AOS-CX 10.14.0001 Release Notes

8325 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 8325 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
JL624A	Aruba 8325-48Y8C 48p 25G SFP/+/28 8p 100G QSFP+/28 Front-to-Back 6 Fans and 2 PSU Bundle	10.02.0001
JL625A	Aruba 8325-48Y8C 48p 25G SFP/+/28 8p 100G QSFP+/28 Back-to-Front 6 Fans and 2 PSU Bundle	10.02.0001
JL626A	Aruba 8325-32C 32-port 100G QSFP+/QSFP28 Front-to-Back 6 Fans and 2 Power Supply Bundle	10.02.0001
JL627A	Aruba 8325-32C 32-port 100G QSFP+/QSFP28 Back-to-Front 6 Fans and 2 Power Supply Bundle	10.02.0001

Important information for 8325 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.

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.

To enable future feature enablement, changes were made to how egress IPv4 VLAN ACLs are implemented. It was possible to deploy an egress IPv4 VLAN ACL in previous software releases concurrently with a either a routed egress IPv4 VLAN ACL or an egress IPv4 port ACL. From 10.06 onward, only one type of ACL is allowed per VLAN.

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)

Browser	Minimum supported versions
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)

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 8325 Switches in AOS-CX 10.14.0001

This section describes the enhancements introduced in this release.

Category	Description
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 anycast RP/MSDP for IPv4 multicast routing in the VXLAN

Category	Description
	overlay fabric design.
Overlay Fabric	Multi-fabric Route-Server for BGP peering for EVPN-AF for provisioning VXLAN tunnels between border VTEPs in a multi-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
Underlay Fabric	VRF support for non-VRF/Namespace aware container applications
Underlay Fabric	Port-mapping for container private IP reachability in a DNAT configuration
Containers	Multiple container infrastructure hardening features to increase overall system stability
Queue Congestion DL GL	Ability to retrieve queue congestion history utilizing local CX time-series-database
Observability	IPFIX support on extended platforms
BSP	AOS-CX 10.14 includes enhancements to how transceiver failures are handled. The software now continuously monitors devices such as transceivers for internal communication bus issues that may affect the overall health of the system. When identified, the switch will now reboot to disable the failing transceiver. Meaningful event logs both prior to, and after a reboot will identify the failing transceiver. You may then hotswap out the failed transceiver and insert a functioning model without the need of a further reboot.
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 interface has been down
Infrastructure Management and Usability	Visibility into link diagnostics for physical L1 components
Infrastructure Management and Usability	SNMP trap filter per host

Category	Description
Infrastructure Management and Usability	SNMP read extended interface MIB for reporting

Resolved Issues for 8325 Switches in AOS-CX 10.14.0001

This section describes the issues resolved in this release.

Com-ponent	Sum-mary	Description
VXLAN	153235	**Symptom**: Error logs continually appear in var/log/messages. `2021-01-26T16:37:13.775494-08:00 SE11-L4 ops-switchd: ovs|10684861netdev_bcmsdk|ERR| netdev_bcmsdk_set_hw_intf_info: invalid hw_unit (null) 2021-01-26T16:37:13.775569-08:00 SE11-L4 ops-switchd: ovs|10684862|netdev_bcmsdk|INFO| netdev_bcmsdk_set_hw_intf_info: interface[vni100095] unit[(null)] port[(null)] split_port_count[0] parent[none] parent_port[(null)]` Scenario: The log messages start appearing when an L3 VNI is configured on the switch.
EVPN	172276	**TBD**, **owner Ramaprasad A.**
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**.
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.
CPU Rx	280972	**Symptom**: ARP entries are not learned across VSX switches. **Scenario**: This issue can occur on a VSX pair using Virtual Active Gateway. If the respective physical interfaces undergo a port split or a change to the LAG configuration, te configuration changes do not get propagated to the Virtual Active Gateway. **Workaround**: After changing the LAG configuration or splitting a port, remove the Virtual Active Gateway configuration and reconfigure it.
BGP	285540	**Symptom:** When both IPv4 and IPv6 neighbors are configured in BGP, an SNMP walk

Com-ponent	Sum-mary	Description
		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.
TPM	289976	**Symptom:** The switch is unable to connect to Activate/Central or other services using the Device Identity certificate. **Scenario:** When this issue occurs, Central will claim a connection failure.
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.
DHCP Relay	292116	**Symptom:** A Stanley Healthcare Exciter will not accept a DHCP Offer via IP Helper when the switch is used as as a Relay Agent. **Scenario:** The Stanley Healthcare Exciter failed to accept a DHCP Offer via IP Helper because the source IP field in L3 header of the OFFER packet martched with the option 54 DHCP Server IP address instead of matching with the Relay Agent IP address.
ACL	292640	**Symptom:** Even if a REST call was successful, there may be DLOG errors and CLI warnings stating that the configuration is invalid. **Scenario:** This issue can occur if a ACL **includes** a source IP or designation IP with no netmask. The address format A.B.C.D is not a supported format in the database; the format must be **A.B.C.D/W.X.Y.Z** **Workaround:** When sending a configuration to the database via REST, use a supported format.
L3 addressing	294569	**Symptoms**: L3 connectivity issues occur with l3-src-mac features enabled on L3 VLAN Interfaces **Scenario:** This issue occurs if an l3-src-mac feature is enabled L3 VLAN interface and you perform one of the following actions: ▪ Bring an L3 VLAN interface down and then up (**shut** followed by **no shut**). ▪ Delete and re-create the L3 VLAN interface. ▪ Remove the l3-src-mac feature ▪ Change the VxLAN VLAN to VNI binding for that particular VLAN. The Internal state for this L3 VLAN interface (specifically Router MAC entry) gets into an incorrect state and doesn't recover. Basic L3 connectivity may get broken.

Com-ponent	Sum-mary	Description
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.
ARP	298045	**Symptom:** Gratuitous ARP packets get dropped in a VXLAN overlay network when ARP suppression is enabled **Scenario:** This issue occurred when ARP suppression was enabled over VXLAN.
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.
L3 routes	300571	**Symptom:** When a large number of host-routes (fully qualified routes) ipv4 routes with /32 or ipv6 routes with /128 are installed on a system, with a matching directly connected host, some network events may result in traffic loss for those routes. **Scenario:** Most commonly this will be se en on reboot, however it may be present on bring-up as well. Link-flaps could also result in seeing this issue. **Workaround:** Clear arp is the current work around, it will allow hosts to be cleared and re-entered and should resolve the incorrect programming.
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.

Com-ponent	Sum-mary	Description
		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.
L3 Routes	309707	**Symptom**:Traffic not getting forwarded via a GRE tunnel. **Scenario**: THis issue can occur in a deployment with a static route(prefix 32) with a tunnel IPas a nexthop, where the tunnel IP also has the longest prefix static route. When the tunnel becomes non-operational, the static route (prefix 32) points to the longest prefix route nexthop. **Workaround**: Configure the nexthop for static route(prefix 32) as GRE tunnel interface instead of tunnel IP
L3 Routes	300609	**Symptom**: AOS-CX canot match the route with AS-path using the regular expression **(^$)**. Scenario: In a multifabric deployment the switch gets a route from the other fabric also and it will advertise to the edge device. If you prefer that one fabric route should not go to the other fabric route on the edge device, the route must be manipulated in the border VTEP directly **Workaround**: Match the route using the communities in the border VTEP and advertise to OSPF towards the edge device.
VXLAN	305156	**Symptom**: Excessive multicast packet flooding occurs on ISL and downstream access links, with traffic utilization around 80%. **Scenario**: The issue appears when VSX switches are repeatedly rebooted, causing stale VXLAN replication group entries to point incorrectly towards ISL links. The flooding intensifies when ICMPv6 multicast traffic hits an access VLAN. **Workaround**: Removing and re-adding the VNI/VLAN configuration for the affected VLAN under the VXLAN interface clears the stale entries.
VXLAN	TMA-4437	**Symptom**: When broadcast or unknown unicast traffic is received over a VXLAN tunnel, after packet decapsulation this traffic will be sent back on the same tunnel it came in on, causing a loop of Broadcast traffic. **Scenario**: In the EVPN scenario, a VXLAN tunnel is initially established as an inter-fabric tunnel (eBGP). Later, this tunnel is deleted and recreated as an intra-fabric tunnel (iBGP), or vice versa.
CX-Licensing	TMA-4234	**Symptom:** The switch advanced feature pack shows as expired. **Scenario:** This issue occurs if the switch is configured with 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.
QoS	When using the REST v10.04 API to retrieve the value of **pfc_priorities_config** and **pfc_priorities_applied** columns from the Interface table, the API returns NULL values irrespective of the switch configuration.
VXLAN	IPV6 vxlan Tunnels on 8325 and 10000 Switch series are supported with only ROP ports as an underlay. MCLAG or LAG as an underlay is not supported.
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.
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.
Subinterfaces	BFD sessions are not supported on sub interfaces. Use a switch virtual interfaces (SVI) to configure a BFD session.
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:
	`!`
	`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`

Feature	Description
	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.
ARP	Duplicate Address Detection (DAD) status indicated a duplicate for IPv6 anycast gateway configuration. As a workaround, configure an active gateway IPv6 address and SVI IPv6 address, as this can prevent DAD issues. Issuing the commands **interface shut** followed by **interface no-shut** can help in resolving the issue.

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	Classifier policies, IPv6 and MAC ACLs are not supported on egress.
Classifiers	Egress ACL logging is not supported.
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	IPv4 egress ACLs can be applied only to route-only ports.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
Counters	Layer 3 Route-only port counters are not enabled by default. Enabling them will reduce ipv4 route scale to 80K.
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.
ICMP Redirect	The switch may incorrectly duplicate an IP frame that triggers ICMP redirect.

Feature	Description
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.
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.
Network Analytics Engine (NAE)	Agents monitoring a resource that has column type enum with a list of strings (as opposed to a single string enum) is not supported.
Network Analytics Engine (NAE)	Network Analects Engine (NAE) agents execute Command Line Interface (CLI) actions as 'admin' user, so they have permission to run any command by default. However, when the authentication, authorization and accounting (AAA) feature is enabled, the same restrictions applied to 'admin' will also apply to NAE agents. When using AAA, make sure to give the admin user the permissions to run all commands needed by enabled NAE agents. Otherwise, some CLI commands may be denied and their outputs won't be available. Actions other than CLI won't be affected and will execute normally. Also, NAE agents won't authenticate, thus the AAA service configuration must not block authorization for unauthenticated 'admin' user. ClearPass doesn't support such configuration, so it cannot be used as a TACACS+ server.
Network Analytics Engine (NAE)	The following tables are not supported for NAE scripts: OSPF_Route, OSPF_ LSA, OSPF_Neighbor, BGP_Route.
OSPF	OSPFv2 and OSPFv3 do not support detailed LSA **show** commands.
RADIUS	Authorization by means of HPE VSAs is not supported.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
RIP/RIPng	Redistribute RIP/RIPng is not supported in BGP/BGP+.
RIP/RIPng	RIP/RIPng metric configuration support is not available.
RPVST+ and MSTP	Spanning Tree can only run in MSTP or RPVST+ mode.
RPVST+ and MVRP	RPVST+ is mutually exclusive with MVRP.
VRF	VRF names are limited to 31 characters.
VRRP-MD5 authentication interop	Not supported with Comware-based switches
EVPN	After an issue with duplicate MAC addresses on a single IP on a VTEP is resolved, the ARP entry does not sync with the EVPN. As a workaround issue the commands shut and no shut on the port that connects to the host.
EVPN	After an issue with duplicate IPs on two VTEPs is resolved, the EVPN does not advertise the MAC/IP entry. As a workaround, clear the ARP table.

Feature	Description
ARP	After an issue with duplicate IPs on two VXLAN tunnel endpoints (VTEPs) is resolved, the kernel will have the ARP entry, but the output of the show arp and show evpn mac-ip commands do not show that IP. As a workaround, flap the physical interface.
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.
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 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.
VXLAN	IPV6 VXLAN tunnels support only ROP ports as underlay. It does not support MCLAG or LAG as underlay.

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
GRE Tunnel	305737	**Symptom**: The **ip address 10.0.0.1/24 secondary** configuration will not appear in any show command output for the GRE Tunnel interface. **Scenario**: This issue occurs when the GRE tunnel interface is configured with **ip address 10.0.0.1/24 secondary** .
L3 Addressing	300571	**Symptom**: When a large number of host-routes (fully qualified routes) ipv4 routes with /32 or ipv6 routes with /128 are installed on a system, with a matching directly connected host, some network events may result in traffic loss for those routes. **Scenario**: This issue is most oftenseen when the switch reboots, however it may be present when it initially is brought up. Link-flaps could also trigger this issue. **Workaround**: Clear the ARP cache.
L3 Routes	300609	**Symptom**: When attempting to match the BGP local route and advertise to OSPF some metric, AOS-CX

Category	Bug ID	Description
		cannot match the route with AS-path using a regular expression(^$). **Scenario**: In a multifabric scenario, the switch is getting route from the other fabric also and it will advertise to the edge device. If on an edge device one fabric route should be preferred, the route should be manipulated in the border VTEP. Workaround: Match the route using the communities in the border VTEP and advertise to OSPF towards the edge.
ARP	295946	**Symptom**: An ARP cache entry with inactive IP addresses on the network may remain in the neighbor database for a long time. **Scenario**: This issue occurs when the MAC address refresh/relearn process occurs for a MAC mapped to inactive IP addresses. **Workaround**: 1. Clear the ARP cache 2. Configure a reduced ARP ageout.

Upgrade information

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 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.

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, GL.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.