AOS-CX 10.05.0051 Release Notes

6300, 6400 Switch Series

a Hewlett Packard Enterprise company

Part Number: 5200-7623a
Published: May 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

To add trademarks: 1. Duplicate this topic. 2. Move your duplicate topic to the appropriate folder. 3. Add trademarks. For information on how to acknowledge trademarks, see the Legal website: https://legal.int.hpe.com/legal/pages/tradeack.aspx. 4. Reference your duplicate Acknowledgments topic in the bookmap. For more information, see the KM Process Guide. ?>

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

Description

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

If you run the `show version` command on the switch, the version number will display FL.10.05.*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 10.05.0001 is the initial build of major version 10.05 software.

Product series supported by this software:

- Aruba 6300 Switch Series
- Aruba 6400 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 10.05.0021 or later (including this 10.06 release) to implement significant improvements to memory usage and prolong the life of the switch.

Switch fans will run at full speed when a fault is detected with the temperature sensors in the switch. This is normal behavior to ensure overheating does not occur. Should the fans run at full speed at unexpected times, check the output of `show environment temperature` and `show environment fans`, then contact support for further assistance.

If the switch is configured with message digest for OSPF authentication, after upgrading from 10.04 or 10.03 to 10.05 you will need to configure the message digest authentication key. For example:

Configuration before 10.05 upgrade:

```
ip ospf authentication message-digest
ip ospf authentication-key ciphertext
   AQBapeXp+hujHs0a6E91yqpHTzr0Q7UTPBXD8AzLyOkBL5BuBgAAACLPigGiCw==
```

Configuration to be added after upgrade to 10.05:

```
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 ciphertext
   AQBapeXp+hujHs0a6E91yqpHTzr0Q7UTPBXD8AzLyOkBL5BuBgAAACLPigGiCw==
```

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

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and this 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.

If the switch has the always-on PoE feature enabled, during the upgrade from a version of software prior to 10.05.0001 to this version of software, PoE Powered Devices (PDs) will lose power from the switch as the switch will power cycle during the update. Plan a time for upgrading the switch when loss of power to the PDs attached to the switch can be mitigated.

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.[[[Undefined variable 10-06_RN_variables.FL.10.06.curr]]] or remove the respective entries from ACLs or Class that failed to apply after the upgrade to 10.06.[[[Undefined variable 10-06_RN_variables.FL.10.06.curr]]].

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
```

AOS-CX 10.05 is enabled for future support of Aruba Central. The switch will automatically attempt to connect to Aruba Central and log a connection failed error until the future version of Central supports AOS-CX. To have the switch stop trying to connect to Central, use the following commands:

```
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

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, FL.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.

Version history

All released versions are fully supported by Aruba, unless noted in the table.

Version number	Release date	Remarks
10.05.0051	2021-02-17	Released, fully supported, and posted on the web.
10.05.0040	2020-12-15	Released, fully supported, and posted on the web.
10.05.0030	2020-11-19	Released, fully supported, and posted on the web.
10.05.0021	2020-10-29	Released, fully supported, and posted on the web.
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 AOS-CX 10.05. Released, fully supported, and posted on the web.

Products supported

This release applies to the following product models:

Product number	Description
JL658A	Aruba 6300M 24-port SFP+ and 4-port SFP56 Switch
JL659A	Aruba 6300M 48-port HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4-port SFP56 Switch
JL660A	Aruba 6300M 24-port HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4-port SFP56 Switch
JL661A	Aruba 6300M 48-port 1GbE Class 4 PoE and 4-port SFP56 Switch
JL662A	Aruba 6300M 24-port 1GbE Class 4 PoE and 4-port SFP56 Switch
JL663A	Aruba 6300M 48-port 1GbE and 4-port SFP56 Switch
JL664A	Aruba 6300M 24-port 1GbE and 4-port SFP56 Switch
JL762A	Aruba 6300M 48-port 1GbE and 4-port SFP56 Power-to-Port 2 Fan Trays 1 PSU Bundle
JL665A	Aruba 6300F 48-port 1GbE Class 4 PoE and 4-port SFP56 Switch
JL666A	Aruba 6300F 24-port 1GbE Class 4 PoE and 4-port SFP56 Switch
JL667A	Aruba 6300F 48-port 1GbE and 4-port SFP56 Switch
JL668A	Aruba 6300F 24-port 1GbE and 4-port SFP56 Switch

Product number	Description
R0X26A	Aruba 6405 Switch
R0X29A	Aruba 6405 96-port 1GbE Class PoE 4 and 4-port SFP56 Switch
R0X30A	Aruba 6405 48-port SFP+ and 8-port SFP56 Switch
R0X27A	Aruba 6410 Switch
JL741A	Aruba 6410 96-port 1GbE Class PoE 4 and 4-port SFP56 Switch
R0X31A	Aruba 6400 Management Module

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	8.2.11.1
NetEdit	2.0.12
Aruba CX Mobile App	2.3.1
Aruba Central	2.5.3
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 (E0506P05)

For more information, see the respective software manuals.

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
R0X26A	Aruba 6405 Switch	10.04.1000
R0X31A	Aruba 6400 Management Module	10.04.1000
R0X38B	Aruba 6400 48-port 1GbE Class 4 PoE Module	10.04.1000
R0X39B	Aruba 6400 48-port 1GbE Class 4 PoE and 4-port SFP56 Module	10.04.1000
R0X40B	Aruba 6400 48-port 1GbE Class 6 PoE and 4-port SFP56 Module	10.04.1000
R0X41A	Aruba 6400 48-port HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4-port SFP56 Module	10.04.1000
R0X42A	Aruba 6400 24-port 10Gbase-T and 4-port SFP56 Module	10.04.1000
R0X43A	Aruba 6400 24-port SFP+ and 4-port SFP56 Module	10.04.1000
R0X44A	Aruba 6400 48-port 10/25GbE SFP28 Module	10.04.2000
R0X45A	Aruba 6400 12-port 40/100GbE QSFP28 Module	10.04.2000
JL762A	Aruba 6300M 48-port 1GbE and 4-port SFP56 Power-to-Port 2 Fan Trays 1 PSU Bundle	10.04.3000
R0X27A	Aruba 6410 Switch	10.05.0001
JL741A	Aruba 6410 96-port 1GbE Class PoE 4 and 4-port SFP56 Switch	10.05.0001

Transceiver Support

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

No new transceiver support

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.

Version 10.05.0051

Category	Description
SNMP	Added additional LAG attributes in order to facilitate a richer NMS experience from tools such as Airwave.

Version 10.05.0040

No enhancements were included in version 10.05.0040.

Version 10.05.0030

Category	Description
Event Log	Added event message to 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`
OSPF	**NOTE:** Applies only to the Aruba 6300 Switch Series. Added two options (`ignore-lost-interface` and `helper strict-lsa-check`) to the `graceful-restart` command to relieve traffic loss seen in various HA environments.
SNMP	Added support for the Q-BRIDGE-MIB.

Version 10.05.0021

Category	Description
LEDs	Added support for the fault LED (blinking amber) to indicate a switch storage device failure. An event log message will also be generated when a storage device failure is detected: `Storage <type> health alert. Imminent failure expected. Please backup data.` Hardware replacement would be necessary if the fault LED is blinking amber and the `show system resource-utilization | inc Endurance` reports 100% Endurance utilization.

SNMP	Added support for SNMP check of unique request IDs
	Syntax
	`snmpv3 unique-req-id`
	`no snmpv3 unique-req-id`
	Description
	Enables a unique request ID check. By default, the unique request ID check is disabled. When this check is enabled, the SNMP agent will drop SNMPv3 packets with a duplicate request ID in a 150 second window.

SNMP	Added SNMP trap support for storage health events.
	`1.3.6.1.2.1.16.9.1.1.1: 9103`
	`1.3.6.1.2.1.16.9.1.1.2: Storage <type> endurance utilization at xx%`
	`1.3.6.1.2.1.16.9.1.1.1: 9102`

Category	Description
	`1.3.6.1.2.1.16.9.1.1.2: Storage <type> health alert. Imminent failure expected. Please backup data.`

Version 10.05.0020

Category	Description
Captive Portal	**NOTE:** Applies only to the Aruba 6400 Switch Series. 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 (`-`).

OSPF	**NOTE:** Applies only to the Aruba 6300 Switch Series.
	Added the following commands to prevent traffic loss when there is a VSF switchover:
	`no graceful-restart helper strict-lsa-check`
	`graceful-restart ignore-lost-interface`

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>*

Category	Description

	Port identifier range.
	statistics
	Clear counters for the interface.
	global
	Clear hardware counters for the interface for all sessions.
	Examples
	On the 6400 Switch Series, interface identification differs.
	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`

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

New features

Category	Description
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.
Dynamic segmentation enhancements	Enhancements were made to the VXLAN-based segmentation solution. Dynamic segmentation with Aruba automates policy and segmentation.
Ehternet Ring Protection Switching (ERPS)	This release adds support for Ethernet Ring Protection Switching that prevents broadcast storms and implements fast traffic switchover on a network where there are loops. This release adds support for non-revertive mode.
EVPN symmetric routing with L3 distributed Anycast	This release introduces Symmetric Integrated Routing and Bridging with Distributed L3 Anycast gateways using L3 VNIs which provides better scalability. It also adds support for EVPN route type 5.

Category	Description
gateway	
Fault monitor	This feature provides the ability to monitor faults, allowing the switch to be protected from network loops, faulty hardware, and other issues.
IP Client Tracker	The IP Client Tracker feature will learn and update the IP address of the access devices and clients connected to the switch. It can track addresses of directly connected clients and the address of clients connected to a downstream device such as a wireless access point. This is supported for both IPv4 and IPv6.
Local MAC match	MAC match provides dynamic attribute assignment (for example, VLAN and QoS) through the use of a locally configured authentication repository. The most common use model is for automatic assignment of a VLAN to IP phones. MAC match also solves dynamic assignment of per client (MAC address) attributes without having to create a RADIUS infrastructure When dot1x MAC authentication fails, MAC match can be used as a fallback.
LLDP over OOBM	This feature enables LLDP support over the Out-of-band management (OOBM) port.
MAC grouping	This is a unique feature leveraging the power of Gen7 Aruba ASICs, allowing a group of MAC addresses to be referenced by a single ACL or classifier policy resulting in highly optimized use of TCAM space.
Quick PoE	Quick PoE allows the Switch to deliver power to the powered device (PD) as early as possible specifically in the case of a cold boot. While the switch system is booting, power is delivered to PDs before the AOS-CX operating system has completed the boot process. The primary use-case for Quick PoE is when the switch is booting after a power outage. It allows for PD's to be powered, and perform their own initialization in parallel with the switch OS before network connectivity is provided.
RA Guard	The RA Guard feature drops the RA(Router Advertisement) and RR(Router Redirect) packets on untrusted ports while allowing them on trusted ports. With ND-Snooping enabled on a VLAN, RA guard is enabled by default. This adds an additional capability to our already rich IPv6 feature-set.
RadSec	This release adds support for RadSec providing a Secure TLS tunnel for RADIUS messaging that transports packets via TCP and TLS.
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.

Enhancements

Category	Description
Diagnostics	Improved the cable diagnostics feature with an additional column providing impedance information for each pair. If there is no fault on a given pair, the output in the `Distance to Fault` column now displays – instead of `0`.

Event Log	Improved the event log message when an uncontrolled reboot occurred, likely due to a power removal:
	`--------------------------------------------------`
	`Boot History`
	`--------------------------------------------------`

Category	Description
	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.

The Bug ID is used for tracking purposes.

Version 10.05.0051

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.
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	89813	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** TX counter drops are seen on VSF and data port links (not specific to VSF).

Category	Bug ID	Description
		Scenario: When two hosts are connected to the switch in the same subnet and have ports assigned to VLAN 1, if ICMP is enabled and packets are sent from one host to the other with the destination MAC set the same as the switch, TX packet drops are observed on the receiving host. When the hosts are connected across VSF members, the drops are seen on the VSF link. **Workaround:** Disable ICMP using the `no ip icmp redirect` command.
Counters	91719, 91969	**Symptom:** TX drops keep incrementing in the system without having an oversubscription. **Scenario:** When the switch is connected to a Cisco device with the keep alive protocol enabled, interfaces in a down state which are sending packets (for example, a flapping interface or returning an interface to its default) may report TX drops. IP exception packets are also dropped and increment the drop counters on the interface.
Counters	94023	**NOTE:** Applies only to the Aruba 6400 Switch Series. **Symptom:** Interface TX drop counters incorrectly increment and do not reflect actual traffic drops. The issue manifests when the switch receives a unicast packet with a learned destination port and that packet is dropped or redirected to the CPU. **Scenario:** There are multiple scenarios where this can happen: 1. ACLs - unicast packet is destined to a learned port but is denied by an ACL 2. Security applications - unicast packet is destined to a learned port but is redirected to the CPU for inspection, such as DHCP Snooping 3. MAC SA = MAC DA - unicast packet that is dropped as a loop prevention mechanism, sometimes transmitted by other network devices 4. ICMP redirects In all cases, the port the packet was destined to is the interface that will show TX drops for the above conditions. **Workaround:** Disable ICMP using the `no ip icmp redirect` command.
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 Client	94134	**Symptom:** The switch continuously receives IP address renewal from the DHCP server. **Scenario:** When VLAN 1 is configured with a dynamic IP address from a DHCP server, an IP address renewal request may be continuously triggered for VLAN 1. **Workaround:** The issue is random. Disabling and re-enabling the VLAN 1 interface may stop the cycle. Or, disable the `new ip` option on renewal.

Category	Bug ID	Description
Fans	93450, 148228, 149287	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** The fans of modular switches (JL658A, JL659A, JL660A, JL661A, JL662A, JL663A, JL664A and JL762A) in a VSF stack spin at a higher speed than expected and fan information does not display in the output of the `show environment fan` command. **Scenario:** After a stack bring-up, reboot, or stack switchover in a VSF stack of switches where at least one switch is modular (conductor or member), the fans on all of the modular switches spin at a higher than expected speed and no fan information displays in the output of the `show environment fan` command. **Workaround:** This issue will not impact functionality of the fan or switch.
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.
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.
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	95065	**Symptom:** VLAN 0 tagged traffic with 802.1p priority tags is not treated as native VLAN and causes multicast packets to be flooded. **Scenario:** If Axia xNodes are configured for various types of live and standard stream traffic with the 802.1p tagging feature enabled, when the switch is rebooted multicast packets are flooded. **Workaround:** Disable the 8021.1p tagging feature.
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 10.05.0040

Category	Bug ID	Description
Counters	89034, 89813, 92972, 93413	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** Interface TX drop counters incorrectly increment and do not reflect actual traffic drops. The issue manifests when the switch receives a unicast packet with a learned destination port and that packet is dropped or redirected to the CPU. **Scenario:** There are multiple scenarios where this can happen: 1. ACLs - unicast packet is destined to a learned port but is denied by an ACL 2. Security applications - unicast packet is destined to a learned port but is redirected to the CPU for inspection, such as DHCP Snooping 3. MAC SA = MAC DA - unicast packet that is dropped as a loop prevention mechanism, sometimes transmitted by other network devices 4. ICMP redirects In all cases, the port the packet was destined to is the interface that will show Tx drops for the above conditions. **Workaround:** Disable ICMP using the `no ip icmp redirect` command.
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.
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 10.05.0030

Category	Bug ID	Description
ACL	91231, 94347	**Symptom:** An ACL causes issues with forming PIM neighbor relationships. **Scenario:** When an ACL is created for a multicast group with the first sequence number as 10 and no actions associated with it, the PIM neighborship may not be established and multicast traffic streams are impacted. **Workaround:** Do not use a sequence value of 10; start with a sequence value of 20.
BFD	88859	**Symptom:** The output of the `show ip ospf interface <IFNAME>` command incorrectly displays `BFD is disabled`. **Scenario:** When BFD is configured using the `bfd all-interfaces` command globally, BFD status on the interface shows

Category	Bug ID	Description
		disabled in the output of the `show ip ospf interface <IFNAME>` command.
Central	94012	**Symptom:** The switch fails to establish a new connection with Aruba Central. **Scenario:** When there is a timeout in the TCP connection of 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.
CLI	91777	**Symptom/Scenario:** The switch fails to display the configured description for SVI, LAG, or loopback interfaces in the output of the `show interface brief` command. **Workaround:** Use the `show run interface <IFNAME>` or `show interface <IFNAME>` commands to see the interface description.
DHCP Relay	91519	**Symptom/Scenario:** The DHCPv6 relay agent uses the wrong UDP port when forwarding DHCPv6 client requests.
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.
EVPN	85637	**Symptom:** VXLAN tunnel endpoint (VTEP) does not advertise the physical MAC address of the VLAN interface in EVPN, causing the flooding of packets destined for the system MAC address of the VTEP. **Scenario:** If the VLAN interface has active-gateway configured, then EVPN advertises only the active-gateway MAC and IP addresses. **Workaround:** Configure end devices to use the active-gateway MAC and IP addresses rather than the system MAC and IP addresses.
IPv6 RA	91560	**Symptom:** The IPv6 ND Prefix Autonomous Address-Configuration Flag is reported incorrectly as set, even though `no-autoconfig` is defined. **Scenario:** If the IPv6 ND configured prefix is the same as the RA prefix, when performing a shutdown/no shutdown on the interface, the IPv6 ND Prefix Autonomous Address-Configuration Flag is reported incorrectly as set, even though `no autoconfig` is defined on the interface.
PBR	92010	**Symptom:** Counters increment after applying or replacing a policy, but the PBR policy does not take effect. **Scenario:** After a PBR policy is applied to a second interface or a PBR policy is replaced with one that is already applied to a different interface, the counter increment, but the PBR policy does not take effect. **Workaround:** Add or remove an entry in one of the classes or in the policy.

Category	Bug ID	Description
PoE	92297	**NOTE:** Applies only to the Aruba 6400 Switch Series. **Symptom:** The switch incorrectly interrupts and restores PoE delivery to connected powered devices (PDs). **Scenario:** During a switchover event to the standby management module, if there is only one PSU present in the chassis, the switch toggles the PoE status for interfaces with connected PDs.
Port Access	90678	**Symptom:** Authenticated clients are unexpectedly logged off. **Scenario:** When existing port-access policy configurations on the switch are relayed from NetEdit, the switch incorrectly logs off existing clients.
QoS	91563	**Symptom:** VXLAN traffic with non-default DSCP values does not use the desired egress queues. **Scenario:** When traffic over a VXLAN is sent with non-default DSCP values which are mapped to the QoS DSCP configuration on the switch, the traffic does not use the desired egress queues.
OSPF	92629	**NOTE:** Applies only to the 6400 Switch Series. **Symptom:** The switch loses current OSPF adjacencies. **Scenario:** In a VSX setup, after adding new VLANs to the configuration, the switch may lose OSPF adjacency. **Workaround:** Add VSX active-forwarding (on both the VSX primary and secondary) for newly added VLANs.
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.
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 logged. **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 logged.

VSX	92243	**NOTE:** >Applies only to the Aruba 6400 Switch Series.
		
		Symptom: The VSX status goes into a non-operational state 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 configuration, causing the VSX status to go into a non-operational state and configuration sync stops working. For example:
		`switch# show vsx status config-sync`
		`Admin State : Enabled`
		`Operational State : Operational`

Category	Bug ID	Description
		`Error State : None` **Workaround:** Reboot the secondary VSX member.
Web UI	92448	**Symptom:** Inconsistent switch module numbering displays in the Front Status LED panel. **Scenario:** Switch module numbers are listed in the Front Status as 1-10 in the Web UI interface, while the LEDs on the physical chassis number switch modules as 3-12.

Version 10.05.0021

Category	Bug ID	Description

Storage	91243	**Symptom:** The switch reports storage failure event messages or fails to find or initialize eMMC during reboot.
		Scenario: A VSF standby or member switch or a standby management module may report event messages similar to:
		`Storage mmc-type-a health alert. Imminent failure expected. Please backup data.`
		`Storage mmc-type-a endurance at xxx%.`
		Or
		`Storage ssd health alert. Imminent failure expected. Please backup data.`
		`Storage ssd endurance at xxx%. · Storage endurance reported by "show system resource-utilization"`
		Workaround: Use the `show system resource-utilization` command to check the system storage health. Hardware replacement is necessary if the fault LED is blinking amber and the `show system resource-utilization` reports 100%.

Switch Module	[illegible]	Applies only to the Aruba 6400 Switch Series. **Symptom/Scenario:** The switch experiences traffic latency, usually 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 switch module using the `reboot module <ID>` command.

Version 10.05.0020

Category	Bug ID	Description
Accounting	88385	**Symptom:** DUR fails and the accounting session for the client is not seen in the CPPM server. **Scenario:** If a client has been authenticated using a CPPM server

Category	Bug ID	Description
		and then a DUR is applied to the client, DUR fails and the accounting session for the client is not seen in the CPPM server. **Workaround:** Force a reauthentication with the `port-access reauthenicate interface` *<IFNAME>* comman
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.
ARP	88165	**Symptom:** A static ARP entry is not listed in the output of the `show arp` command. **Scenario:** When a static ARP entry is created for a neighbor that has not been learned by the switch, the entry is not listed in the output of the `show arp` command. **Workaround:** Create a dynamic entry in the ARP table for the interface using the `shut` and `no shut` commands and then add the static ARP entry.
ARP	90488	Applies only to the Aruba 6300 Switch Series. **Symptom:** Client traffic behind a phone is lost due to an ARP resolution issue with ARP inspection enabled. **Scenario:** When a client behind a phone is connected to the standby in a VSF stack with ARP inspection enabled and the phone interface is flapped or ARP is cleared from the client, the ping from client will fail as ARP does not get resolved on the client PC. **Workaround:** Disable the ARP inspection feature on the VSF stack.
ARP Security	91206	**Symptom:** The MAC address moves to the wrong port, causing attached switches to misdirect traffic. **Scenario:** When features that intercept/steal packets for evaluation by the CPU before forwarding such as ARP/ND Inspection/Snooping and DHCP snooping are enabled, the intercepted packets can occasionally be inadvertently sent out the port they arrived on. Since the MAC Source Address is not updated, this can cause the MAC address to move to the wrong port on the attached switch and cause attached switches to misdirect traffic.
Authentication	88317	**Symptom:** The switch displays the `Internal error. Password not set.` error message. **Symptom:** After a reboot, the switch may rarely show an incorrect error message `Internal error. Password not set.` during login. **Workaround:** There is no impact. Login is still successful.
Authentication	89803	**Symptom/Scenario:** An attempt to access the switch console when the uplink port is disabled or the cable has been removed from the interface, the switch does not fail over to local authentication, preventing access.
CLI	87625	**Symptom/Scenario:** When the `top cpu` command is executed

Category	Bug ID	Description
		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	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 deploy that configuration from NetEdit. **Workaround:** Remove the empty lines from the banner statement.
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.
CPU Rx	90709	**Symptom:** Network latency on an uplink port. **Scenario:** With ICMP redirect enabled by default, traffic on a subnet that could have been sent directly to a host, such as a firewall, is instead sent to the switch, which then forwards it to the correct host on the same subnet, can cause network latency. **Workaround:** Configure `no ip icmp redirect` on the switch.
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.

DHCP Relay	88137	Applies only to the Aruba 6400 Switch Series.
		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	88395	**Symptom:** The ipbinding entries on a port are unexpectedly cleared. **Scenario:** When MAC auth is enabled on a port and the port is subsequently disabled and re-enabled with the `shut` and `no shut` commands, the ipbinding entries are cleared from the port.
DHCP Snooping	89192	**Symptom:** The switch is flooded with DHCP packets.

Category	Bug ID	Description
		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.
Dynamic Segmentation	88390	**Symptom:** The username provided by the RADIUS/CPPM server is not shown in the Aruba Mobility Controller. **Scenario:** When UBT is configured on the switch with MAC authentication, the username provided by the RADIUS/CPPM server is replaced with the UBT client's MAC address in the Aruba Mobility Controller.
Dynamic Segmentation	90913	**Symptom:** The client user name, as per the authentication profile in ClearPass, is not reflected in the Aruba Mobility Controller. **Scenario:** When a UBT client moves from dot1x to MAC-Auth, or from MAC-Auth to dot1x, to re-authenticate on the switch, the client user name found in the authentication profile in ClearPass is not reflected in the Aruba Mobility Controller. **Workaround:** Shutdown and restart the user port or logout the UBT client and have the user attempt to log in again.

IP Client Tracker	87672	**Symptom:** Switch fails to track the IP address for certain VOIP clients (for example, IP phones).
		Scenario: When IP Client Tracker is enabled in default mode (`auto`) for a port with a PC connected behind an IP phone, the switch fails to track the IP address of the phone.
		Workaround: Configure IP Client Tracker mode as `enable` for the ports with a PC connected behind an IP phone For example:
		`switch(config)# interface 1/1/1`
		`switch(config-if)# client track ip enable`

Link Aggregation	89558	**Symptom/Scenario:** The switch returns an incorrect value "0" when querying `ifHighSpeed` OID for a LAG interface.
Loop Protect	90376	**Symptom:** Tx drops increment unexpectedly. **Scenario:** When VLANs and loop protect are configured on ports and some of the ports are in the up state and other are not, all ports that are not connected report Tx drops.
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.
Mirroring	90642	**Symptom/Scenario:** The switch limits the number of source interfaces per mirror session to four.
NAE	87678	**Symptom/Scenario:** If the Network-Health_Monitor NAE script monitors a LAG interface, it fails to re-start when the LAG interface is shutdown and subsequently comes back up. **Workaround:** Update Network-Health_Monitor script from Aruba

Category	Bug ID	Description
		ASC to the latest version.
NAE	89615	**Symptom/Scenario:** When using the arp_request_monitor NAE script, the switch may log multiple error messages similar to `Traceback error - hpe-policyd[11691]: Intermittent memory spike`. **Workaround:** Update arp_request_monitor script from Aruba ASC to the latest version.
Physical Interfaces	87565	**Symptom:** The switch fails to detect collisions. **Scenario:** The switch autonegotiates to 100-HDx, but the hardware does not support 100-HDx and actually runs at 100-FDx, causing issues detecting collisions.
Physical Interfaces	89661	**Symptom:** Smart Rate ports connected to 100-full ports report 100-half as the speed in the output of the `show interface` command **Scenario:** On the link partner, configure for autonegotiation or force to 100-full to avoid collisions. Do not force to 100-half as there would be a duplex mismatch with the switch.
RADIUS	82521	**Symptom:** Some clients with IP addresses in the binding table do not have those IP addresses included int eh RADIUS `Framed-IP-Address` field in RADIUS accounting packets. **Scenario:** When port access and client IP tracker are enabled, some clients with IP addresses in the binding table do not have those IP addresses included int eh RADIUS `Framed-IP-Address` field in RADIUS accounting packets.
RADIUS	90331	**Symptom:** The NAS-ID attribute in RADIUS packets is sent as connection type rather than the switch hostname. **Scenario:** When a management user remove authentication with CPPM is performed and the CPPM server is a few hops distant, the NAS-ID attribute in RADIUS is sent as a connection type instead of the switch hostname.
RADIUS Port Accounting	88385	**Symptom:** DUR fails and the accounting session for the client is not seen in the CPPM server. **Scenario:** When a client is authenticated with CPPM and DUR has been applied, the switch checks for a role and when the role is not present, the switch requests a download from the CPPM server, causing DUR to fail and the accounting session to not be recorded on the CPPM server. **Workaround:** Force a client reauthentication with the `port-access reauthenticate interface` *<IFNAME>* comman
RADIUS Port Accounting	90646	**Symptom:** Copying support files fails or takes longer than expected. **Scenario:** When copying support files using the `copy support-files` *<URL>* command, th than expected.
REST	86920	**Symptom/Scenario:** Executing a GET REST API request to retrieve the queue counters for an interface shows empty or obsolete

Category	Bug ID	Description
		values. **Workaround:** Use the `show interface <IFNAME> queues`
Secure Roles	88732	**Symptom:** Clients fail to load advanced roles. **Scenario:** When using Downloadable User Roles (DUR), clients fail to load advanced roles. The output of the `show port-access client` command shows `In Progress`. **Workaround:** Reboot the switch.
SNMP	89339 	Applies only to the Aruba 6300 Switch Series. **Symptom/Scenario:** An SNMP walk times out when walking a large SNMP MIB.
SSH	86570 	Applies only to the Aruba 6300 Switch Series. **Symptom:** The switch refuses an SSH connection for about 30 seconds. **Scenario:** In a VSF stack, during a failover event to "standby", the switch refuses SSH connection via in-band IP SVI for approximately 30 seconds. **Workaround:** The switch accepts the SSH connection 30 second after the failover event occurs. Retry the SSH connection 30 sec later.
Switch buttons	90279 	Applies only to the Aruba 6300 Switch Series. **Symptom:** The switch becomes stuck in a boot loop. **Scenario:** When the reset button on a member switch that is part of a VSF stack is pressed, the switch becomes stuck in a boot loop.
TACACS	90604	**Symptom:** Unable to log into the switch using TACACS credentials. **Scenario:** After a VSF failover, users are unable to log into the switch using TACACS credentials.
Thermal Manager	90047 	Applies only to the Aruba 6400 Switch Series. **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 after three minutes and remains down for five minutes. After the switch is back up, the boot history shows the reboot reason as having insufficient fans.
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`.

Category	Bug ID	Description
		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.
VSF	87240 	Applies only to the Aruba 6300 Switch Series. **Symptom:** Some VSF stack members unexpectedly reboot after a master-standby failover event. **Scenario:** When a failover event occurs from master to standby due to any reason, some VSF member switches may also reboot. **Workaround:** There is no functional impact. The VSF members successfully rejoin the stack after their reboot.
VSF	89248 	Applies only to the Aruba 6300 Switch Series. **Symptom/Scenario:** A VSF stack member switch takes a longer time to reboot and join the stack after the Master and Standby switches have completed the reboot. **Workaround:** There is no functional impact. The VSF member successfully reboots and rejoins the stack.
VXLAN	84176	**Symptom:** An exclamation mark (!) displays at the end of every VXLAN VNI context in the output of the `show running-config` and `show running interface vxlan` commands. **Scenario:** When at least one VNI is configured under a VXLAN interface, an exclamation mark (!) displays in the output of the `show running-config` and `show running interface vxlan` commands.
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

Category	Bug ID	Description
TACACS	90604	**Symptom:** Unable to log into the switch using TACACS credentials. **Scenario:** After a VSF failover, users are unable to log into the switch using TACACS credentials.

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	**NOTE:** Applies only to the Aruba 6400 Switch Series.
		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`

SNMP	89235	**Symptom:** The `ifHighSpeed` MIB OID returns an invalid value. **Scenario:** When querying the `ifHighSpeed` OID on a high-speed port (10G or higher), the switch returns a 0 value.
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.
VSF	87240	**NOTE:** >Applies only to the Aruba 6300 Switch Series. **Symptom:** Some VSF stack members unexpectedly reboot after a master-standby failover event.

Category	Bug ID	Description
		Scenario: When a failover event occurs from master to standby, some VSF member switches may also reboot. **Workaround:** The VSF members will rejoin the stack after the reboot.
VSF	89248	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom/Scenario:** A VSF stack member takes longer than expected to rejoin the stack after a reboot. **Workaround:** There is no functional impact. The member switch just takes longer than expected to reboot and rejoin the stack.

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.
Config	87792, 88852	**Symptom:** The switch fails certain configuration validation via

Category	Bug ID	Description
management		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.
Counters	85810	**Symptom:** The switch reboots with a `critical service fault` error message. **Scenario:** When the switch interface counters are repeatedly queried from the CLI, SNMP pollers, or REST calls, the switch may encounter a `critical service fault` error and reboot. **Workaround:** Avoid simultaneous CLI queries for all switch interfaces or decrease the frequency of SNMP polling and/or REST calls to five minutes or more when counters for all switch interfaces are queried.
Counters	87734, 88272	**Symptom:** Interface counters jump to extremely high values, including on interfaces that are not connected. In addition, the command `show interface error-statistics` fails to provide any output. **Scenario:** This issue may occur when NAE or network monitoring tools are polling counters. **Workaround:** Use other `show interface` commands, specifying the interfaces of interest.
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.
Fans	79837	Applies only to the Aruba 6300 Switch Series. **Symptom:** The switch does not display fan information. **Scenario:** In a VSF stack configuration, independent of the stack size, the switch does not display the fan information for the member switch configured with ID 10 in the output of the `show environment fan` command.
Firmware management	87089	**Symptom:** Firmware upgrade fails with a message similar to `Firmware update failed due to timeout 300000 ms`

Category	Bug ID	Description
		`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.
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.
Physical port	86246	**Symptom:** The switch experiences unexpected link failures or mismatched duplex links at 100M. **Scenario:** When a Smart Rate port is configured for 100-full or 100-half speed, the configuration is ignored and the port autonegotiates, resulting in link failures. **Workaround:** Configure link partners for 100Mbps with autonegotiation enabled.

Physical port	86886	**Symptom:** The switch fails to establish a link with a peer device.
		Scenario: When the switch is configured with a forced 1000-full speed duplex for an update port, after a system reboot, the switch fails to establish a link with the connected partner.
		Workaround: After the reboot, set the port speed to `auto` then back to `1000-full`. For example:
		`switch(config)# interface 1/1/52`
		`switch(confi-if)# speed auto`
		`switch(confi-if)# speed 1000-full`
		`switch(confi-if)# exit`

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` 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 	Applies only to the Aruba 6400 Switch Series. **Symptom:** The switch fails to execute `show` commands to get remote data from the VSX peer switch using the `vsx-peer` option.

Category	Bug ID	Description
		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.
User Based Tunnels	83116	**Symptom:** The switch fails to tunnel to an Aruba controller for some users. **Scenario:** When VSAs are included in RADIUS or CPPM user authentication, the switch fails to create the user tunnel to the Aruba controller for that user. **Workaround:** Configure a client Local User Role (LUR) for secondary/controller for RADIUS/CPPM authentication.
VSX	85141 	Applies only to the Aruba 6400 Switch Series. **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.
VXLAN	86105	**Symptom:** The switch fails to program certain static routes. **Scenario:** After one VSX switch member is rebooted, the switch fails to program static routes with nexthop in a VLAN used for VXLAN.
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
Counters	75958	**NOTE:** >Applies only to the Aruba 6300 Switch Series. **Symptom/Scenario:** The switch reports Tx drops or errors on ports that are not connected.
Dynamic Segmentation	76541	**Symptom:** Client authentication or authorization fails. **Scenario:** When UBT is enabled and the UBT client VLAN is dynamically changed, client authentication or authorization fails. **Workaround:** Remove the current UBT configuration before changing the UBT client VLAN, then re-configure UBT using these steps: 1. Delete the UBT profile (remove the full UBT configuration)

Category	Bug ID	Description
		2. Delete the reserved VLAN. 3. Configure the reserved VLAN. 4. Configure the UBT client VLAN. 5. Configure UBT.
LLDP	82582	**Symptom:** The LLDP process crashes. **Scenario:** If multiple interfaces experience link-state transitions, the LLDP process crashes and restarts.
OSPF/NetEdit	71167	**Symptom/Scenario:** Unable to validate/deploy a switch config using NetEdit if there is a route-map that matches a VLAN interface. **Workaround:** Remove the VLAN interface matching from the route-map or use the CLI to configure the switch.
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	**NOTE:** Applies only to the Aruba 6400 Switch Series. **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 10.05.0051

Category	Bug ID	Description
ACLs	68878	**NOTE:** Applies only to the Aruba 6300 switch series. **Symptom:** The switch fails to create ACL log messages. **Scenario:** In a VSF stack, the switch may fail to log events for the matching access-list entries, causing the switch to generate an error similar to `List and seq# unknown....` **Workaround:** The ACL functionality is not impacted; access-list entries are applied properly and only the logging functionality is incorrectly generated.
Counters	94723	**Symptom/Scenario:** Interface Tx drop counts may increment when a port transitions to down with traffic in flight to that port. **Workaround:** Clear the interface statistics.
ICMP Redirect	86208	**NOTE:** Applies only to the Aruba 6400 switch series. **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	94722	**Symptom:** The switch fails to establish OSPF adjacencies. **Scenario:** When configured with OSPF message digest, the switch fails to establish OSPF adjacencies after an upgrade from version 10.03 or 10.04 to version 10.05. **Workaround:** Configure a message digest authentication key using the `ip ospf message-digest-key <KEY_ID> md5 ciphertext <KEY>` command.
SFTP	65321	**Symptom:** In certain conditions, an SFTP file transfer fails. **Scenario:** When the path to the SFTP server crosses segments with different MTU frame sizes, the file transfer over SFTP fails. **Workaround:** Configure the same MTU on all network segments on the path to the SFTP server.
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.

Feature caveats

Feature	Description
BFD echo (6400 only)	BFD echo is not supported.
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	Policies containing both MAC and IPv6 classes are not allowed.
Counters	A small number of dropped counters may be observed on interfaces that are in the down state.

Feature	Description
Counters (6400 only)	Bytes/errors/drops count in show interface <IF-NAME> and show interface <IF-NAME> queues can have up to 10% deviation. This will manifest mainly when running at line rate with small packet sizes and after a port goes up/down.
Counters (6400 only)	The "Bytes" counter is not supported in show interface <INTERFACE-NAME> queues output.
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.
Dynamic segmentation	Dynamic segmentation does not work with RADIUS server group configured with FQDN. Use IP address configuration.
Flow control (6400 only)	Flow control is not supported.
Line module Hot Swap and Reboot (6400 only)	Concurrent physical hot insert/removal or reboot of a line-module is not supported. Subsequent insert/removal or reboot of a line-module must be initiated only after preceding attempts have been completely processed by the system. For hot insert you must wait until the preceding line-module has reached the "ready" state before inserting subsequent line-modules. For hot removal you must wait until the line-module is no longer present in the system. See the CLI command `show module` for line-module status information. Aruba recommends line-modules be gracefully shut down before removal. Use the CLI config command `module` *<SLOT-ID>* `admin-state [diagnos` administrative state of the line-module.
Multicast and VXLAN	Multicast routing with VXLAN is not supported
Priority queues (6400 only)	A maximum of four (4) priority queues is supported.
RADIUS	Authorization by means of HPE VSAs not supported.
Reduction in TCAM entries (6400 only)	On some line cards, a small number (~200) of TCAM entries are used for internal purposes.
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.
VSX and Static VXLAN (6400 only)	Static VXLAN on VSX configuration is not supported. Use VSX and EVPN or VSX and HSC.
VXLAN	VRRP and VXLAN are mutually exclusive

Feature	Description
VXLAN	No support for IPv6 overlay hosts
VXLAN	IVRL with EVPN enabled VRF is not supported.
VXLAN	EVPN Graceful Restart on HA is not supported

Upgrade information

Version 10.05.0051 uses ServiceOS FL.01.06.0004.

If the switch is configured with message digest for OSPF authentication, after upgrading from 10.04 or 10.03 to 10.05 you will need to configure the message digest authentication key. For example:

Configuration before 10.05 upgrade:

```
ip ospf authentication message-digest
ip ospf authentication-key ciphertext
   AQBapeXp+hujHs0a6E91yqpHTzr0Q7UTPBXD8AzLyOkBL5BuBgAAACLPigGiCw==
```

Configuration to be added after upgrade to 10.05:

```
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 ciphertext
   AQBapeXp+hujHs0a6E91yqpHTzr0Q7UTPBXD8AzLyOkBL5BuBgAAACLPigGiCw==
```

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and this 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.

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.[[[Undefined variable 10-06_RN_variables.FL.10.06.curr]]] or remove the respective entries from ACLs or Class that failed to apply after the upgrade to 10.06.[[[Undefined variable 10-06_RN_variables.FL.10.06.curr]]].

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 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, FL.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.

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

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 FL.10.05.0051 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 FL.10.04 or earlier, upon the first time booting to FL.10.05.0051, a new version of ServiceOS will be installed along with the new BootROM update. On the switch console port an output similar to the following will be displayed as various components are being updated:

```
switch# boot system secondary
Default boot image set to secondary.

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.

4 device(s) need to be updated during the boot process.
The estimated update time is 3 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.
```

```
. . .

Looking for SVOS.

Primary SVOS:  Checking...Loading...Finding...Verifying...Booting...

ServiceOS Information:
    Version:          FL.01.05.0005
    Build Date:       yyyy-mm-dd hh:mm:ss PDT
    Build ID:         ServiceOS:FL.01.05.0005:39e3a582f027:202104151404
    SHA:              39e3a582f0273a97699e51368636a7caea5f8f64

Boot Profiles:

0. Service OS Console
1. Primary Software Image [FL.10.05.0051]
2. Secondary Software Image [FL.10.04.3070]

Select profile(secondary):

4 device(s) need to be updated by the ServiceOS during the boot process.
The estimated update time by the ServiceOS is 3 minute(s).
There may be multiple reboots during the update process.


MODULE 'mc' DEVICE 'svos_primary' :
    Current version  : 'FL.01.05.0005'
    Write-protected  : NO
    Packaged version : 'FL.01.06.0004'
    Package name     : 'svos_talladega'
    Image filename   : 'FL.01.06.0004.svos'
    Image timestamp  : 'Day Mon dd hh:mm:ss yyyy'
    Image size       : 22833451
    Version upgrade needed

Starting update...

Writing...    Done.
Erasing...    Done.
Reading...    Done.
Verifying...  Done.
Reading...    Done.
Verifying...  Done.


Update successful (0.5 seconds).

reboot: Restarting system
```

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.

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.