AOS-CX 10.06.0110 Release Notes

8360 Switch Series

a Hewlett Packard Enterprise company

Part Number: 5200-7910a
Published: March 2021
Edition: 2

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 10.06 Release Notes

Description

This release note covers software versions for the AOS-CX 10.06 branch of the software.

If you run the `show version` command on the switch, the version number will display LL.10.06.*xxxx*, where *xxxx* is the minor version number.

AOS-CX is a new, modern, fully programmable operating system built using a database-centric design that ensures higher availability and dynamic software process changes for reduced downtime. In addition to robust hardware reliability, the AOS-CX operating system includes additional software elements not available with traditional systems, including the features included in the Features section of this release note.

Version 10.06.0001 is the initial build of major version 10.06 software.

Product series supported by this software:

- Aruba 8360 Switch Series

Important Information

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

Multicast flows in symmetric IRB with VXLAN overlay is not supported when the multicast source is connected to the switch.

Industry and Government Certifications

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

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

License Written Offer

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

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

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

Version History

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

Version number	Release date	Remarks
10.06.0110	2021-03-17	Released, fully supported, and posted on the web.
10.06.0101	2021-03-01	Released, fully supported, and posted on the web.
10.06.0100	2021-02-16	Released, fully supported, and posted on the web.
10.06.0010	2020-12-15	Released, fully supported, and posted on the web.
10.06.0002	2020-12-03	Released, fully supported, and posted on the web.
10.06.0001	2020-11-10	Initial release of AOS-CX 10.06. Released, fully supported, and posted on the web.

Products Supported

This release applies to the following product models:

Product number	Description
JL700A	Aruba 8360-32Y4C with MACSec Port to Power 3 Fans 2 PSU Bundle
JL701A	Aruba 8360-32Y4C with MACSec Power to Port 3 Fans 2 PSU Bundle
JL702A	Aruba 8360-16Y2C Port to Power 3 Fans 2 PSU Bundle
JL703A	Aruba 8360-16Y2C Power to Port 3 Fans 2 PSU Bundle
JL706A	Aruba 8360-48XT4C Port to Power 3 Fans 2 PSU Bundle
JL707A	Aruba 8360-48XT4C Power to Port 3 Fans 2 PSU Bundle
JL708A	Aruba 8360-12C Port to Power 3 Fans 2 PSU Bundle
JL709A	Aruba 8360-12C Power to Port 3 Fans 2 PSU Bundle
JL710A	Aruba 8360-24XF2C Port to Power 3 Fans 2 PSU Bundle
JL711A	Aruba 8360-24XF2C Power to Port 3 Fans 2 PSU Bundle

Compatibility/Interoperability

The switch web agent supports the following web browsers:

Browser	Minimum supported versions
Edge (Windows)	41
Chrome (Ubuntu)	76 (desktop)
Firefox (Ubuntu)	56
Safari (MacOS)	12
Safari (iOS)	10Version 12 is not supported

Internet Explorer is not supported.

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

Management software	Recommended version(s)
Airwave	8.2.12.0
NetEdit	2.0.12
Aruba CX Mobile App	2.4.6
Aruba Central	2.5.3
Network Automation	10.10, 10.11, 10.20, 10.21, 10.30, 10.40
Network Node Manager	10.10, 10.20, 10.21, 10.30, 10.40
IMC	7.3 (E0506P05)

For more information, see the respective software manuals.

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

Transceiver Support

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

No new transceiver support

Refer to the *Transceiver Guide* for complete details on all supported transceivers.

Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

Version 10.06.0110

No enhancements were included in version 10.06.0110.

Version 10.06.0101

No enhancements were included in version 10.06.0101.

Version 10.06.0100

Category	Description
BGP	Added the new command `redistribute local loopback` to allow redistribution of /32 (IPv4) and /128 (IPv6) addresses by BGP.
Multicast	Added support for IPv4 multicast over VXLAN.
SNMP	Added additional LAG attributes in order to facilitate a richer NMS experience from tools such as Airwave.

Version 10.06.0010

Category	Description
SNMP	Added support for the `hh3cifVLANType`, `dot3StatsDuplexStatus`, and `dot3StatsTable` OIDs.

Version 10.06.0002

Cat-egory	Description
Event Log	Added an event message to the switch event log when a duplicate IP address is detected from ARP Reply or Neighbor Advertisement packets for one or more neighbors. Example: Event Log:ndmd[407]: Event|6131|LOG_ERR|AMM|1/1|Duplicate IPv4 address 1.1.1.2 is detected on port 1/1/1 with a MAC address of 02:00:00:00:00:02Error Log:ndmd|LOG_ERR|AMM|-|NDM|NDM_NBRTABLE|[nd_nbr_mgr_process_arp_rcv_reply_event (636)] Duplicate IPv4 address 1.1.1.2 is detected on port 1/1/1 with a MAC address of 02:00:00:00:00:02

Version 10.06.0001

Category	Description
Core	■ Added Route Map Continue capability to route maps allowing for further flexibility. See the *IP Routing Guide* for more information. ■ BGP enhancements include support for the advertisement of multiple paths (ADD-PATH capability), confederations, and outbound route filtering (ORF). See the *IP Routing Guide* for more information. ■ Enabled BFD support for BGP6 neighbor sessions, allowing for faster failover on non-directly connected neighbors. See the *IP Routing Guide* for more information. ■ OSPF enhancements to enable the display of ABR and ASBR status. See the *IP Routing Guide* for more information.
Enrollment over Secure Transport (EST)	Adds the capability for enabling secure certificate enrollment, allowing for easier enterprise management of PKI. See the *Security Guide* for more information.
EVPN and VXLAN	■ VXLAN support for use in Data Center environments. See the *VXLAN Guide* for more information. ■ EVPN MAC dampening provides a protection mechanism against endless MAC moves. See the *VXLAN Guide* for more information. ■ ARP/ND suppression allows for suppressing ARPs/NDs in a VXLAN/EVPN network to limit wasted bandwidth consumed by ARP broadcasts and ND messages. See the *VXLAN Guide* for more information. ■ IPv6 VXLAN/EVPN overlay support enables IPv6 traffic over the VXLAN overlay. See the *VXLAN Guide* for more information.
MACsec	Support for MACsec encryption from AES128 and AES256 with 2SAK as well as 4SAK mode of Static Key provisioning enabling secure communication for all traffic on Ethernet links. Supported for switch-switch connections.
NAE	Added a graph showing average consumption for each daemon.
Removal of the sFlow and port mirroring mutual exclusion	Allows sFlow RX sampling and RX port mirroring to function on the same port.

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 number that precedes the fix description is used for tracking purposes.

Version 10.06.0110

Category	Bug ID	Description
CDP	155876	**Symptom:** The switch experiences an increase in memory utilization, slowing the performance of the system over a period of days. **Scenario:** When a large number of CDP neighbors are connected, there is a potential memory leak that occurs when packets from each neighbor reach the switch during the same time interval, or when a large number of CDP reply messages need to be sent on each interface for each connected neighbor. This memory leak could grow over a period of time as the CDP Rx packet count increases. **Workaround:** Restart the `cdpd` process to recover the leaked memory.
DHCP Relay	149237	**Symptom:** DHCP clients are not assigned IP addresses. **Scenario:** When an IVRL is set up without configuring the source interface in an inter-VRF scenario where the DHCP relay and server are on different VRFs and reachable through an IVRL route, DHCP clients do not get IP addresses. **Workaround:** Configure the source interface.
LACP	155575	**Symptom:** LAG port(s) remain in an `out-of-sync` state following a LAG port flap event. **Scenario:** When the peer device is configured with a non-default port priority other than 1 and non-default system priority other than 65534, and one of the LAG ports bounces, if the peer device takes more than 3 seconds to send the first PDU packet after the link comes back up, the LAG on the primary device will remain out-of-sync. This is unlikely to happen when physical links are tightly coupled with LACP. **Workaround:** Reset the LAG by disabling and re-enabling it.
SNMP	155880	**Symptom:** The switch experiences high CPU utilization and a restart of the OVSDB IDL daemon. **Scenario:** When the switch receives frequent SNMP requests, it will experience a high CPU utilization and the OVSDB IDL daemon will restart. **Workaround:** Restart the SNMP process.
SSH Server	153325	**Symptom/Scenario:** Switch generates a 2048-bit RSA SSH host key when attempting to generate a 4096-bit host key. **Workaround:** Use the `ssh-keygen` command in the Linux shell (using the `start-shell` command) to generate a 4096-bit RSA SSH host key.
VSX	153141	**Symptom:** The HPE-Relay daemon on the primary switch in a VSX pair crashes every two to three minutes, flooding the logs with the following event message: `Message Event|1201|LOG_CRIT|AMM|-|hpe-relay crashed due to signal:11 - Severity Critical (Priority: 2) - Syslog ID systemd-coredump`. **Scenario:** When DHCP traffic is running as expected through the primary VSX switch and then the secondary switch is rebooted, the HPE-Relay daemon on the primary switch in a VSX pair crashes every two to three minutes, flooding the logs with the following event message: `Message Event|1201|LOG_CRIT|AMM|-|hpe-relay crashed due to signal:11 - Severity Critical (Priority: 2) - Syslog ID systemd-coredump`.

Category	Bug ID	Description
		Workaround: Pause DHCP traffic before rebooting the secondary switch, then resume the traffic once the secondary switch is back in sync with the primary.
VSX	148521, 149288, 151440, 151543, 154798	**NOTE:** Applies only to the 6400 Switch Series. **Symptom:** VSX status goes into a non-operational state and configuration-sync does not work. **Scenario:** When a new configuration that is expected to be synced to the secondary VSX device (for example, one with static routes or VLANs) is added, the VSX pair may unexpectedly fail to update the secondary member's configuration, causing VSX to go into non-operational status and blocking configuration sync. **Workaround:** Reboot the secondary VSX member, or disable and re-enable VSX-sync on the secondary VSX device.

Version 10.06.0101

Category	Bug ID	Description
Central	157054	**Symptom/Scenario:** The switch goes offline in Central after a Central cluster upgrade. **Workaround:** Switch functionality and data flow is not affected. Restart the REST daemon with the `https-server session close all` command. **NOTE:** With this fix, if RESTd is restarted due to a disconnect from Central a core dump will be reported. This is expected behavior.

Version 10.06.0100

Category	Bug ID	Description
Airwave	95929	**Symptom:** In Airwave, the usage and description fields for LAG interfaces are empty if a description gets added to the interface. **Scenario:** If a LAG interface contains a description, and if Airwave polls the switch, the description and usage details for the interface are empty.
CDP	149252	**Symptom/Scenario:** An unexpected CDP core dump is found in the output of the `show core-dump` command.
Central	95378	**Symptom:** A switch software upgrade from Central fails. **Scenario:** Where there is a delay in DNS resolution during the software upgrade process initiated from Aruba Central, the switch fails to download the new version and complete the upgrade. **Workaround:** Add a configuration entry to the switch configuration template in Aruba Central for the HPE file server `ip dns host h30326.www3.hpe.com 23.197.193.219`, then re-initiate the new software upgrade from Aruba Central.
Counters	94803	**Symptom:** Drop counters get incremented incorrectly.

Category	Bug ID	Description
		Scenario: When a client is moved from one port to another or when the client sends an unsolicited NA, the `prefix mismatch` drop counter gets incremented incorrectly. When a prefix has been configured and sends NA with a non-matching prefix, the `NA packets failed ND snooping validation checks` drop counter gets incremented incorrectly.
DHCP Snooping	151555	**Symptom/Scenario:** DHCP clients do not receive an IP address from the DHCP server and the switch experiences high CPU utilization from the IPSAVD daemon.
IGMP Snooping	70340	**Symptom:** The output from the `show ip igmp snooping` command does not display in the output of the `show tech` command. **Scenario:** IGMP snooping group information is not present in the output of the `show tech` command.
IP Address	149740	**Symptom/Scenario:** IP addresses in the form *x.y.z*.255/31 cannot be configured on the switch.
IP Lockdown	91303	**Symptom:** User based tunneling fails. **Scenario:** When IP lockdown is enabled on a port, and then a user based tunnel is enabled on the same port, the user based tunnel fails. **Workaround:** Remove IP lockdown from the port.
Multicast	95279	**Symptom:** The PIM-SM Rendezvous Point (RP) drops Register messages from PIM Designated Routers (DRs). **Scenario:** When the source router sends register packets to the active gateway MAC of the interface, the MAC self check fails and the packets are dropped. **Workaround:** On the upstream router, configure the nexthop IP to reach the RP as one of the interface IPs of the RP router instead of the active gateway IP.
SNMP	95114	**Symptom:** SNMP restarts every 15 minutes and the event log displays SNMP startup events. **Scenario:** When the SNMP server community string is configured with special characters, SNMP restarts every 15 minutes. **Workaround:** Configure the community string with special characters in single quotes.
SNMP	94223	**Symptom:** SNMP restarts every 15 minutes and the event log displays SNMP startup events. **Scenario:** When the SNMP server agent is configured with a port other than the default, SNMP restarts every 15 minutes and the event log displays SNMP startup events.
SNMP	153440	**Symptom/Scenario:** The SNMP walk output of OID BRIDGE-MIB::dot1dTpFdbAddress returns fewer MAC addresses than the `show mac-address-table` command. **Workaround:** Unconfigure and reconfigure the SNMP server.
TFTP	150150	**Symptom:** Copy operation fails with the error `curl: (28) TFTP response timeout`.

Category	Bug ID	Description
		Scenario: When attempting to copy a configuration checkpoint to a TFTP server using the blocksize option, the copy fails with the error `curl: (28) TFTP response timeout`.
VLAN	92950	**Symptom:** Pinging the active gateway IP address succeeds even after shutting down the VLAN interface on which the active gateway is configured. **Scenario:** When an active gateway IP address is configured on a virtual interface and the virtual interface is shut down, a ping to the active gateway from the same switch succeeds.
VLAN	95065	**Symptom:** VLAN 0 tagged traffic with 802.1p priority tags is not treated as native VLAN and causes multicast packets to be flooded. **Scenario:** If Axia xNodes are configured for various types of live and standard stream traffic with the 802.1p tagging feature enabled, when the switch is rebooted multicast packets are flooded. **Workaround:** Disable the 8021.1p tagging feature.
VSX	91601	**Symptom:** VSX keepalive stays in an `INIT` state after a checkpoint restore. **Scenario:** When changing the VRF assignment on a VSX keepalive interface using a checkpoint restore, VSX fails to detect the peer status, reporting the keepalive state stuck at `INIT`.
VSX	92243	**Symptom:** VSX state changes to non-operational and configuration sync stops working. **Scenario:** When adding any new configuration that is expected to be synced to the VSX secondary, the VSX pair may unexpectedly fail to upgrade the secondary member's configuration, causing the VSX status to go into a non-operational state and configuration sync stops working: switch# **show vsx status config-sync** Admin State : Enabled Operational State : Non-Operational Error State : Configuration Sync is disabled
VXLAN	94566	**Symptom:** The switch experiences unexpected VXLAN traffic loss for a few seconds. **Scenario:** When a new configuration is applied using NetEdit or a checkpoint rollback, unexpected VXLAN traffic loss is experienced for a few seconds, even if the new configuration is the same as the configuration the switch was running previously. **Workaround:** Use the CLI to make configuration changes.

Version 10.06.0010

Category	Bug ID	Description
Central	94012	**Symptom:** The switch fails to re-establish a new connection with Aruba Central. **Scenario:** When there is a timeout in the TCP connection to Aruba Central due to WAN link issues, the switch fails to reconnect to Aruba Central. **Workaround:** Clear all existing REST sessions using the `https-server session close` all command.

Category	Bug ID	Description
Counters	89034, 89813, 92972, 93413	**Symptom:** Interface TX drop counters incorrectly increment and do not reflect actual traffic drops. The issue manifests when the switch receives a unicast packet with a learned destination port and that packet is dropped or redirected to the CPU. **Scenario:** There are multiple scenarios where this can happen: 1. ACLs - unicast packet is destined to a learned port but is denied by an ACL 2. Security applications - unicast packet is destined to a learned port but is redirected to the CPU for inspection, such as DHCP Snooping 3. MAC SA = MAC DA - unicast packet that is dropped as a loop prevention mechanism, sometimes transmitted by other network devices 4. ICMP redirects In all cases, the port the packet was destined to is the interface that will show Tx drops for the above conditions. **Workaround:** Disable ICMP using the `no ip icmp redirect` command.
NetEdit	93906	**Symptom/Scenario:** CoPP policies that exist in the running config are not retained when editing/updating/pushing a config using NetEdit. **Workaround:** Use the switch CLI instead of NetEdit when editing a running config that has a CoPP policy.
PBR	93218	**Symptom/Scenario:** Policy-based routing does not work when the next hop is on the VXLAN tunnel.
Spanning Tree	94199	**Symptom:** An unexpected spanning tree topology change is displayed. **Scenario:** When pushing any configuration changes through NetEdit onto a switch that has PVST enabled on a LAG port with default port priority, an STP topology change occurs.
VRF	91612	**Symptom:** An error message similar to `00001|nl_utils|ERR|Unable to set namespace VRF_10 in the thread, error 22 Internal error, vrf not found.` is displayed. **Scenario:** When multiple features, such as RADIUS or ping, access a name space or one feature accesses a name space multiple times, an error message similar to `00001|nl_utils|ERR|Unable to set namespace VRF_10 in the thread, error 22 Internal error, vrf not found.` is displayed.
VSX	92243	**Symptom:** The VSX status is seen as non-operational and configuration sync does not work. **Scenario:** When adding any new configuration that is expected to be synced to the VSX secondary, the VSX pair may unexpectedly fail to upgrade the secondary member's configuration, causing the VSX status to change to non-operational and configuration sync to stop working. **Workaround:** Reboot the secondary VSX member.

Version 10.06.0002

Category	Bug ID	Description
DHCP Server	93746	**Symptom:** The switch CPU is elevated and the output of the `top` command shows a DHCP process consuming 100% of the CPU. **Scenario:** If VSX is enabled with empty content and the DHCP server is configured on the switch, the DHCP server daemon uses 100% of the CPU and restarts. **Workaround:** Remove the VSX configuration using the `no vsx` command.
QoS	91563	**Symptom/Scenario:** VXLAN traffic having non-default DSCP values does not use the desired egress queues, which are mapped to the QoS DSCP configuration on the switch.
SNMP	93608	**Symptom:** The switch reports an incorrect value for the `ifSpeed` MIB object. **Scenario:** When a LAG interface has a bandwidth greater than 4.2GB, the switch reports an incorrect value for the LAG interface in the `ifSpeed` MIB object.
Web UI	90636	**Symptom:** The NAE graph for LAG Health Monitor is frozen with a spinning circle animation indicating the graph is fetching data. **Scenario:** When the LAG Health Monitor NAE script has been installed and an agent created for the script, but only one LAG has been configured, if a second LAG is added to the agent, the LAG Health Monitor graph freezes and will not display new data. **Workaround:** Remove the agent and recreate it with both LAGs.

Version 10.06.0001

Category	Bug ID	Description
CLI	93570	**Symptom:** Interface descriptions for logical interfaces are missing from the output of the `show interface brief` command. **Scenario:** Even after adding descriptions to logical interfaces like SVIs and LAGs, the description column of the `show interface brief` command displays `--`.
REST	86959	**Symptom/Scenario:** The REST API returns an empty list [ ] instead of an empty dictionary { } when no data is available.

Category	Bug ID	Description
SNMP	78836	**Symptom:** The switch displays the `No such object available on this agent at this OID` message. **Scenario:** When an SNMP walk of the Q-Bridge MIB is performed, the message `No such object available on this agent at this OID` is displayed.
SSH	76056	**Symptom:**`Permission denied` messages, that are not relevant to the performed task, are displayed. **Scenario:** When a switch administrator, whose CLI session was authenticated through TACACS or RADIUS, issues a `copy support-fails all` command, and the location they specify is a remote SFTP server, a `Permission denied` error message is incorrectly displayed. **Workaround:** Do not perform SSH/SFTP client operations as a TACACS or RADIUS user.

Issues and Workarounds

The following are known open issues with this branch of the software.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue.

Version 10.06.0110

Category	Bug ID	Description
BGP	37739	**Symptom:** When the switch uses route leaking and a BGP peer to learn the same route, the switch may incorrectly install the two routes as ECMP routes. **Scenario:** In a multi-VRF environment, while performing mutual route leaking on the VRRP peers with BGP neighborship established in between and towards the upstream network, the switch installs both routes as ECMP instead of preferring the leaked route. **Workaround:** Use OSPF routing between VRRP peers instead of BGP.
ICMP Redirect	86208	**Symptom:** The switch sends duplicate ICMP packets. **Scenario:** In a VSX topology with ICMP redirect enabled, the switch may incorrectly duplicate redirected ICMP packets. **Workaround:** Disable the ICMP redirect feature.
OSPF	08491	**Symptom/Scenario:** OSPFv2 and OSPFv3 do not support detailed LSA `show` commands. **Workaround:** Use the `diag ospf[v6] lsdb dump` command under the `diagnostics` menu to view LSA details.

Category	Bug ID	Description
VRF	72044	**Symptom:** The switch fails to program routes for some VRFs if the VRF name is over 31 characters. **Scenario:** When configuring multiple VRFs with names matching up to the first 31 characters, the switch fails to correctly program some route entries. **Workaround:** Configure VRF names with less than 31 characters.
VRRP	24910	**Symptom:** Unable to configure the same IPv6 link-local address as the primary virtual IP address under different VRFs. **Scenario:** Unique virtual link-local addresses have to be configured for all VRRP IPv6 instances irrespective of VRF. **Workaround:** Do not use the same virtual link-local address across different VRFs.

Feature Caveats

Feature	Description
Classifiers	For Classifier policy modifications to be secure, Aruba strongly encourages modifications be done as a two-step process: Bring down the port and then modify.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
DHCP Server and DHCP Relay	DHCP Relay and DHCP Server cannot co-exist on the same switch.
MACsec	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	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	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	In an environment with devices running AOS-Switch, do not enable UDLD on both links. The UDLD session can toggle between up and down continuously when both MACsec and UDLD is enabled on the same link.
Multicast and VXLAN	RP on VSX is not supported. ROP extension for VSX border leaf for clients is not supported.

Feature	Description
	VXLAN must be configured prior to configuring VSX.
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.
VRRP and VXLAN	VRRP and VXLAN are mutually exclusive.
VSX and Static VXLAN	Static VXLAN on VSX configuration is not supported. Use VSX and EVPN or VSX and HSC.

Upgrade Information

Version 10.06.0110 uses ServiceOS LL.01.07.0003.

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*.

Multicast flows in symmetric IRB with VXLAN overlay is not supported when the multicast source is connected to the switch.

Performing the upgrade

1. Copy the LL.10.06.0110 image into the primary boot bank on the switch using your preferred method.
2. Invoke the command to allow unsafe updates to proceed after a switch reboot. Proceed to step 3 within the configured time.

```
switch# config
switch(config)# allow-unsafe-updates 30

This command will enable non-failsafe updates of programmable devices for
the next 30 minutes.  You will first need to wait for all line and fabric
modules to reach the ready state, and then reboot the switch to begin
applying any needed updates.  Ensure that the switch will not lose power,
be rebooted again, or have any modules removed until all updates have
finished and all line and fabric modules have returned to the ready state.

WARNING: Interrupting these updates may make the product unusable!
```

```
Continue (y/n)? y
```

3. On the switch console port an output similar to the following will be displayed as various components are being updated:
4. Multiple components will be updated and several reboots will be triggered during these updates. When all component updates are completed, the switch console port will arrive at the login prompt with a display similar to following:

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

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

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

switch login:
```

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

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 10.06.0100

For 10.06 versions starting with 10.06.0100, in the *AOS-CX 10.06 VXLAN EVPN Guide*, on page 56 the "VSX failure scenarios" table, the rows that currently read:

Failure scenarios	Result with split recovery off	Result with split recovery on (default)
a) ISL down, VSX Keepalive up.	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure that VXLAN traffic is only sent to the primary VSX switch.	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure VXLAN traffic is only sent to the primary VSX switch.

Failure scenarios	Result with split recovery off	Result with split recovery on (default)
a) ISL down, VSX Keepalive up. b) Then, after sometime, VSX Keepalive down as well.	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure VXLAN traffic is only sent to the primary VSX switch. Secondary VSX LAGs and logical VTEP stay down.	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure that VXLAN traffic is only sent to the primary VSX switch. Secondary VSX node restores VSX LAG member ports and brings up logical VTEP. **NOTE:** Without ISL ARP sync, in routing scenarios, this split condition may lead to traffic loss where ARP request originated from a VSX device and reply lands on the peer VSX device.
a) ISL and keepalive are down b) Keepalive restore	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP(If it was UP earlier) to ensure that VXLAN traffic is only sent to primary VSX switch.	Secondary VSX node tears down VSX LAG member ports and brings down logical VTEP to ensure that VXLAN traffic is only sent to primary VSX switch.

should be changed to read:

Failure scenarios	Result with split recovery off	Result with split recovery on (default)
a) ISL down, VSX Keepalive up.	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VXLAN traffic is only sent to the primary VSX switch from other VTEPs.	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VXLAN traffic is only sent to the primary VSX switch from other VTEPs.
a) ISL down, VSX Keepalive up. b) Then, after sometime, VSX Keepalive down as well.	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VXLAN traffic is only sent to the primary VSX switch from other VTEPs. Secondary VSX LAGs and logical VTEP reachability stay down.	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VXLAN traffic is only sent to the primary VSX switch from other VTEPs Secondary VSX node restores VSX LAG members and reachability to the logical VTEP is restored in the underlay. **NOTE:** Without ISL ARP sync, in routing scenarios, this split condition may lead to traffic loss where ARP request originated from a VSX device and reply lands on the peer VSX device.

Failure scenarios	Result with split recovery off	Result with split recovery on (default)
a) ISL and keepalive are down b) Keepalive restore	Secondary VSX node tears down VSX LAG member ports and Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VxLAN traffic is only sent to the primary VSX switch from other VTEPs.	Secondary VSX node tears down VSX LAG member ports and it withdraws the reachability to the logical VTEP IP in the underlay to ensure that VxLAN traffic is only sent to the primary VSX switch from other VTEPs.

The original wording of the table still applies to all 10.06 versions released prior to version 10.06.0100.

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.