AOS-CX 10.14.0001 Release Notes

8100, 8360 Switch Series

May 2024
Edition: 1

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 10.14.0001 Release Notes

This release applies to the 8100 and 8360 Switch Series. The following table lists any applicable minimum software versions required for that model of switch.

If your product is not listed in the below table, no minimum software version is required.

Product number	Product name	Minimum software version
R9W94A	Aruba 8100 24x10G SFP+ 4x40/100G QSFP28 switch	10.12.0001
R9W95A	Aruba 8100 24x10G Base-T 4x10G SFP+ 4x40/100G QSFP28 switch	10.12.0001
R9W96A	Aruba 8100 48x10G SFP+ 4x40/100G QSFP28 switch	10.12.0001
R9W97A	Aruba 8100 40x10G Base-T 8x10G SFP+ 4x40/100G QSFP28 switch	10.12.0001

Product number	Product name	Minimum software version
JL700A	Aruba 8360-32Y4C with MACSec Port to Power 3 Fans 2 PSU Bundle	10.06.0001
JL701A	Aruba 8360-32Y4C with MACSec Power to Port 3 Fans 2 PSU Bundle	10.06.0001
JL702A	Aruba 8360-16Y2C Port to Power 3 Fans 2 PSU Bundle	10.06.0001
JL703A	Aruba 8360-16Y2C Power to Port 3 Fans 2 PSU Bundle	10.06.0001
JL706A	Aruba 8360-48XT4C Port to Power 3 Fans 2 PSU Bundle	10.06.0001
JL707A	Aruba 8360-48XT4C Power to Port 3 Fans 2 PSU Bundle	10.06.0001
JL708A	Aruba 8360-12C Port to Power 3 Fans 2 PSU Bundle	10.06.0001
JL709A	Aruba 8360-12C Power to Port 3 Fans 2 PSU Bundle	10.06.0001
JL710A	Aruba 8360-24XF2C Port to Power 3 Fans 2 PSU Bundle	10.06.0001
JL711A	Aruba 8360-24XF2C Power to Port 3 Fans 2 PSU Bundle	10.06.0001
JL700C	Aruba 8360-32Y4C v2 32p 25G SFP/+/28 4 Sec 4p 100G QSFP+/28 Front-to-Back 3 Fans 2 AC Bdl	10.09.1000

Product number	Product name	Minimum software version
JL701C	Aruba 8360-32Y4C v2 32p 25G SFP/+/28 4 Sec 4p 100G QSFP+/28 Back-to-Front 3 Fans 2 AC Bdl	10.09.1000
JL702C	Aruba 8360-16Y2C v2 16p 25G SFP/SFP+/SFP28 2p 100G QSFP+/28 Front-to-Back 3 Fans 2 AC Bdl	10.09.1000
JL703C	Aruba 8360-16Y2C v2 16p 25G SFP/SFP+/SFP28 2p 100G QSFP+/28 Back-to-Front 3 Fans 2 AC Bdl	10.09.1000
JL706C	Aruba 8360-48XT4C v2 48p 1G/10GBase-T 4p 100G QSFP+/28 Front-to-Back 3 Fans 2 AC Bundle	10.09.1000
JL707C	Aruba 8360-48XT4C v2 48p 1G/10GBase-T 4p 100G QSFP+/28 Back-to-Front 3 Fans 2 AC Bundle	10.09.1000
JL708C	Aruba 8360-12C v2 12-port 100G QSFP+/QSFP28 Front-to-Back 3 Fans 2 AC Bundle	10.09.1000
JL709C	Aruba 8360-12C v2 12-port 100G QSFP+/QSFP28 Back-to-Front 3 Fans 2 AC Bundle	10.09.1000
JL710C	Aruba 8360-24XF2C v2 24p 10G SFP/SFP+ 2p 100G QSFP+/28 Front-to-Back 3 Fans 2 AC Bundle	10.09.1000
JL711C	Aruba 8360-24XF2C v2 24p 10G SFP/SFP+ 2p 100G QSFP+/28 Back-to-Front 3 Fans 2 AC Bundle	10.09.1000
JL704C	Aruba 8360-48Y6C v2 48p 25G SFP/+/28 4 Sec 6p 100G QSFP+/28 2 Sec Frnt-to-Bck 5 Fans 2 AC Bdl **NOTE:** Support for 50G introduced in AOS-CX 10.09.1000	10.09.0001
JL705C	Aruba 8360-48Y6C v2 48p 25G SFP/+/28 4 Sec 6p 100G QSFP+/28 2 Sec Bck-to-Frnt 5 Fans 2 AC Bdl **NOTE:** Support for 50G introduced in AOS-CX 10.09.1000	10.09.0001
JL719C	Aruba 8360-48Y6C v2 48p 25G SFP/SFP+/SFP28 4 Sec 6p 100G QSFP+/QSFP28 2 Sec Switch **NOTE:** Support for 50G introduced in AOS-CX 10.09.1000	10.09.0001
JL718C	Aruba 8360-16Y2C v2 16-port 25G SFP/SFP+/SFP28 2-port 100G QSFP+/QSFP28 Switch	10.09.1000

Product number	Product name	Minimum software version
JL717C	Aruba 8360-32Y4C v2 32-port 25G SFP/SFP+/SFP28 4 Sec 4-port 100G QSFP+/QSFP28 Switch	10.09.1000
JL720C	Aruba 8360-48XT4C v2 48-port 1G/10GBase-T 4-port 100G QSFP+/QSFP28 Switch	10.09.1000
JL722C	Aruba 8360-24XF2C v2 24-port 10G SFP/SFP+ 2-port 100G QSFP+/QSFP28 Switch	10.09.1000
JL721C	Aruba 8360-12C v2 12-port 100G QSFP+/QSFP28 Switch	10.09.1000

Important information for 8100 and 8360 Switches

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 10.06.0100 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.

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.

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 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 10.11.0001, the command **route recursive-lookup default-route** has been introduced under the **vrf** context to support BGP route's nexthop resolving to a default route in the Route table. This command is enabled by default.

For information about Short Supported Releases (SSRs) and Long Supported Releases (LSRs), see https://www.arubanetworks.com/support-services/end-of-life/arubaos-software-release/.

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

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 HPE Aruba Networking, unless noted in the table.

Version number	Release date	Remarks
10.14.0001	21 May 2024	Initial release.

The switch web agent supports the following web browsers:

Browser	Minimum supported versions
Edge (Windows)	41
Chrome (Ubuntu)	76 (desktop)
Firefox (Ubuntu)	113
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)
NetEdit	2.11.0
Aruba Central	2.5.8
Aruba Fabric Composer	7.0.2
Aruba CX Mobile App	Support for version 2.9.3 or later.
IMC	(708P03)(8360-V2 not supported)

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.

Enhancements for 8100 and 8360 Switches in AOS-CX 10.14.0001

This section describes the enhancements introduced in this release.

Category	Description
ARP Security	AOS-CX 10.14 supports additional event log messages that allow network admins to see on which port ARP packets are getting dropped when the ARP packets are getting dropped with valid reason.
EVPN	EVPN routes can be matched against additional **evpn-type** values: ▪ evpn-type-2 MAC/IP Advertisement Route ▪ evpn-type-3 Inclusive Multicast Ethernet Tag Route ▪ evpn-type-5 IP Prefix route
Classifier	In previous releases, the ACL Logging text could display a value of **unknown** for either the sequence number or the list type. This issue could occur if an ACL is configured with the **log** keyword *and* the switch is are using QoS or VSX features. Starting with AOS-CX 10.14.0001, the logging message includes source and destination addresses and protocol. The **unknown** value no longer appears if there is no sequence number to display.
Overlay Fabric	Multicast inter-VXLAN L2 bridging support over static VXLAN tunnels.
Overlay Fabric	VXLAN tunnel source and destination using IPv6 in a multi-fabric design.
Overlay Fabric	Multicast anycast RP/MSDP for IPv4 multicast routing in the VXLAN overlay fabric design.
Overlay Fabric	EVPN route types [1 to 5] match support in a route-map.
Underlay Fabric	Increased range of the OSPF process ID from 1-63 to 1- 65535

Category	Description
Underlay Fabric	VRF support for non-VRF/Namespace aware container applications
Underlay Fabric	Port-mapping for container private IP reachability in a DNAT configuration
Underlay Fabric	Blocking of unknown multicast packets in a VLAN configured with: IGMP Snooping, MLD Snooping, VSX, and VXLAN. Default behavior is to allow initial flooding; to enable this feature, an explicit configuration command is required.
Underlay Fabric	Fix for setting multiple communities and extended communities in a route-map. Ability to set multiple and extended communities per prefix in a route-map used by BGP for both IPv4 and IPv6 address families.
Underlay Fabric	Number of PVLAN secondary ports is increased to 48
MACsec	(for 8360 Switch series only) WAN MACsec enhancement to support a custom Ether-Type for EAPoL frames
Containers	Multiple container infrastructure hardening features to increase overall system stability
Security	ACL support for L3 VXLAN VNI
Security	Port-access over LAG for Device Profile now is supported over MCLAG
Observability	Visibility into blocked flows by PAP, GBP, ABP, RACL policies applied on the user role
Observability	Visibility into blocked flows dropped by ACLs applied on L2 interface, L2 LAGs, VLANs, and Interface VLANs
Observability	IPFIX per VRF export source interface or source IPv4 / IPv6 addresses
OSPF	Ability to configure a different AD for multiple OSPF process in a VRF
Infrastructure Management and Usability	Visibiity into configuration history from previous sessions
Infrastructure Management and Usability	Local switch WebUI connections over IPv6
Infrastructure Management and Usability	SNMPv3 enablement without any SNMPv2 or community configured
Infrastructure Management and Usability	Ability to display all the deprecated CLI commands and new version of those commands in the CLI
Infrastructure Management and Usability	Output of the show interfacecommand now displays how long the

Category	Description
	interface has been down
Infrastructure Management and Usability	AOS-CX introduces support for NAE-Lite
Infrastructure Management and Usability	SNMP trap filter per host
Infrastructure Management and Usability	SNMP read extended interface MIB for reporting

Resolved Issues for 8100 and 8360 Switches in AOS-CX 10.14.0001

This section describes the issues resolved in this release.

Component	Summary	Description
Central	294122	**Symptom**: Some hpe-restd core dumps may be generated after the switch reboots.This will not interrupt the normal switch operation. **Scenario**: This can occur every time the switch reboots. **Workaround**: The hpe-restd core dumps generated after after the switch is rebooted have no impact to switch operation, and can be ignored
IGMP	215677	**Symptom**: IGMP/MLD configuration changes do not take effect when the **hpe-mgmdd** process is flooded with IGMP/MLD control packets. **Scenario**: In a situation where IGMP or MLD control packets (Joins or Leaves) are part of a loop, or if misbehaving clients send continuous streams of IGMP/MLD control packets, the **hpe-mgmdd** daemon's packet queue can become continuously full. **Workaround**: Restart the MGMD daemon using the command **systemctl restart hpe-mgmdd**.
Physical Interfaces	224311	**Symptom**: When parallel detection is enabled, autonegotiating interfaces that are linked with non-autonegotiating interfaces are expected link up at the detected speed, but in half duplex mode. BASE-T ports on AOS-CX switches have parallel detection enabled and are compliant the IEEE 802.3 standard. However, there are some interfaces that are not conforming to this behavior due to hardware limitations. **Scenario**: The following ports have non-conforming parallel detection, or does not have parallel detection enabled. ■ JL659A: Ports 1-48, Enabled for 100M but links at full duplex ■ JL660A: Ports 1-24, Enabled for 100M but links at full duplex ■ JL720A, JL720C: Ports 11-48, Enabled for 100M but links at

Component	Summary	Description
		full duplex ■ R0X41A, R0X41C: Ports 1-48, Enabled for 100M but links at full duplex ■ R0X42A, R0X42C, S1T83A: Ports 1-24, Enabled for 100M but links at full duplex ■ R9W95A: Ports 1-24, Enabled for 100M but links at full duplex ■ R9W97A: Ports 11-40, Enabled for 100M but links at full duplex ■ R8Q71A, R8V12A: Ports 37-48, Not enabled (will not link with non-autonegotiating partner) ■ R8S89A: Ports 1-24, Not enabled (will not link with non-autonegotiating partner) ■ R8S90A, R8S91A: Ports 11-48, Not enabled (will not link with non-autonegotiating partner) ■ S0E91A, S0X44A: Ports 1-48, Not enabled (will not link with non-autonegotiating partner) **Workaround**: Enable autonegotiation on the link partner whenever possible to ensure linking up at highest speed. If not possible, you can also explicitly force speed through the **speed 100-full** command in the **interface-config** context to link up with a non-negotiating link partner (assuming the link partner is 100M full duplex).
DNS	230380	**Symptom:** The switch experiences high CPU utilization . **Scenario:** High CPU utilization occurs when SNMP invokes DNS resolution, due to access of source IP which causes CPU overhead.
Internal srvcs: linux	273640	**Symptom:** The ARM kernel Unimplemented Instruction (UI) trap had an error that caused incorrect information to be logged in the rare circumstance of an unhandled UI. **Scenario:** This issue is seen only in the uncommon circumstance of a kernel corruption of the UI.
BGP	285540	**Symptom:** When both IPv4 and IPv6 neighbors are configured in BGP, an SNMP walk displays incorrect information on IPv4 peer sessions. **Scenario:** If the customer configures both IPv4 and IPv6 neighbors, the SNMP walk output will include information on non-existent IPv4 peers. The IPv6 peer information displays as expected.
LLDP	287305	**Symptom:** A Client is assigned a role VLAN instead of a Port VLAN ID (PVID). **Scenario:** This issue occurs on a Device-profile client onboarded with LLDP neighbor info, whenever the user disconnects AP, which is already assigned DP profile, then unplugs the AP and connects the Notebook/Workstation. It received the IP address from the device profile native role assigned VLAN. HOwever, It is supposed to receive the VLAN IP address from the PVID VLAN . **Workaround:** Wait for the LLDP neighbor entry to age out for the device that was unplugged before plugging in a different device to the same port.

Component	Summary	Description
Internal srvcs: Security PA infra	290068	**Symptom:** The **port-accessd** process crashes and restarts, and a core-dump file is generated. **Scenario:** This issue occurs if a client continuously moves from one port to another port. **Workaround:** Avoid frequently the client between the ports.
DHCP Relay	291742	**Symptom:** DHCP relay does not change the source IP address of the DHCP discover frame **Scenario:** This issue occurs if the DHPCP client does not use **0.0.0.0** as the source IP, for example. when the DHCP packet is generated by the client with a valid private IP as source IP. **Workaround:** Use the source interface configuration.
BGP	295703	**Symptom**: When the **show bgp vrf info** command is run, the , vtysh session is logged out. **Scenario:** This issue occurs when VRF is configured with export RT (Route Target). **Workaround:** Use the command **show running-config vrf** to prevent the vtysh session from logging out.
RADIUS Port-Access	296010	**Symptom**: The port-access daemon crashes continually. **Scenario**: This issue occurs if the RADIUS server is added user server group without configuring a group priority via REST or the Aruba Fabric Composer **Workaround**: Use the switch CLI to add a server to the user group or pass the user priority along with group using the REST interface.
VSX-Sync	299838	**Symptom**: An Interface VLAN configuration is not getting synced to secondary switch. **Scenario**: This issue can occur n a pair of switches in VSX configuration, when the user creates an Interface VLAN with VSX-Sync configuration in primary switch, then the user creates the same Interface VLAN on secondary, but the configuration is not synced. **Workaround**: Once VSX-Sync has been enabled on primary Interface VLAN, wait ~15 seconds before creating the Interface VLAN on the secondary interface. Another workaround is to first create the Interface VLAN on the secondary and then enable VSX-Sync on the primary Interface VLAN. (There is no need to wait in this second workaround).
VSX	299851	**Symptom:** The VSX software upgrade software version is not properly validated when upgrading using TFTP. **Scenario:** When upgrading using TFTP, it is possible to load mismatched software versions, resulting in a VSX upgrade failure and a VSX software mismatch between the primary and secondary VSX nodes. **Workaround:** Confirm that software image versions are compatible. Software upgrades using boot banks rather than TFTP will perform a proper version check before completing the upgrade.
MAC Tables	300754	**Symptom**: An attempt to learn a number of MAC addresses on the switch equal to the capacity of the MAC Table could trigger a Critical Service Fault. **Scenario**: This issue is triggered by connecting an extremely

Component	Summary	Description
		large number of devices or running test scripts/tools that generate traffic with a large number of Source MACs **Workaround**: Limit the number of Source MAC addresses in the environment to 90% of the MAC table Capacity.
Internal srvcs: Security PA infra	301734	**Symptom:** A role assigned by CoA gets overridden by low-priority methods, such as a RADIUS assigned role. **Scenario:** This issue occurs on a switch with the default auth-priority on port ifyou configure both mac-auth and dot1x and assign a role from RADIUS on successful mac-auth authentication and concurrent on boarding. While dot1x is in authenticating state, if you assign a different role RADIUS using CoA, you can observe that role assigned by CoA gets overridden by the RADIUS-assigned role (during mac-auth success) **Workaround:** Remove concurrent onboarding.
RADsec	308854	**Symptom**: Client authentication failures can occur, and packets sent to a RADIUS server are timed out by the switch. **Scenario**: In some scenarios when the RADSec server connection is lost and restored while multiple port-access users are authenticated to the RADIUS server the switch might incorrectly time out the RADIUS packets. **Workaround**: Unconfigure and reconfigure the RADSec server.
SNMP	303650	**Symptom**: The snmpd process crashes and SNMP polling stops for a few seconds. **Scenario**: This issue can occur when polling by SNMP (snmpwalk), and simultaneously performing a snmpget/snmpbulkget on a non-existent OID. The SNMP process will recover itself after the crash.
VXLAN	306920	**Symptom**: A reboot of compute-leaf-1 causes intermittent ping loss to hosts that move from compute-leaf-2 to compute-leaf-1. Pings originating from net-leaf-1 are affected, and net-leaf-1's route programming shows an incorrect transition between states. **Scenario**: This issue can occur when the switch reboots.
Physical Interfaces	307277	**Symptom**: A module interface error is observed on physical interfaces. Scenario: This issue can occur after reboot or enabling a port. **Workaround**: Disable the port using the **shut** command and wait for the port to exit the error state before enabling it.
BGP	309608	**Symptom**: OSPF routes are not redistributed to BGP **Scenario**: This issue is observed when the network command configuration moves from a subset of the VRF to another subset. **Workaround**: Remove the network command configuration and add it again.
CX-Licensing	TMA-4234	**Symptom:** The switch advanced feature pack shows as expired. **Scenario:** This issue occurs if the switch is configured with

Component	Summary	Description
		non-UTC time. After installing a feature pack to enable the advanced features on the switch, the feature pack expiration date is incorrectly flagged as expired **Workaround:** Set the switch to UTC time to activate the feature pack.

Feature Caveats

The following are feature caveats that should be taken into consideration when using this version of the software.

Feature	Description
Central	When a switch is able to connect to Aruba Central but is not registered in the Aruba Central inventory or does not have a proper license, the switch will get disconnected. This connect/disconnect process will continue until the switch is properly registered in Aruba Central. To avoid this unnecessary reconnection cycle, best practices is to disable Aruba Central until the switch is registered in Aruba Central, or a license is obtained for that device.
Hot Patch	When a hot-patch file download is triggered using the switch WebUI, log messages can incorrectly state that the file is added to the database with a **missing** status. This is a temporary state, and will correctly change to **Not applied** once the download is completed.
PIM-SM	Pim Active-Active is not supported on overlay VXLAN SVIs.
SNMP	When SNMP is enabled via the switch CLI, it can take between 1-2 minutes for the SNMP daemon to be ready to respond to requests. If a local or external SNMP MIB walk is performed in the interval between when SNMP is first enabled and the SNMP daemon is ready, the MIB walk action will return an error.
VXLAN	VXLAN encapsulation does not copy the ECN bits from inner header to outer header. If you create a traffic stream between connected hosts and enable the ECN bit for the hosts and start the traffic, a traffic capture may show that ECN bits arent copied from the inner header to the outer header.
Certificates	When a switch uses a certificate with a legacy certificate name that is not supported in 10.12 because it contains disallowed characters, the information will migrate properly in the upgrade, but that certificate can no longer be edited. For new certificate names, only alphanumeric characters, dots, dashes, and underscores are allowed.
REST	Boundary values for **match vni** and **set local preference** in a route-map system cannot be set via the REST API and must be manually configured on the switch via the CLI.
BGP	In environments with VRRP or VSX peers, 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:

Feature	Description
	`` ! 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.
BGP	The **next-hop-unchanged** option needs to be explicitly configured to preserve nexthop while advertising routes to eBGP peers, in the L2VPN EVPN address-family. For example: ``` router bgp 1 neighbor 1.1.1.1 remote-as 2 address-family l2vpn evpn neighbor 1.1.1.1 activate neighbor 1.1.1.1 next-hop-unchanged neighbor 1.1.1.1 send-community extende exit-address-family ```
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	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
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.
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.
EVPN	The iBGP split-horizon rule is not followed between different address families. Use route-map to block the routes getting advertised to the iBGP peer.
IP-SLA	Reserved ports or ports used by other applications/services with in the system are not recommended to be used for other services. When two services use the same port there is chance of unexpected behaviors from these services. Best practices is to use unique port for each service across system.

Feature	Description
ICMP Redirect	The switch may only software forward at a rate of 100pps if the packets that trigger ICMP redirect.
IGMP/PIM on 6-in-6, Loopback and GRE interfaces	IGMP cannot be enabled on either Loopback or GRE interfaces. IGMP and PIM is not supported on a 6-in-6 Tunnel.
MACsec	(for 8360 Switch Series only) In an environment with a Cisco device, the Cisco device must be designated as the key server. Designating the AOS-CX as the key server results in complete traffic loss.
MACsec	(for 8360 Switch Series only) In an environment with Cisco and FlexFabric or H3C devices, do not update confidentiality-offset on the live channel. There can be complete traffic loss for an extended period on the MACsec channel when confidentiality-offset is updated on both ends.
MACsec	(for 8360 Switch Series only) MACsec uses a software-based implementation to track start and stop times for secure channels and secure associations. As the implementation is software-based, the stop times for MACsec secure channel and secure associations are only updated when they are deleted and therefore never updated in the output of the **show macsec status detailed** command.
MACsec and UDLD	(for 8360 Switch Series only) In an environment with devices running AOS-Switch, do not enable UDLD on the same link. The UDLD session can toggle between up and down continuously when both MACsec and UDLD is enabled on the same link.
MACsec	(for 8360 Switch Series only) In an environment with Cisco devices, when the GCM-AES-XPN-128 or GCM-AES-XPN-256 cipher suite is used for establishing the MACsec channel, the MKA policy on the Cisco device must be configured with **ssci-based-on-sci**.
MACsec	(for 8360 Switch Series only) MACsec works between a CX device and a Windows VM running AnyConnect with AES-128 cipher. AnyConnect does not support AES-256 in the NAM module (works only for the VPN module).
MACsec	(for 8360 Switch Series only) When Cisco AnyConnect is used as dot1x supplicant, it is recommended to configure cak-length to be 16 under dot1x-authenticator mode.
MACsec	(for 8360 Switch Series only) Ensure the cipher suite **GCM-AES-128** is configured when AOS-CX is acting as a key server. This is because, by default AOS-CX will use the most secure cipher suite **gcm-aes-xpn-256** for establishing MACsec secure link and Comware/PVOS doesn't support an XPN cipher suite.
MPLS	▪ ICMP Ping/Traceroute with ip-options are not supported over an L3VPN. ▪ MPLS/LDP - config restore using a checkpoint is not supported. Performing this action may lead to VPNV4 neighbor struck in a **bgp idle** state with a **cease/connection rejected** error. ▪ MPLS is supported on Core-Spine and Aggregation-Leaf profiles only. ▪ Dual IGP paths on MPLS core (that is, between PE to P) supported only in Active Standby.

Feature	Description
	▪ Route-map, ORF, aggregate-address, add-path capability, carrying MED are not supported with VPNV4 neighbours. ▪ MPLS is not supported on sub-interfaces or split-ports ▪ Explicit-null support only. Any 3rd party PE will need to be configured with Explicit-null for proper forwarding. ▪ It is recommended to configure Jumbo frame support on all MPLS-enabled interfaces to avoid any un-expected drops in the network, as fragmentation on MPLS frames is not possible. ▪ Static LSP must be used in single label forwarding deployments and LDP/BGP configurations must be used for all L3VPN deployments. ▪ For site connectivity redundancy, two stand-alone PE devices connected to the CE device at the site must be used rather than two PE devices in the VSX mode. ▪ While using site connectivity redundancy, the same RD must be configured on both stand-alone PE devices to provide BGP best path selection. ▪ On leaving MPLS core, QOS EXP bit is copied to both Ethernet and IP header at Label Edge Router (LER).
Multicast and VXLAN	▪ VXLAN must be configured prior to configuring VSX. ▪ IPv6 multicast is not supported for VXLAN overlay. ▪ Multicast support for static VXLAN in the overlay has limited support. Contact Aruba Support for details.
PFC	Priority-based flow control (PFC) is not supported on a split port.
MVRP and VSX	MVRP is mutually exclusive with VSX.
OSPF	OSPFv2 and OSPFv3 do not support detailed LSA **show** commands.
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.
Sub-interface	BFD is not supported on a sub-interface. A sub-interface as underlay for EVPN-VXLAN is not supported
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
Traceroute	Issuing the **traceroute** command with the i**p-option loosesourceroute** parameter fails inan overlay EVPN-VxLAN deployment.
Traceroute	Traceroute v4/v6 over VXLAN fails to find intermediate next-hop IP information from a source VTEP in Virtual Active Gateway environment (the

Feature	Description
	SVI is the same as theActive Gateway IP).
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.
PTP	End clients offset might be slightly high when using PTP Default profile 1588v2 with default PTP parameters (1 PPS)
VXLAN	A shared-core VTEP cannot be used as a stub VTEP. As a workaround, configure a single dedicated stub VTEP and enable evpn sessions to the shared-core VTEP.

Known Issues

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.

Category	Bug ID	Description
PTP	206756	**Symptom:** The precision time protocol (PTP) offset is not accurate. **Scenario:** When configuring transceivers to a non-default forward error correction (FEC) setting, the PTP offset will not be accurate due to an inaccuracy in PTP latency. **Workaround:** Use the default FEC.
MPLS	194381	**Symptom:** Extended RTs (via ext communities) received from a local side PE are not installed on the remote side PE. **Scenario:** In an L3VPN network, the extended RTs that are used as route attributes in the VPNv4 routes will not get installed on the other side PE. If those values are used to influence the route selection or policy, it may not work. **Workaround:** Use standard communities, other BGP attributes locally on the remote side to influence the route selection or policy.
TFTP	269619	**Symptom**: TFTP Software image upload/download transfer operation fails. **Scenario**: Downloading/uploading the software Image via sm ubuntu IPv6 TFTP server fails. **Workaround**: Use the **blocksize** option in the copy command with a blocksize of 1375 or less. For example : `copy tftp://[20:1::100];blocksize=1375/image.swi secondary vrf vrf1`

Upgrade information

Each VSX switch in a pair must run the same version of AOS-CX. If a primary VSX switch is upgraded to 10.10.xxxx, the secondary VSX switch must be immediately upgraded to that same version. If the ISL link is disabled and enabled on VSX switches that are running different versions of AOS-CX, a VSX secondary switch running an older version of AOS-CX may be unable to synch information from the VSX primary, which can cause the port state to become blocked and lead to traffic loss.

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

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, LL.10.xx.*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 software upgrade

For additional upgrade and downgrade scenarios, including limitations of automatic upgrade and downgrade scenarios provided by the Configuration Migration Framework (CMF), refer to the **AOS-CX 10.14 Fundamentals Guide**.

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, three 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.10.13.1000]
2. Secondary Software Image [xx.10.14.0001]

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 2017-2024 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.

Chapter 2
Other resources

Aruba is committed to ensuring you have the resources you need to be successful. Check out these learning and documentation resources:

- AOS-CX switch software documentation portal: https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
- AOS-CX technical training videos on YouTube: https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS

Chapter 3
Aruba security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

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