YC.16.02.0020 Release Notes

Part Number: 5200-3973
Published: July 2017
Edition: 1

Notices

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

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

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

Acknowledgments

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

Description

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

Version YC.16.02.0012 was the initial build of Major version YC.16.02 software.

Product series supported by this software:

- Aruba 2540 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
YC.16.02.0020	2017-07-07	YC.16.02.0019	Released, fully supported, and posted on the web.
YC.16.02.0019	n/a	YC.16.02.0018	Never released.
YC.16.02.0018	2017-03-31	YC.16.02.0017	Released, fully supported, and posted on the web.
YC.16.02.0017	n/a	YC.16.02.0016	Never released.
YC.16.02.0016	2017-01-27	YC.16.02.0015	Released, fully supported, and posted on the web.
YC.16.02.0015	n/a	YC.16.02.0014	Never released.
YC.16.02.0014	2016-10-28	YC.16.02.0013	Released, fully supported, and posted on the web.
YC.16.02.0013	n/a	YC.16.02.0012	Never released.
YC.16.02.0012	2016-08-31		Initial release of the YC software. Released, fully supported, and posted on the web.

Products supported

This release applies to the following product models:

Product number	Description
JL354A	Aruba 2540 24G 4SFP+ Switch
JL356A	Aruba 2540 24G PoE+ 4SFP+ Switch
JL355A	Aruba 2540 48G 4SFP+ Switch
JL357A	Aruba 2540 48G PoE+ 4SFP+ 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 YC.16.02.0020

No enhancements were included in version YC.16.02.0020.

Version YC.16.02.0019

Version YC.16.02.0019 was never released.

Version YC.16.02.0018

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.`

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.

Version YC.16.02.0017

Version YC.16.02.0017 was never released.

Version YC.16.02.0016

VLAN

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

Version YC.16.02.0015

Version YC.16.02.0015 was never released.

Version YC.16.02.0014

TCP Push Preserve

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

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

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

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

Version YC.16.02.0013

Version YC.16.02.0013 was never released.

Version YC.16.02.0012

128 RPVST enabled VLANs

This increases the maximum number of supported VLANs in RPVST from 64 to 128. There is no other change. The switch will not allow a user to configure more than 128 RPVST enabled VLANs.

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.

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

Central - ACL configuration

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

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

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

Central - Dot 1x/RADIUS REST

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).

Common Access Card

A common access card (CAC) is a United States Department of Defense (DoD) smart card for multifactor authentication. CACs are issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, non-DoD government employees, state employees of the National Guard, and eligible contractor personnel. In addition to its use as an ID card, a CAC is required for access to government buildings and computer networks.

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.

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

IP Service Level Agreement

YC does not support IP-SLA for voice.

IP Service Level Agreement (IP SLA) is a feature that helps administrators collect information about network performance in real time.

Only 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 Aruba Controller (as VPN concentrator). 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 Controller (connected to an AirWave server).

Please note: This feature only supports traffic to the AMP; it is not a general-purpose IPsec VPN. 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.

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.

MAS feature: LLDP Authentication bypass with AP

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

NextGen Web UI

The NextGen Web UI is a new browser-based user interface that has been introduced to improve usability over that of the legacy web UI. This first phase release is establishing the new look and feel, navigation model, and

dashboard layout. It also provides additional system monitoring capabilities. The intent is to build upon this framework in future releases to ultimately deliver a full featured web UI that will simplify the user experience with an emphasis on system monitoring and troubleshooting.

See Compatibility/interoperability for supported browsers.

Current OS support: Windows Server 2008, Windows Server 2012, Windows Client 2007 and Windows Client 2008, MacOS.

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.

Trap generation with hardware removal/insertion

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

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.

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 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 YC.16.02.0020

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.

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.

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.

Version YC.16.02.0019

Version YC.16.02.0019 was never released.

Version YC.16.02.0018

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.
```

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.

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.

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.

Routing
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.

Syslog
CR_0000210928

Symptom: Syslog messages do not contain the configured source IP address.

Scenario: When a source IP address or interface is configured for syslog protocol (`ip source-interface syslog {<IP-ADDR> | vlan <VLAN-ID> | loopback <LOOPBACK-ID>}`), the syslog message always contains the IP address of the VLAN the syslog is sourced from, instead of the configured source IP address, VLAN or loopback interface.

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_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.

Version YC.16.02.0017

Version YC.16.02.0017 was never released.

Version YC.16.02.0016

Banner
CR_0000225460

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

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

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

Cable Diagnostic
CR_0000222089

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

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

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

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

DHCP
CR_0000222120

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

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

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

DHCP Server
CR_0000216603

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

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

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

Event Log
CR_0000225392

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

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

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

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

Job Scheduler
CR_0000221236

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

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

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

CR_0000222032

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

Scenario: If a job is scheduled to copy data files to/from a remote server configured via hostname, the switch may crash with an error message similar to `Health Monitor: Read Error Restr Mem Access <...> Task='tCron000001' <...>` when executing the job at scheduled time.

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

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

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

SNMP

CR_0000217437

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

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

Spanning Tree

CR_0000201299

Symptom: A switch configured with RPVST may crash with an error message similar to `Software exception at bttfMsgSysDrv.c <...> -- in 'mPvstSlvCtrl' <...>`.

Scenario: When disabling spanning tree on a switch that is part of RPVST topology, an external loop may be created. As a result, a broadcast of RPVST BPDUs may be received by the switch, potentially leading to a crash with an error message similar to `Software exception at bttfMsgSysDrv.c <...> -- in 'mPvstSlvCtrl' <...> ASSERT: No resources available!`

Workaround: Make sure that no external loops are created when disabling spanning tree on any switch that is part of an RPVST topology.

CR_0000217382

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

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

```
 Port      Type |   Alert    Enabled Status  Mode      Mode    Ctrl
 ----- ---------- + --------- ------- ------ ---------- ---- ----
  1    10/100TX |   No          Yes    Down   100FDx                MDI        off
```

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

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

Terminal

CR_0000223941

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

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

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

Trunking

CR_0000211583

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

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

Example: Copy & Paste from text file:

trunk 1-4 trk1

trunk 5-9 trk1

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

Version YC.16.02.0015

Version YC.16.02.0015 was never released.

Version YC.16.02.0014

Authorization

CR_0000216097

Symptom: In certain conditions, the User Roles feature may be unintentionally disabled.

Scenario: If the User Role feature is already enabled on the switch and an unsuccessful switch configuration restore using a file transfer occurs, the User Role may become disabled.

Workaround: Manually disable and then re-enable the User Role feature using the CLI command `aaa authorization user [disable | enable]`.

CR_0000221546

Symptom: When executing unauthorized commands, the switch may fail to include a blank line before printing the error message `Not authorized to run this command`.

Scenario: When the switch is configured for TACACS+ command authorization and an unauthorized command is executed, the switch may fail to include a blank line before printing the error message `Not authorized to run this command`. This may cause some applications, such as IMC, to misunderstand the message.

Console

CR_0000206708

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

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

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

MAC Authentication

CR_0000210511

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

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

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

mDNS
CR_0000216815

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

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

SSH
CR_0000201108

Symptom: Switch configured with DSA key refuses SSH connections.

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

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

CR_0000217201

Symptom: The SSH server cannot be bound to well-known port numbers ranging from 0 to 1023.

Scenario: When using the CLI command `ip ssh port <port-num>`, the switch does not allow the SSH server to be configured to listen to well-known or system ports ranging from 0 to 1023. The switch displays the error message `Cannot bind reserved TCP port <port-num>`, except when using `"default"` and `22` as the `<port-num>`.

Workaround: Configure the SSH server to listen for SSH connections on ports `"default"`, `22`, or ports greater than 1023.

Version YC.16.02.0013

Version YC.16.02.0013 was never released.

Upgrade information

Upgrading restrictions and guidelines

YC.16.02.0020 uses BootROM YC.16.01.0001. 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 YC.16.02*.

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.

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*.

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.