AOS-CX 10.08.1021 Release Notes

6300, 6400 Switch Series

a Hewlett Packard Enterprise company

Published: November 2021
Edition: 1

Open Source Code

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

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Notices

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

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

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

Acknowledgments

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

Chapter 1
AOS-CX 10.08 release notes

Description

This release note covers software versions for the AOS-CX 10.08 branch of the software.

If you run the `show version` command on the switch, the version number will display FL.10.08.*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 10.08.0001 is the initial build of major version 10.08 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 10.05.0060 or 10.06.0100 or later (including this release) to implement significant improvements to memory usage and prolong the life of the switch.

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

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.

In this and previous releases, AOS-CX BGP implementations support resolving a BGP route's nexthop to a default route (0.0.0.0/0). However, this is not generally recommended in network deployments. Considering the default route to be the last resort route, resolving the BGP route's nexthop to a default route can cause potential routing loops in the network, if they are not properly designed and monitored. Route flaps and/or traffic drops may be observed in such cases.

In a future release, AOS-CX will not support the BGP route's nexthop resolving to a default route in the Route table. To avoid this problem and to be prepared for the update, Aruba recommends configuring a more specific static route (or host route) for BGP nexthops that are multihops away that are resolving via the default route.

10.06 is the minimum required software version prior to upgrading to 10.08. If your device is using a version of software prior to 10.06, you must first upgrade to a version of 10.06 before upgrading to 10.08. Check release notes for the software version you will upgrade to for instructions on performing the upgrade to 10.06.

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

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00*xx* version of software to 10.08.*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.

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

1. Use the `show checkpoint` command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the `Image Version` column in the output of the command, for example, FL.10.0*x*.*yyyy*).

   

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

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

Industry and government certifications

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

- Common Criteria: https://www.niap-ccevs.org/Product/
- FIPS 140-2: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search
- DoDIN APL: https://aplits.disa.mil/processAPList.action

License written offer

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

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

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

Version history

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

Version number	Release date	Remarks
10.08.1021	2021-11-08	Released, fully supported, and posted on the web.

Version number	Release date	Remarks
10.08.1010	2021-09-21	Released, fully supported, and posted on the web.
10.08.0001	2021-08-13	Initial release of AOS-CX 10.08. 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
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)	10 (Version 12 is not supported)

Internet Explorer is not supported.

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

Management software	Recommended version(s)
Airwave	8.2.13.1
NetEdit	2.1.2
Aruba CX Mobile App	2.6.6 (or later)
Aruba Central	2.5.4 (6400 supports only Template group) (6300 supports both Template and UI groups)
Network Automation	10.10, 10.11, 10.20, 10.21, 10.30, 10.40
Network Node Manager	10.10, 10.20, 10.21, 10.30, 10.40
IMC	7.3 (E0705P12)

For more information, see the respective software manuals.

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

Minimum supported software versions

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

Product number	Product name	Minimum software version
R0X26A	Aruba 6405 Switch	10.04.1000

Product number	Product name	Minimum software version
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

Changes to transceiver support 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.

The number listed with the category is used for tracking purposes.

Version 10.08.1021

Category	Description
CDP 193074	Added the new `cdp mode pre-standard-voice` command to allow the switch to replay back with CDPv2 packets containing the configured voice VLAN when a VoIP VLAN request is received from an attached Cisco phone, allowing the phone to boot properly.

Category	Description
	See Documentation Updates and Corrections for more information.
DHCP Server 187222	Added next-server support for BOOTP options in DHCP server for the client's bootstrap process. This option can be added to the DHCP server option configuration using the next-server command. See Documentation Updates and Corrections for more information.
Forward error correction 201047	**NOTE:** Applies only to the Aruba 6300 Switch Series. Added forward error correction. See Documentation Updates and Corrections for more information.
SNMP 195627	The `hpSwitchPortFdbVidList` MIB OID has been added to display port VLAN membership.
Telnet	Added the ability to manage the switch using Telnet. See Documentation Updates and Corrections for more information.

Version 10.08.1010

Category	Description
Analytics	AIOPS - NAE Agent and Engine improvements for unicast routing. AIOPS - NAE Agent and Engine improvements for client servcies.

Version 10.08.0001

Category	Description
Auto VLAN creation	Automates VLAN creation on access switches for authenticated clients.
BGP	BGP fast-external-failover is now enabled by default.
Device fingerprinting	Support for device fingerprinting collector for CPDI integration, enables visibility of hostname, device type and device OS.
DHCP relay	Added DHCP relay coexistence with DHCP server for both IPv4 and IPv6.
Inclusive terminology	As part of advancing HPE's and Aruba's commitment to racial justice, we are taking a much-needed step in overhauling engineering terminology to reflect our belief system of diversity and inclusion. See https://blogs.arubanetworks.com/spectrum/our-responsibility-to-stand-up-to-racism-and-inequality/ for Aruba's stand on inclusivity.
IP client tracker	Enables IP address visibility of UBT clients for RADIUS accounting.
IP sub-interface	Allows multiple IP addresses on a single routed interface. Supports unicast and multicast routing for both IPv4 and IPv6. Supports OSPF, BGP and PIM for both IPv4 and IPV6. Supported on RoP and L3 lags.
Job Scheduler	Added the ability to execute required CLI commands at a specific time and date. This can be repeated at periodic intervals.

Category	Description
Loopback IP redistribution in OSPF	Allows redistribution of IPv4 and IPv6 addresses of loopback interfaces in OSPFv2 and OSPFv3.
MAC Tables 74408	Added an SNMP trap notification if there is a MAC address change.
MAC Tables 84378	Added the `clear mac` command to delete a specific MAC on one or more VLANs.
Mixed role	Added ability to override role attributes with standard or Vendor Secific Attributes (VSAs). Enabled downloadable GW role, captive portal, and VLAN override.
Multi Domain Authentication	Allows port access for a specified number of voice and data devices.
Network Load Balancing (NLB)	Provides load balancing technology for server clustering developed on Microsoft Windows Server. Supports load sharing and redundancy among servers within a cluster.
Precision Time Protocol (PTP)	Enables precise clock synchronization across distributed devices, needed for time critical applications like AVB and financial systems. Support for transparent clock with end-to-end delay mechanism. (Aruba 6300 Switch Series only)
Private VLAN	Enables traffic isolation for users on the same VLAN. Support for isolated, community, and primary VLANs.
Security	Ensures configuration integrity. Limit concurrent users for web access.
Services on the overlay	Supports RADIUS server over VXLAN for IPv4 and IPv6.
Transceivers 160269	Added display in dBM for DOM thresholds in the output of the `show interface dom detail` command.
Troubleshooting on the overlay	Supports ping over VXLAN for IPv4 and IPv6. Supports traceroute over VXLAN for IPv4 and IPv6.
VSX 162842	**NOTE:** Applies only to the Aruba 6400 Switch Series. Updated the warning message displayed when shutting down an Switch Virtual Interface (SVI) with an active gateway enabled to be more informative about the risks of doing such a shutdown.
VXLAN	VXLAN GBP and Role-based Policies: Enables micro segmentation and role based policies across the VXLAN overlay. Dual VTEP termination and VXLAN GBP relay: Allows stub fabric extender VTEPs to relay VXLAN GBP between static and dynamic VXLAN tunnels.

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 10.08.1021

Category	Bug ID	Description
Accounting	197544	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** Accounting does not start for Port Access clients that transition from Machine Auth to User Auth or when a client goes to unauthorized state and then is re-authorized. **Scenario:** Missing class attribute in the RADIUS accounting packets means ClearPass fails to associate them with the correct Access-Accept and session. **Workaround:** Disable and re-enable the interface using the `shutdown` and `no shutdown` commands to temporarily fix the issue.
Boot	200607	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** The switch displays a kernel panic and reboots. **Scenario:** During a boot, the switch displays a kernel panic and reboots. On the next boot a kernel panic is listed in the boot-history and in the list of coredumps. If watching the boot on a serial console, a hang will be observed during boot and after the ServiceOS prompt has passed, but before getting to the login prompt.
Config Management	163281	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** Validating a switch configuration from within NetEdit fails. **Scenario:** When a configuration contains the line `banner motd #`, an attempt to validate the configuration in NetEdit fails with unexpected errors. **Workaround:** Remove the banner or change the `#` delimiter to a different character such as `@`.
L3 Routes	195719	**Symptom:** Static and dynamic routes are not installed. **Scenario:** After a switch boot or switchover, when using the `show ip route` or `show ipv6 route` commands, no dynamic or static routes are displayed. **Workaround:** Reboot the switch.
L3 Routes	197292	**Symptom:** Route 128.0.0.0/1 is not installed in the routing table. **Scenario:** If BGP/OSPF has learned the route 128.0.0.0/1 from its peer, it will be present in the BGP/OSPF table but is not installed into the routing table RIB (`show ip route`).
Link Aggregation	194007	**Symptom:** The LAG interface is stuck in LACP-block.

Category	Bug ID	Description

		Scenario: When the startup config has a LAG interface configured and the configuration is loaded using the management port, LAG creation fails and a message similar to the following is seen in `/var/log/messages`:
		`2021-08-16T02:11:20.900439+00:00 6300 ip[4566]: 2021-08-16T02:11:20Z|00003|portd_linux_bond|ERR|bond: Failed to create bond lag1 in linux table 0`
		`2021-08-16T02:11:20.900490+00:00 6300 ip[4566]: 2021-08-16T02:11:20Z|00004|portd_tx|ERR|LAG bond lag1 - netdev creation failed in vrf table 0`
		Workaround: Reboot the switch.

Logging	195946	**Symptom:** An error message is logged that says the cron daemon was unable to move a log file because the name is too long. **Scenario:** When the switch hostname contains non-numeric characters, the logrotate feature incorrectly renames the file, causing an error message because the name is too long.
OSPF	194375	**Symptom:** A UBT client is unable to get a DHCP IP address post-authorization or the switch experiences a total traffic loss for already-authorized and working UBT clients. **Scenario:** When a two-member VSF access switch is connected to a VSX core switch with two ROP uplinks (ECMP) to each VSX core switch and OSPF is enabled on both uplinks, if one of the uplinks is flapped from the VSF switch or both uplinks are flapped one after the other in quick succession (less than 30 seconds) or one of the VSX core switches is rebooted, UBT clients are unable to get a DHCP address or the switch experiences a total loss of traffic for already-authorized UBT clients. **Workaround:** Any of these three workarounds can be used: Delete and add the impacted UBT zone configuration. Reboot the VSF switch stack. Configure OSPF interface cost on the VSF switch stack.
PBR	196525	**Symptom:** The switch crashes and a core dump is generated. **Scenario:** Under certain conditions, when a PBR policy is applied to an SVI and checkpoints are saved and restored, a crash occurs and a core dump is generated. **Workaround:** Reboot the switch.
Port Access	196642	**Symptom:** RADIUS applied ACLs have incorrect IP ranges. **Scenario:** When using RADIUS attribute `Filter-Rule` to apply ACLs with IP ranges (CIDR notation) to authenticated clients, the switch may incorrectly translate IP ranges outside the standard classes A, B, and C. **Workaround:** Configure the ACLs with IP ranges on the switch and use RADIUS attribute `Filter-ID` to apply the respective ACL to the authenticated client.
Port Access	200259	**Symptom:** Port access clients do not get authorized and are stuck in an in-progress state. **Scenario:** When the port access policy is configured and the cfg_ version column of the port access policy table is updated to a different number other than the in_progress_version number when the `port-accessd` daemon is not running, port access clients do not get authorized and are stuck in an in-progress state.

Category	Bug ID	Description
		Workaround: Delete and reconfigure the policy configurations.
REST	200118	**Symptom:** User authentication in the Web UI fails. **Scenario:** When using RADSEC as the authentication server, attempts to authenticate in the Web UI fail.
SNMP	195302	**Symptom:** When queried for sysObjectID.0, the switch returns an error, `no such object`. **Scenario:** During a boot of the switch, if AOS-CX is still loading and a query is made for sysObjectID.0, the switch will return an error that the object does not exist. **Workaround:** Wait a few moments for the switch to complete booting and perform the query again.
Spanning Tree	195422	**Symptom:** MAC addresses are not learned, causing a loss in network connectivity. **Scenario:** When a VLAN is removed and re-added for a LAG, the LAG is not seen in the spanning tree list, preventing MAC addresses from being learned and causing a loss in network connectivity. **Workaround:** Remove the VLAN and re-add it, along with the spanning tree instance.
TFTP	194251	**Symptom:** Copying the running or startup config using TFTP with a non-default blocksize fails. **Scenario:** When the `ip source-interface tftp` command has been used on the default VRF, a subsequent attempt to copy the running or startup config to a TFTP server using the default VRF blocksize will fail. **Workaround:** Remove the `ip source-interface tftp` command from the config or do not use the blocksize when copying the configuration file.
VSX Sync	196010	**NOTE:** Applies only to the Aruba 6400 Switch Series. **Symptom:** DHCP server configurations between VSX pairs do not match. **Scenario:** In a VSX topology using `vsx-sync dhcp-server` in the VSX context, the DHCP server configuration fails to copy to the secondary switch. **Workaround:** Turn off the DHCP server configuration sync in the `vsx` context and perform a manual configuration on the secondary switch.
VSX Sync	201013	**NOTE:** Applies only to the Aruba 6400 Switch Series. **Symptom:** The config changes made to the primary switch stop syncing to the secondary switch. **Scenario:** With a large config, after a long time without changes to the config, the `vsx-syncd` daemon becomes unresponsive and changes to the primary are not synced to the secondary. **Workaround:** Restart the `vsx-syncd` daemon.
VXLAN	188001	**Symptom:** The switch fails to import the routing table (RT) for some VRFs. **Scenario:** When a VRF is named with the keyword `mgmt` in the name (for example, `testmgmt` or `mgmt-aps`), the switch fails to import the

Category	Bug ID	Description
		RT to the EVPN table. **Workaround:** Rename the VRF to remove the `mgmt` keyword.

Version 10.08.1010

Category	Bug ID	Description
802.1X	192424	**Symptom:** The port-access daemon crashes when an 802.1X supplicant attempts to authenticate. **Scenario:** When an 802.1X supplicant responds with an empty identity in response to an EAP request/identity message from the switch, the port-access daemon on the switch crashes. **Workaround:** Configure the supplicant to send a non-empty identity.
ACLs	193057	**Symptom:** The switch crashes when a VLAN ACL is configured using REST. **Scenario:** When REST is used to configure a VLAN ACL using `in` rather than `routed-in`, the switch crashes.
Boot	190850	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** A VSF member switch times out during boot and displays a failure message. **Scenario:** When the VSF master takes longer than expected to boot or has a misconfiguration or a hardware problem on the VSF ports, VSF member switches time out and display a failure message indicating a possible credential or security issue: Failure - management/VSF role decision pending. [OK] Started Boot failure triage. [FAILED] Failed to start HPE Credential Manager. See 'systemctl status hpe-credmgr.service' for details.
Counters	192225	**Symptom:** The switch counts CRC errors and runt packets rather than reporting collisions properly. **Scenario:** When the switch partner operates in HDx mode, downlink ports suffer from a duplex mismatch, resulting in collisions being counted as CRC errors and runt packets.
Counters	192677	**Symptom:** The switch reports collision errors or collision error counters increment incorrectly. **Scenario:** If the switch is operating at half duplex and traffic is sent at a 90% or greater line rate, TX PFC priorities 1-6 may report values that correspond with collision errors. If the switch is operating at full duplex on uplinks where PFC is enabled and traffic requiring PFC frames is sent through the iterface, collision error counters increase along with TX PFC priorities 4 and 5.
Event Logs	188421	**Symptom/Scenario:** A warning similar to `Excessive write to coredump partition in module 1/2 observed. 7.07GB written over past 1 hour` is logged in the event log.

Category	Bug ID	Description
		Workaround: The message is due to incorrect reporting and does not indicate an actual problem.
IGMP	194105	**NOTE:** Applies only to the Aruba 6400 Switch Series. **Symptom:** Multicast stream does not work with Internet Protocol televisions (IPTVs) connected to slot number 12. **Scenario:** When the network is configured with multicast source and receivers connected in the same VLAN, IPTVs connected to slot 12 of the chassis do not receive multicast streams. **Workaround:** Move the IPTVs to a slot other than 12.
Interfaces	190053	**Symptom/Scenario:** Devices negotiated to 10BASE-T half duplex intermittently drop links.
Internal Service	191456	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom/Scenario:** On rare occasions, VSF links may not be unblocked quickly enough on members during VSF initialization, causing VSF members to miss getting a response from the master, resulting in the switch booting as a one member VSF stack. **Workaround:** Reboot the VSF members that failed to join the stack.
Logging	195946	**Symptom:** An error message is logged that says the cron daemon was unable to move a log file because the name is too long. **Scenario:** When the switch hostname contains non-numeric characters, the logrotate feature incorrectly renames the file, causing an error message because the name is too long.
OVSDB	193273	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** The OVSDB server crashes, resulting in a switch reboot. **Scenario:** When the switch is connected to multiple access points running traffic, the OVSDB server may crash, resulting in a switch reboot.
PIM-SM	190657	**Symptom/Scenario:** The switch does not elect the correct BSR after changing the BSR priority or changing to auto RP from static RP. **Workaround:** Configure the candidate BSR on only one note of the VSX environment or toggle the router PIM status using the `router pim disable` and `router pim enable` commands.
PoE	165619, 176530	**Symptom/Scenario:** Ubiquity powered device UniFi AP HD does not power up when connected to a PoE class-6 switch even though it does power up when connected to a PoE class-4 switch.
Port Access	161484	**Symptom:** The port access daemon crashes with the following log message: `debug|LOG_EMERG|CDTR|1|PORTACCESS|PORTACCESS_ SERVICES|DB operation failed for Secure MAC. Event|1201|LOG_CRIT|AMM|1/1|port-accessd crashed due to signal:6` **Scenario:** When the port-access client moves from one VSX peer to another VSX peer, without first logging off the port-access client on the older port, the port access daemon crashes. **Workaround:** Perform the port-access client log-off manually

Category	Bug ID	Description
		before theclient starts moving.
Port Access	196642	**Symptom:** RADIUS applied ACLs have incorrect IP ranges. **Scenario:** When using RADIUS attribute `Filter-Rule` to apply ACLs with IP ranges (CIDR notation) to authenticated clients, the switch may incorrectly translate IP ranges outside the standard classes A, B, and C. **Workaround:** Configure the ACLs with IP ranges on the switch and use RADIUS attribute `Filter-ID` to apply the respective ACL to the authenticated client.
RADIUS	195419	**Symptom:** A disconnect request is rejected with error `session-context-not-removable`. **Scenario:** When concurrent onboarding is enabled on a port and a disconnect request is received after a lower auth-priority method is successful and a higher -auth-priority method is still in progress, the disconnect request is rejected. The default auth-priority levels with concurrent onboarding is `dot1x` followed by `macauth`. **Workaround:** Set the preferred auth method to be a higher priority. For example, if macauth is the preferred method, run the `aaa authentication port-access auth-priority mac-auth dot1x` command.
SNMP	189372	**Symptom:** `dot1dStpPortPathCost` reflects the open-path-cost and does not match the CLI. **Scenario:** When using SNMP to identify spanning tree state and values, `dot1dStpPortPathCost` does not report the value it should. **Workaround:** Use the `show spanning-tree` command to view the correct values.
SNMP	189953	**Symptom/Scenario:** snmpget returns an error message of `Unsupported security level`. **Workaround:** Reboot the switch.
TACACS	194803	**Symptom:** The user is authenticated as local rather than remote (TACACS). **Scenario:** When the TACACS server is configured with FQDN and TACACS authentication is configured, the user is authenticated with local credentials instead of with remote TACACS authentication. **Workaround:** Configure the TACACS server with an IP address rather than FQDN.
Temperature	192845	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** The switch fans unexpectedly spin at maximum speed. **Scenario:** When an inlet air sensor failure occurs, the sensor is marked with a fault and the fans spin at maximum speed.
UBT	189682	**Symptom:** After a client is logged off or aged out, the client is not able to get onboarded on the same port. **Scenario:** This condition can occur in two different cases: 1.When the client has a pre-auth role configured with UBT zone, during a switch reboot if the UBT daemon takes time to update the UBT VLAN in the VLAN table, the client will experience this issue. 2. Clients on boarded without configuring the UBT VLAN can also

Category	Bug ID	Description
		experience this issue. **Workaround:** For case 1, restart the port-accessd daemon. For case 2, configure the UBT VLAN before triggering traffic from the client and restart the port-accessd daemon if any clients are already in this state after configuring the UBT VLAN.
VLAN	191196	**Symptom/Scenario:** On trunk ports, once VLAN translation is configured, traffic is allowed only for translated VLANs with native VLAN and other trunk member VLANs dropping traffic.
VSF	194135	**Symptom:** Users can log mistakenly log into the VSF master switch using local credentials. **Scenario:** When accessing the VSF master which is protected with TACACS from a VSF member with local credentials rather than TACACS credentials, the user is able to gain access.
VSX Sync	193962	**NOTE:** Applies only to the Aruba 6400 Switch Series. **Symptom:** VSX sync stops working. Logs still show activity in the secondary VSX sync, but no updates are received from the primary switch. **Scenario:** In a VSX topology when both switches become disconnected (for example, through an ISL disconnect or a failover) for an extended period of time, VSX sync stops working when the switches come back online. **Workaround:** On the secondary switch, restart VSX sync using the `systemctl restart vsx-syncd` command.

Version 10.08.0001

Category	Bug ID	Description
ARP	191536	**Symptom/Scenario:** When the switch is rebooted with an SVI shutdown, if the IP address is changed and the SVI re-enabled, the old VLAN IP address still replies to an ARP request received. **Workaround:** Delete and then add back the SVI.
BSP	95761	**NOTE:** Applies only to the Aruba 6400 Switch Series. **Symptom/Scenario:** The line module fails to boot after an FPGA update has been interrupted.
Config Management	191612	**Symptom:** Copying a configuration file to startup either fails or completes but does not configure everything defined in it. **Scenario:** When copying a configuration file that uses windows style CRLF (`\r\n`) to the startup config, it either fails or completes but does not configure everything defined in it. **Workaround:** Change the file line endings to UNIX format (`\n`)
Credential Manager	94938	**Symptom:** During boot, the following message is observed, after which the features to not function: `----------`

Category	Bug ID	Description
		... ... [OK] Starting HPE Credential Manager. ... ... [FAILED] Failed to start HPE Credential Manager. See 'systemctl status hpe-credmgr.service' for details. [DEPEND] Dependency failed for Halon NTP Helper Daemon. [DEPEND] Dependency failed for Radius Server Tracking Daemon. [DEPEND] Dependency failed for Port Access Security Daemon. [DEPEND] Dependency failed for Captive Portal daemon. [DEPEND] Dependency failed for TACACS+ Server Tracking Daemon. [DEPEND] Dependency failed for IPsec Configurator Module Daemon. [DEPEND] Dependency failed for Tunneled Node Daemon. [OK] Stopped HPE Credential Manager. Starting HPE Credential Manager. ... ... ---------- **Scenario:** If the startup config is large and takes an extensively long time to load or in a VSF environment if members must wait an excessively long time for the conductor to come up or if a hardware failure delays or blocks the VSF role determination for an excessive amount of time, an error message displays during boot and various features do not function after boot. **Workaround:** If there is no hardware defect, a power cycle of the switch or entire VSF stack typically resolves the issue.
Diagnostics	173341	**Symptom/Scenario:** The `IPtraf` diagnostic utility does not work.
Interfaces	177432	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** An interface is set as available for receiving traffic before it is ready, causing an issue for internal VLANs used by the ports that belong to a LAG. **Scenario:** After an event related to system reboot, for example an image upgrade or switchover, the OSPFv2/v3 sessions do not resume, causing traffic to not flow through the network. **Workaround:** Perform the following steps: 1. Remove the LAG from the LAG member ports (physical interfaces). 2. Shut down the physical interfaces. 3. Add the physical interfaces back to the LAG. 4. Enable the physical interfaces using the `no shutdown` command.

Category	Bug ID	Description
L3 Addressing	164817	**Symptom/Scenario:** The SNMP MIB OID `IP-FORWARD-MIB::inetCidrRouteIfIndex` returns an invalid output.
L3 Addressing	174746	**Symptom:** Packets entering a tunnel trigger an MTU violation; however, the violation does not trigger an ICMP message as expected. **Scenario:** When large MTU packets enter a tunnel with a smaller MTU, the packets trigger an MTU violation that does not trigger the expected ICMP message from the switch back to the sender. **Workaround:** Use statically configured MTU rather than PMTU discovery when using tunnels.
L3 Routes	159221	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** Traffic is not forwarded on some routes or routes experience slow forwarding with a log message similar to `switchd_agent[9044]: debug|LOG_ERR|LC|1/5|L3|L3_ASIC|Hardware Route, create failed for prefix: ....` **Scenario:** The route forwarding engine has six tables to hold "common" prefixes and a "best match" table to hold all the rest. If the local site network makes heavy use of prefixes not hard-coded as "common" prefixes, the "best match" table can run out of space. Once the tables are full, additional prefixes in the tables fail to forward or forward very slowly. **Workaround:** Renumber the network to fit into the per-prefix capacities of the switch.
L3 Routes	78485	**NOTE:** Applies only to the Aruba 6300 Switch Series. **Symptom:** A VXLAN packet is encapsulated in the wrong VLAN. **Scenario:** When the switch is configured with a VXLAN VNI to VLAN mapping for VLAN x and a packet is received for another VLAN (VLAN y), the VXLAN packet is encapsulated in the wrong VLAN.
MAC Tables	86543, 154852, 159156, 190398	**NOTE:** Applies only to the Aruba 6400 Switch Series. **Symptom:** Traffic in a VSX pair is dropped. **Scenario:** When a VSX pair is in VRRP BACKUP/BACKUP mode, traffic using VRRP MAC as the destination MAC that hits the VSX pair will be dropped.
Port Access	188042	**Symptom:** Clients fail to onboard and the error `Failed to apply Port Access Policy` is seen in the log. **Scenario:** When the `port-access onboard-method precedents device-profile aaa` command is executed and clients logoff and attempt to login again, the clients fail to onboard and an error is logged. **Workaround:** Reboot the line card where the port-access policy failed to apply.
sFlow	151822	**Symptom:** The sFlow sampled packets from a LAG contain the ifIndex of the member port instead of the LAG itself. **Scenario:** When sFlow sampling is enabled on a LAG interface, the sFlow sampled packets from the LAG contain the ifIndex of the member port rather than the ifIndex of the LAG.
VSF	91074	**NOTE:** Applies only to the Aruba 6300 Switch Series.

Category	Bug ID	Description
		Symptom: Unable to log into the CLI of stack members. **Scenario:** After a series of continuous reboots lasting about 15 hours of a member of the stack, users are unable to log into the CLI of that member and logging into the master switch is delayed. **Workaround:** Power cycle the entire stack.

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 10.08.1021

Category	Bug ID	Description
EVPN	173356	**Symptom/Scenario:** Attribute values on EVPN routes reset to default after a VXLAN flap. **Workaround:** Clear BGP using the `clear bgp *` command.
EVPN	174088	**Symptom/Scenario:** The configured value for the BGP default local preference is not carried over EVPN routes. **Workaround:** Inject the local preference from the non-EVPN fabric neighbor using the `route-map` command.
OSPF	149301	**Symptom:** The switch shows unexpected behavior in the OSPFv2/3 DLOGs. **Scenario:** When `debug ospfv2 packet` or `debug ospfv3 packet` is enabled with the `ip` filter, the switch shows unexpected behavior in the OSPFv2/3 DLOGs. **Workaround:** Use `debug ospfv2 packet` or `debug ospfv3 packet` with the `port` filter and grep for the required IP (v4 or v6) address.
OSPF	160179	**Symptom/Scenario:** ARB does not inject the default route in a Totally Stubby Area with loopback in Area 0.0.0.0. **Workaround:** Assign one or more physical interfaces to Area 0.0.0.0.
Port Access	156628	**Symptom:** The `port-access` daemon crashes. **Scenario:** When port security is enabled on a port where the `port-security client-limit` is configured with a value lower than the number of the port-security static clients configured on the port, after a downgrade from 10.07 to 10.05 or 10.06 the `port-access` daemon crashes. **Workaround:** Prior to the downgrade, set the port-security limit configuration to a value equal to or higher than the number of static port-security clients configured on the port.

Feature Caveats

Feature	Description
ACLs	**NOTE:** Applies only to the Aruba 6300 Switch Series. In a VSF stack, the swtich may fail to log events for the matching access-list entries. ACL functionality is not impacted; access-list entries are applied properly and only the logging is incorrectly generated.
Aruba CX Mobile App	**NOTE:** Applies only to the Aruba 6300 Switch Series. VSF stack formation is blocked when there are reserved autojoin interfaces (25, 26, 49, 50) in the stack topology.

BGP	In a multi-VRF environments, while performing mutual route leaking on the VRRP peers with BGP neighborship established in between and towards the upstream network, the switch will install both routes as ECMP instead of preferring the leaked route. Use route-maps to give lower/higher preference to the routes received from an iBGP peer. For example:
	`!`
	`route-map rmap permit seq 10`
	`  set local-preference 50`
	`!`
	`router bgp 100`
	`  vrf red`
	`  neighbor 1.1.1.2 remote-as 100`
	`  address-family ipv4 unicast`
	`  neighbor 1.1.1.2 activate`
	`  neighbor 1.1.1.2 route-map rmap in`
	`  exit-address-family`
	In the above example, since a lower value of local-preference (i.e. 50, whereas default value is 100) has been set to the routes received from iBGP peer, the leaked routes get preferred and get installed as best routes.

Classifiers	For Classifier policy modifications to be secure, Aruba strongly encourages modifications be done as a three-step process: Bring down the port, modify, and bring the port back up.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	Automatic downgrade of the startup–config is not supported during a software downgrade. To restore a configuration use the procedure documented under Manual configuration restore for software downgrade.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
Counters (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 <IF-NAME>` queues output.
DHCP Server, DHCP Relay, and DHCP Snooping	DHCP Relay and DHCP Snooping can 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.

Feature	Description
Dynamic segmentation	Dynamic segmentation does not work with RADIUS server group configured with FQDN. Use IP address configuration.
EVPN	iBGP split-horizon rule is not followed between different address families. Use route-map to block the routes getting advertised to the iBGP peer.
Flow control (6400 only)	Flow control is not supported.
ICMP Redirect	The switch may only software forward 100pps IP frame that trigger ICMP redirect.
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 [diagnostic | down | up]` to change the administrative state of the line-module. Line module reboot and hot removal is not a hitless operation. Up to 2 seconds of traffic loss may be expected when any module is rebooted or removed from the system. Hot insert does not result in any traffic loss.
Multicast and VXLAN	ROP extension for VSX border leaf for clients is not supported. VXLAN must be configured prior to configuring VSX. Distributed Anycast Gateway is not supported (same IP address for SVI and AG). IPv6 multicast is not supported for VXLAN overlay. Multicast support for static VXLAN in the overlay has limited support. Contact Aruba Support for details. Multicast traffic with a Null Source IP (0.0.0.0) gets flooded.
Priority queues (6400 only)	A maximum of four (4) priority queues is supported.
RADIUS	Authorization by means of HPE VSAs is 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.
RIP/RIPng	Redistribute RIP/RIPng is not supported in BGP/BGP+.
RIP/RIPng	RIP/RIPng metric configuration support is not available.
SFTP	When the path to the SFTP server crosses segments with different MTU frame sizes, file transfers will fail. Configure the same MTU on all nework segments on the path to the SFTP server to use SFTP to transfer files.
Sub-interface	BFD is not supported on a sub-interface. For multicast support on a sub-interface: 1. When ROP/Sub-interface as uplink is used towards multicast source, a

Feature	Description
	PIM enabled point-to-point Transit VLAN over ISL between VSX devices should be added to ensure an alternate path to reach upstream multicast source. This Transit VLAN is not carried on VSX LAGs. (A dedicated point-to-point link between VSX primary and secondary can also be used.) 2. PIM Active/Active configuration is recommended for multicast clients connected to downstream VSX LAGs. PIM active/active does not provide DR redundancy for upstream receivers connected over ROP or sub-interfaces (i.e. multicast traffic impact when DR fails) 3. Anycast RP with MSDP is recommended. For BSR/C-RP, a PIM peering over point-to-point Transit VLAN between VSX devices is needed. In case of BSR/C-RP, convergence time is higher than Anycast RP configuration when active RP fails. 4. If KA is used for the P2P sub-interface link, KA has to be in a different VRF.
Tunnels	When configuring tunnels (VXLAN/IP tunnels) with the underlay as a static route, the next-hop IP should be an SVI or ROP IP and not configured as the Active-Gateway.
VRF	VRF names are limited to 31 characters.
VRRP-MD5 authentication interop	Not supported with Comware-based switches
VRRP	VRRP Preemption Delay Timer (preempt delay minimum) may be ignored after a switch reboot or power cycle.
VRRP and VXLAN	VRRP and VXLAN are mutually exclusive.
VSX and Static VXLAN (6400 only)	Static VXLAN on VSX configuration is not supported. Use VSX and EVPN or VSX and HSC.

Upgrade information

Version 10.08.1021 uses ServiceOS FL.01.09.0002.

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00*xx* version of software to 10.08.*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 10.08.1021 or remove the respective entries from ACLs or Class that failed to apply after the upgrade to 10.08.1021.

When upgrading from a version of software prior to version 10.05.0001, if the switch is configured with IGMP or MLD snooping options such as "forward", "fastleave", "forced-fastleave", or "blocked" at the VLAN context, after upgrading to this software version, you will need to reconfigure these options for each interface from the interface configuration context.
Example config before 10.05.0001:

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

Example config to be added after upgrade to this software version:

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

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

Manual configuration restore for software downgrade

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

1. Use the `show checkpoint` command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the `Image Version` column in the output of the command, for example, FL.10.0*x*.*yyyy*).

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

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

Performing the upgrade

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

1. Copy the new image into the non-current boot bank on the switch using your preferred method.
2. Depending on the version being updated, there may be device component updates needed. Preview any devices updates needed using the `boot system <BOOT-BANK>` command and entering `n` when asked to continue.

   For example, if you copied the new image to the secondary boot bank and no device component updates are needed, you will see this:

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

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

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

   In this example, 3 device updates will be made upon reboot, one of which is a non-failsafe device:

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

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

2 device(s) need to be updated during the boot process.
The estimated update time is between 2 and 3 minute(s).
```

```
There may be multiple reboots during the update process.

1 non-failsafe device(s) also need to be updated.
Please run the 'allow-unsafe-updates' command to enable these updates.

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

3. When ready to update the system, if a non-failsafe device update is needed, make sure the system will not have any power interruption during the process. Invoke the `allow unsafe updates` command to allow updates to proceed after a switch reboot. Proceed to step 4 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

    Unsafe updates      : allowed (less than 30 minute(s) remaining)
```

4. Use the `boot system <BOOT-BANK>` command to initiate the upgrade. 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.
Checking if the configuration needs to be saved...

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

3 device(s) need to be updated during the boot process.
The estimated update time is between 2 and 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:          <serviceOS_number>
    Build Date:       yyyy-mm-dd hh:mm:ss PDT
    Build ID:         ServiceOS:<serviceOS_number>:6303a2a501ba:202006171659
    SHA:              6303a2a501bad91100d9e71780813c59f19c12fe

Boot Profiles:

0. Service OS Console
1. Primary Software Image [xx.10.07.0030]
2. Secondary Software Image [xx.10.08.1021]

Select profile(secondary):

ISP configuration:
    Auto updates        : enabled
    Version comparisons : match (upgrade or downgrade)
    Unsafe updates      : allowed (less than 29 minute(s) remaining)

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

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


MODULE 'mc' DEVICE 'svos_primary' :
    Current version  : '<serviceOS_number>'
    Write-protected  : NO
    Packaged version : '<version>'
    Package name     : '<svos_package_name>'
    Image filename   : '<filename>.svos'
    Image timestamp  : 'Day Mon dd hh:mm:ss yyyy'
    Image size       : 22248723
    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 may be updated and several reboots will be triggered during these updates. When all component updates are completed, the switch console port will arrive at the login prompt with a display similar to following:

```
(C) Copyright 2017-2021 Hewlett Packard Enterprise Development LP

                    RESTRICTED RIGHTS LEGEND
```

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

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

switch login:
```

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

Documentation Updates and Corrections

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

Version 10.08.1021

This version introduces:

- CDP-compatible voice VLAN discovery. This content will be included in a future edition of the *Fundamentals Guide* in the "Device discovery and configuration" chapter.
- DHCP Server `next-server`. This content will be included in a future edition of the *IP Services Guide* in the "DHCP" chapter.
- Telnet access for the switch. This content will be included in a future edition of the *Fundamentals Guide* in the "Initial configuration" chapter.
- Forward error correction (FEC). This content will be included in a future edition of *Fundamentals Guide* in the "Interface configuration" chapter.

cdp mode pre-standard-voice

```
cdp mode pre-standard-voice {tx-rx | rx-only | disable}
```

Description

Enables CDP-compatible voice VLAN discovery with pre-standard VoIP phones.

Parameter	Description
`tx-rx`	Sets transmit and receive mode. The switch replies with continuous voice VLAN packets every 60 seconds.
`rx-only`	Sets receive mode. The switch replies with a voice VLAN packet on reception of a query.
`disable`	Disables the pre-standard-voice mode. The switch does not send any CDP reply message when this is set.

Command History

Release	Modification
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	`config-if`	Administrators or local user group members with execution rights for this command.

next-server

```
next-server <IP-ADDR>
no next-server <IP-ADDR>
```

Description

Configures the address of the server to use in the next step of the client bootstrap process. A DHCP server may return its own address in the `siaddr` (TFTP server IP address) field, if the server is prepared to supply the next bootstrap service. If `siaddr` is a TFTP server address other than DHCP Server address then the next-server address needs to be configured.

The `no` form of this command removes the configured next-server.

Examples

Configure a DHCP server on a VRF named **RED** with a pool named **test** and the next-server with IP address **10.0.0.10**:

```
switch(config)# dhcp-server vrf RED
switch(config-dhcp-server)# pool test
switch(config-dhcp-server-pool)# next-server 10.0.0.10
```

Parameter	Description
<IP-ADDR>	Specifies the next-server IP address.

Command History

Release	Modification
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	`config-dhcp-server-pool`	Administrators or local user group members with execution rights for this command.

Telnet access

Telnet server enables switches to accept Telnet connections from clients to manage the switch. The user authentication is password based authentication (RADIUS, TACACS+ or locally stored password). The server can be implemented on any VRF using the `telnet server` command. The maximum number of sessions per VRF is five (5).

In the default configuration, Telnet access is disabled.

Telnet commands

show telnet server

```
show telnet server
```

Description

Displays the Telnet server configuration.

Examples

Display the Telnet server configuration on the switch:

```
switch(config)# show telnet server

TELNET Server Configuration:

    IP Version        : IPv4
    TCP Port          : 23
    Enabled VRFs      : default, vrf1, vrf2,
                        red, green
```

Command History

Release	Modification
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

show telnet server sessions

```
show telnet server sessions [vrf <VRF-NAME> | all-vrfs]
```

Description

Displays all active Telnet sessions for the specified VRF or all VRFs. If no VRF is provided, the session on the `default` VRF is shown.

Parameter	Description
`vrf <VRF-NAME>`	Specifies the Telnet sessions for a specific VRF.
`all-vrfs`	Specifies the Telnet sessions for all VRFs

Examples

Display the Telnet session on the `default` VRF:

```
switch(config)# show telnet server sessions

TELNET sessions on VRF default:

    IPv4 TELNET Sessions:
        Server IP        : 10.1.1.1
        Client IP        : 10.1.1.2
        Client Port      : 58835
```

Display the Telnet session on all VRFs:

```
switch(config)# show telnet server sessions all-vrfs

TELNET sessions on VRF mgmt:

    IPv4 TELNET Sessions:
        Server IP        : 10.1.1.1
        Client IP        : 10.1.1.2
        Client Port      : 58835

TELNET sessions on VRF default:
    IPv4 TELNET Sessions:
        Server IP        : 20.1.1.1
        Client IP        : 20.1.1.2
        Client Port      : 58837
```

Command History

Release	Modification
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

telnet server

```
telnet server vrf <VRF-NAME>
no telnet server vrf <VRF-NAME>
```

Description

Enables the Telnet server on the desired VRF. Telnet is disabled by default.

The `no` form of this command disables the Telnet server.

Parameter	Description
`vrf <VRF-NAME>`	Specifies the VRF on which the Telnet server will be enabled.

Examples

Configuring the Telnet server on the `mgmt` VRF:

```
switch(config)# telnet server vrf mgmt
```

Command History

Release	Modification
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

Forward error correction

Forward error correction (FEC) is used to control errors in transmissions where the source sends redundant data and the destination only recognizes the data portion that contains no apparent errors. FEC does not require a handshake between the source and destination at the cost of a higher forward channel bandwidth. It is therefore best used in scenarios where re-transmissions are costly or impossible, such as using multicast one-way communication.

error-control

Applies only to the Aruba 6300 Switch Series.

```
error-control {auto | none | base-r-fec | rs-fec}
no error-control {auto | non | base-r-fec | rs-fec}
```

Description

Configures the forward error correction (FEC) mode to use for an interface. When not configured, the system will automatically select the FEC mode based on the installed transceiver. In most cases, the standard FEC mode will work best, but certain link partners may require a non-standard mode.

The `no` and `auto` forms of this command configure the interface to automatically use the standard FEC mode of the currently installed transceiver.

FEC configuration only applies to 25G transceivers. The default for the installed transceiver is used in all other cases.

Transceivers for which FEC is auto-negotiated will request the mode configured by this command, but may resolve to a different mode.

Parameter	Description
`auto`	Use the transceiver default.
`none`	Do not use any FEC.
`base-r-fec`	Use IEEE Clause 74 BASE-R (Firecode) FEC.
`rs-fec`	Use IEEE Clause 91 RS (Reed-Solomon) FEC.

Command History

Release	Modification
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300	`config-if`	Administrators or local user group members with execution rights for this command.

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.