB.16.01.0005

Version WB.16.01.0005 was never released.

Version WB.16.01.0004

CLI

CR_0000157943

Symptom: When copy command-output `show tech all tftp <server addr> <file name>` command is executed, the switch might crash.

Scenario: The switch might crash when IPv6 route entries in the system grows to a huge value.

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

Symptom/Scenario: 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 BGP 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 BGP 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.

Upgrade information

Upgrading restrictions and guidelines

WB.16.01.0012 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.16.01*.

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*.

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.

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.

Websites

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**.

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

  http://www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

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

Information to collect

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

Accessing updates

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

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

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an 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.