

AOS-CX 10.06.0100 Release Notes

6100 Switch Series



a Hewlett Packard
Enterprise company

Part Number: 5200-7905a
Published: May 2021
Edition: 2

Copyright Information

© Copyright 2021 Hewlett Packard Enterprise Development LP.

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.

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 PL.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 6100 Switch Series

Important Information

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



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.



AOS-CX 10.06 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
```

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
10.06.0100	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
JL675A	Aruba 6100 48G Class4 PoE 4SFP+ 370W Switch
JL676A	Aruba 6100 48G 4SFP+ Switch
JL677A	Aruba 6100 24G Class4 PoE 4SFP+ 370 Switch
JL678A	Aruba 6100 24G 4SFP+ Switch
JL679A	Aruba 6100 12G Class4 PoE 2G&2SFP+ 139W Switch

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	8.2.12.0
NetEdit	2.0.12
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



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.

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 10.06.0100

Category	Description
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 <code>hh3cifVLANType</code> , <code>dot3StatsDuplexStatus</code> , and <code>dot3StatsTable</code> OIDs.

Version 10.06.0002

Category	Description
Event Log	<p>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.</p> <p>Example:</p> <pre>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 02:00:00:00:02Error 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</pre>

Version 10.06.0001

Category	Description
Access	<ul style="list-style-type: none">Energy Efficient Ethernet (EEE) provides power optimization capability for Ethernet. See the <i>Monitoring Guide</i> for more information.Parallel authentication speeds up authentication by allowing all authentication methods to start concurrently. See the <i>Security Guide</i> for more information.
Accounting	Added support to enable accounting interim update on successful reauthentication and separate accounting mode for RADIUS accounting and local accounting. See the <i>Security Guide</i> for more information.
Enrollment over Secure Transport (EST)	Adds the capability for enabling secure certificate enrollment, allowing for easier enterprise management of PKI. See the <i>Security Guide</i> for more information.

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 10.06.0100

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.
CDP	149252	Symptom/Scenario: An unexpected CDP core dump is found in the output of the <code>show core-dump</code> 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 <code>ip dns host h30326.www3.hpe.com 23.197.193.219</code> , 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 <code>prefix mismatch</code> drop counter gets incremented incorrectly. When a prefix has been configured and sends NA with a non-matching prefix, the <code>NA packets failed ND snooping validation checks</code> 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 <code>new ip</code> option on renewal.
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 <code>show ip igmp snooping</code>

Category	Bug ID	Description
		command does not display in the output of the <code>show tech</code> command. Scenario: IGMP snooping group information is not present in the output of the <code>show tech</code> command.
IP Address	149740	Symptom/Scenario: IP addresses in the form <code>x.y.z.255/31</code> cannot be configured on the switch.
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 <code>BRIDGE-MIB::dot1dTpFdbAddress</code> returns fewer MAC addresses than the <code>show mac-address-table</code> command. Workaround: Unconfigure and reconfigure the SNMP server.
TFTP	150150	Symptom: Copy operation fails with the error <code>curl: (28) TFTP response timeout</code> . Scenario: When attempting to copy a configuration checkpoint to a TFTP server using the <code>blocksize</code> option, the copy fails with the error <code>curl: (28) TFTP response timeout</code> .

Version 10.06.0010

Category	Bug ID	Description
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.

Version 10.06.0002

Category	Bug ID	Description
SNMP	93608	<p>Symptom: The switch reports an incorrect value for the <code>ifSpeed</code> MIB object.</p> <p>Scenario: When a LAG interface has a bandwidth greater than 4.2GB, the switch reports an incorrect value for the LAG interface in the <code>ifSpeed</code> MIB object.</p>

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 10.06.0100

No known issues in this release.

Feature Caveats

Feature	Description
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	Policies containing both MAC and IPv6 classes are not allowed.
CMF	Automatic downgrade of the startup-config is not supported during a software downgrade.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
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.

Upgrade Information

Version 10.06.0100 uses ServiceOS PL.01.07.0004.



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

Performing the upgrade

1. Copy the PL.10.06.0120 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.

```
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
```

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.