



Hewlett Packard
Enterprise

WB.16.02.0011 Release Notes

Abstract

This document contains supplemental information for the WB.16.02.0011 release.

Part Number: 5200-2253
Published: September 2016
Edition: 1

© Copyright 2016 Hewlett Packard Enterprise Development LP

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®, Windows®, and Windows Server® are U.S. registered trademarks of the Microsoft group of companies.

Contents

1 WB.16.02.0011 Release Notes.....	5
Description.....	5
Important information.....	5
Version history.....	5
Products supported.....	6
Compatibility/interoperability.....	7
Minimum supported software versions.....	7
Enhancements.....	7
Version WB.16.02.0011.....	7
Central - ACL configuration.....	7
Central - DHCP REST API [add, delete, and query].....	7
Central - Dot 1x/RADIUS REST.....	7
Central - LED blink for Central connection.....	7
MAS feature: LLDP Authentication bypass with AP.....	8
Tunneled Node enhancement: fallback to switching and CoA.....	8
Version WB.16.02.0010.....	8
Version WB.16.02.0009.....	8
BootROM.....	8
Version WB.16.02.0008.....	8
Add MTU to Device Profile.....	8
Add 'no CoS' to Device Profile.....	8
AirWave Management Platform (AMP) Server MIB Changes.....	9
Central support.....	9
Connection via Management VLAN.....	9
IP Service Level Agreement.....	9
IPsec for AirWave Connection.....	9
Instrumentation Enhancements.....	10
Local User Roles.....	10
MAC Authentication Toggle.....	10
OSPF Routed Access Support.....	10
Per Port Trust.....	11
Per Port Tunneled Node.....	11
User Policies.....	11
Username VSA support.....	11
ZTP for Activate.....	11
Fixes.....	12
Version WB.16.02.0011.....	12
GVRP.....	12
IP Tunnels.....	12
MAC Authentication.....	12
OpenFlow.....	12
Redundancy.....	13
Transceivers.....	13
Version WB.16.02.0010.....	13
Stacking.....	13
Version WB.16.02.0009.....	13
Aruba Management Software.....	13
Trunking.....	13
Version WB.16.02.0008.....	13
Banner.....	13
CLI.....	14
Console.....	14

Counters.....	14
CPPM.....	14
DHCP.....	14
Display Issue.....	14
File Transfer.....	14
GVRP.....	15
IGMP.....	15
IPv6 ND.....	15
MAC-Based VLANs.....	15
Menu.....	15
NTP.....	16
OOBM.....	16
OpenFlow.....	16
PoE.....	16
SNMP.....	16
Spanning Tree.....	17
Supportability.....	17
Switch Module.....	17
Trunking.....	17
Issues and workarounds.....	17
IGMP.....	17
Stacking.....	18
Upgrade information.....	18
Upgrading restrictions and guidelines.....	18
Support and other resources.....	18
Accessing Hewlett Packard Enterprise Support.....	18
Accessing updates.....	19
Hewlett Packard Enterprise security policy.....	19
Documents.....	19
Related documents.....	19
Websites.....	20
Customer self repair.....	20
Remote support.....	20
Documentation feedback.....	21

1 WB.16.02.0011 Release Notes

Description

This release note covers software versions for the WB.16.02 branch of the software.

Version WB.16.02.0008 was the initial build of Major version WB.16.02 software. WB.16.02.0008 includes all enhancements and fixes in the WB.16.01.0004 software, plus the additional enhancements and fixes in the WB.16.02.0008 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.

To enable ZTP for Activate in switches that are updated to 16.02.0010 or later from a version previous to 16.02.0010, the switches have to be reset to factory default (see the *Installation and Getting Started Guide* for your switch for details on resetting the switch).

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 16.02*.

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.16.02.0011	2016-08-24	WB.16.02.0010	Released, fully supported, and posted on the web.
WB.16.02.0010	2016-08-11	WB.16.02.0009	Released, fully supported, and posted on the web.
WB.16.02.0009	n/a	WB.16.02.0008	Never released.
WB.16.02.0008	2016-07-08	WB.16.01.0004	Initial release of the WB.16.02 branch. Released, fully supported, and posted on the web.
WB.16.01.0008	2016-08-02	WB.16.01.0007	Please see the WB.16.01.0008 release notes for detailed information on the WB.16.01 branch. Released, fully supported, and posted on the web.
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.

Version number	Release date	Based on	Remarks
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.
WB.15.18.0012	2016-08-02	WB.15.18.0012	Please see the WB.15.18.0012 release notes for detailed information on the WB.15.18 branch. 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.15.18 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 operating system and web browser combinations:

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

Minimum supported software versions

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

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

Enhancements

This section lists enhancements found in the WB.16.02 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.16.02.0011

Central - ACL configuration

Added a new REST API to return all ACL rules. This enhancement must be enabled by Aruba Central.

Central - DHCP REST API [add, delete, and query]

Added REST APIs for DHCP Server configuration. This enhancement must be enabled by Aruba Central.

Central - Dot 1x/RADIUS REST

Added REST APIs for RADIUS configuration. This enhancement must be enabled by Aruba Central.

Central - LED blink for Central connection

Central connectivity is visually indicated by LED's for Cloud customers who are going to use existing products. If the device is not connected to Central then LEDs will indicate the connection

status (super state) which broken down into further substrate error. USR/FDX LED, Locator LED and Port Mode LED are used to indicate various states. Customer will press the mode button to enter USR/FDx mode then see the port mode LED behavior (if cloud enabled).

MAS feature: LLDP Authentication bypass with AP

This feature by-passes authentication for an AP that sends LLDP TLV.

Tunneled Node enhancement: fallback to switching and CoA

When tunneled node is enabled on a port and controller is not reachable, an option is added to continue to do local switching on the port traffic.

Once the tunnel is established to the controller, the port traffic is tunneled to the controller.

Version WB.16.02.0010

No enhancements are included in version WB.16.02.0010.

Version WB.16.02.0009

BootROM

The BootROM version was updated to WB.16.02.

Version WB.16.02.0008

Add MTU to Device Profile

ArubaOS-Switch-based switches support the jumbo frame attribute in device profile. When an Aruba AP is attached to the port, the configured MTU is applied to the port.

The default size of the MTU is 9K. This value is not configurable through device profile context commands. If the user wants to change this value, they manually configure it in the switch global configuration. Users can enable or disable Jumbo frame support through device profile. By default, jumbo frame support is disabled.

If jumbo frame support is already enabled on a VLAN, but disabled in the device profile for the same VLAN, jumbo frame support will remain enabled even if the device profile is active. Non device-profile configuration takes precedence over device profile configuration.

When the user enables jumbo frame support, all the VLANs configured in the device profile will get jumbo frame enabled. All ports belonging to that VLAN can handle packets up to 9k size (default size). This includes ports where an Aruba AP is not connected if that port belongs to a VLAN configured in the device profile.

Add 'no CoS' to Device Profile

Class of service (CoS) is applied on the packets received on the port. The default value is "none". If a user wants to change the CoS configuration, the user can set any CoS value from 0-7.

Whenever the configured value is "none," the switch honors the CoS value of the packet. If the CoS value is set via the Device Profile, the CoS setting on the Device Profile is used instead.

Please note: In the 16.01 release, the CoS value could be set to any value from 0 to 7. From 16.02 onwards, the CoS value can be configured as "none" also.

The commands to set CoS value to "none" are:

```
(config)#device-profile name abc
(device-profile)#no cos
```


AirWave Management Platform (AMP) Server MIB Changes

SNMP MIB support for AMP-Server and IPSec tunnel for AMP management traffic are available in 16.02.

Central support

Functionality to enable management of ArubaOS-Switch-based switches from a cloud-based Aruba Central network management system is included in this software release. Aruba Central is a software-as-a-service subscription in the cloud and streamlines management of multiple network devices.

Central allows the deployment of network devices on sites with no IT personnel (such as branch offices or retail stores). The deployed devices are managed from a centralized system called Central. The following management capabilities are supported for ArubaOS-Switch-based switches:

- Configuration of basic switch functionality like VLANs and ports
- Monitoring of system details and ports
- Remote Console service for remote debugging and troubleshooting
- Firmware upgrade

Connection via Management VLAN

When the Management VLAN is configured and enabled (active), connection to the AMP Server will be allowed only via Management VLAN.

IP Service Level Agreement

IP Service Level Agreement (IP SLA) is a feature that helps administrators collect information about network performance in real time. With increasing pressure on maintaining agreed-upon Service Level Agreements on Enterprises and ISPs alike, the IP SLA serves as a useful tool.

The IP SLA feature provides:

- Application-aware monitoring that simulates actual protocol packets.
- Predictable measures that aid in ease of deployment and help with assessment of existing network performance.
- Measures of delay and packet loss for time-sensitive applications.
- End-to-end measurements to represent actual user experience.

The following SLA types are supported:

- UDP Echo, including connectivity testing of transport layer (UDP) services, Round-Trip-Time (RTT) measurement, one-way delay, and packet loss details.
- ICMP Echo, including connectivity testing, RTT measurement, and packet loss details.
- TCP Connect, including connectivity testing of transport layer (TCP) services, and handshake time measurement.

IPsec for AirWave Connection

Support for secure communication between ArubaOS-Switches and an Aruba mobility controller (VPN concentrator) for the management traffic sent to or received from the AirWave Management Platform (AMP) server.

This feature provides necessary support for Zero Touch Provisioning (ZTP) by establishing a secure channel between an ArubaOS-Switch-based switch and the Network Management Server (AirWave). ZTP is a feature by which switches discover their respective management system

(AirWave or Aruba Central) during initial boot up using DHCP or Activate. This enables switches to be configured and managed automatically without admin intervention.

In a deployment scenario where a switch at a remote branch and an AirWave server located at corporate headquarters or datacenter are connected via an un-trusted public network (Internet), communication between the switch and the AirWave server must be protected. This feature ensures that communication between ArubaOS-Switch-based switches and an AirWave Server (management traffic) is protected by establishing a secure channel between the switches and an Aruba VPN Controller (connected to an AirWave server) using an IPsec tunnel for the management traffic between the AMP server and the switch.

Please note: This feature only works with the following ArubaOS-Switch-based switches as these switches fully support TPM certificates: 2920, 2930F, 3800, 3810, and 5400R. This feature is restricted to work only with an Aruba Controller (as VPN concentrator) for the IPsec tunnel between the switch and the AMP server.

This feature is currently supported only with Aruba Controller running ArubaOS 6.5.0.0.

Instrumentation Enhancements

Provide additional/enhanced information that can assist in diagnostics, monitoring, and troubleshooting of various switch features.

- DT, STP, and LLDP `show tech` enhancements
- Multicast `show tech` enhancements

Local User Roles

When this feature is enabled, every authenticated client is associated with a user role (even when authentication fails), which determines the client's network privileges, frequency of re-authentication, VLAN, captive portal profile, rate-limit, and QoS (Quality of Service).

The feature is globally enabled for all authentication methods and does not impact clients connected to ports without port-security.

User Roles are locally created in an ArubaOS-Switch-based switch and applied based on a client's MAC Address for Local-MAC-Authentication or via the HPE-User-Role VSA (Vendor Specific Attribute) returned by the RADIUS server for MAC-Authentication, Web-Authentication, and 802.1X.

MAC Authentication Toggle

Port-based MAC authentication allows an infrastructure device to be authenticated with a port-based policy that dictates the distribution switch to open the authenticator port to all clients from the authenticated device. This is similar to the existing port-based 802.1X authentication available on HPE switches, except that the new port-based 802.1X authentication can also be statically configured on an authenticator port to be persistent over port toggling and switch reboot, while the existing port-based mode MAC authentication will be dynamic, triggered by the dynamic policy an authenticated client will receive.

OSPF Routed Access Support

OSPF (OSPFv2 and OSPFv3) is supported on K, KA, KB platforms in earlier software releases.

From 16.02.0008 onwards, OSPF Routed Access support is enabled on WB and WC platforms with the following limitations:

- Only one area is allowed for both OSPFv2 and OSPFv3
- Same area ID should be used for OSPFv2 and OSPFv3
- Maximum of 8 OSPF interfaces supported for each OSPFv2 and OSPFv3
- ABR configuration and Virtual-links are not supported

- Max supported routes: 200 for each OSPFv2 and OSPFv3
- OSPFv3 tunnels and BFD are not supported.

Per Port Trust

The per-port Trust QoS feature allows customers to select which packet fields are used to determine inbound service-priority:

Packet fields	Description
Default	Use the VLAN cos (Priority Code Point, or PCP) value and preserve any IP-ToS values.
dot1p	Same as default mode.
ip-prec	Use the QoS value corresponding to the IP-Precedence priority-mapping for the IP-ToS field.
Dscp	Use the QoS value corresponding to the Differentiated Services priority-mapping for the IP-ToS field.
None	Use none of the inbound packet-priority information.

For details about the QoS Type-of-Service IP-Precedence or Differentiated-Services priority mappings, please refer to the *Advanced Traffic Management Guide* for your switch.

Please note: QoS trust modes other than “default” or “none” are **mutually exclusive** with the QoS port-priority feature.

Per Port Tunneled Node

Tunneled node, also known as a wired tunneled node, provides access and security using an overlay architecture.

The tunneled node connects to one or more client devices at the edge of the network and then establishes an L2 GRE tunnel to the controlling concentrator server. This approach allows the controller to support all the centralized security features, such as 802.1x authentication, captive-portal authentication, and stateful firewall.

The Tunneled Node feature is enabled on a per-port basis. Any traffic coming from non-tunneled node interfaces will be forwarded “normally” without being tunneled to a Mobility Controller.

User Policies

User Policies are new QoS (Quality of Service) Policies that are used in conjunction with User-Roles to provide control over ingress traffic originating from User-Role assigned clients. This feature supports IPv4 and IPv6 traffic. Classified user traffic is matched and shaped by user policy actions. User Policy actions allow traffic to be rate-limited, permitted, and denied. It also allows VLAN priority, DSCP, and IP-Precedence (DSCP & IP-precedence are mutually exclusive) to be assigned to matching traffic. User Policies are assigned to User-Roles.

Username VSA support

This feature enables the ‘Client Name’ field on the switch to be updated with a value configured via the User-Name VSA (Vendor Specific Attribute) returned by the RADIUS server. This improves the data displayed via the Consolidated Client View output generated by the CLI command `show port-access client`, especially when using MAC-Authentication.

ZTP for Activate

The Aruba Activate service is part of the larger Mobility as a Service (MaaS) cloud initiative from Aruba. The Aruba Activate service consists of many services like Tracking, Provisioning, Upgrade and Inventory. Due to a limitation in the Activate server, this feature is only available for switch

units manufactured after February 1, 2016 (the 3rd and 4th letters in the serial number have to be 62 or higher).

Zero Touch Provisioning (ZTP) enables auto-configuration of an ArubaOS-Switch-based switch without requiring any admin intervention on the switch. When a Cloud-enabled ArubaOS-Switch-based switch with factory default configuration becomes active on the network, it first contacts the NTP server, then contacts the Activate server, where it gets validated and forwarded to a Central or AirWave server to start further communications for auto provisioning.

The Activate ZTP process:

- Redirects the switch to AirWave or Central. Activate is not responsible for the actual switch configuration.
- If Activate returns an Aruba Mobility Controller IP address (in addition to AirWave parameters), the switch establishes an IPSec tunnel with the Controller and sends traffic over this tunnel.

Fixes

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

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

Version WB.16.02.0011

GVRP

CR_0000204332 Symptom: The detailed information about mac-addresses dynamically learnt by the switch is not correctly displayed in the output of CLI command `show mac-address <mac-address>`.

Scenario: When mac-addresses are learnt 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`.

IP Tunnels

CR_0000212791 Symptom: In certain conditions, tunnel interface activation may fail.

Scenario: When the switch IP address configuration is modified after a tunnel interface was already configured on the switch, the tunnel activation may fail.

Workaround: Delete then re-create the tunnel interface after modifying the switch IP 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 then re-enable after the data cable is plugged into the port. Disable or enable the port using CLI command `interface <port-num> disable | enable`.

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.

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`.

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.

Version WB.16.02.0010

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.

Version WB.16.02.0009

Aruba Management Software

CR_0000214536 Symptom/Scenario: The ArubaOS-Switch-based switch fails to connect to the Aruba Activate server, potentially impacting Aruba Central connectivity and ZTP (zero-touch provisioning) using Activate for the AirWave and IPsec (connection with Aruba Controller for AirWave management traffic) solution. The switch logs an event message similar to `Activate: Received failure "response from the Activate server with status code: None"`.

Trunking

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.16.02.0008

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_0000157943 Symptom: When the CLI command `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.

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

Workaround: Upgrade to the most recent switch software revision.

Console

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

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

Counters

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

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

CPPM

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

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

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

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.

Display Issue

CR_0000190925 Symptom/Scenario: A 100% CPU usage spike occurs every 10 minutes caused by the HTTP task calling the Entropy function.

File Transfer

CR_0000192894 Symptom: Setting the session idle-timeout to lower settings can cause a file transfer to hang indefinitely.

Scenario: When session idle-timeout is configured to lower values, a file transfer exceeding the configured idle-timeout may hang indefinitely when executed from a remote session to the switch.

Workaround: Configure session idle-timeout value to a higher value to allow file transfers to complete before the idle timer expires.

GVRP

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

Scenario:

1. Connect an Aruba AP to the switch and enable device profile.
2. Configure AP to send GVRP PDUs with some VLANs.
3. Check VLAN status on the switch port connected to Aruba AP, GVRP VLANs advertised by AP would not be seen for the AP connected port.

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

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 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-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.

Menu

CR_0000198649 Symptom: Incorrect maximum number of supported authorized managers specified in the help text message of the Menu interface.

Scenario: The message text of the IP Authorized Managers "Help Screen" Menu interface states A maximum of 10 addresses is supported. The switch allows the configuration of up to 100 authorized managers.

Workaround: Use the CLI command `ip authorized-managers help` to determine the maximum number of authorized managers that can be configured on the switch.

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' <...>` and reboot.

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.

PoE

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

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

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

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

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

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: 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 configuration related to the root-guard, tcn-guard, bpdu-filter, and pvst-filter after removing VLAN. For example:

```
(config)# no vlan <vlan1>
(config)# spanning-tree <vlan2> root guard tcn-guard bpdu-filter pvst-filter
(config)# spanning-tree <vlan3> root-guard tcn-guard bpdu-filter pvst-filter
```

Supportability

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

Scenario: The crash log memory is corrupted for one of the crash records.

CR_0000200816 Symptom: In some cases, switch may halt or crash when executing the CLI command `show tech all`.

Scenario: A switch hang or crash may be encountered during execution of 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_0000198470 Symptom: A v3 switch module might crash with an error message similar to `Software exception at alloc_free.c <...> buf already freed <...>`.

Scenario: In cases of high traffic volume through a v3 switch module with traffic sampling enabled, if the switch needs to drop lot of the samples, the switch module might crash.

Workaround: Disable SFLOW using CLI command `no sflow <INSTANCE>`.

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`.

Issues and workarounds

The following are known open issues with the WB.16.02.0011 release.

IGMP

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.

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.

Upgrade information

Upgrading restrictions and guidelines

WB.16.02.0011 uses BootROM WB.16.02. 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.16.02*.

-
- ① **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 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 16.02*.

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

Information to collect

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

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
 - Hewlett Packard Enterprise Support Center **Get connected with updates** page:
www.hpe.com/support/e-updates
 - HPE Networking Software:
www.hpe.com/networking/software
 - To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
www.hpe.com/support/AccessToSupportMaterials

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

Hewlett Packard Enterprise security policy

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

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

To find security bulletins:

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

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

www4.hpe.com/signup_alerts

Documents

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

Related documents

The following documents provide related information:

- *HPE ArubaOS-Switch Access Security Guide WB.16.02*
- *HPE ArubaOS-Switch Advanced Traffic Management Guide WB.16.02*

- *HPE ArubaOS-Switch Basic Operation Guide Version 16.02*
- *HPE ArubaOS-Switch Feature and Commands Index Version 16.02*
- *HPE ArubaOS-Switch IPv6 Configuration Guide WB.16.02*
- *HPE ArubaOS-Switch Management and Configuration Guide WB.16.02*
- *HPE ArubaOS-Switch Multicast and Routing Guide WB.16.02*
- *HPE ArubaOS-Switch Software OpenFlow v1.3 Administrator Guide 16.02*
- *HPE ArubaOS-Switch Service Insertion Guide 16.02*

Websites

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

Customer self repair

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

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

www.hpe.com/support/selfrepair

Remote support

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

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

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