LAB GUIDE

Layer 2 Access Switch Management & Connectivity Part II Additions

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.

https://www.eve-ng.net/index.php/documentation/howtos/howto-add-aruba-cx-switch/

TABLE OF CONTENTS

Lab Objective

A prerequisite for this lab is to have completed the lab Layer 2 Access Switch Management & Connectivity.

The lab will enable the user to gain hands on knowledge and experience in setup basic management reachability and connectivity to access Layer 2 switches such as the Aruba CX 6100 to and from an upstream network.

To simulate the Aruba CX 6100, we will limit the features we use in the simulator to replicate this product, such as using default VRF and static routing.

For further details on Aruba CX 6100 switches and other features please refer to the latest Aruba documentation located on https://asp.arubanetworks.com/

This lab provides some additional features that are configurable on the Aruba CX Simulator **but may not function** as expected due to simulator limitations. However, it provides the user some understanding for adapting for real world “Use Cases”

Lab Overview

This lab set up is as shown in Figure 1. Aruba CX simulator will be used at both Access, Aggregation and Management, for completeness to replicate a possible 3 tier topology.

In the *previous* lab SSH Management was achieved to the Layer 2 access switch from the upstream management network was as well as sending traffic from an endpoint to the upstream next hop.

In the overall network architecture, we trunked VLANS from Access to Aggregation for User Data, and made one VLAN have a Layer 3 address on the Access switch to make it reachable for management purposes.

In the *Additional* Items we will look at components to provide some real-world Use Cases, that could be practically used.

- Provide protection on the Layer 2 Access Switch

Lab Network Layout

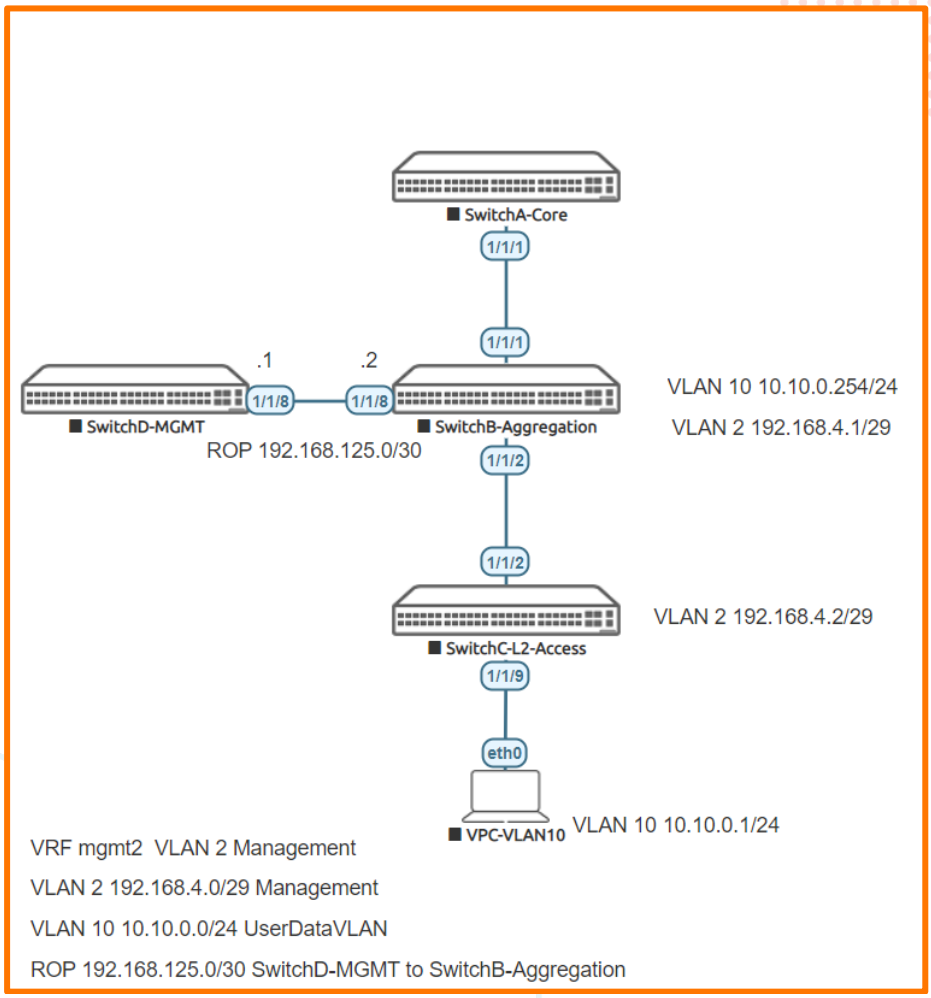

Figure 1. Lab topology

Lab Tasks-Objective

- Limit SNMP and SSH access on the Layer 2 Access Switch
- Minimal SNMP configuration

Task 1 – ACL management protection

We will provide some control plane policing on the access switch to limit management access.
In such a design we must be careful not to block other types of traffic this could provide untoward impacts and block traffic we are actually whishing the switch to process for normal functions.
Thus we take the following approach we specifically allow protocol from known defined hosts, essentially this rule in itself will block and protect from undesirable actors on that protocol. We then create an allow rule for other traffic.

- Allow SSH and SNMP from a particular host
- Block any other SSH and SNMP
- Allow anything else
- On **Switch C**

```
SwitchC#
Configure
access-list ip auth-management
        5 comment allow ssh and snmp
        10 permit tcp 192.168.125.1 192.168.4.2 eq 22 count
        20 permit udp 192.168.125.1 192.168.4.2 eq 161
        30 permit udp 192.168.125.1 192.168.4.2 eq 162
        40 deny tcp any any eq 22
        50 deny udp any any eq 161
        60 deny udp any any eq 162
        190 comment allow anything else
       200 permit any any any
      exit
 apply access-list ip auth-management control-plane vrf default
```

- Now SSH from Switch D to Switch C .

```
admin@192.168.4.2's password:

Last login: 2021-06-30 13:14:24 from the console
User "admin" has logged in 6 times in the past 30 days
SwitchC#
```

- Your SSH session should be successful.
- On Switch C or from your successful SSH Session (D to C) check the ACL counters you should see hits on rule 10

```
show access-list hitcounts ip auth-management control-plane vrf default
```

```
SwitchC# show access-list hitcounts ip auth-management control-plane vrf default
Statistics for ACL auth-management (ipv4):h-management control-plane vrf default
vrf default (control-plane):
     Matched Packets  Configuration
                  12  10 permit tcp 192.168.125.1 192.168.4.2 eq 22 count
                   -  20 permit udp 192.168.125.1 192.168.4.2 eq 161
                   -  30 permit udp 192.168.125.1 192.168.4.2 eq 162
                   -  40 deny tcp any any eq 22
                   -  50 deny udp any any eq 161
                   -  60 deny udp any any eq 162
                   -  200 permit any any any
                   0  implicit deny any any any count
```

- Exit out of your SSH session
- On switch C L2 Access switch remove rule 10 that permits SSH

```
SwitchC#
    configure
    access-list ip auth-management
    no 10
```

- Now attempt SSH from Switch D to Switch C . This
- The session from D should fail, due to rule 40.
- Note on the CX simulator Deny counts are not registered, as of writing this lab (10.06.0110)
- We have no SNMP host and thus will not test it is left to the user to add a host for testing.

Task 2 – SNMP

- The following configurations are provided for completeness, which can serve as a minimal basic template. Task 2 is to complement the previous task, no testing of the configuration with reference to SNMP are provided.

- On **Switch C**

    - Add SNMP access to hosts we need to add a community
    - SNMP traps to a factitious host 1.2.3.4 host are shown

```
SwitchC#
Configure
snmp-server community mypassword
snmp-server host 1.2.3.4 trap version v2c community mypassword
```

NOTE: Default level of SNMP access for CX is typically read only. In actual switching products AOS-CX 10.07 the default behavior can be changed to read write, as well as providing SNMP ACL, not shown on this lab which was written using 10.06.0110 simulator.

Please see the Airheads Community Learning Discussion page for Aruba CX Simulator for details of SNMP labs.

End of lab

Appendix – Complete Configurations

- If you face issues during your lab, you can verify your configs with the configs listed in this section
- If configs are the same, try powering off/powering on the switches to reboot them.

Switch B

```
SwitchB#
led locator on
vrf mgmt2
!
!
!
!
ssh server vrf mgmt
vlan 1
vlan 2
    description management
vlan 10
    description userData
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
interface 1/1/2
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 2,10
interface 1/1/8
    no shutdown
    vrf attach mgmt2
    ip address 192.168.125.2/30
interface vlan 2
    vrf attach mgmt2
    ip address 192.168.4.1/29
interface vlan 10
    ip address 10.10.0.254/24
!
!
!
!
!
https-server vrf mgmt
SwitchB#
```

Switch C

```
hostname SwitchC
led locator on
!
!
!
!
ssh server vrf default
ssh server vrf mgmt
access-list ip auth-management
    5 comment allow ssh and snmp
    20 permit udp 192.168.125.1 192.168.4.1 eq 22 count
    30 permit udp 192.168.125.1 192.168.4.2 eq 162
    40 deny tcp any any eq 22 count
    50 deny udp any any eq 161
    60 deny udp any any eq 162
    190 comment allow anything else
    200 permit any any any
apply access-list ip auth-management control-plane vrf default
vlan 1
vlan 2
    description management
vlan 10
    description UserData
```

```
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/2
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 2,10
interface 1/1/9
    no shutdown
    no routing
    vlan access 10
interface vlan 2
    ip address 192.168.4.2/29
snmp-server community mypassword
snmp-server host 1.2.3.4 trap version v2c community mypassword
ip route 0.0.0.0/0 192.168.4.1
!
!
ip source-interface tftp 192.168.4.2
ip source-interface syslog 192.168.4.2
https-server vrf mgmt
```

Switch D

```
SwitchD#
hostname SwitchD
led locator on
!
!
ssh server vrf mgmt
vlan 1
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/8
    no shutdown
    ip address 192.168.125.1/30
ip route 0.0.0.0/0 192.168.125.2
!
!
!
!
!
https-server vrf mgmt
SwitchD#
```

aruba
a Hewlett Packard
Enterprise company

www.arubanetworks.com

3333 Scott Blvd. Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com