WB.16.03.0005 Release Notes

Part Number: 5200-3977b
Published: July 2017
Edition: 3

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Description

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

Version WB.16.03.0003 is the initial build of Major version WB.16.03 software. WB.16.03.0003 includes all enhancements and fixes in the WB.16.02.0008 software, plus the additional enhancements and fixes in the WB.16.03.0003 enhancements and fixes sections of this release note.

Product series supported by this software:

- Aruba 2920 Switch Series

Important information

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

Version history

All released versions are fully supported by Hewlett Packard Enterprise, unless noted in the table.

Version number	Release date	Based on	Remarks
WB.16.03.0005	2017-07-07	WB.16.03.0004	Released, fully supported, and posted on the web.
WB.16.03.0004	2017-04-17	WB.16.03.0003	Released, fully supported, and posted on the web.
WB.16.03.0003	2016-12-20	WB.16.02.0008	Initial release of the WB.16.03 branch. Released, fully supported, and posted on the web.
WB.16.02.0014	2016-10-28	WB.16.02.0013	Please see the WB.16.02.0114 release notes for detailed information on the WB.16.02 branch. Released, fully supported, and posted on the web.
WB.16.02.0013	n/a	WB.16.02.0012	Never released.
WB.16.02.0012	2016-08-31	WB.16.02.0011	Released, fully supported, and posted on the web.
WB.16.02.0011	2016-08-24	WB.16.02.0010	Released, fully supported, and posted on the web.
WB.16.02.0010	2016-08-11	WB.16.02.0009	Released, fully supported, and posted on the web.
WB.16.02.0009	n/a	WB.16.02.0008	Never released.
WB.16.02.0008	2016-07-08	WB.16.01.0004	Initial release of the WB.16.02 branch. Released, fully supported, and posted on the web.

Table Continued

Version number	Release date	Based on	Remarks
WB.16.01.0008	2016-08-02	WB.16.01.0007	Please see the WB.16.01.0008 release notes for detailed information on the WB.16.01 branch. Released, fully supported, and posted on the web.
WB.16.01.0007	2016-05-31	WB.16.01.0006	Released, fully supported, and posted on the web.
WB.16.01.0006	2016-03-28	WB.16.01.0005	Released, fully supported, and posted on the web.
WB.16.01.0005	n/a	WB.16.01.0004	Never released.
WB.16.01.0004	2016-01-20	WB.15.18.0007	Initial release of the WB.16.01 branch. Released, fully supported, and posted on the web.

Products supported

This release applies to the following product models:

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

Compatibility/interoperability

The switch web agent supports the following web browsers:

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

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

Version WB.16.03.0005

Static IP visibility

Added support for static IP visibility for IP addresses in DHCP Snooping database.

Version WB.16.03.0005

No enhancements were included in version WB.16.03.0005.

Version WB.16.03.0004

Accounting

Added support for `Called Station ID` and `NAS Port Type` fields to ClearPass RADIUS Accounting for clients with static IP addresses.

Cable Diagnostics

Added support for cable diagnostics to detect faults in 1G copper cable. This feature supports detection for distance to fault on a good cable. The feature can be used via CLI command `test cable-diagnostic`.

When the command is run, the following message is presented:

```
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)?
```

Central

LLDP stats support for Central integration has been added.

IPsec

Added support for custom trusted anchor (GlobalSign TA) certificate for the Private Central and the Virtual Mobility Controller (VPN concentrator). This feature allows an ArubaOS switch to be fully managed by Private Central while services like CPPM and Syslog, can be accessed through the IPsec tunnel to the VMC as the VPN concentrator. Aruba Activate provides the Custom TA (one CA for the entire deployment for all the services including NMS) and the Private Central URL.

IPsec Tunnel

Support for creating an IPsec tunnel between the switch and the Aruba mobility controller acting as a VPN concentrator has been added. This functionality allows the creation of a secure channel for communication between the switch and certain services such as Airwave, ClearPass, Syslog, and DNS. The ability to set routes to multiple destinations through the IPsec tunnel, as well as a default gateway route from the switch to the controller for non-IPsec traffic, is now possible.

The CLI command `aruba <vpn-type> peer-ip` initiates the IPsec session with the controller. The `<vpn-type>` can be either `amp` or `any`. If type `amp` is used, the switch will perform ZTP by triggering check-in (to

Airwave) through the IPsec channel. If type `any` is used, the switch will not automatically add a route to Airwave IP through the tunnel.

To configure Routes (to services behind the Aruba VPN Controller, such as CPPM, Syslog, DNS, etc.) through the IPsec channel use the CLI command `ip route /mask interface tunnel aruba-vpn`. Before adding/deleting a route to service network through the IPsec tunnel, it is recommended to execute the following CLI commands in case the controller IP also belongs to service network. These commands add/delete a static route to reach the controller IP through the default gateway:

```
aruba-vpn default-gateway enable
```

```
aruba-vpn default-gateway disable
```

IPsec VPN Type

Added a new aruba-vpn type "any" to enable control plane traffic protection for a Remote Access VPN session.

Example: `aruba-vpn type any`

When deleting an existing aruba-vpn configuration and before configuring with a new aruba-vpn type, a warning message is prompted: `Remove the existing aruba-vpn configuration before configuring with a new aruba vpn type.`

Switch software downgrade to a previous version is not allowed with Aruba VPN type "any" configured. An error message is displayed: `Firmware downgrade is not allowed if aruba vpn is configured with type any. Please unconfigure it before attempting to downgrade.`

Expanded TCP port range

The TCP port range allowed to configure an OpenFlow instance or a controller has been expanded from a range of 1024 through 65534 to a range of 1 through 65534. The new range can now be used in the *<tcp-port>* variable in the following commands:

```
openflow instance listen-port <tcp-port>
```

```
openflow controller-id <id> [ip <ip-address>] [port <tcp-port>]
```

OpenFlow

Added support for 'stats' flag in OpenFlow meter. The switch advertises OFPMF_STATS as a configurable flag when creating/modifying a meter. You are now able to get the meter statistics using the multipart message for any configured meter.

With the added support of STATS, the users will be able to query the statistics only if the STATS flag is configured along with the KBPS/PKTPS flags. Users will no longer be able to query the statistics without STATS.

REST ACL Rules

Support for ICMP and IGMP protocols, ToS, precedence, and log options have been added to the REST API for ACL rules.

REST System Details

Removed version dependency on displaying VLAN ID and IP address in REST interface for System Details. VLAN ID and assigned IP address of Aruba Central connection is now supported with REST v2.

Routing

Added support of /31 subnet mask when configuring IPv4 addresses on VLAN Interfaces. The switch allows you to configure the IP address with a subnet mask of 255.255.255.254 on a point-to-point link as described in RFC 3021.

`[no] ip address IP-ADDR/MASK-LENGTH`

Version WB.16.03.0003

DHCP Snooping

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

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

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

Federal Government certifications

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

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

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

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

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

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

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

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

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

Hiding sensitive information

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

IPsec

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

Job Scheduler

Minor enhancements to the job scheduler feature to:

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

LLDP

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

Netdestinations and Netservices

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

Next Gen Web UI

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

Warning message for configuring PoE allocate-by-value

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

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

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

REST

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

show interface Command

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

show power-over-ethernet Display

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

show system Commands

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

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

Static IP visibility

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

TCP Push Preserve

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

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

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

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

VLAN range addition

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

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

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

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

Version WB.16.03.0005

Authentication

CR_0000232197

Symptom: The switch may delay the request for authentication credentials.

Scenario: When accessing telnet and console session, the switch prompts for authentication credentials with a slight delay.

Workaround: Use SSH to access the switch to get the prompt for authentication credentials immediately.

Central

CR_0000233323

Symptom/Scenario: When a switch configuration is pushed via Aruba Central, the configuration may not be entirely pushed to the switch, resulting in an incomplete or truncated switch configuration.

Console
CR_0000230819

Symptom: The switch console may become unresponsive.

Scenario: When disconnecting the console session, connected to a standby or member switch of a stack, using **ESC + ~**, the console may not disconnect properly and become unresponsive causing the respective stack member to crash with an error message similar to `Software exception at multMgmtUtil.c:141 -- in 'mLoopPTx' <...>`.

LLDP
CR_0000232922

Symptom: The switch reports an incorrect error message when it fails to configure the loopback interface IP address for LLDP advertisements.

Scenario: When attempting to configure the loopback interface IP address for LLDP advertisements, the switch displays an incorrect error message:

```
This IP address is not configured or is a DHCP address
```

Instead, the following error message should be displayed:

```
This IP address is not configured or is a DHCP/Loopback address
```

Workaround: Configure a statically assigned VLAN IP address for LLDP advertisements.

OOBM
CR_0000230467

Symptom: Communication through OOBM port may not be working.

Scenario: After executing the CLI command `reload`, the OOBM interface status may not be correctly initialized.

Workaround: Execute the CLI command `show oobm` or `show oobm ip` to resolve the issue.

OpenFlow
CR_0000229081

Symptom: OpenFlow flow statistics counters may reset to zero and fail to increment after that.

Scenario: Packet count in the flow statistics reported in the CLI command `show openflow instance <name> flows` may stop incrementing. OpenFlow flows may fail to age out and the hard/idle timeout for the affected flows may not expire.

Workaround: Disable and re-enable OpenFlow instance state.

CR_0000229248

Symptom: OpenFlow traffic may not be sent to the correct priority queue.

Scenario: OpenFlow traffic with DSCP priority remarked by the configured traffic meter is sent to the default priority queue, instead of the remarked priority queue.

CR_0000229987

Symptom: OpenFlow may not be forwarding LLDP and CDP traffic to the specified port.

Scenario: LLDP and CDP traffic on OpenFlow enabled VLANs may not be properly redirected to the OpenFlow port.

OSPF
CR_0000233729

Symptom: The output of OSPF related commands, such as `show ip ospf [ external-link-state | link-state | statistics ]`, take an extended amount of time to run or display incomplete data.

Scenario: Any show command which includes `show ip ospf [ external-link-state | link-state | statistics ]`, takes an extended amount of time to run. Commands such as `show tech` contain multiple iterations which further exacerbate the amount of time needed to run the commands or data collected regarding OSPF status may be incomplete.

PoE
CR_0000229939

Symptom: Switch port PoE status cannot be changed from the Web UI.

Scenario: In a stacked switch environment, the Web UI does not allow you to change the PoE status of a port belonging to a stack member other than commander switch. It reports an error message: `Not a valid PoE port`.

Workaround: Use the following CLI command to change PoE status for the port:

`[no] interface <PORT-LIST> power-over-ethernet`

Private VLAN
CR_0000233782

Symptom: The switch may not properly forward traffic to the promiscuous port in the private VLAN.

When there is a client connected on a security enabled port and the port is an access port of the secondary VLAN, the client is not able to reach the router connected on the promiscuous port.

Scenario: In a private VLAN configuration, when using security enabled VLAN (for example, radius assigned attributes) on the secondary VLAN, the switch may fail to forward traffic from authenticated client to the promiscuous port.

Workaround: Disable security on the access port.

CR_0000234099

Symptom: The switch may not properly move a client's MAC address from one port to another.

Scenario: In a private VLAN, when a client moves from one access port to another on the same secondary VLAN across the ISL, the switch may not correctly move the client's MAC address to the new access port.

The MAC will clear when MAC age time expires, allowing the MAC address to be re-learned on the new port.

Workaround: Manually clear the MAC address from CLI to allow immediate MAC address re-learning on the new port.

RMON
CR_0000230643

Symptom: The switch may generate false RMON alarm traps.

Scenario: After an uptime of over 500 days, the switch may generate false RMON alarm traps for the monitored MIB objects.

sFlow

CR_0000228486

Symptom: sFlow displays invalid levels of dropped samples.

Scenario: When using trunk interfaces, sFlow is incorrectly calculating the levels of dropped samples displayed in the output of the CLI command `show sflow <INSTANCE> sampling-polling`.

Smart Link
CR_0000229453

Symptom: The switch may fail to forward traffic on ports with SmartLink enabled.

Scenario: When changing the Spanning Tree mode or the port status of the Spanning Tree enabled ports, the SmartLink enabled ports may stop forwarding the traffic.

Workaround: Disable and re-enable the affected SmartLink enabled ports.

CR_0000233339

Symptom: The SmartLink port might flood VLAN traffic even though it is not a member of that VLAN.

Scenario: When the switch is configured with SmartLinks and multiple VLANs, VLAN traffic is sent on SmartLink ports that are not a member of those VLANs.

Workaround: No workaround. Remove the SmartLink port configuration to avoid this issue.

SSH
CR_0000229176

Symptom: Unable to access switch via SSH.

Scenario: When using raw console terminal (`console terminal none`) with message of the day banner configured (`banner motd`) and SSH session to the switch may fail with the error message `Session terminated, unable to login`.

Workaround: Configure console ANSI or VT100 console terminal or disable message of the day banner.

CR_0000232500

Symptom: Switch fails to authenticate an SSH client using keyboard-interactive method.

Scenario: When the switch access is enabled for SSH public key authentication (for example, `aaa authentication ssh login public-key`), if the SSH client fails to authenticate using client private key for N-1 configured number of authentication attempts (for example, `aaa authentication num-attempts N`), the switch does not failover to authenticate the client using keyboard-interactive method. The switch causes the client authentication to fail with an error message similar to `Too many authentication failures`, even when one more attempt is available.

UDLD
CR_0000229788

Symptom: In a redundant configuration, the switch may stop forwarding traffic on LACP aggregated ports.

Scenario: In a redundant configuration with Spanning Tree enabled, when multiple redundancy switchover events occur, the switch may fail to forward traffic over an LACP trunk which has UDLD enabled in "verify-then-forward" mode.

Workaround: Disable and re-enable Spanning Tree. Alternatively, disable and re-enable the affected port.

Version WB.16.03.0004

CDP

CR_0000228335

Symptom: Switch reports an error message `Module command missing for port or invalid port <TRUNK-NAME>` when a configuration file is restored from backup.

Scenario: When a backup configuration file contains a CDP setting (for example, `no cdp enable <TRUNK-NAME>`) for a trunk port, the switch fails to restore it and reports an error message similar to:

```
line: 6. Module command missing for port or invalid port <TRUNK-NAME>.
Corrupted download file.
```

Device Profile
CR_0000213606

Symptom: Device profile removed and re-applied after a redundancy switchover event.

Scenario: After failing over to standby in an HA (high availability) configuration, the Device Profile is removed and reapplied to the port. This may result in service interruption on that port.

DHCP Snooping
CR_0000228042

Symptom: An incorrect RMON message is logged when a DHCP RELEASE message is dropped by DHCP Snooping on the switch.

Scenario: If DHCPv4-Snooping and IPv4 routing are enabled when the switch receives a unicast DHCP client message (RELEASE/DECLINE), the switch logs an incorrect RMON message `Attempt to release address <IPv4 address> leased to port <lport_src> detected on port <lport_src>`. However, this switch does not have the lease entry updated in the DHCPv4-Snooping binding state table (BST).

In environments with multiple DHCP servers reachable through different network paths, the message is logged repeatedly.

Direct Attach Cables
CR_0000218616

Symptom: Partner devices may prematurely detect link UP state when connected with DAC cable.

Scenario: During the switch reboot with DAC cable connected to a partner device, the port may be set in ready state too soon causing the link partner device to initiate traffic before the switch is ready.

Workaround: Disable and re-enable the switch interface to re-negotiate the L2 state.

Fault Finder
CR_0000223670

Symptom: The switch incorrectly allows ports with fault-finder enabled for broadcast-storm to be configured for link aggregation.

Scenario: The switch should prevent a port configured for fault-finder alarms to also be configured for link aggregation (trunk). Similarly, in case a port is already in a link aggregation (trunk), the switch should not allowed to configure it with fault-finder alarms for broadcast storm. For such instances, the switch should deny the requested configuration and prompt an error message similar to:

```
Fault-finder broadcast-storm configuration cannot be applied to members of a trunk
port(s) <PORT-NUM>.
```

```
Port <PORT-NUM> with fault-finder broadcast-storm configuration cannot be added to
a trunk.
```

IGMP

CR_0000227470

Symptom: In certain scenarios, the multicast traffic may not flow towards clients and traffic may not be forwarded to IGMP Querier or PIM routers from a non-Querier.

Scenario: In the event that a port, identified as a router-detect port for more than one IGMP-enabled VLAN, stops being the router-detected port for one of the VLANs, the switch may stop forwarding IGMP Membership Reports from Non Querier to Querier device for all IGMP-enable VLANs for which the port is identified as router-detected port. A port may stop being a router-detected port for a VLAN whenever the querier for that VLAN changes and it is no longer detected via respective port, or due to administratively disabling IGMP or PIM on that VLAN, or in case of a DT topology, distributed trunk port membership configuration changes are made.

Workaround: Enable IGMP isolation for un-joined multicast groups using CLI command `igmp filter-unknown-mcast` on global context. This filter limits multicast traffic flooding only on interfaces that contain queriers that are on the same VLAN as the multicast traffic. Enabling of the `igmp filter-unknown-mcast` will consume one filter per IGMP enabled VLAN, impacting the IGMP Group Capacity (i.e. the number of IGMP groups that can be forwarded without flooding). For more information on using the `igmp filter-unknown-mcast` command, see the *HPE ArubaOS-Switch Multicast and Routing Guide* for your switch.

LSA

CR_0000225246

Symptom: Intermittent connectivity loss to certain IPv6 destinations after an extended period of switch uptime.

Scenario: It is possible after an extended period of uptime for the switch to incorrectly calculate the OSPFv3 Link State Advertisement (LSA) Refresh Age time and fail to refresh its self-originated LSAs. As a result, peer switches may incorrectly delete the routes to the prefixes in these LSAs from their Routing Information Base (RIB) for 30 minutes.

Workaround: On the originator switches, enabling `debug ipv6 ospfv3` and then disabling (`no debug ipv6 ospfv3`) will trigger an immediate refresh for LSAs which are over the age of 1800 seconds.

MAC Authentication

CR_0000228130

Symptom: Switch may not correctly forward traffic on a successfully authenticated port with mac-authentication.

Scenario: When a switch port is configured for concurrent mac-authentication and 802.1X in client-mode, if this setting is overridden and changed to port-mode through RADIUS VSA 'HP-Port-Auth-Mode-MA' after a successful client authentication on the port with this RADIUS attribute, the switch may not correctly forward traffic when configured for ingress traffic control.

Example: `aaa port-access <PORT-LIST> controlled-direction in`

Workaround: Disable 802.1X on the port and reconnect or re-authenticate the client with RADIUS VSA 'HP-Port-Auth-Mode-MA' attribute.

Mirroring

CR_0000227861

Symptom: The switch displays incorrect mirroring policy status.

Scenario: The switch displays incorrect 'inactive' status in the output of CLI command `show monitor` when a mirror policy is applied to a VLAN.

Workaround: Execute CLI command `show monitor <mirror-session>` to check the mirror policy status.

PoE

CR_0000226003

Symptom: An invalid config entry is added to the switch for a port where some PDs are connected: `power-over-ethernet 0`.

Scenario: When connected PDs request port priority via LLDP MED, such as Cisco 7910G or similar PDs, and poe-lldp-detect is enabled on the respective switch port, an invalid config entry is added to the switch for the respective port `power-over-ethernet 0`. For switches which support stacking, this may cause the switch to crash with a message similar to:

```
Health Monitor: Read Error Restr Mem Access <…> Task='mPoeMgrCtl' <…>
```

Workaround: Disable `poe-lldp-detect` on the port where the respective PD is connected to clean up the invalid configuration entry.

CR_0000229080

Symptom: Missing information from the output of CLI command `show power-over-ethernet brief`.

Scenario: On a PoE capable switch, the columns "PLC CIs" and "PLC Type" are missing from the output of CLI command `show-power-ethernet brief`.

Port Configuration

CR_0000229450

Symptom: Unable to assign long names to a switch interface.

Scenario: When configuring a switch interface with a name greater than 50 characters using the CLI command `interface <PORT-LIST> name <PORT-NAME>`, the switch may crash with an error message similar to `Software exception at pvDmaV1Tx in mCntrsCtrl`.

Workaround: Configure the switch interface name with up to 50 characters.

QoS

CR_0000227806

Symptom: The switch may crash with an error message similar to `Software exception in ISR at btmDmaApi.c <...> No resources available!`

Scenario: When QoS for IP protocol is enabled and IPv6 traffic such as DHCP requests or IPv6 multicast is running on the network, the switch may crash with an error message similar to `Software exception in ISR at btmDmaApi.c <...> No resources available!`

Workaround: Disable QoS for IP protocol.

Routing

CR_0000223965

Symptom: Default route is not listed in the output of CLI command `show ip route`.

Scenario: When a VLAN interface is configured as the next-hop for the default static route, the route entry is not displayed in the output of the CLI command `show ip route`, while the static route counter is incremented in the output of the CLI command `show ip route summary`.

CR_0000228710

Symptom: In certain scenarios, the switch may have connectivity issues to certain destinations or induce routing loops in the network.

Scenario: The switch may incorrectly process certain routes in the routing table and erroneously choose less specific routes over more specific ones. These routes will remain in the routing table until they are flushed. This behavior may cause routing loops to occur, inability to reach the default gateway, or other similar routing

symptoms that could vary by routing protocol. This condition may be exacerbated by the number of routes being learned within a short time.

Spanning Tree
CR_0000227215

Symptom: Incorrect VLAN ID is displayed in the output of CLI command `display stp region-configuration`.

Scenario: A 4-digit VLAN ID number is truncated to 3 digits in the output of CLI command `display stp region-configuration`.

Example: Correct VLAN ID using `show spanning-tree mst-config`:

```
Instance ID Mapped VLANs
  ----------- ------------------------------------------------------------
  1           2,6-8,10-14,20-22,1022,1029,1035
```

Example: Truncated VLAN ID using `display stp region-configuration`:

```
Instance     Vlans Mapped
  1           2, 6 to 8, 10 to 14, 20 to 22, 102, 102, 103
```

Workaround: Use CLI command `show spanning-tree mst-config` to get the correct VLAN IDs mapped to the Spanning Tree instance.

Switch Module
CR_0000228591

Symptom: The switch may crash with an error message similar to `Software exception in kernel context at ghsException.c Internal system error`.

Scenario: When running traffic through the 10G ports of the expansion switch module, the switch may crash with an error message similar to `Software exception in kernel context at ghsException.c Internal system error`.

Virus Throttling
CR_0000228950

Symptom: An invalid message is displayed when configuring connection-rate-filter on a static LACP trunk interface.

Scenario: When a connection-rate-filter is applied to a static LACP trunk interface, although the configuration is supported and applied successfully to the trunk interface, the switch displays a misleading error message similar to `LACP has been disabled on CRF enabled port(s)`.

Web UI
CR_0000227147

Symptom: Interface Rx/Tx utilization is incorrectly calculated in the NextGenUI.

Scenario: Interfaces receiving or transmitting traffic levels that exceed 20% of their maximum bandwidth will erroneously have their utilization levels capped and reported at a maximum of 20% on "Interface Monitor" page of the NextGenUI web interface.

Workaround: Use "Total Frames" values to determine the interface utilization levels via the CLI commands `show interfaces port-utilization` or `show interfaces <PORT-LIST>`.

CR_0000227777

Symptom: Port mode setting may be incorrectly shown in the VLAN Properties section of the VLAN Management web page.

Scenario: When a port is selected in the VLAN Properties section of the VLAN Management web page, the "Mode for selected ports" may be different from what is displayed in the output of CLI command `show vlan <VLAN-ID>`.

Workaround: Use CLI command `show vlan <VLAN-ID>` to obtain the configured port mode.

CR_0000228869

Symptom: Switch modules may have incorrect graphical representation in NextGenUI switch view.

Scenario: When flexible switch modules are installed in the switch, the switch modules may show *(Empty)*, be missing altogether, or be mis-aligned in the Ports Status View of the NextGenUI web interface.

Workaround: Use Device View in the legacy NextGenUI to view the switch module status.

Version WB.16.03.0003

ARP
CR_0000200474

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

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

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

Cable Diagnostic
CR_0000222089

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

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

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

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

DHCP
CR_0000222120

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

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

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

DHCP Server
CR_0000216603

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

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

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

Job Scheduler
CR_0000221236

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

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

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

CR_0000222032

Symptom: 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"`.

OpenFlow
CR_0000219687

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

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

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

SNMP
CR_0000217437

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

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

Upgrade information

Upgrading restrictions and guidelines

WB.16.03.0005 uses BootROM WB.16.03. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

For more information about BootROM, see the *HPE ArubaOS-Switch Management and Configuration Guide WB.16.03*.

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

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

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

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the *HPE ArubaOS-Switch Basic Operations Guide Version 16.03*.

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

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

Finding Security Bulletins

Procedure

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

Security Bulletin subscription service

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

Networking Websites

Hewlett Packard Enterprise Networking Information Library

www.hpe.com/networking/resourcefinder

Hewlett Packard Enterprise Networking Software

www.hpe.com/networking/software

Hewlett Packard Enterprise Networking website

www.hpe.com/info/networking

Hewlett Packard Enterprise My Networking website

www.hpe.com/networking/support

Hewlett Packard Enterprise My Networking Portal

www.hpe.com/networking/mynetworking

Hewlett Packard Enterprise Networking Warranty

www.hpe.com/networking/warranty

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

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

Accessing Hewlett Packard Enterprise Support

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

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

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

Information to collect

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

Accessing updates

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

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:

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

  www.hpe.com/support/AccessToSupportMaterials

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

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts

do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

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

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

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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