

Understanding and Deploying PKI on Aruba CX Switches

!!IMPORTANT!!

THIS GUIDE ASSUMES THAT THE AOS-CX OVA HAS BEEN INSTALLED AND WORKS IN GNS3 OR EVE-NG. PLEASE REFER TO GNS3/EVE-NG INITIAL SETUP LABS IF REQUIRED.

TABLE OF CONTENTS

Lab Objective.....	1
Lab Overview.....	1
Lab Network Layout.....	2
Lab Tasks.....	2
Task 1 - Lab setup.....	3
Task 2 - Testing a switch configuration in checkpoint auto mode.....	3
Task 3 – Viewing Checkpoint differences.....	4
Task 4 – Checkpoint rename.....	5
Task 5 – Checkpoint rollback.....	6
Task 6 – Copy Checkpoint.....	6
Task 7 – Removing a Configuration Checkpoint.....	6

Lab Objective

At the end of this workshop, you should be able to describe and demo how to manage the Aruba CX Checkpoint structure and features. This lab will focus on understanding the basics with Aruba CX Switch Checkpoint configurations including checkpoints, rollbacks, copying and removing.

Lab Overview

Checkpoints

A checkpoint is a snapshot of the running configuration of an Aruba CX switch and its relevant metadata during the time of creation. Checkpoints can be used to apply the switch configuration stored within a checkpoint whenever needed, such as to revert to a previous, clean configuration. Checkpoints can be applied to other switches of the same platform.

The Aruba CX switches support the following types of checkpoints (up to 64 total - including the startup configuration):

- **System generated checkpoints:** The switch automatically generates a system checkpoint whenever a configuration

change occurs.

- System generated checkpoints are automatically created by default. Whenever a configuration change occurs, the switch starts a timeout counter (300 seconds by default). For each additional configuration change, the timeout counter is restarted. If the timeout expires with no additional configuration changes being made, the switch generates a new checkpoint.
- System generated checkpoints are named with the prefix CPC followed by a time stamp in the format <YYYYMMDDHHMMSS>. For example: CPC20170630073127.
- System checkpoints can be applied using the checkpoint rollback feature or copy command.
- Maximum system checkpoints: 32
- **User generated checkpoints:** The administrator can manually generate a checkpoint whenever required.
 - User checkpoints can be created at any time, as long as one configuration difference exists since the last checkpoint was created. Checkpoints can be applied to either the running or startup configurations on the switch.
 - All user generated checkpoints include a time stamp to identify when a checkpoint was created.
 - Maximum user checkpoints: 32

The Aruba CX switches support configuration rollbacks which is when the switch configuration is reverted to a pre-existing checkpoint.

Checkpoint auto mode configures the switch with failover support, causing it to automatically revert to a previous configuration if it becomes inoperable or inaccessible due to configuration changes that are being made.

Lab Network Layout

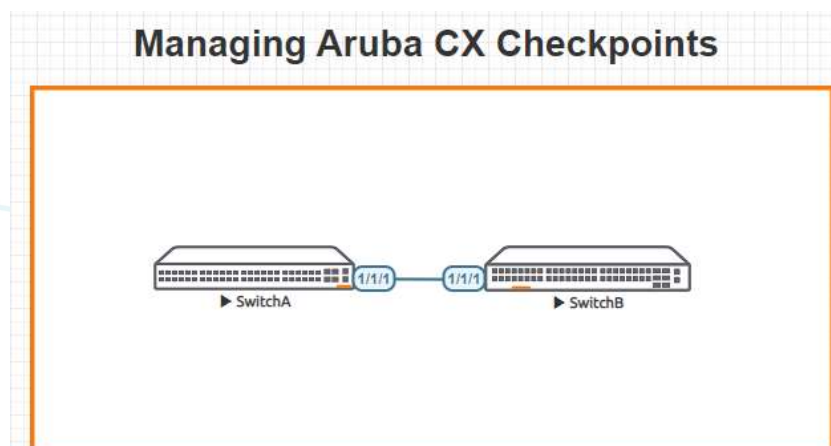


Figure 1. Lab topology

Lab Tasks

Task 1 - Lab setup

For this lab refer to Figure 1 for topology and IP address details.

- Start all the devices, including host and client
- Open each switch console and log in with user "admin" and no password
- Change all hostnames as shown in the topology:
hostname ...
- On all devices, bring up required ports:
int 1/1/1
no shutdown
- Validate LLDP neighbors appear as expected
show lldp neighbor

SwitchB

```
SwitchB# show lldp neighbor
```

```
LLDP Neighbor Information
=====
```

```
Total Neighbor Entries      : 2
Total Neighbor Entries Deleted : 0
Total Neighbor Entries Dropped : 0
Total Neighbor Entries Aged-Out : 0
```

LOCAL-PORT	CHASSIS-ID	PORT-ID	PORT-DESC	TTL	SYS-NAME
1/1/1	08:00:09:ee:11:82	1/1/1	1/1/1	120	SwitchA

Task 2 - Testing a switch configuration in checkpoint auto mode

- Enable the checkpoint auto mode.
- To save the configuration, enter the checkpoint auto confirm command before the specified time set when running the checkpoint auto command.
- The generated checkpoint name will be in the format AUTO<YYYYMMDDHHMMSS>. If the checkpoint auto confirm command is not entered during the specified time lapse interval, the previous runtime configuration is restored.

SwitchA

```
SwitchA# checkpoint auto 20
Auto checkpoint mode expires in 20 minute(s)
WARNING Please "checkpoint auto confirm" within 2 minutes
```

```
SwitchA# checkpoint auto confirm
checkpoint AUTO20170801011133 created
```

SwitchB

```
SwitchB# checkpoint auto 20
Auto checkpoint mode expires in 20 minute(s)
WARNING Please "checkpoint auto confirm" within 2 minutes
```

```
SwitchA# checkpoint auto confirm
checkpoint AUTO20170801011154 created
```

- Verify with show commands

SwitchA

```
SwitchA# show checkpoint list
CPC20210331205654
CPC20210628171235

SwitchA# show checkpoint CPC20210628171235
Checkpoint configuration:
!Version ArubaOS-CX Virtual.10.05.0001
!export-password: default
hostname SwitchA
led locator on
!
!
!
!
ssh server vrf mgmt
vlan 1
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/1
    no shutdown
!
!
!
!
!
https-server vrf mgmt
-- MORE --, next page: Space, next line: Enter, quit: q
```

Task 3 – Viewing Checkpoint differences

- The `checkpoint diff` command allows users to view the difference in configuration between two configurations. Users can compare checkpoints, the running configuration, or the startup configuration.
 - Syntax = {<CHECKPOINT-NAME1> | running-config | startup-config} {<CHECKPOINT-NAME2> | running-config | startup-config}
 - The plus sign (+) at the beginning of a line indicates that the line exists in the comparison but not in the baseline.
 - The minus sign (-) at the beginning of a line indicates that the line exists in the baseline but not in the comparison.
 - Note that the `checkpoint post-configuration` command enables the creation of system generated checkpoints in the event a configuration changes occur. This feature is enabled by default, and the `no` form of this command disables system generated checkpoints.

SwitchA

```
SwitchA# show checkpoint list
CPC20210331205654
CPC20210628171235
```

```
SwitchA# checkpoint diff running-config CPC20210331205654
--- /tmp/running-config16249029269182021-06-28 17:55:26.917772935 +0000
+++ /tmp/CPC2021033120565416249029269212021-06-28 17:55:26.919772935 +0000
@@ -1,22 +1,17 @@
!
!Version ArubaOS-CX Virtual.10.05.0001
!export-password: default
-hostname SwitchA
+user admin group administrators password ciphertext AQBapaCynQRzUmjzOevmgnBTG9pG9EP
aLYjyj2kk4R2h72vQYgAAACrYeudyX6/UhmfCfbqKTOxQvB+LH+DYmCOIME2DNHJtsNY9WcquQLpKtSTsQZU
8hhEIBcaFrL3btBEVpOJxVoCC+049Zlemzjru/TYrQxr4Xkspy33nNhnABoMyf5sfCiej
 led locator on
-no checkpoint post-configuration
!
!
!
!
 ssh server vrf mgmt
-vlan 1,200
+vlan 1
 interface mgmt
     no shutdown
     ip dhcp
-interface 1/1/1
- no shutdown
-interface vlan 200
- ip address 192.168.200.1/24
```

Task 4 – Checkpoint rename

- The checkpoint rename command allows you to rename a checkpoint to a more preferred name.

SwitchA

```
ARUBACXSWITCH# show checkpoint list
CPC20210331205654
CPC20210628171235
Latest

ARUBACXSWITCH# checkpoint rename latest Mon-June-28-2021

ARUBACXSWITCH# show checkpoint list
CPC20210331205654
CPC20210628171235
Mon-June-28-2021
```

Task 5 – Checkpoint rollback

- The `checkpoint rollback` command provides an easy way to apply a configuration from a pre-existing checkpoint or assign the startup configuration to the running configuration.

```
ARUBACXSWITCH# show checkpoint list
CPC20210331205654
CPC20210628171235
Mon-June-28-2021

ARUBACXSWITCH# checkpoint rollback CPC20210331205654
Copying configuration: [Success]
ARUBACXSWITCH#
switch#
```

Task 6 – Copy Checkpoint

- The Checkpoint Copy command allows you to easily copy an existing checkpoint configuration to the running configuration or to the startup configuration.
- Users can copy the running configuration or the startup configuration to a remote file in either CLI or JSON format using the following syntax
 - `copy {running-config | startup-config} <REMOTE-URL> {cli | json} [vrf <VRF-NAME>]`
- You can also use configs from a remote URL using the following syntax
 - `copy <REMOTE-URL> {running-config | startup-config } [vrf <VRF-NAME>]`

```
switch# show checkpoint list
CPC20210331205654
CPC20210628171235
Mon-June-28-2021

switch# copy checkpoint Mon-June-28-2021 running-config
Copying configuration: [Success]
switch#
ARUBACXSWITCH#
```

Task 7 – Removing a Configuration Checkpoint

- Users can remove a Checkpoint by using the `erase checkpoint` command.

```
ARUBACXSWITCH# show checkpoint list
CPC20210331205654
CPC20210628171235
Mon-June-28-2021

ARUBACXSWITCH# erase checkpoint CPC20210628171235
Erase checkpoint CPC20210628171235 ? (y/n): y

ARUBACXSWITCH# show checkpoint list
```

CPC20210331205654
Mon-June-28-2021
ARUBACXSWITCH#

