ArubaOS-CX 10.05.0020 Release Notes for the Aruba 8400 Switch Series

a Hewlett Packard
Enterprise company

Part Number: 5200-7555
Published: September 2020
Edition: 1

Notices

Acknowledgments

Description

This release note covers software versions for the ArubaOS-CX 10.05 branch of the software.

NOTE: If you run the `show version` command on the 8400, the version number will display XL. 10.05.*xxxx*, where *xxxx* is the minor version number.

ArubaOS-CX is a new, modern, fully programmable operating system built using a database-centric design that ensures higher availability and dynamic software process changes for reduced downtime. In addition to robust hardware reliability, the ArubaOS-CX operating system includes additional software elements not available with traditional systems, including the features included in the Enhancements section of this release note.

Version 10.05.0001 is the initial build of major version 10.05 software.

Product series supported by this software:

Aruba 8400 Switch Series

Important information

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

If the switch has RPVST enabled and the native VLAN ID configured for the trunk interface is not equal to 1 and this VLAN ID is also used as the management VLAN, after an upgrade from any 10.04.00*xx* version of software to 10.05.*xxxx* or 10.04.1*xxx*, the switch may not be accessible over the trunk interface.

To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where <*VLAN_ID*> is the native VLAN ID configured on the trunk interface.

If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

IMPORTANT: If the switch is configured with an entry in a Class or Access list that matches specifically on AH or ESP traffic, that policy or ACL is no longer permitted in 10.05.0001 and it will fail to apply. Remove such entries from the configuration prior to upgrading to 10.05.0001 or remove the respective entries from ACLs or Class that failed to apply after the upgrade to 10.05.0001.

IMPORTANT: If the switch is configured with IGMP or MLD snooping options such as "forward", "fastleave", "forced-fastleave", or "blocked" at the VLAN context, after upgrading to 10.05.0001 you will need to reconfigure these options for each interface from the interface configuration context.

Example config before 10.05.0001:

```
vlan 2
   ip igmp snooping forward 1/1/1
   ip igmp snooping blocked 1/1/2
   ip igmp snooping force-fastleave 1/1/3
   ip igmp snooping fastleave 1/1/4
```

Example config to be added after upgrade to 10.05.0001:

```
interface 1/1/1
    ip igmp snooping forward vlan 2
interface 1/1/2
    ip igmp snooping blocked van 2
interface 1/1/3
    ip igmp snooping forced-fastleave vlan 2
interface 1/1/4
    ip igmp snooping fastleave vlan 2
```

NOTE: 10.03 is the minimum required software version prior to upgrading to 10.05. If your device is using a version of software prior to 10.03, you must first upgrade to a version of 10.03 before upgrading to 10.05. Check release notes for the software version you will upgrade to for instructions on performing the upgrade to 10.03.

IMPORTANT: To restore a previous configuration when downgrading to a previous version of software, follow these steps:

1. Use the `show checkpoint list all` command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the `Image Version` column in the output of the command, for example, XL.10.04.3000).

   This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.

2. Copy the backup checkpoint into the startup-config.

3. Boot the switch to the target version (lower version), making sure to select `no` when prompted to save the current configuration.

1. If you are upgrading from version 10.03, upon the first time booting to XL.10.04.3030 a new version of ServiceOS will be installed. At the switch console port an output similar to the following will be displayed as various components are being updated:

```
8400X# boot system primary
Default boot image set to primary.

Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.

Checking for updates needed to programmable devices...
Done checking for updates.

2 device(s) need to be updated during the boot process.
The estimated update time is 5 minute(s).
There may be multiple reboots during the update process.
```

```
This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y

Press Esc for boot options
ServiceOS Information:
    Version:          GT.01.03.0007
    Build Date:       2019-02-06 17:59:30 PST
    Build ID:         ServiceOS:GT.01.03.0007:d75d3b9f7679:201902061759
    SHA:              d75d3b9f767954313017103d0c43413abec33550

Boot Profiles:

0. Service OS Console
1. Primary Software Image [XL.10.04.3030]
2. Secondary Software Image [XL.10.03.0051]

Select profile(primary):

2 device(s) need to be updated by the ServiceOS during the boot process.
The estimated update time by the ServiceOS is 5 minute(s).
There may be multiple reboots during the update process.


ISP configuration:
    Auto updates        : enabled
    Version comparisons : match (upgrade or downgrade)
    Unsafe updates      : allowed (less than 16 minute(s) remaining)

Advanced:
    Config path         : /fs/nos/isp/config [DEFAULT]
    Log-file path       : /fs/logs/isp [DEFAULT]
    Write-protection    : disabled [DEFAULT]
    Package selection   : 0 [DEFAULT]

MODULE 'mc' DEVICE 'svos_primary' :
    Current version  : 'GT.01.03.0007'
    Write-protected  : NO
    Packaged version : 'GT.01.05.0003'
    Package name     : 'svos'
    Image filename   : 'GT_01_05_0003.svos'
    Image timestamp  : 'Tue Oct  8 11:54:19 2019'
    Image size       : 25773563
    Version upgrade needed

Starting update...

Erasing   [****************************************] 100%  (592 KB/sec)
Verifying [****************************************] 100%  (3285 KB/sec)
Writing   [****************************************] 100%  (875 KB/sec)
Verifying [****************************************] 100%  (3284 KB/sec)


Update successful (101.4 seconds).
```

2. Multiple components will be updated and several reboots will be triggered during these updates. When all component updates are completed, the switch console port will arrive at the login prompt with a display similar to following:

```
(C) Copyright 2017-2019 Hewlett Packard Enterprise Development LP

                      RESTRICTED RIGHTS LEGEND
```

```
 Confidential computer software. Valid license from Hewlett Packard Enterprise
 Development LP 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.

We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events
Please register your products now at: https://asp.arubanetworks.com


8400X login:
```

IMPORTANT: HPE recommends waiting until all upgrades have completed before making any configuration changes.

Industry and government certifications

Refer to the Approved Product Lists sites for the Common Criteria, FIPS 140-2 and DoDIN APL to obtain the product certification details. Products should be used as evaluated and defined in the respective configuration guides.

- Common Criteria: **https://www.niap-ccevs.org/Product/**
- FIPS 140-2: **https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search**
- DoDIN APL: **https://aplits.disa.mil/processAPList.action%3bjsessionid=f2l2uEoOL6g4YYsEyVrFgx4W4f8J-Fgu4DLFZZmPXCvl-7Ft9SGf%21809605859**

License written offer

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open-source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

```
Hewlett Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
U.S.A.
```

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at: **https://hpe.com/software/opensource**

Version history

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

Version number	Release date	Remarks
10.05.0020	2020-09-23	Released, fully supported, and posted on the web.
10.05.0011	2020-08-28	Released, fully supported, and posted on the web.
10.05.0010	2020-08-21	Released, fully supported, and posted on the web.
10.05.0001	2020-07-10	Initial release of ArubaOS-CX 10.05. Released, fully supported, and posted on the web.

Products supported

This release applies to the following product models:

Product number	Description
JL375A	Aruba 8400 8-slot Chassis/3xFan Trays/18xFans/Cable Manager/X462 Bundle
JL376A	Aruba 8400 1x Mgmt Mod 3x PS 2x 8400X Fabric Mod 1x 32p 10G Mod and 1x 8p 40G Mod Bundle (includes JL375A)

Compatibility/interoperability

The switch web agent supports the following web browsers:

Browser	Minimum supported versions
Edge (Windows)	41
Chrome (Ubuntu)	76 (desktop)
Firefox (Ubuntu)	56
Safari (MacOS)	12
Safari (iOS)	10[1]

[1] Version 12 is not supported

NOTE: Internet Explorer is not supported.

Compatibility of the switches found in this release note with network management software:

Management software	Supported version(s)
Airwave	8.2.11.1
Network Automation	10.10, 10.11, 10.20, 10.21, 10.30, 10.40

Table Continued

Management software	Supported version(s)
Network Node Manager	10.10, 10.20, 10.21, 10.30, 10.40
IMC	7.3 (E0506P03)

NOTE: For more information, see the respective software manuals.

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
JL366A	Aruba 8400X 6-port 40GbE/100GbE QSFP28 Advanced Module	10.00.0006
JL687A[1]	Aruba 8400X-32Y 32p 1/10/25G SFP/SFP+/SFP28 Module	10.04.2000

[1] The SFP28 ports in the JL687A module are organized into eight groups of 4 ports each: interface-group 1 (ports 1-4), interface-group 2 (ports 5-8), interface-group 3 (ports 9-12), and so forth. See the *Aruba 8400 Installation and Getting Started Guide* for more information.

Transceiver support

Transceivers supported for the first time with this version of software:

No new transceiver support

Refer to the *Transceiver Guide* for information on all transceivers that are supported.

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 10.05.0020

Category	Description
Captive Portal	Added support for the use of the following characters in the Captive Portal URL string: question mark (?), colon (:), slash (/), equal sign (=), ampersand (&), period (.), underscore (_), and hyphen (–).

Version 10.05.0012

No enhancements were included in version 10.05.0012.

Version 10.05.0011

No enhancements were included in version 10.05.0011.

Version 10.05.0010

Category	Description
BGP	Added support for community list matching when redistributing BGP routes into OSPF using a route map.

Counters	Added the new `global` option to the `clear interface statistics` command to clear hardware interface statistics, allowing an administrator to permanently clear global counters across CLI sessions.
	Syntax
	`clear interface [<IF-NAME>|<IF-RANGE>] statistics [global]`
	Description
	Resets interface statistics for the current session or, if the global option is selected, across all sessions.
	Command context
	Any context
	Authority
	Administrators or local user group members with execution rights for this command.
	Parameters
	`<IF-NAME>`
	Name of the interface.
	`<IF-RANGE>`
	Port identifier range.
	`statistics`
	Clear counters for the interface.
	`global`
	Clear hardware counters for the interface for all sessions.
	Examples
	Clear counters for interface 1/1/1:
	`switch> clear interface 1/1/1 statistics`
	Globally clear hardware counters for interface 1/1/1:
	`switch> clear interface 1/1/1 statistics global`
	`Warning: clearing statistics globally will be reflected in`
	`all CLI sessions, any agents running in the analytics engine, and`
	`any external agents monitoring switch statistics.`
	
	`Continue (y/n)? y`

Table Continued

Category	Description
Firmware management	Added a warning message when the switch gets rebooted to a software version older than the currently running version: `The switch will be downgraded from version <current version> to <new version>. To avoid losing incompatible configurations, restore the latest system checkpoint matching <current version> before rebooting.`
OSPF	Added support for displaying the route tag in the output of the `show ip route <A.B.C.D/M>` command.

Version 10.05.0001

Table 1: *New features*

Category	Description
Breakout cable support	This feature adds support for split ports and cables. **NOTE:** Path MTU discovery is not supported with breakout cables.
DHCP Relay support for multi-VRF	This feature allows DHCP Relay to be enabled even if the DHCP Server is a different VRF. With this, you can have the DHCP Server in an EVPN underlay for Anycast gateway.
IP Explicit Congestion Notification (ECN)	In an environment where congestion management features are required, IP ECN can be configured on queues carrying delay-sensitive traffic. The desired result is that a network devices' port-queue utilization is actively managed, resulting in packets being CE marked when queue utilization reaches or exceeds a configured threshold. This feature enables storage use-cases in the Data Center.
LLDP over OOBM	This feature enables LLDP support over the Out-of-band management (OOBM) port.
RIPv2 and RIPng	Added support for RIP and RIPng routing protocols increasing the overall customer options for routing protocols.
Terminal monitor	This feature allows the user to enable debug on SSH sessions.

Table 2: *Enhancements*

Category	Description

Event Log	Improved the event log message when an uncontrolled reboot occurred, likely due to a power removal:
	`--------------------------------------------------`
	`Boot History`
	`--------------------------------------------------`
	`Index : 1`
	`Boot ID : 3e0b17427b684716a0963ddfbe9a6f38`
	`19 Jun 20 17:38:07 : Uncontrolled reboot, likely due to power removal.`
	`--------------------------------------------------`
	`Event logs`
	`--------------------------------------------------`
	`crash-tools[2938]: Event|1206|LOG_CRIT||Module rebooted. Reason : Uncontrolled reboot,`
	`likely due to power removal.,`
	`Boot-ID : 3e0b17427b684716a0963ddfbe9a6f38`

REST	Enabled the REST API to enforce integer constraints for MTU configuration.
UDP Forwarder	Added support for any value from 1 – 65535 when configuring the port number for the UDP forwarder.

Fixes

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

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

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

Version 10.05.0020

Category	Bug ID	Description
CLI	87625	**Symptom/Scenario:** When the `top cpu` command is executed multiple times, the `%Cpu(s)` value at the top of the output is invalid and does not change when the command is executed again. **Workaround:** Execute start-shell and run the `top` command from there.
Config Management	89149	**Symptom:** The switch fails certain configuration validations with NetEdit. **Scenario:** NetEdit fails to validate switch configurations applied to a VRF name that is not configured on the switch. **Workaround:** Configure the respective VRF name before adding any switch configuration for that VRF when using NetEdit.

Table Continued

Category	Bug ID	Description

DHCP Relay	88137	**Symptom:** Users fail to obtain an IP address from the DHCP server.
		Scenario: In a VSX setup, when the VSX secondary switch is rebooted and subsequently the VSX primary switch is also rebooted (for example, during an upgrade process), the DHCP Relay agent may stop processing DHCP packets.
		Workaround: Restart the hpe-relay process on each VSX switch from the switch's bash shell:
		`# start-shell ~$ sudo su`
		`# pkill -9 hpe-relay`
		`# exit~$ exit`

DHCP Snooping	89192	**Symptom:** The switch is flooded with DHCP packets. **Scenario:** When at least two access switches are configured with DHCP snooping and are connected to the same core/agg switch where a DHCP client and DHCP server are connected, if a client MAC is lost on the core/agg switch tables before a unicast DHCP reply arrives from the server to the switch, the switch may be flooded with DHCP packets.
Link Aggregation	89558	**Symptom/Scenario:** The switch returns an incorrect value "0" when querying `ifHighSpeed` OID for a LAG interface.
Mirroring	87295	**Symptom:** Port mirroring causes port flap. **Scenario:** When port mirroring is configured on a system with multiple LAGs and the source and destination mirror ports are LACP-enabled ports, port flap may be experienced on the interface. **Workaround:** Set the port mirror destination to a non-LACP-enabled interface.
Thermal Manager	90047	**Symptom:** The switch shuts down unexpectedly and stays down for five minutes. **Scenario:** Fans on the switch incorrectly report as faulted and if enough fans report faulted, the switch shuts down immediately and remains down for five minutes. After the switch is back up, the boot history shows the reboot reason as having insufficient fans.

Table Continued

Category	Bug ID	Description
User Authentication	84774	**Symptom:** Unable to log into the switch through the console or SSH, with an error message similar to `error: resolving name clearpass.reamed.us:49 Temporary failure in name resolution`. **Scenario:** If console and SSH access are configured to use remote authentication (RADIUS, TACACS) and the FQDN of the authentication server is used rather than the server IP address to authenticate, when the physical ethernet interface that connects to the authentication server is removed, the switch does not fail over to local authentication, causing an error message similar to `error: resolving name clearpass.reamed.us:49 Temporary failure in name resolution` to display. **Workaround:** Do one of the following: • Use the IP address of the authentication server rather than the FQDN. • Shut down the port connecting to the authentication server. • Remove remote user authentication from the switch config.
Web UI	90636	**Symptom:** The network_health script agent stops working. **Scenario:** In some circumstances, removing and re-adding the network_health script agent causes the script to stop working and become stuck in a state where removing and re-adding will not work. The event log reports this as an error inserting NAE data.

Version 10.05.0012

Category	Bug ID	Description
LAG	89558	**Symptom/Scenario:** The switch returns an incorrect value "0" when querying `ifHighSpeed` OID for a LAG interface

Version 10.05.0011

Category	Bug ID	Description
Certificates	89547	**Symptom:** REST calls remove expired certificates from the switch. **Scenario:** When a switch has an expired certificate installed in a TA profile, the expired certificate will be automatically removed when any configuration change is applied with REST calls or through NetEdit. **Workaround:** To keep the expired certificate in place, use the CLI to configure the switch, rather than REST or NetEdit. Note that the expired certificate is not used for any switch identification purposes.
Config Management	89149	**Symptom:** The switch fails VRF configuration validations with NetEdit. **Scenario:** NetEdit fails to validate configurations applied to a VRF name that is not configured on the switch. **Workaround:** Configure the respective VRF name before adding any switch configuration for that VRF when using NetEdit.

DHCP Relay	88137	**Symptom:** Users fail to obtain a DHCP IP address.
		Scenario: In a VSX setup, when the VSX secondary switch is rebooted and subsequently the VSX primary switch is also rebooted (for example, during a VSX upgrade process), the DHCP relay agent may stop processing DHCP packets.
		Workaround: Restart the `hpe-relay` process on each VSX switch from the switch shell:
		`# start-shell`
		`~$ sudo su`
		`# pkill -9 hpe-relay`
		`# exit`
		`~$ exit`

Supportability	81991	**Symptom:** Copying of support files fails. **Scenario:** When attempting to extract the switch support files using the `copy support-files` command, the copy may get stuck during execution and never finish. **Workaround:** Press Ctrl+C to interrupt and exit the CLI execution.

Version 10.05.0010

Category	Bug ID	Description
CDP	85476	**Symptom:** The switch incorrectly flags the severity level for event throttling messages. **Scenario:** When the switch is throttling the CDP event messages, it incorrectly flags the throttling event severity as an informational message instead of a debug message. **Workaround:** There is no functional impact; throttling events are expected to be debug level events.
CDP	86685	**Symptom:** The `no cdp` command does not show up in the output of the `show running-config interface` command. **Scenario:** After configuring the switch with the `no cdp` command, the configuration does not show up in the output of the `show running-config interface` command. **Workaround:** There is no functional impact; the `no cdp` command was successful. Use the `show cdp` or `show running-config` commands to see the CDP interface configuration.
Central	85934, 88033	**Symptom:** The REST process encounters periodic crashes that generate core dump files. **Scenario:** When the switch repeatedly fails to connect to the Aruba Central Platform because it is not provisioned for Aruba Central or there is no connectivity with Aruba Cloud or for any other reason, the REST process encounters random crashes which generate core dump files and automatic restarts of the process. **Workaround:** If the switch is not expected to be provisioned in Aruba Central, disable the Aruba Central service on the switch using the `aruba-central disable` command. Note that the Aruba Central service is enabled by default. You may also remove the recurrent core dump files using the `erase core-dump daemon hpe-restd` command.
Certificates	87093	**Symptom:** Validation of a current running-config fails in NetEdit with an error message that the TA certificate has expired. **Scenario:** When NetEdit is used to validate a configuration change to a copy of the current running-config which contains a TA certificate that has expired, the validation fails even if the config is not related to the TA certificate. **Workaround:** Remove the expired TA certificate from the switch.

Table Continued

Category	Bug ID	Description
Config management	87792, 88852	**Symptom:** The switch fails certain configuration validation via NetEdit. **Scenario:** NetEdit fails to validate certain switch configurations, such as RADIUS or TACACS+ server group configurations or VRF attach configurations. **Workaround:** Use the CLI to configure the switch, rather than using NetEdit.
Config management	88957	**Symptom:** The switch fails to download certain configuration files in CLI format or deploy some configurations from NetEdit. **Scenario:** When the configuration file contains a banner statement with empty lines, the switch fails to download the configuration file via TFTP in CLI format or to deploy the configuration from NetEdit. **Workaround:** Remove the empty lines from the banner statement.
Diagnostics	88046	**Symptom:** Memory usage on the switch unexpectedly increases. **Scenario:** If the `copy support-files all` command is executed and the CLI session is closed before the command completes execution, memory usage on the switch increases.
ERPS	77700	**Symptom:** The ERPS daemon crashes and ERPS status is set to `NULL`. **Scenario:** When configuring protected VLAN using a VLAN list with a string length greater than 100, the ERPS daemon crashes. **Workaround:** Reduce the VLAN list length when configuring protected VLAN.
Firmware management	87089	**Symptom:** Firmware upgrade fails with a message similar to `Firmware update failed due to timeout 300000 ms exceeded`. **Scenario:** When using the web UI to upgrade firmware over a slow WAN link or with bandwidth throttled links, the firmware upgrade fails with a message similar to `Firmware update failed due to timeout 300000 ms exceeded`. **Workaround:** Use the CLI to upgrade firmware.
LEDs	86646	**Symptom:** The locator LED is on or flashing. **Scenario:** After a reboot, even when the switch does not have an LED locator configuration set, the locator LED is on or flashing on the switch.
Multicast	86693	**Symptom:** A line card crashes. **Scenario:** Under rare circumstances where a collection of multicast support logs happen within milliseconds, the line card crashes.

Table Continued

Category	Bug ID	Description
OOBM	87381	**Symptom:** The management interface loses connectivity. **Scenario:** After a management module (MM) failover or redundancy switchover, connectivity to the new active MM is lost. **Workaround:** Log into the new standby MM and issue the `systemctl stop mgmt-intf.service` command from a shell prompt.
OSPF	85617	**Symptom:** The switch prefers an incorrect default route. **Scenario:** When the switch receives a default router advertised via OSPF, the switch might incorrectly prefer a default route learned from an iBGP peer. **Workaround:** Filter out the default route from the BGP peer.
PIM	85224	**Symptom:** The switch fails to refresh certain mroute entries. **Scenario:** If the switch receives a PIM packet with a TTL=1, the switch will remove the mroute entry, causing periodic flooding.
REST	86920	**Symptom:** Empty or obsolete counter values display for an interface. **Scenario:** Executing a GET REST API request to retrieve queue counters for an interface shows either empty or obsolete counter values. **Workaround:** Use the `show interface <IFNAME> queues` command to retrieve queue counters.
Routing	85109	**Symptom:** The switch fails to correctly blackhole certain routes. **Scenario:** When a /32 or /128 host route is configured for blackhole matches a route learned through OSPF, BGP, or any other routing protocol, the switch fails to correctly blackhole it.
TACACS	84277	**Symptom:** The switch fails to execute `show` commands to get remote data from the VSX peer switch using the `vsx-peer` option. **Scenario:** When the switch is configured for TACACS command authorization, the switch fails to execute `show` commands with the `vsx-peer` parameter. **Workaround:** Run the `show` command on each VSX member console.

Table Continued

Category	Bug ID	Description
VSX	85141	**Symptom:** Unable to access secondary VSX switch through some VLANs. **Scenario:** After a VSX upgrade of the primary VSX with spanning tree enabled, the VSX secondary may become inaccessible through some VLANs. **Workaround:** Reboot the VSX secondary switch.
Web UI	85773	**Symptom:** Users cannot log into the switch using the web UI or manage the switch using NetEdit. **Scenario:** In rare conditions, the switch may receive an incomplete response from Aruba Activate, causing the switch REST daemon to crash and preventing users from logging in with the web UI or using NetEdit to manage the switch. **Workaround:** Disable Aruba Central support on the switch with the `aruba-central disable` command.

Version 10.05.0001

Category	Bug ID	Description
BGP	75592	**Symptom/Scenario:** When `debug bgp all` is enabled, options to see the details of the capabilities of a neighbor switch are not available.
BGP	76807	**Symptom:** The BGP admin status shows UP, but the state is stuck in capacities-mismatch. **Scenario:** When the switch is connected to a checkpoint firewall and BGP is configured between the firewall and the switch, the BGP admin status shows UP but the BGP state is stuck in capacities-mismatch.
DHCP Relay	79620	**Symptom:** The switch stops relaying DHCPv6 packets. **Scenario:** When the DHCPv6 Relay Agent is removed from a VLAN or ports are removed from a VLAN with the DHCPv6 Relay Agent enabled, the switch stops processing DHCPv6 relay traffic for all other VLANs. **Workaround:** Disable and re-enable the DHCPv6 Relay Agent on the VLAN.
ERPS	77700	**Symptom:** The ERPS daemon crashes and the ERPS status is set to `NULL`. **Scenario:** When using a VLAN list with a string length greater than 100, if a protected VLAN is configured the ERPS daemon crashes. **Workaround:** Reduce the length of the VLAN list of the protected VLAN to less than 100.

Table Continued

Category	Bug ID	Description
L3 Addressing	12008	**Symptom/Scenario:** The switch does not send out RA Packets with lifetime=0 values before rebooting. **Workaround:** Do one of the following: **1.** Configure minimum values for lifetime and advertisement intervals. **2.** Have multiple gateway routers and enable IPv6 Neighbor Unreachability Detection (NUD) on hosts.
LLDP	82582	**Symptom:** The LLDP process crashes. **Scenario:** If multiple interfaces experience link-state transitions, the LLDP process crashes and restarts.
Multicast	81857	**Symptom:** MLD and IGMP snooping do not operate as expected. **Scenario:** When MLD snooping or IGMP snooping are enabled on one port or VLAN and MLD or IGMP are enabled on a different interface, incorrect behavior of MLD or IGMP packets on those interfaces are experienced.
NTP	75270	**Symptom:** The NTP primary server connection is lost. **Scenario:** When two NTP servers are configured with the same stratum values, a flap occurs causing a loss of connection. **Workaround:** When configuring NTP, use the `prefer` option for one of the NTP servers.
OSPF	35544	**Symptom:** OSPFv3 neighbor is not formed when the area type is changed on the fly. **Scenario:** In a scaled setup with a large number of interfaces, when the area type is changed from Normal to NSSA, the OSPFv3 Neighborship may get stalled in Exchange state. **Workaround:**Shut down the OSPF peering interface or stop the current traffic on this interface and then make the OSPF area changes.
OSPF/NetEdit	71167	**Symptom/Scenario:** Unable to validate/deploy a switch config using NetEdit if there is a route-map that matches a VLAN iterface. **Workaround:** Remove the VLAN interface matching from the route-map or use the CLI to configure the switch.
Physical Interfaces	43622	**Symptom:** All interfaces on a secondary peer switch go down. **Scenario:** In a VSX configuration where the ISL is split across multiple line cards on the primary switch, the ISL may get out of sync when one of the line cards is brought down, leading all interfaces on the secondary peer switch to go down.

Table Continued

Category	Bug ID	Description
PIM-SM	69837	**Symptom:** The switch experiences high CPU utilization, duplicate traffic and/or traffic loss. **Scenario:** When PIM-SM is enabled on VLAN interfaces and IGMP snooping is enabled on VLANs with a large number of IPv4 multicast groups, the switch may experience intermittent high CPU utilization, duplicate traffic, and/or traffic loss. **Workaround:** Remove and re-add the multicast entries.
REST	78484	**Symptom:** The switch generates a generic error code `500 (internal server error).` **Scenario:** When an invalid URI is provided as values for reference fields ("/") in a REST payload, the switch returns a generic fail error code `500 (internal server error)` instead of a more specific error. **Workaround:** Use a valid REST payload.
Spanning Tree	74670	**Symptom:** The switch experiences frequent spanning tree state changes. **Scenario:** When multiple virtual switches (VSF, VSX) participate in a spanning tree domain with multiple regions and a redundancy switchover from the primary/commander to the secondary/standby occurs, the switch experiences frequent spanning tree state changes (blocking-learning) for the non-root bridge.
VSX	51107	**Symptom:** The switch fails to remove active forwarding from a VLAN interface. **Scenario:** The active gateway and active forwarding features are mutually exclusive on VLAN interfaces. In some cases, when active forwarding was previously configured and enabled on a VLAN interface, then later VSX sync and active gateway are enabled, the active forwarding configuration cannot be removed from the interface. **Workaround:** Disable VSX sync on the primary switch, then remove the active forwarding configuration and re-enable VSX sync.

Issues and workarounds

The following are known open issues with this branch of the software.

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.

Version 10.05.0020

Category	Bug ID	Description
ARP	47466	**Symptom/Scenario:** The switch fails to apply ARP cache entry limit configured with the `arp cache-limit <LIMIT>` command.
ARP	87640	**Symptom:** The ARP neighbor is deleted and re-added every time the base reachable time expires. **Scenario:** In an environment with Cisco Gateway Load Balancing Protocol (GLBP) enabled, the ARP neighbor is deleted and re-added every time the base reachable time expires. **Workaround:** Configure static ARP to the master GLBP router.
BGP	37739	**Symptom:** When the switch uses route leaking and a BGP peer to learn the same route, the switch may incorrectly install the two routes as ECMP routes. **Scenario:** In a multi VRF environment, while performing mutual route leaking on the VRRP peers with BGP neighborship established in between and towards the upstream network, the switch installs both routes as ECMP instead of preferring the leaked route. **Workaround:** Use OSPF routing as the interconnect between VRRP peers instead of BGP.
DHCP	81179	**Symptom:** The switch does not correctly update sub-options 5 and 11 in DHCP option 82. **Scenario:** When configured with Active Gateway, the switch does not correctly update the Active Gateway IP address in sub-options 5 and 11 in the DHCP discover packet.
ICMP Redirect	86208	**Symptom:** The switch sends duplicate ICMP packets. **Scenario:** In a VSX topology with ICMP redirect enabled, the switch may incorrectly duplicate redirected ICMP packets. **Workaround:** Disable the ICMP redirect feature.
OSPF	08491	**Symptom/Scenario:** OSPFv2 and OSPFv3 do not support detailed LSA `show` commands. **Workaround:** Use the `diag` command, instead.

Table Continued

Category	Bug ID	Description
VRF	72044	**Symptom:** The switch fails to program routes for some VRFs. **Scenario:** When configuring multiple VRFs with names matching up to the first 31 characters, the switch fails to correctly program some route entries. **Workaround:** Configure VRF names with less than 31 characters.
VRRP	24910	**Symptom:** Unable to configure same IPv6 link local address as primary virtual IP address under different VRFs. **Scenario:** Unique virtual link local addresses have to be configured for all VRRP IPv6 instances irrespective of VRF. **Workaround:** Do not use the same virtual link local address across different VRFs.

Feature caveats

Feature	Description
Classifiers	Classifier policies, IPv6 and MAC ACLs are not supported on egress.
Classifiers	DSCP remarking is performed only on routed packets.
Classifiers	For Classifier policy modifications to be secure, HPE strongly encourages modifications be done as a two step process: Bring down the port and then modify.
Classifiers	IPv4 egress ACLs can be applied only to route-only ports.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	Downgrades not supported.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
Counters	Classifier Counters: Max number Classifier entries with count action: JL363A=32K, JL365A=32K, JL366A=16K.
Counters	Counters are shared between ACL and Layer 3 ports. The Max number of ACL entries with count action plus Layer 3 counters is: JL363A=24K, JL365A=24K, JL366A=8K. Enabling counters on a Layer 3 port consumes 6 ACL counter entries.
Counters	Layer 3 Route-only port counters are not enabled by default. Enabling them will remove them from the counter resources shared with ACLs.
DHCP Server, DHCP Relay, and DHCP Snooping	DHCP Relay and DHCP Snooping can co-exist on the same switch. DHCP Relay and DHCP Server cannot co-exist on the same switch. DHCP Snooping and DHCP Server cannot co-exist on the same switch. DHCP Snooping, DHCP Relay, and DHCP Server together cannot co-exist on the same switch.

Table Continued

Feature	Description
IGMP/PIM on Loopback and GRE interfaces	PIM and IGMP cannot be enabled on both Loopback and GRE interfaces. PIMv4 and PIMv6 can be enabled on a Loopback interface. PIM will not work on GRE tunnels and 6in6.
MVRP and VSX	MVRP is mutually exclusive with VSX.
Network Analytics Engine (NAE)	After management module failover, up to 5 minutes of alert history could be lost.
Network Analytics Engine (NAE)	Agents monitoring a resource that has column type enum with a list of strings (as opposed to a single string enum) is not supported.
Network Analytics Engine (NAE)	Network Analytics Engine (NAE) agents execute Command Line Interface (CLI) actions as 'admin' user, so they have permission to run any command by default. However, when the authentication, authorization and accounting (AAA) feature is enabled, the same restrictions applied to 'admin' will also apply to NAE agents. Keep that in mind when configuring the AAA service, e.g. TACACS+, and make sure to give admin user permission to run all commands needed by enabled agents. Otherwise, some CLI commands may be denied and their outputs won't be available. Actions other than CLI won't be affected and will execute normally. Also, NAE agents won't authenticate, thus the AAA service configuration must not block authorization for unauthenticated 'admin' user. ClearPass doesn't support such configuration, so it cannot be used as a TACACS+ server.
Network Analytics Engine (NAE)	The following tables are not supported for NAE scripts: OSPF_Route, OSPF_LSA, OSPF_Neighbor, BGP_Route.
RADIUS	Authorization by means of HPE VSAs not supported.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
REST	With the exception of ACLs and VLANs, REST APIs using POST/PUT/DELETE are not validated before performing the function. Therefore, to avoid unintended results or side effects, HPE recommends testing the API write action first.
RIP/RIPng	Redistribute RIP/RIPng is not supported in BGP/BGP+.
RIP/RIPng	RIP/RIPng metric configuration support is not available.
RPVST+ and MSTP	Spanning Tree can only run in MSTP or RPVST+ mode.
RPVST+ and MVRP	RPVST+ is mutually exclusive with MVRP.
sFlow and Mirroring	sFlow and port mirroring are mutually exclusive per port. A port cannot support both sFlow and mirroring at the same time.
UDLD	For a UDLD-enabled interface to not lose traffic during a failover operation, the result of multiplying 'interval' and 'retries' should be at least 8 seconds. The default values are 7000 ms (interval) x 4 (retries) = 28 seconds.
VRRP and Proxy ARP	VRRP is mutually exclusive with Proxy ARP on the same interface.

Upgrade information

Version 10.05.0020 uses ServiceOS GT.01.05.0004.

If the switch has RPVST enabled and the native VLAN ID configured for the trunk interface is not equal to 1 and this VLAN ID is also used as the management VLAN, after an upgrade from any 10.04.00*xx* version of software to 10.05.*xxxx* or 10.04.1*xxx*, the switch may not be accessible over the trunk interface.

To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where <*VLAN_ID*> is the native VLAN ID configured on the trunk interface.

If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

NOTE: 10.03 is the minimum required software version prior to upgrading to 10.05. If your device is using a version of software prior to 10.03, you must first upgrade to a version of 10.03 before upgrading to 10.05. Check release notes for the software version you will upgrade to for instructions on performing the upgrade to 10.03.

IMPORTANT: Do not interrupt power to the switch during this important update.

IMPORTANT: If the switch is configured with an entry in a Class or Access list that matches specifically on AH or ESP traffic, that policy or ACL is no longer permitted in 10.05.0001 and it will fail to apply. Remove such entries from the configuration prior to upgrading to 10.05.0001 or remove the respective entries from ACLs or Class that failed to apply after the upgrade to 10.05.0001.

IMPORTANT: If the switch is configured with IGMP or MLD snooping options such as "forward", "fastleave", "forced-fastleave", or "blocked" at the VLAN context, after upgrading to 10.05.0001 you will need to reconfigure these options for each interface from the interface configuration context.

Example config before 10.05.0001:

```
vlan 2
   ip igmp snooping forward 1/1/1
   ip igmp snooping blocked 1/1/2
   ip igmp snooping force-fastleave 1/1/3
   ip igmp snooping fastleave 1/1/4
```

Example config to be added after upgrade to 10.05.0001:

```
interface 1/1/1
    ip igmp snooping forward vlan 2
interface 1/1/2
    ip igmp snooping blocked van 2
interface 1/1/3
    ip igmp snooping forced-fastleave vlan 2
interface 1/1/4
    ip igmp snooping fastleave vlan 2
```

IMPORTANT: To restore a previous configuration when downgrading to a previous version of software, follow these steps:

1. Use the `show checkpoint list all` command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the `Image Version` column in the output of the command, for example, XL.10.04.3000).

   This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.

2. Copy the backup checkpoint into the startup-config.
3. Boot the switch to the target version (lower version), making sure to select `no` when prompted to save the current configuration.

NOTE: Some Network Analytics Engine (NAE) scripts may not function properly after an upgrade. HPE recommends deleting existing NAE scripts before an upgrade and then reinstalling the scripts after the upgrade. For more information, see the *Network Analytics Engine Guide*.

Performing the upgrade

1. Upon first time booting to XL.10.05.0020 the ServiceOS update will start. At the switch console port an output similar to following will be displayed:

```
switch# boot system primary
Default boot image set to primary.
Checking if the configuration needs to be saved...

Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.

Checking for updates needed to programmable devices...
Done checking for updates.

2 device(s) need to be updated during the boot process.
The estimated update time is 5 minute(s).
There may be multiple reboots during the update process.


This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.

 Jul 20 08:26:55 hpe-mgmtmd[3919]: RebootLibPh1: Reboot reason: Reboot requested by user

:
:

Press Esc for boot options
ServiceOS Information:
    Version:          GT.01.05.0003
    Build Date:       2019-10-08 11:47:31 PDT
    Build ID:         ServiceOS:GT.01.05.0003:aa9f6d11bfb6:201910081147
    SHA:              aa9f6d11bfb6de885f0b7f5ec936497ea6e8f7a0

Boot Profiles:

0. Service OS Console
1. Primary Software Image [XL.10.05.0001]
2. Secondary Software Image [XL.10.04.3000]
```

```
Select profile(primary):

2 device(s) need to be updated by the ServiceOS during the boot process.
The estimated update time by the ServiceOS is 5 minute(s).
There may be multiple reboots during the update process.


MODULE 'mc' DEVICE 'svos_primary' :
    Current version   : 'GT.01.05.0003'
    Write-protected   : NO
    Packaged version : 'GT.01.05.0004'
    Package name      : 'svos_internal'
    Image filename    : 'GT_01_05_0004.svos'
    Image timestamp   : 'Thu Jan 23 16:40:29 2020'
    Image size        : 25787867
    Version upgrade needed

Starting update...

Erasing   [**************************************] 100%  (579 KB/sec)
Verifying [**************************************] 100%  (3282 KB/sec)
Writing   [**************************************] 100%  (875 KB/sec)
Verifying [**************************************] 100%  (3282 KB/sec)


Update successful (102.7 seconds).

watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system
```

2. Multiple components will be updated and several reboots will be triggered during these updates. When all component updates are completed, the switch console port will arrive at the login prompt with a display similar to following:

```
 (C) Copyright 2017-2020 Hewlett Packard Enterprise Development LP

                      RESTRICTED RIGHTS LEGEND
 Confidential computer software. Valid license from Hewlett Packard Enterprise
 Development LP 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.

We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events
Please register your products now at: https://asp.arubanetworks.com


switch login:
```

IMPORTANT: Aruba recommends waiting until all upgrades have completed before making any configuration changes.

Chapter 2
Aruba 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.

The Aruba security policy can be found at **https://www.arubanetworks.com/en-au/support-services/sirt/**. Security bulletins can be found at **https://www.arubanetworks.com/en-au/support-services/security-bulletins/**.

Security Bulletin subscription service

You can sign up at **https://sirt.arubanetworks.com/mailman/listinfo/security-alerts_sirt.arubanetworks.com** to initiate a subscription to receive future Aruba Security Bulletin alerts via email.