AOS-CX 10.08.1010 Release Notes
8320 Switch Series
Copyright Information
© Copyright 2021 Hewlett Packard Enterprise Development LP.

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

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

Notices
The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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

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

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

If you run the `show version` command on the switch, the version number will display TL.10.08.xxxx, where xxxx is the minor version number.

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

Version 10.08.0001 is the initial build of major version 10.08 software.

Product series supported by this software:

- Aruba 8320 Switch Series

**Important information**

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

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

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

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

If using the Web UI, you should clear the browser cache after upgrading to this version of software before logging into the switch using a Web UI session. This will ensure the Web UI session downloads the latest changes.
If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00xx version of software to 10.08.xxxx. To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where `<VLAN_ID>` is the native VLAN ID configured on the trunk interface.

If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

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, TL.10.06.0100). This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.
2. Copy the backup checkpoint into the startup-config.
3. Boot the switch to the target version (lower version), making sure to select `no` when prompted to save the current configuration.

**Industry and government certifications**

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

- Common Criteria: [https://www.niap-ccevs.org/Product/](https://www.niap-ccevs.org/Product/)
- FIPS 140-2: [https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search)
- DoDIN APL: [https://aplis.disa.mil/processAPList.action](https://aplis.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:
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](https://hpe.com/software/opensource)

## Version history

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

<table>
<thead>
<tr>
<th>Version number</th>
<th>Release date</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08.1010</td>
<td>2021-09-21</td>
<td>Released, fully supported, and posted on the web.</td>
</tr>
<tr>
<td>10.08.0001</td>
<td>2021-08-13</td>
<td>Initial release of AOS-CX 10.08. Released, fully supported, and posted on the web.</td>
</tr>
</tbody>
</table>

## Products supported

This release applies to the following product models:

<table>
<thead>
<tr>
<th>Product number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JL479A</td>
<td>Aruba 8320 48p 10G SFP/SFP+ and 6p 40G QSFP+ with X472 5 Fans 2 Power Supply Switch Bundle</td>
</tr>
<tr>
<td>JL579A</td>
<td>Aruba 8320 32p 40G QSFP+ with X472 5 Fans 2 Power Supply Switch Bundle</td>
</tr>
<tr>
<td>JL581A</td>
<td>Aruba 8320 48p 1G/10GBASE-T and 6p 40G QSFP+ with X472 5 Fans 2 Power Supply Switch Bundle</td>
</tr>
</tbody>
</table>

## Compatibility/interoperability

The switch web agent supports the following web browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Minimum supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge (Windows)</td>
<td>41</td>
</tr>
<tr>
<td>Chrome (Ubuntu)</td>
<td>76 (desktop)</td>
</tr>
<tr>
<td>Firefox (Ubuntu)</td>
<td>56</td>
</tr>
<tr>
<td>Safari (MacOS)</td>
<td>12</td>
</tr>
<tr>
<td>Safari (iOS)</td>
<td>10 (Version 12 is not supported)</td>
</tr>
</tbody>
</table>
Recommended versions of network management software for switches found in this release note:

<table>
<thead>
<tr>
<th>Management software</th>
<th>Recommended version(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airwave</td>
<td>8.2.13.1</td>
</tr>
<tr>
<td>NetEdit</td>
<td>2.1.2</td>
</tr>
<tr>
<td>Aruba CX Mobile App</td>
<td>2.6.6 (or later)</td>
</tr>
<tr>
<td>Aruba Central</td>
<td>2.5.4 (supports both Template and UI groups)</td>
</tr>
<tr>
<td>Network Automation</td>
<td>10.10, 10.11, 10.20, 10.21, 10.30, 10.40</td>
</tr>
<tr>
<td>Network Node Manager</td>
<td>10.10, 10.20, 10.21, 10.30, 10.40</td>
</tr>
<tr>
<td>IMC</td>
<td>7.3 (E0705P12)</td>
</tr>
</tbody>
</table>

For more information, see the respective software manuals.

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

Minimum supported software versions

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

<table>
<thead>
<tr>
<th>Product number</th>
<th>Product name</th>
<th>Minimum software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>JL579A</td>
<td>Aruba 8320 32p 40G QSFP+ with X472 5 Fans 2 Power Supply Switch Bundle</td>
<td>10.00.0008</td>
</tr>
<tr>
<td>JL581A</td>
<td>Aruba 8320 48p 1G/10GBASE-T and 6p 40G QSFP+ with X472 5 Fans 2 Power Supply Switch Bundle</td>
<td>10.00.0013</td>
</tr>
</tbody>
</table>

Transceiver support

Changes to transceiver support with this version of software:

- No new transceiver support

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

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

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

### Version 10.08.1010

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics</td>
<td>AIOPS - NAE Agent and Engine improvements for unicast routing. AIOPS - NAE Agent and Engine improvements for client services.</td>
</tr>
</tbody>
</table>

### Version 10.08.0001

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>BGP fast-external-failover is now enabled by default.</td>
</tr>
<tr>
<td>DHCP relay</td>
<td>Added DHCP relay coexistence with DHCP server for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>Inclusive terminology</td>
<td>As part of advancing HPE’s and Aruba’s commitment to racial justice, we are taking a much-needed step in overhauling engineering terminology to reflect our belief system of diversity and inclusion. See <a href="https://blogs.arubanetworks.com/spectrum/our-responsibility-to-stand-up-to-racism-and-inequality/">https://blogs.arubanetworks.com/spectrum/our-responsibility-to-stand-up-to-racism-and-inequality/</a> for Aruba’s stand on inclusivity.</td>
</tr>
<tr>
<td>Job Scheduler</td>
<td>Added the ability to execute required CLI commands at a specific time and date. This can be repeated at periodic intervals.</td>
</tr>
<tr>
<td>Loopback IP redistribution in OSPF</td>
<td>Allows redistribution of IPv4 and IPv6 addresses of loopback interfaces in OSPFv2 and OSPFv3.</td>
</tr>
<tr>
<td>MAC Tables 74408</td>
<td>Added an SNMP trap notification if there is a MAC address change.</td>
</tr>
<tr>
<td>MAC Tables 84378</td>
<td>Added the <code>clear mac</code> command to delete a specific MAC on one or more VLANs.</td>
</tr>
<tr>
<td>Network Load Balancing (NLB)</td>
<td>Provides load balancing technology for server clustering developed on Microsoft Windows Server. Supports load sharing and redundancy among servers within a cluster.</td>
</tr>
<tr>
<td>Security</td>
<td>Ensures configuration integrity. Limit concurrent users for web access.</td>
</tr>
<tr>
<td>Transceivers 160269</td>
<td>Added display in dBM for DOM thresholds in the output of the <code>show interface dom detail</code> command.</td>
</tr>
<tr>
<td>VSX 162842</td>
<td>Updated the warning message displayed when shutting down an Switch Virtual Interface (SVI) with an active gateway enabled to be more informative about the risks of doing such a shutdown.</td>
</tr>
</tbody>
</table>
Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The Bug ID is used for tracking purposes.

Version 10.08.1010

<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| ACLs     | 193057 | **Symptom:** The switch crashes when a VLAN ACL is configured using REST.  
**Scenario:** When REST is used to configure a VLAN ACL using in rather than routed-in, the switch crashes. |
| Logging  | 195946 | **Symptom/Scenario:** An error message is logged that says the cron daemon was unable to move a log file because the name is too long. |
| PIM-SM   | 190657 | **Symptom/Scenario:** The switch does not elect the correct BSR after changing the BSR priority or changing to auto RP from static RP.  
**Workaround:** Configure the candidate BSR on only one note of the VSX environment or toggle the router PIM status using the `router pim disable` and `router pim enable` commands. |
| SNMP     | 189372 | **Symptom:** `dot1dStpPortPathCost` reflects the open-path-cost and does not match the CLI.  
**Scenario:** When using SNMP to identify spanning tree state and values, `dot1dStpPortPathCost` does not report the value it should.  
**Workaround:** Use the `show spanning-tree` command to view the correct values. |
| SNMP     | 189953 | **Symptom/Scenario:** `snmpget` returns an error message of Unsupported security level.  
**Workaround:** Reboot the switch. |
| TACACS   | 194803 | **Symptom:** The user is authenticated as local rather than remote (TACACS).  
**Scenario:** When the TACACS server is configured with FQDN and TACACS authentication is configured, the user is authenticated with local credentials instead of with remote TACACS authentication.  
**Workaround:** Configure the TACACS server with an IP address rather than FQDN. |
| VRRP     | 189958 | **Symptom:** The VRRP high priority master ignores the configured Preempt Delay Timer (PDT) and assumes the Master role only after the Master Down Timer (MDT) expiry after reboot.  
**Scenario:** When the PDT is configured with a higher value than the
### Category: Bug | Bug ID: 9 | Description:

MDT, the PDT is ignored by the VRRP high priority master which waits for the PDT to expire before going to Master after a reboot. **Workaround:** Configure the MDT to be greater than or equal to the PDT.

### Category: VSX Sync | Bug ID: 193962 | Description:

**Symptom:** VSX sync stops working. Logs still show activity in the secondary VSX sync, but no updates are received from the primary switch.

**Scenario:** In a VSX topology when both switches become disconnected (for example, through an ISL disconnect or a failover) for an extended period of time, VSX sync stops working when the switches come back online.

**Workaround:** On the secondary switch, restart te VSX sync using the `systemctl restart vsx-syncd` command.

### Version 10.08.0001

<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>191536</td>
<td><strong>Symptom/Scenario:</strong> When the switch is rebooted with an SVI shutdown, if the IP address is changed and the SVI re-enabled, the old VLAN IP address still replies to an ARP request received. <strong>Workaround:</strong> Delete and then add back the SVI.</td>
</tr>
</tbody>
</table>
| Credential Manager | 94938 | **Symptom:** During boot, the following message is observed, after which the features to not function:

```
... ...
[OK] Starting HPE Credential Manager.
... ...
[FAILED] Failed to start HPE Credential Manager.
See 'systemctl status hpe-credmgr.service' for details.
[OK] Stopped HPE Credential Manager.
Starting HPE Credential Manager.
... ...
``` |
### Issues and workarounds

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

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

#### Version 10.08.1010

<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| OSPF       | 149301 | **Symptom:** The switch shows unexpected behavior in the OSPFv2/3 DLOGs.  
**Scenario:** When `debug ospfv2 packet` or `debug ospfv3 packet` is enabled with the `ip` filter, the switch shows unexpected behavior in the OSPFv2/3 DLOGs.  
**Workaround:** Use `debug ospfv2 packet` or `debug ospfv3 packet` with the `port` filter and `grep` for the required IP (v4 or v6) address. |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| **BGP**                         | In a multi-VRF environments, while performing mutual route leaking on the VRRP peers with BGP neighborship established in between and towards the upstream network, the switch will install both routes as ECMP instead of preferring the leaked route. Use route-maps to give lower/higher preference to the routes received from an iBGP peer. For example:  
  
  ```  
  !  
  route-map rmap permit seq 10  
  set local-preference 50  
  !  
  router bgp 100  
  vrf red  
  neighbor 1.1.1.2 remote-as 100  
  address-family ipv4 unicast  
  neighbor 1.1.1.2 activate  
  neighbor 1.1.1.2 route-map rmap in  
  exit-address-family  
  ```  
  In the above example, since a lower value of local-preference (i.e. 50, whereas default value is 100) has been set to the routes received from iBGP peer, the leaked routes get preferred and get installed as best routes. |
| Classifiers                     | 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                             | Automatic downgrade of the startup-config is not supported during a software downgrade. To restore a configuration use the procedure documented under Manual configuration restore for software downgrade.                               |
| CMF                             | No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.                                                                                                                 |
| Counters                        | Layer 3 Route-only port counters are not enabled by default. Enabling them will reduce ipv4 route scale to 80K.                                                                                                 |
| ICMP Redirect                   | The switch may incorrectly duplicate an IP frame that triggers ICMP redirect.                                                                                                                                   |
| IGMP/PIM on Loopback and GRE interfaces | IGMP cannot be enabled on both Loopback and GRE interfaces. PIM can be enabled on a Loopback interface. PIM will not work on GRE tunnels and 6in6.                                                            |
| Multicast and VXLAN             | Multicast traffic with a Null Source IP (0.0.0.0) gets flooded.                                                                                                                                               |
| 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 Analytics 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Analytics Engine (NAE)</td>
<td>The following tables are not supported for NAE scripts: OSPF_Route, OSPF_LSA, OSPF_Neighbor, BGP_Route.</td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPFv2 and OSPFv3 do not support detailed LSA show commands.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Authorization by means of HPE VSAs is not supported.</td>
</tr>
<tr>
<td>REST</td>
<td>REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.</td>
</tr>
<tr>
<td>RIP/RIPng</td>
<td>Redistribute RIP/RIPng is not supported in BGP/BGP+.</td>
</tr>
<tr>
<td>RIP/RIPng</td>
<td>RIP/RIPng metric configuration support is not available.</td>
</tr>
<tr>
<td>RPVST+ and MSTP</td>
<td>Spanning Tree can only run in MSTP or RPVST+ mode.</td>
</tr>
<tr>
<td>RPVST+ and MVRP</td>
<td>RPVST+ is mutually exclusive with MVRP.</td>
</tr>
<tr>
<td>VRF</td>
<td>VRF names are limited to 31 characters.</td>
</tr>
<tr>
<td>VRRP</td>
<td>The same virtual link-local address cannot be used across different VRFs.</td>
</tr>
<tr>
<td>VRRP-MD5 authentication interop</td>
<td>Not supported with Comware-based switches</td>
</tr>
<tr>
<td>VRRP</td>
<td>VRRP Preemption Delay Timer (preempt delay minimum) may be ignored after a switch reboot or power cycle.</td>
</tr>
</tbody>
</table>

**Upgrade information**

Version 10.08.1010 uses ServiceOS TL.01.08.0002.
If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00xx version of software to 10.08.xxxx.

To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where `<VLAN_ID>` is the native VLAN ID configured on the trunk interface.

If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

10.03 is the minimum required software version prior to upgrading to 10.06. If your device is using a version of software prior to 10.03, you must first upgrade to a version of 10.03 before upgrading to 10.06. Check release notes for the software version you will upgrade to for instructions on performing the upgrade to 10.03.

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

When upgrading from software versions before 10.05.0001, if the switch is configured with an entry in a class-map or an Access List that matches AH or ESP traffic, the policy will fail to apply, as these options are no longer permitted. Remove such entries from the configuration prior to upgrading to 10.08.1010 or remove the respective entries from ACLs or Class that failed to apply after the upgrade to 10.08.1010.
When upgrading from a version of software prior to version 10.05.0001, if the switch is configured with IGMP or MLD snooping options such as "forward", "fastleave", "forced-fastleave", or "blocked" at the VLAN context, after upgrading to this software version, you will need to reconfigure these options for each interface from the interface configuration context.

Example config before 10.05.0001:

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

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

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

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

### Manual configuration restore for software downgrade

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

1. Use the `show checkpoint` command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the Image Version column in the output of the command, for example, TL.10.06.0100). This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.

2. Copy the backup checkpoint into the startup-config.

3. Boot the switch to the target version (lower version), making sure to select no when prompted to save the current configuration.

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

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

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

   ```
   switch# boot system secondary
   Default boot image set to secondary.
   Checking if the configuration needs to be saved...
   Checking for updates needed to programmable devices...
   Done checking for updates.
   This will reboot the entire switch and render it unavailable until the process is complete.
   Continue (y/n)? n
   ```

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

   ```
   switch# boot system secondary
   Default boot image set to secondary.
   Checking if the configuration needs to be saved...
   Checking for updates needed to programmable devices...
   Done checking for updates.
   2 device(s) need to be updated during the boot process.
   The estimated update time is between 2 and 3 minute(s).
   There may be multiple reboots during the update process.
   1 non-failsafe device(s) also need to be updated.
   Please run the 'allow-unsafe-updates' command to enable these updates.
   This will reboot the entire switch and render it unavailable until the process is complete.
   Continue (y/n)? n
   ```

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

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

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

WARNING: Interrupting these updates may make the product unusable!

Continue (y/n)? y

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

4. Use the `boot system <BOOT-BANK>` command to initiate the upgrade. On the switch console port an output similar to the following will be displayed as various components are being updated:

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

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

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

This will reboot the entire switch and render it unavailable until the process is complete.
Continue (y/n)? y
The system is going down for reboot.

Looking for SVOS.

Primary SVOS:  Checking...Loading...Finding...Verifying...Booting...

ServiceOS Information:
Version:  <serviceOS_number>
Build Date:  yyyy-mm-dd hh:mm:ss PDT
Build ID:  ServiceOS:<serviceOS_number>:6303a2a501ba:202006171659
SHA:  6303a2a501bad91100d9e71780813c59f19c12fe

Boot Profiles:
0. Service OS Console
1. Primary Software Image [xx.10.07.0020]
2. Secondary Software Image [xx.10.08.1010]

Select profile(secondary):

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

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

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

MODULE 'mc' DEVICE 'svos_primary':
  Current version : '<serviceOS_number>'
  Write-protected : NO
  Packaged version : '<version>'
  Package name : '<svos_package_name>'
  Image filename : '<filename>.svos'
  Image timestamp : 'Day Mon dd hh:mm:ss yyyy'
  Image size : 22248723
  Version upgrade needed

Starting update...

Writing... Done.
Erasing... Done.
Reading... Done.
Verifying... Done.
Reading... Done.
Verifying... Done.

Update successful (0.5 seconds).
reboot: Restarting system

Multiple components may be updated and several reboots will be triggered during these updates. When all component updates are completed, the switch console port will arrive at the login prompt with a display similar to following:

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

RESTRICTED RIGHTS LEGEND

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

switch login:

Aruba recommends waiting until all upgrades have completed before making any configuration changes.
A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

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


**Security bulletin subscription service**