AOS-CX 10.06.0140 Release Notes

8400 Switch Series

a Hewlett Packard Enterprise company

Published: August 2021
Edition: 1

Open Source Code

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
6280 America Center Drive
San Jose, CA 95002
USA

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.

Chapter 1
AOS-CX 10.06 Release Notes

Description

This release note covers software versions for the AOS-CX 10.06 branch of the software.

If you run the `show version` command on the switch, the version number will display XL.10.06.*xxxx*, where *xxxx* is the minor version number.

AOS-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 AOS-CX operating system includes additional software elements not available with traditional systems, including the features included in the Features section of this release note.

Version 10.06.0001 is the initial build of major version 10.06 software.

Product series supported by this software:

- Aruba 8400 Switch Series

Important Information

Aruba switches covered by this release note use eMMC or SSD storage. This is non-volatile memory for persistent storage of config, files, databases, scripts, and so forth. Aruba recommends updating to version 10.05.0060 or 10.06.0100 or later (including this release) to implement significant improvements to memory usage and prolong the life of the switch.

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

10.03 is the minimum required software version prior to upgrading to 10.06. 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 10.06. Check release notes for the software version you will upgrade to for instructions on performing the upgrade to 10.03.

If using the Web UI, you should clear the browser cache after upgrading to this version of software before logging into the switch using a Web UI session. This will ensure the Web UI session downloads the latest changes.

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00*xx* version of software to 10.06.*xxxx*.
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.

When upgrading from software versions before 10.05.0001, if the switch is configured with an entry in a class-map or an Access List that matches AH or ESP traffic, the policy will fail to apply, as these options are no longer permitted. Remove such entries from the configuration prior to upgrading to 10.06.0140 or remove the respective entries from ACLs or Class that failed to apply after the upgrade to 10.06.0140.

When upgrading from a version of software prior to version 10.05.0001, 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 this software version, 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 this software version:

```
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
```

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

1. Use the `show checkpoint` 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.10.06.0100).

   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.

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

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 Aruba, unless noted in the table.

Version number	Release date	Remarks
10.06.0140	2021-08-03	Released, fully supported, and posted on the web.

Version number	Release date	Remarks
10.06.0130	2021-06-10	Released, fully supported, and posted on the web.
10.06.0120	2021-04-29	Released, fully supported, and posted on the web.
10.06.0113	2021-04-16	Released, fully supported, and posted on the web.
10.06.0112	2021-03-25	Released, fully supported, and posted on the web.
10.06.0110	2021-03-17	Released, fully supported, and posted on the web.
10.06.0101	2021-03-01	Released, fully supported, and posted on the web.
10.06.0100	2021-02-16	Released, fully supported, and posted on the web.
10.06.0010	2020-12-15	Released, fully supported, and posted on the web.
10.06.0002	2020-12-03	Released, fully supported, and posted on the web.
10.06.0001	2020-11-10	Initial release of AOS-CX 10.06. 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)	10Version 12 is not supported

Internet Explorer is not supported.

Recommended versions of network management software for switches found in this release note:

Management software	Recommended version(s)
Airwave	8.2.13.0
NetEdit	2.0.12
Aruba CX Mobile App	2.4.6
Aruba Central	2.5.3 (supports only Template group)
Network Automation	10.10, 10.11, 10.20, 10.21, 10.30, 10.40
Network Node Manager	10.10, 10.20, 10.21, 10.30, 10.40
IMC	7.3 (E0705P12)

For more information, see the respective software manuals.

To upgrade software using NetEdit, make sure to upgrade to the above version of NetEdit first and then execute the switch software upgrade on devices discovered by this version of NetEdit.

Minimum Supported Software Versions

If your product is not listed in the below table, it runs on all versions of software.

Product number	Product name	Minimum software version
JL366A	Aruba 8400X 6-port 40GbE/100GbE QSFP28 Advanced Module	10.00.0006
JL687A*	Aruba 8400X-32Y 32p 1/10/25G SFP/SFP+/SFP28 Module	10.04.2000

*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:

- TAA transceivers for 1G and 10G added

Refer to the *Transceiver Guide* for complete details on all supported transceivers.

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.

The number in the Category column is used for tracking purposes.

Version 10.06.0140

Category	Description
Show Tech 171820	Added the `all` parameter to the `show system resource-utilization` command to be able to display both commander and member information for all switches in a VSF stack.

Version 10.06.0130

Category	Description
REST 164024	Provided more information and examples about how to use the selector `writable` in the REST API (versions 10.04 and later) GET and PUT verbs.

Version 10.06.0120

Category	Description
Object Groups	Added support for up to 2000 object groups.

Version 10.06.0113

No enhancements were included in version 10.06.0113.

Version 10.06.0112

No enhancements were included in version 10.06.0112.

Version 10.06.0110

No enhancements were included in version 10.06.0110.

Version 10.06.0101

No enhancements were included in version 10.06.0101.

Version 10.06.0100

Category	Description
BGP	Added the new command `redistribute local loopback` to allow redistribution of /32 (IPv4) and /128 (IPv6) addresses by BGP.
Multicast	Added support for IPv4 multicast over VXLAN.

Category	Description
NTP	To prevent drift between the system clock and the real-time clock when NTP is enabled, the switch now performs a clock sync every eight minutes.
SNMP	Added additional LAG attributes in order to facilitate a richer NMS experience from tools such as Airwave.

Version 10.06.0010

Category	Description
SNMP	Added support for the `hh3cifVLANType`, `dot3StatsDuplexStatus`, and `dot3StatsTable` OIDs.

Version 10.06.0002

Cat-egory	Description
Event Log	Added an event message to the switch event log when a duplicate IP address is detected from ARP Reply or Neighbor Advertisement packets for one or more neighbors. Example: Event Log:ndmd[407]: Event|6131|LOG_ERR|AMM|1/1|Duplicate IPv4 address 1.1.1.2 is detected on port 1/1/1 with a MAC address of 02:00:00:00:00:02Error Log:ndmd|LOG_ERR|AMM|-|NDM|NDM_NBRTABLE|[nd_nbr_mgr_process_arp_rcv_reply_event (636)] Duplicate IPv4 address 1.1.1.2 is detected on port 1/1/1 with a MAC address of 02:00:00:00:00:02

Version 10.06.0001

Category	Description
Core	■ Added Route Map Continue capability to route maps allowing for further flexibility. See the *IP Routing Guide* for more information. ■ BGP enhancements include support for the advertisement of multiple paths (ADD-PATH capability), confederations, and outbound route filtering (ORF). See the *IP Routing Guide* for more information. ■ Enabled BFD support for BGP6 neighbor sessions, allowing for faster failover on non-directly connected neighbors. See the *IP Routing Guide* for more information. ■ OSPF enhancements to enable the display of ABR and ASBR status. See the *IP Routing Guide* for more information.

Category	Description
Enrollment over Secure Transport (EST)	Adds the capability for enabling secure certificate enrollment, allowing for easier enterprise management of PKI. See the *Security Guide* for more information.
EVPN and VXLAN	▪ VXLAN support for use in Data Center environments. See the *VXLAN Guide* for more information. ▪ EVPN MAC dampening provides a protection mechanism against endless MAC moves. See the *VXLAN Guide* for more information. ▪ IPv6 VXLAN/EVPN overlay support enables IPv6 traffic over the VXLAN overlay. See the *VXLAN Guide* for more information.
NAE	Added a graph showing average consumption for each daemon.

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 Bug ID is used for tracking purposes.

Version 10.06.0140

Category	Bug ID	Description
ACLs	167355	**Symptom:** The switch experiences a `vtysh` daemon core dump. **Scenario:** When a user logs into the console of the management module, a `vtysh` daemon core dump occurs. **Workaround:** Use SSH to log into the management module.
BGP	176058	**Symptom:** The `bgp fast-external-fallover` command will not work for a peer if it is attached to a peer group. **Scenario:** With BGPpeer group configurations that include fast-external-fallover, a link flap/toggle event will not clear the BGP peering state nor existing routes, causing the `bgp fast-external-fallover` command to fail. **Workaround:** Remove the peer from the peer grouping and have the required configuration applied independently.
IGMP	162792	**Symptom:** In a multicast environment, an increasing number of `Drops Tx` are seen on the interfaces of an access switch, which is connected to an 8400 core. **Scenario:** When a spanning tree topology change notification is received in a VLAN, the MAC table is flushed and multicast traffic is flooded to the VLAN for ~3 seconds.

Category	Bug ID	Description
L3 Addressing	173170	**Symptom:** IPv6 RA packets are sent with the autonomous address-configuration flag set incorrectly. **Scenario:** When an interface is configured with a default prefix using the `ipv6 nd prefix` command, IPv6 RA packets are sent with the autonomous flag set. **Workaround:** Configure each prefix explicitly.
L3 Routes	174260	**Symptom:** New L3 resources cannot be programmed in the hardware. **Scenario:** In a large scale environment, all hardware resources can be used, causing new L3 resources (such as, L3 destination, L3 group, neighbors, and routes) to not be programmable. **Workaround:** Use the `show capacities-status l3-resources` command to check L3 capacities, then reduced scale until below capacity.
MSTP	187026	**Symptom:** A line card module is down unexpectedly. **Scenario:** When a spanning tree group MSTP instance is configured and the line card containing the interfaces in the VLAN of the spanning tree instance is hot swapped, the line module will remain down after reinserting it in the chassis.
SNMP	186663	**Symptom/Scenario:** SNMPWalk or SNMPGet fail intermittently and the `hpe-snmpd` daemon keeps restarting. **Workaround:** Increase the SNMPWalk and/or SNMPGet timeout.

Version 10.06.0130

Category	Bug ID	Description
Boot Process	169690	**Symptom:** Firmware update from Central fails. **Scenario:** When the network has a high latency WAN connection to the Internet, firmware updates from Central may fail. with an event log entry of `Event|4403|LOG_ERR|UKWN|1|User admin: primary image update failed via HTTP from h30326.www3.hpe.com`. **Workaround:** Download firmware manually from the web and update the switch through TFTP, SFTP, USB, or local HTTP.
Multicast	169703	**Symptom:** Requested multicast streams never reach the clients. **Scenario:** When adding multicast routes with unicast group IP addresses, programming route entry into hardware fails while still reserving hardware resources. Over time, the incorrectly programmed hardware resources become exhausted, eventually causing multicast traffic to drop for valid streams. **Workaround:** Performing a redundancy switchover on the device will free the hardware resources and recover multicast traffic.
PIM-SM	166773	**Symptom:** The VSX software upgrade becomes stuck for a long time. **Scenario:** When a software upgrade is initiated on the VSX secondary, the multicast daemon (PIM) transitions all the traffic forwarding role to the VSX primary. During this process the VSX software upgrade becomes stuck for a long time. **Workaround:** Manually upgrade the software or re-initiate the VSX software upgrade process.

Category	Bug ID	Description
RADsec	165479	**Symptom:** SSH authentication fails. **Scenario:** When trying to log into the switch using SSH, if the authentication server is using RADsec and the server is unreachable, the SSHD daemon restarts and SSH authentication fails.
REST	162640	**Symptom/Scenario:** REST timeouts when doing a GET operation to the Interfaces collection using REST v10.04 API.
REST	164324	**Symptom:** REST request fails for firmware update with the REST swagger UI with authenticated TACACS user with privilege level 15. **Scenario:** When logged into the switch WebUI with a TACACS user (privilege 15), executing a PUT request to update the firmware version fails with following error: `Error executing cmd: exit status 1.` **Workaround:** Use admin credentials (or any other administrator user with privilege 15) to perform this request without any issues.
Slot Management	162649	**Symptom/Scenario:** Performing a REST GET operation to retrieve system/interfaces with the `selector = configuration` category results in a list of interfaces that have not been configured.
VSX-Sync	165068	**Symptom:** CPU usage for the VSX-sync daemon is high for more than five minutes. **Scenario:** In a VSX diamond topology with multiple features in sync, if the DHCP server feature sync is enabled, the CPU experiences higher than normal usage for more than five minutes. **Workaround:** Disable and re-enable VSX synchronization from the VSX configuration context using the `no vsx-sync` and `vsx-sync` commands.
VSX	169707	**Symptom:** Traffic ingress MCLAG not redirected properly after MM failover. **Scenario:** In a VSX configuration with MCLAG where one peer has no MCLAG configured, a dump MCLAG, or MCLAG in a down state, some traffic is redirected over the ISL to reach the next hop device through the VSX peer. If a failover event occurs from software upgrade or due to an HA event, the redirect traffic flow can sometimes be missing after failover due to a timing issue. **Workaround:** Reconfigure the MCLAG to trigger the redirect programming again. Since the MCLAG is not affecting traffic, reconfiguration is safe to perform.

Version 10.06.0120

Category	Bug ID	Description
ARP	162712	**Symptom/Scenario:** During switch bring up or after a switch reboot, a `Resource temporarily unavailable` error log message is flooded. **Workaround:** There is no functional impact, just the error message is logged.
BGP	160803	**Symptom:** BGP connection is stuck in connect state rather than

Category	Bug ID	Description
		established. **Scenario:** When the switch configuration includes a BGP neighbor with an MD5 password and the system is booted through Service OS, the BGP connection is stuck in connect state rather than established and on the remote peer, error logs will be created for a missing MD5 authentication for the incoming TCP connection. **Workaround:** Remove the `neighbor <> password <>` configuration and reconfigure it.
Config	157945	**Symptom:** Output of the `show startup-config json` command incorrectly includes information from the `show checkpoint list` command. **Scenario:** When multiple checkpoints exist, executing the `show startup-config json` command will incorrectly include information from the `show checkpoint list` command. **Workaround:** Use the Web UI to check the startup-config and checkpoints.
Diagnostics	159410	**Symptom:** Traceback or warning messages related to iotop utility are observed. **Scenario:** When executing the `copy support-files [all]` command, through an SSH connection or with different namespaces than the default, such as ntb or swns, traceback or warning messages related to the iotop utility are seen. This does not affect the functionality of the command. **Workaround:** Execute the `copy support-files [all]` in the default namespace. Note that this warning message does not affect the copy support-files functionality, so it can be ignored.
EVPN	152859	**Symptom:** The EVPN MAC address on a remote VTEP gets overwritten unexpectedly. **Scenario:** When a host MAC address is configured as a system/AG/static MAC and a sticky bit is not set, the corresponding EVPN MAC address on a remote VTEP gets overwritten when the same MAC address as the local is received. **Workaround:** Do not configure the host with a system/AG/static MAC address.
IP Neighbor Flood	163776	**Symptom:** The switch reboots unexpectedly. **Scenario:** If the switch has a static or dynamic route that uses an interface-VLAN connected port to get to the next hop and the IP Neighbor Flood feature configured, when the physical port where the neighbor is learned goes down or when the `clear mac-address` command on that VLAN is executed, a switch reboot will occur due to a switchd crash. **Workaround:** Unconfigure the IP Neighbor Flood feature on the interface-VLAN or have a route's nexthop over a pure L3 connection (rather than over an L2 connection).
Loop Protect	151772	**Symptom:** Loop protect blocks ports improperly. **Scenario:** In a square topology, after rebooting the VSX peers or toggling the ISL link, a loop is incorrectly detected by the loop protect feature, resulting in ports getting blocked improperly even though the network topology has not changed. **Workaround:** Disable loop protect temporarily and ensure all VSX peers are in a stable Established state, the re-enable loop protect. Alternatively, configure the loop-protect re-enable-timer with the

Category	Bug ID	Description
		minimum value so that the links can come back up.
MAC	159697	**Symptom/Scenario:** Traffic drops to certain hosts whose MAC addresses are still learned on a downed port until the MAC addresses age out or are manually cleared on that port. **Workaround:** The issue cannot be avoided, however, after getting into this problem state, use the `clear mac port` command to clear all the MAC addresses learned on the downed port, or, if there is no other traffic from the MAC address, wait until the MAC ages out to recover.
Multicast	159654	**Symptom:** Multicast flow programming is slow and causes delays when switching between multicast streams. **Scenario:** When the number of multicast routes is high, and IGMP joins/leave packet processing occurs at a very rapid interval, CPU usage for the `hpe-repld` daemon consumes more than 80% of the system resources. As a result, multicast flow programming can be slow and cause delays when switching between multicast streams. **Workaround:** Reduce multicast scale.
OSPF	162332	**Symptom:** OSPF neighborship do not form on point-to-point networks and virtual links. **Scenario:** When different network masks are configured on either side of point-to-point networks or virtual links, OSPF neighborship is not formed. **Workaround:** Use the same network mask on both sides of the point-to-point or virtual links.
PIM-SM	161951	**Symptom:** Certain PIM commands (like `show ip pim rp-candidate` and `show ip pim bsr`) cause a core dump. **Scenario:** When an interface is configured as the PIM RP-candidate or BSR and the IP address is removed from the interface, executing certain PIM commands causes a core dump. **Workaround:** Ensure the IP address on the RP-candidate/BSR interface is not removed after PIM parameters are configured.
RADIUS	161529, 161960	**Symptom:** The switch experiences intermittent login failures. **Scenario:** When remote authentication is configured for a RADIUS server with FQDN, the user may experience intermittent login failures when attempting to access the switch through REST or the WebUI. **Workaround:** Configure the RADIUS server with an IP address.
RADIUS	161502	**Symptom:** RADIUS server performance is impacted by a flood of RADIUS traffic. **Scenario:** When an IP source interface is configured on the RADIUS server and the RADIUS server is reachable through multiple interfaces, the server is flooded by RADIUS requests, impacting the server's performance negatively.
SNMP	155468	**Symptom:** Heartbeat failures are experienced on stack members. **Scenario:** When the SNMP type is configured as both TRAP and INFORMS and the system is rebooted to change the status of members, heartbeat failures are seen on members of the stack. **Workaround:** Disable the INFORMS configuration.

Category	Bug ID	Description
Spanning Tree	161244	**Symptom:** A PVST convergence failure is seen between PVST instances. **Scenario:** When the port VLAN mode is changed from access to trunk mode, a PVST convergence failure is seen between PVST instances. **Workaround:** Enable the PVST instance for VLAN 1.
UDLD	164668	**Symptom:** LAG member interfaces unexpectedly go into an `err-disabled` state. **Scenario:** When a LAG is configured on the switch and a LAG is configured on a peer Cisco switch, both with UDLD in RFC 5171 aggressive mode, the LAG member interfaces to into an `err-disabled` state. **Workaround:** Disable UDLD on the blocked interfaces to avoid losing traffic.
VLAN	160299	**Symptom:** VLAN configurations on the ISL interface are reset to the default `vlan trunk native 1 tag`. **Scenario:** When the ISL interface is configured with a native VLAN other than the default `vlan trunk native 1 tag`, upon rebooting the device, the VLAN configuration on the ISL interface will be reverted to the default. **Workaround:** Manually override the default config.
VRRP	157551, 162611	**Symptom:** Both VRRP peers appear as Master. **Scenario:** When an AOS-CX switch is paired with a third-party switch or router as a VRRPv3 peer with an IPv4 address family, both peers appear as `Master`. **Workaround:** Use VRRPv2 for the IPv4 address family.
VSX-Sync	161921	**Symptom/Scenario:** With vsx-sync configured, a configuration sync from the primary VSX switch to the secondary VSX switch fails. **Workaround:** Restart the VSX daemon or reboot the secondary switch.
VSX	157884	**Symptom:** Network connectivity issues are experienced for hosts resolved through a VSX peer that has an L2 firewall connected. **Scenario:** In a VSX environment, when an L2 active firewall is connected to only one of the VSX peers and a new VLAN is added or an ARP clear is performed, traffic is not forwarded corectly. **Workaround:** Configure a static MAC address for the VSX peer system to the L2 Firewall port instead of the ISL. This only applies if the L2 Firewall does not have an Active/Standby deployment.
Web UI	152994	**Symptom/Scenario:** In a scaled configuration, the Web UI does not display any data for resources such as interfaces, VLANs, and LAGs after a JSON config has been applied. **Workaround:** Execute the `https-server session close all` command.
Web UI	163746	**Symptom:** In the Web UI, the port speed value changes unexpectedly from `auto negotiation` to 100mpbs. **Scenario:** When using the Web UI to edit interface options, if the port speed is set to the default of `auto negotiation`, any other edits causes the port speed to change to 100mpbs. **Workaround:** Use the command line to make changes to the interface.

Version 10.06.0113

Category	Bug ID	Description
ARP	162646	**Symptom:** The neighbor is learned with the wrong MAC address and physical port from the DAD ARP probe. **Scenario:** When ARP suppression is enabled and an ARP request with sender protocol address of 0.0.0.0 is received, it is learned with the wrong MAC address and physical port which may lead to a traffic backhole until the actual host which owns the IP address sends the GRAT ARP. **Workaround:** Clear ARP.
VSX	160299	**Symptom:** VLAN configurations on the ISL interface are reset to the default `vlan trunk native 1 tag`. **Scenario:** When the ISL interface is configured with a native VLAN other than the default `vlan trunk native 1 tag`, upon rebooting the device, the VLAN configuration on the ISL interface will be reverted to the default. **Workaround:** Manually override the default config.

Version 10.06.0112

Category	Bug ID	Description
Multicast	159654	**Symptom:** Multicast flow programming is slow and causes delays when switching between multicast streams. **Scenario:** When the number of multicast routes is high, and IGMP joins/leave packet processing occurs at a very rapid interval, CPU usage for the `hpe-repld` daemon consumes more than 80% of the system resources. As a result, multicast flow programming can be slow and cause delays when switching between multicast streams. **Workaround:** Reduce multicast scale.

Version 10.06.0110

Category	Bug ID	Description
BFD	154627	**Symptom:** The `show resources` command shows that some of the configured features have not been able to get resources. **Scenario:** When BFD has been configured and at least two other features that use TCAM lookups at the same time (for example, VSX, egress routed IPv4 unicast counters, and ingress port MAC ACL), the `show resources` command shows that some of the configured features have not been able to get resources. **Workaround:** Remove BFD, disable echo functionality with the `bfd echo disabled` command, or limit the number of other features requiring TCAM lookups.
CDP	155876	**Symptom:** The switch experiences an increase in memory utilization, slowing the performance of the system over a period of days. **Scenario:** When a large number of CDP neighbors are connected, there is a potential memory leak that occurs when packets from

Category	Bug ID	Description
		each neighbor reach the switch during the same time interval, or when a large number of CDP reply messages need to be sent on each interface for each connected neighbor. This memory leak could grow over a period of time as the CDP Rx packet count increases. **Workaround:** Restart the `cdpd` process to recover the leaked memory.
DHCP Relay	149237	**Symptom:** DHCP clients are not assigned IP addresses. **Scenario:** When an IVRL is set up without configuring the source interface in an inter-VRF scenario where the DHCP relay and server are on different VRFs and reachable through an IVRL route, DHCP clients do not get IP addresses. **Workaround:** Configure the source interface.
IP-SLA	154180	**Symptom:** Unable to configure IP-SLA addresses with .0 or .255 as the last octet. **Scenario:** When configuring the SLA type's source and destination IP addresses, an attempt to configure the addresses with .0 or .255 as the last octet will fail.
LACP	155575	**Symptom:** LAG port(s) remain in an `out-of-sync` state following a LAG port flap event. **Scenario:** When the peer device is configured with a non-default port priority other than 1 and non-default system priority other than 65534, and one of the LAG ports bounces, if the peer device takes more than 3 seconds to send the first PDU packet after the link comes back up, the LAG on the primary device will remain out-of-sync. This is unlikely to happen when physical links are tightly coupled with LACP. **Workaround:** Reset the LAG by disabling and re-enabling it.
PIM XL	154086	**Symptom:** The Mroute entry is not removed after the interface is pruned from PIM, causing unwanted network flow. **Scenario:** The PIM router adds and immediately prunes a downstream interface without removing the interface from the Mroute, causing unwanted network flow. **Workaround:** Stop and restart the traffic, or disable and re-enable PIM.
PoE	151840	**Symptom:** The powered device (PD) is denied power and reboots. **Scenario:** When the PD attempts to draw more power than the IEEE 802.3 standard for the requested class advertised by the PD, the PD is denied power and reboots. For instance, a class-0 PD attempting to draw more than 15.4W will hit the power policing threshold of the switch, resulting in an over-current fault, which will deny power to the PD and cause it to reboot. **Workaround:** Enable `pd-class-override` on the interface connected to the PD and configure the `User set Assigned class` to reflect the higher class power required. **This configuration is made available to provide higher power to non-IEEE 802.3 compliant PDs at the user's own risk and caution should be exercised.**
SNMP	155880	**Symptom:** The switch experiences high CPU utilization and a restart of the OVSDB IDL daemon. **Scenario:** When the switch receives frequent SNMP requests, it

Category	Bug ID	Description
		will experience a high CPU utilization and the OVSDB IDL daemon will restart. **Workaround:** Restart the SNMP process.
SSH Server	153325	**Symptom/Scenario:** Switch generates a 2048-bit RSA SSH host key when attempting to generate a 4096-bit host key. **Workaround:** Use the `ssh-keygen` command in the Linux shell (using the `start-shell` command) to generate a 4096-bit RSA SSH host key.
VSX	153141	**Symptom:** The HPE-Relay daemon on the primary switch in a VSX pair crashes every two to three minutes, flooding the logs with the following event message: `Message Event|1201|LOG_CRIT|AMM|-|hpe-relay crashed due to signal:11 - Severity Critical (Priority: 2) - Syslog ID systemd-coredump`. **Scenario:** When DHCP traffic is running as expected through the primary VSX switch and then the secondary switch is rebooted, the HPE-Relay daemon on the primary switch in a VSX pair crashes every two to three minutes, flooding the logs with the following event message: `Message Event|1201|LOG_CRIT|AMM|-|hpe-relay crashed due to signal:11 - Severity Critical (Priority: 2) - Syslog ID systemd-coredump`. **Workaround:** Pause DHCP traffic before rebooting the secondary switch, then resume the traffic once the secondary switch is back in sync with the primary.
VSX	148521, 149288, 151440, 151543, 154798	**Symptom:** VSX status goes into a non-operational state and configuration-sync does not work. **Scenario:** When a new configuration that is expected to be synced to the secondary VSX device (for example, one with static routes or VLANs) is added, the VSX pair may unexpectedly fail to update the secondary member's configuration, causing VSX to go into non-operational status and blocking configuration sync. **Workaround:** Reboot the secondary VSX member, or disable and re-enable VSX-sync on the secondary VSX device.

Version 10.06.0101

Category	Bug ID	Description
Central	157054	**Symptom/Scenario:** The switch goes offline in Central after a Central cluster upgrade. **Workaround:** Switch functionality and data flow is not affected. Restart the REST daemon with the `https-server session close all` command. **NOTE:** With this fix, if RESTd is restarted due to a disconnect from Central a core dump will be reported. This is expected behavior.

Version 10.06.0100

Category	Bug ID	Description
Airwave	95929	**Symptom:** In Airwave, the usage and description fields for LAG interfaces are empty if a description gets added to the interface. **Scenario:** If a LAG interface contains a description, and if Airwave polls the switch, the description and usage details for the interface are empty.
BFD	149136	**Symptom:** BFD sessions remain even after BFD is globally disabled. **Scenario:** When BFD gets globally disabled using the `bfd disable` command and the subscriber settings are subsequently removed, the BFD sessions are still present. **Workaround:** Remove subscriber configurations while BFD is still enabled, then disable BFD.
CDP	149252	**Symptom/Scenario:** An unexpected CDP core dump is found in the output of the `show core-dump` command.
Central	95378	**Symptom:** A switch software upgrade from Central fails. **Scenario:** Where there is a delay in DNS resolution during the software upgrade process initiated from Aruba Central, the switch fails to download the new version and complete the upgrade. **Workaround:** Add a configuration entry to the switch configuration template in Aruba Central for the HPE file server `ip dns host h30326.www3.hpe.com 23.197.193.219`, then re-initiate the new software upgrade from Aruba Central.
Counters	94803	**Symptom:** Drop counters get incremented incorrectly. **Scenario:** When a client is moved from one port to another or when the client sends an unsolicited NA, the `prefix mismatch` drop counter gets incremented incorrectly. When a prefix has been configured and sends NA with a non-matching prefix, the `NA packets failed ND snooping validation checks` drop counter gets incremented incorrectly.
DHCP Snooping	151555	**Symptom/Scenario:** DHCP clients do not receive an IP address from the DHCP server and the switch experiences high CPU utilization from the IPSAVD daemon.
IGMP Snooping	70340	**Symptom:** The output from the `show ip igmp snooping` command does not display in the output of the `show tech` command. **Scenario:** IGMP snooping group information is not present in the output of the `show tech` command.
IP Address	149740	**Symptom/Scenario:** IP addresses in the form *x.y.z*.255/31 cannot be configured on the switch.
MSDP	93106	**Symptom:** MSDP SA-message filtering is not working as expected when an ACL containing object groups is used as a match parameter. **Scenario:** When an ACL has been created with ACEs with match parameters as the object-group, if the ACL is configured to filter the SA-cache, MDSP SA-message filtering does not work as expected. **Workaround:** Use IP addresses as match parameter in the ACL instead of object groups.

Category	Bug ID	Description
Multicast	95279	**Symptom:** The PIM-SM Rendezvous Point (RP) drops Register messages from PIM Designated Routers (DRs). **Scenario:** When the source router sends register packets to the active gateway MAC of the interface, the MAC self check fails and the packets are dropped. **Workaround:** On the upstream router, configure the nexthop IP to reach the RP as one of the interface IPs of the RP router instead of the active gateway IP.
SNMP	95114	**Symptom:** SNMP restarts every 15 minutes and the event log displays SNMP startup events. **Scenario:** When the SNMP server community string is configured with special characters, SNMP restarts every 15 minutes. **Workaround:** Configure the community string with special characters in single quotes.
SNMP	94223	**Symptom:** SNMP restarts every 15 minutes and the event log displays SNMP startup events. **Scenario:** When the SNMP server agent is configured with a port other than the default, SNMP restarts every 15 minutes and the event log displays SNMP startup events.
SNMP	153440	**Symptom/Scenario:** The SNMP walk output of OID BRIDGE-MIB::dot1dTpFdbAddress returns fewer MAC addresses than the `show mac-address-table` command. **Workaround:** Unconfigure and reconfigure the SNMP server.
TFTP	150150	**Symptom:** Copy operation fails with the error `curl: (28) TFTP response timeout`. **Scenario:** When attempting to copy a configuration checkpoint to a TFTP server using the blocksize option, the copy fails with the error `curl: (28) TFTP response timeout`.
VLAN	92950	**Symptom:** Pinging the active gateway IP address succeeds even after shutting down the VLAN interface on which the active gateway is configured. **Scenario:** When an active gateway IP address is configured on a virtual interface and the virtual interface is shut down, a ping to the active gateway from the same switch succeeds.
VSX	91601	**Symptom:** VSX keepalive stays in an `INIT` state after a checkpoint restore. **Scenario:** When changing the VRF assignment on a VSX keepalive interface using a checkpoint restore, VSX fails to detect the peer status, reporting the keepalive state stuck at `INIT`.
VSX	92243	**Symptom:** VSX state changes to non-operational and configuration sync stops working. **Scenario:** When adding any new configuration that is expected to be synced to the VSX secondary, the VSX pair may unexpectedly fail to upgrade the secondary member's configuration, causing the VSX status to go into a non-operational state and configuration sync stops working: switch# **show vsx status config-sync** Admin State : Enabled Operational State : Non-Operational Error State : Configuration Sync is disabled

Category	Bug ID	Description
VXLAN	88591	**Symptom:** VLAN interfaces that are enabled as part of VXLAN tunnels but are not part of VSX MCLAGs go down as `Disabled by VSX`. **Scenario:** When one of the switches in a VSX pair is rebooted or the ISL is flapped, causing traffic loss for the flows using an interface VLAN, the VLAN's interfaces which are enabled as VXLAN tunnels but are not part of the VSX MCLAGs go down as `Disabled by VSX`.
VXLAN	94566	**Symptom:** The switch experiences unexpected VXLAN traffic loss for a few seconds. **Scenario:** When a new configuration is applied using NetEdit or a checkpoint rollback, unexpected VXLAN traffic loss is experienced for a few seconds, even if the new configuration is the same as the configuration the switch was running previously. **Workaround:** Use the CLI to make configuration changes.

Version 10.06.0010

Category	Bug ID	Description
Central	94012	**Symptom:** The switch fails to re-establish a new connection with Aruba Central. **Scenario:** When there is a timeout in the TCP connection to Aruba Central due to WAN link issues, the switch fails to reconnect to Aruba Central. **Workaround:** Clear all existing REST sessions using the `https-server session close` all command.
NetEdit	93906	**Symptom/Scenario:** CoPP policies that exist in the running config are not retained when editing/updating/pushing a config using NetEdit. **Workaround:** Use the switch CLI instead of NetEdit when editing a running config that has a CoPP policy.
OSPF	94016	**Symptom:** OSPF experiences neighbor loss for 60 - 90 seconds. **Scenario:** Following a redundancy switchover, OSPF experiences a neighbor loss for 60 - 90 seconds, then recovers.
PBR	93218	**Symptom/Scenario:** Policy-based routing does not work when the next hop is on the VXLAN tunnel.
Physical Interfaces	90228, 91975, 93589	**Symptom:** A LAG member port intermittently goes down for less than one second and comes right back up, causing the LAG state to change and traffic to be interrupted. **Scenario:** When traffic has been flowing through the port (JL363A, ports 25 - 32; JL365A ports 7 and 8) for a long period of time, a LAG member port may intermittently go down for less than one second and come back up immediately, causing the LAG state to change and traffic to be interrupted.
Spanning Tree	94199	**Symptom:** An unexpected spanning tree topology change is displayed. **Scenario:** When pushing any configuration changes through NetEdit onto a switch that has PVST enabled on a LAG port with default port priority, an STP topology change occurs.

Category	Bug ID	Description
VRF	91612	**Symptom:** An error message similar to `00001|nl_utils|ERR|Unable to set namespace VRF_10 in the thread, error 22 Internal error, vrf not found.` is displayed. **Scenario:** When multiple features, such as RADIUS or ping, access a name space or one feature accesses a name space multiple times, an error message similar to `00001|nl_utils|ERR|Unable to set namespace VRF_10 in the thread, error 22 Internal error, vrf not found.` is displayed.
VSX	92243	**Symptom:** The VSX status is seen as non-operational and configuration sync does not work. **Scenario:** When adding any new configuration that is expected to be synced to the VSX secondary, the VSX pair may unexpectedly fail to upgrade the secondary member's configuration, causing the VSX status to change to non-operational and configuration sync to stop working. **Workaround:** Reboot the secondary VSX member.

Version 10.06.0002

Category	Bug ID	Description
DHCP Server	93746	**Symptom:** The switch CPU is elevated and the output of the `top` command shows a DHCP process consuming 100% of the CPU. **Scenario:** If VSX is enabled with empty content and the DHCP server is configured on the switch, the DHCP server daemon uses 100% of the CPU and restarts. **Workaround:** Remove the VSX configuration using the `no vsx` command.
SNMP	93608	**Symptom:** The switch reports an incorrect value for the `ifSpeed` MIB object. **Scenario:** When a LAG interface has a bandwidth greater than 4.2GB, the switch reports an incorrect value for the LAG interface in the `ifSpeed` MIB object.
VSX	93940	**Symptom:** The switch experiences traffic loss to hosts which are configured as policy-based routing (PBR) nexthops. **Scenario:** In a VSX setup with VRRP enabled, where PBR has been applied to the SVIs, **Workaround:** Do not use the same virtual link local address across different VRFs.
Web UI	90636	**Symptom:** The NAE graph for LAG Health Monitor is frozen with a spinning circle animation indicating the graph is fetching data. **Scenario:** When the LAG Health Monitor

Category	Bug ID	Description
		NAE script has been installed and an agent created for the script, but only one LAG has been configured, if a second LAG is added to the agent, the LAG Health Monitor graph freezes and will not display new data. **Workaround:** Remove the agent and recreate it with both LAGs.

Version 10.06.0001

Category	Bug ID	Description
CLI	93570	**Symptom:** Interface descriptions for logical interfaces are missing from the output of the `show interface brief` command. **Scenario:** Even after adding descriptions to logical interfaces like SVIs and LAGs, the description column of the `show interface brief` command displays `--`.
Physical Interface	81223	**Symptom:** The port remains in the `waiting for link` state after a DAC is connected. **Scenario:** When using a 721064-B21 40G QSFP+ 4x10G SFP+ 3m DAC connected to an HPE 731628-B21 621SFP28 NIC, after a reboot the NIC may not link and the switch port remains n the `waiting for link` state. **Workaround:** Toggle the port state using the `shutdown` and `no shutdown` commands.
REST	86959	**Symptom/Scenario:** The REST API returns an empty list [ ] instead of an empty dictionary { } when no data is available.
SNMP	78836	**Symptom:** The switch displays the `No such object available on this agent at this OID` message. **Scenario:** When an SNMP walk of the Q-Bridge MIB is performed, the message `No such object available on this agent at this OID` is displayed.
SSH	76056	**Symptom:**`Permission denied` messages, that are not relevant to the performed task, are displayed. **Scenario:** When a switch administrator, whose CLI session was authenticated through TACACS or RADIUS, issues a `copy support-fails all` command, and the location they specify is a remote SFTP server, a `Permission denied` error message is incorrectly displayed. **Workaround:** Do not perform SSH/SFTP client operations as a TACACS or RADIUS user.

Category	Bug ID	Description
Switch Module	92738	**Symptom/Scenario:** The switch experiences traffic latency localized to ports in a specific switch module. The latency can degrade in time to the point of no traffic being passed through the respective switch module. **Workaround:** Reboot the affected module using the `reboot module <ID>` command.
Transceivers	80785	**Symptom/Scenario:** When a supported transceiver is inserted into a switch, a message similar to `Event|3809|LOG_WARN|AMM|-|Transceiver SFP-BT inserted in 1/2/1 is unsupported. Third party pluggable module is not supported in this interface` is logged.

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 10.06.0140

Category	Bug ID	Description
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 between VRRP peers instead of BGP.
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.
IGMP	172309	**Symptom:** A delay of 5-10 seconds is seen during the IPTV channel change along with high CPU usage observed with `hpe-repld` daemon. **Scenario:** When there are a high number of SSDP-related multicast flows along with regular multicast flows, a delay of 5-10 seconds is seen during an IPTV channel change along with high CPU usage. **Workaround:** Disable SSDP flows at the source or add an ACL to drop SSDP joins.
OSPF	08491	**Symptom/Scenario:** OSPFv2 and OSPFv3 do not support detailed

Category	Bug ID	Description
		LSA `show` commands. **Workaround:** Use the `diag ospf[v6] lsdb dump` command under the `diagnostics` menu to view LSA details.
SNMP	169584	**Symptom/Scenario:** An SNMP walk provides the wrong output for the ifNumber (total number of interfaces in a system) object and does not provide the management interface name for the ifName object.
VRF	72044	**Symptom:** The switch fails to program routes for some VRFs if the VRF name is over 31 characters. **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 the same IPv6 link-local address as the 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
ARP/ND suppression	ARP/ND suppression is not supported.
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, Aruba 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	Automatic downgrade of the startup–config is not supported during a software downgrade. To restore a configuration use the procedure documented under Manual Configuration Restore for Software Downgrade.
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.

Feature	Description
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 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.
IGMP/PIM on Loopback and GRE interfaces	IGMP cannot be enabled on both Loopback and GRE interfaces. PIM can be enabled on a Loopback interface. PIM will not work on GRE tunnels and 6in6.
IP Tunnels	GRE, 6in4, and 6in6 tunnels are not supported on Aruba 8400X-32Y 32p 1/10/25G SFP/SFP+/SFP28 Module (JL687A).
Multicast and VXLAN	RP on VSX is not supported. ROP extension for VSX border leaf for clients is not supported. VXLAN must be configured prior to configuring VSX. Distributed Anycast Gateway is not supported (same IP address for SVI and AG).
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. When using AAA, make sure to give the admin user the permissions to run all commands needed by enabled NAE 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.
OSPF	ABR does not inject a default route in a Totally Stubby Area with loopback in AREA 0.0.0.0.
RADIUS	Authorization by means of HPE VSAs is not supported.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
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.

Feature	Description
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 when configured on the same interface.
VRRP and VXLAN	VRRP and VXLAN are mutually exclusive.
VRRP-MD5 authentication interop	Not supported with Comware-based switches
VSX and Static VXLAN	Static VXLAN on VSX configuration is not supported. Use VSX and EVPN or VSX and HSC.
VXLAN	Aggregated links (LAG or MCLAG) are not supported for underlay.
VXLAN	No support for IPv6 overlay hosts.
VXLAN	DSCP-enabled packets carried in a VXLAN tunnel are treated as best-effort traffic.

Upgrade Information

Version 10.06.0140 uses ServiceOS GT.01.07.0001.

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00*xx* version of software to 10.06.*xxxx*.
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.

10.03 is the minimum required software version prior to upgrading to 10.06. 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 10.06. Check release notes for the software version you will upgrade to for instructions on performing the upgrade to 10.03.

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

When upgrading from software versions before 10.05.0001, if the switch is configured with an entry in a class-map or an Access List that matches AH or ESP traffic, the policy will fail to apply, as these options are no longer permitted. Remove such entries from the configuration prior to upgrading to 10.06.0140 or remove the respective entries from ACLs or Class that failed to apply after the upgrade to 10.06.0140.

When upgrading from a version of software prior to version 10.05.0001, 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 this software version, 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 this software version:

```
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
```

Some Network Analytics Engine (NAE) scripts may not function properly after an upgrade. Aruba 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*.

Manual Configuration Restore for Software Downgrade

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

1. Use the `show checkpoint` 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.10.06.0100).

   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.

Performing the upgrade

This version may contain a change of BootROM from the current running version. A BootROM update is a non-failsafe update. Do not interrupt power to the switch during the update process or the update could permanently damage the device.

1. Copy the XL.10.06.0140 image into the primary boot bank on the switch using your preferred method.
2. Invoke the command to allow unsafe updates to proceed after a switch reboot. Proceed to step 3 within the configured time.

```
switch# config
switch(config)# allow-unsafe-updates 30

This command will enable non-failsafe updates of programmable devices for
the next 30 minutes.  You will first need to wait for all line and fabric
modules to reach the ready state, and then reboot the switch to begin
applying any needed updates.  Ensure that the switch will not lose power,
be rebooted again, or have any modules removed until all updates have
finished and all line and fabric modules have returned to the ready state.

WARNING: Interrupting these updates may make the product unusable!

Continue (y/n)? y
```

3. If upgrading from XL.10.05 or earlier, upon the first time booting to 10.06.0140, a new version of ServiceOS will be installed along with the new BootROM update if the version you are upgrading from has an older version of ServiceOS. On the switch console port an output similar to the following will be displayed as various components are being updated:

```
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.

:
:

Press Esc for boot options
ServiceOS Information:
    Version:          [[[Undefined variable 10-06_RN_variables.XL.10.05.SOS]]]
    Build Date:       yyyy-mm-dd hh:mm:ss PDT
    Build ID:         ServiceOS:[[[Undefined variable 10-06_RN_
variables.XL.10.05.SOS]]]:aa9f6d11bfb6:201910081147
    SHA:              aa9f6d11bfb6de885f0b7f5ec936497ea6e8f7a0

Boot Profiles:

0. Service OS Console
1. Primary Software Image [XL.10.06.0140]
2. Secondary Software Image [XL.10.05.[[[Undefined variable 10-06_RN_
variables.XL.10.05.curr]]]]

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  : '[[[Undefined variable 10-06_RN_
variables.XL.10.05.SOS]]]'
    Write-protected  : NO
    Packaged version : 'GT.01.07.0001'
    Package name     : 'svos_internal'
    Image filename   : 'GT.01.07.0001.svos'
    Image timestamp  : 'Day Mon dd hh:mm:ss yyyy'
    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
```

4. 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 2017-2021 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:
```

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

Documentation Updates and Corrections

This section lists changes to the user manuals based on the particular release of software. The change applies to the listed version and all subsequent versions, unless indicated otherwise.

Version 10.06.0100

For 10.06 versions starting with 10.06.0100, in the *AOS-CX 10.06 VXLAN EVPN Guide*, on page 56 the "VSX failure scenarios" table, the rows that currently read:

Failure scenarios	Result with split recovery off	Result with split recovery on (default)
a) ISL down, VSX Keepalive up.	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure that VXLAN traffic is only sent to the primary VSX switch.	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure VXLAN traffic is only sent to the primary VSX switch.
a) ISL down, VSX Keepalive up. b) Then, after sometime, VSX Keepalive down as well.	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure VXLAN traffic is only sent to the primary VSX switch. Secondary VSX LAGs and	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure that VXLAN traffic is only sent to the primary VSX switch. Secondary VSX node restores VSX LAG member ports and brings up logical VTEP.

Failure scenarios	Result with split recovery off	Result with split recovery on (default)
	logical VTEP stay down.	**NOTE:** Without ISL ARP sync, in routing scenarios, this split condition may lead to traffic loss where ARP request originated from a VSX device and reply lands on the peer VSX device.
a) ISL and keepalive are down b) Keepalive restore	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP(If it was UP earlier) to ensure that VXLAN traffic is only sent to primary VSX switch.	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure that VXLAN traffic is only sent to primary VSX switch.

should be changed to read:

Failure scenarios	Result with split recovery off	Result with split recovery on (default)
a) ISL down, VSX Keepalive up.	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VXLAN traffic is only sent to the primary VSX switch from other VTEPs.	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VXLAN traffic is only sent to the primary VSX switch from other VTEPs.
a) ISL down, VSX Keepalive up. b) Then, after sometime, VSX Keepalive down as well.	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VXLAN traffic is only sent to the primary VSX switch from other VTEPs. Secondary VSX LAGs and logical VTEP reachability stay down.	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VXLAN traffic is only sent to the primary VSX switch from other VTEPs Secondary VSX node restores VSX LAG members and reachability to the logical VTEP is restored in the underlay. **NOTE:** Without ISL ARP sync, in routing scenarios, this split condition may lead to traffic loss where ARP request originated from a VSX device and reply lands on the peer VSX device.
a) ISL and keepalive are down b) Keepalive restore	Secondary VSX node tears down VSX LAG member ports and Secondary VSX node tears down VSX LAG member ports and it withdraws the	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VxLAN traffic is only sent to the primary VSX switch from

Failure scenarios	Result with split recovery off	Result with split recovery on (default)
	reachability to the logical VTEP IP in the underlay to ensure that VxLAN traffic is only sent to the primary VSX switch from other VTEPs.	other VTEPs.

The original wording of the table still applies to all 10.06 versions released prior to version 10.06.0100.

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.