LAB GUIDE

a Hewlett Packard Enterprise company

Part II Campus 2 Tier. Layer 3 Access with OSPF and Security

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

The lab will enable the user to gain hands on knowledge and experience in setup basic Campus 2 Tier Network with L3 Access using OSPF with Security for OSPF links.

Aruba CX 6200 and 6300 typically can be used for L3 access in the Campus.

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

Lab Overview

This lab set up is as shown in Figure 1. This lab is a follow and it is a prerequisite to have Part I Campus Tier 2 Layer 3 Access with OSPF completed where the underpinning infrastructure was built.

In this follow on lab we will secure the OSPF links, this acts as a precaution so that limited influence can be injected into the network by unknowingly misconfigurations or from potential bad actors. Some basic trouble shooting steps are also shown and explained

Lab Network Layout

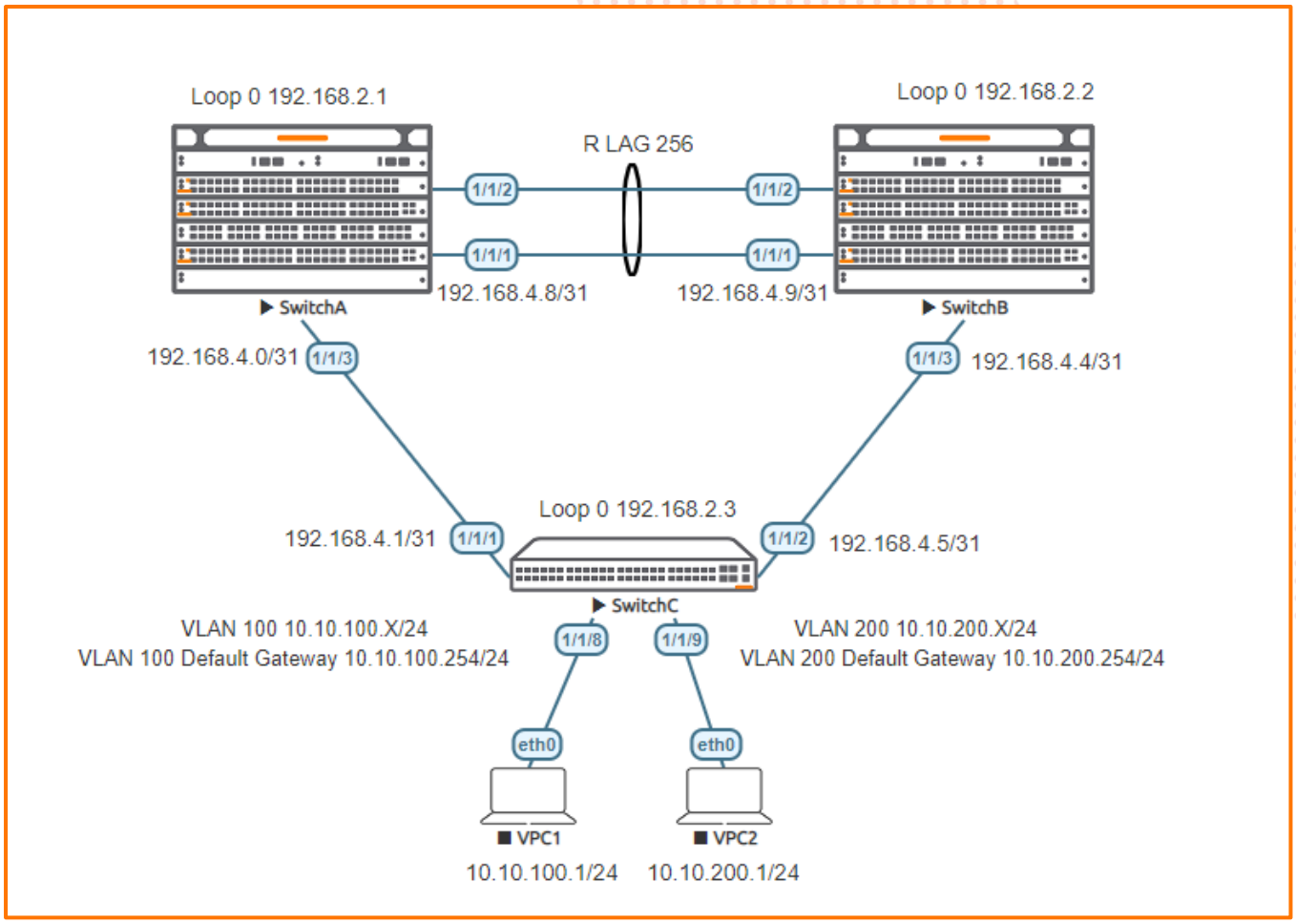

Figure 1. Lab topology

Lab Tasks

Task 1 - Lab setup

Prerequisite please complete the lab “Part I Campus Tier 2 Layer 3 Access with OSPF”

Task 2 - Configure OSPF security between links between Campus Core

On **Switch A and B** Core configure:

- Add MD5 authentication between the two cores
- **Note** as part of the configuration you add a password between the communicating links these must match on both sides of the link for the link to come up correctly

SwitchA#	**SwitchB#**

`interface lag 256`
`ip ospf authentication message-digest`
`ospf message-digest-key 1 md5 plaintext`
`<your_password_here>`
	`interface lag 256`
	`ip ospf authentication message-digest`
	`ospf message-digest-key 1 md5 plaintext`
	`<your_password_here>`

- Ensure the OSPF neighbors remain intact after the configuration as shown below. Here we show output from Switch A

```
SwitchA#
show ip ospf neighbors
VRF : default                          Process : 1
================================================

Total Number of Neighbors : 2

Neighbor ID      Priority  State            Nbr Address      Interface
-------------------------------------------------------------------------
192.168.2.3      n/a       FULL             192.168.4.1        1/1/3

192.168.2.2      n/a       FULL             192.168.4.9        lag256
```

- You can show you have authentication on the LAG

```
SwitchA#
show ip ospf interface lag 256
Codes: DR - Designated router  BDR - Backup Designated router

Interface lag256 is up, line protocol is up
-------------------------------------------

VRF             : default                        Process             : 1
IP Address      : 192.168.4.8/31                 Area                : 0.0.0.0

Status          : up                             Network Type        : Point-to-poi
nt
Hello Interval  : 10  sec                        Dead Interval       : 40  sec
Transit Delay   : 1   sec                        Retransmit Interval : 5   sec
Authentication  : Md5                            Link Speed          : 2000Mbps
Cost Configured : NA                             Cost Calculated     : 50
State/Type      : Point-to-point                 Router Priority     : n/a
DR              : No                             BDR                 : No
Link LSAs       : 0                              Checksum Sum        : 0
BFD             : Disabled
```

- To trouble shoot you can use the ospf statistics command. The authentication errors should not increment this may point to a mismatch in passwords or configuration. A small number of authentication errors are expected during the initial configuration change as links are not configured simultaneously.

```
show ip ospf statistics interface lag 256
OSPF Process ID 1 VRF default, interface lag256 statistics  (cleared 3h54m27s ago)
================================================================================

Tx Hello Packets      : 1407         Rx Hello Packets      : 1386
Tx Hello Bytes        : 98480        Rx Hello Bytes        : 96876
Tx DD Packets         : 4            Rx DD Packets         : 4
Tx DD Bytes           : 320          Rx DD Bytes           : 320
Tx LS Request Packets : 1            Rx LS Request Packets : 1
Tx LS Request Bytes   : 56           Rx LS Request Bytes   : 56
Tx LS Update Packets  : 25           Rx LS Update Packets  : 27
Tx LS Update Bytes    : 3664         Rx LS Update Bytes    : 3756
Tx LS Ack Packets     : 16           Rx LS Ack Packets     : 14
Tx LS Ack Bytes       : 1104         Rx LS Ack Bytes       : 984

Total Number of State Changes : 18
Number of LSAs                : 0
LSA Checksum Sum              : 0
Total Transmit Failures       : 0
Total OSPF Packets Discarded  : 15

Reason                        Packets Dropped
-------------------------------------------
Invalid type                  0
Invalid length                0
Invalid checksum              0
Invalid version               0
Bad or unknown source         0
Area mismatch                 0
Self-originated               0
Duplicate router ID           0
Interface standby             0
Total Hello packets dropped   0
  Network Mask mismatch       0
  Hello interval mismatch     0
  Dead interval mismatch      0
  Options mismatch            0
  MTU mismatch                0
  Neighbor ignored            0
Authentication errors         15
```

```
  Type mismatch              12
  Authentication failures    3
Wrong protocol               0
Resource failures            0
Bad LSA length               0
Bad DD packets               0
Others                       0

Total LSAs Ignored : 0
Bad Type           : 0
Bad Length         : 0
Invalid Data       : 0
Invalid Checksum   : 0
```

Task 3 – Add OSPF security between remaining links and Access

- Add MD5 authentication between the two cores that connect to Access Switch C
- Initial loss of communication is expected to the access switch on first configuration as changes are not done simultaneously.

SwitchA#	**SwitchB#**
! interface 1/1/3 ip ospf authentication message-digest ospf message-digest-key 1 md5 plaintext <your_password_here>	! interface 1/1/3 ip ospf authentication message-digest ospf message-digest-key 1 md5 plaintext <your_password_here>

- Add MD5 authentication on the Access uplinks that lead to Switch A and B respectively.

```
SwitchC#
configure
interface 1/1/1-1/1/2
ip ospf authentication message-digest
ospf message-digest-key 1 md5 plaintext <your_password_here>
```

- Carry out similar checks and troubleshooting as in the previous steps
- Ensure the OSPF neighbors remain intact

```
show ip ospf neighbors
VRF : default                          Process : 1
=================================================

Total Number of Neighbors : 2

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
192.168.2.1      n/a       FULL              192.168.4.0        1/1/1

192.168.2.2      n/a       FULL              192.168.4.4        1/1/2
```

- You can show you have authentication on the link

```
SwitchC# show ip ospf interface 1/1/1
Codes: DR - Designated router  BDR - Backup Designated router

Interface 1/1/1 is up, line protocol is up
------------------------------------------

VRF             : default                        Process             : 1
IP Address      : 192.168.4.1/31                 Area                : 0.0.0.0
Status          : up                             Network Type        : Point-to-point
Hello Interval  : 10  sec                        Dead Interval       : 40  sec
Transit Delay   : 1   sec                        Retransmit Interval : 5   sec
Authentication  : Md5                            Link Speed          : 1000Mbps
Cost Configured : NA                             Cost Calculated     : 100
State/Type      : Point-to-point                 Router Priority     : n/a
DR              : No                             BDR                 : No
Link LSAs       : 0                              Checksum Sum        : 0
```

```
BFD             : Disabled

SwitchC# show ip ospf interface 1/1/2
Codes: DR - Designated router  BDR - Backup Designated router

Interface 1/1/2 is up, line protocol is up
------------------------------------------

VRF             : default                       Process             : 1
IP Address      : 192.168.4.5/31                Area                : 0.0.0.0
Status          : up                            Network Type        : Point-to-point
Hello Interval  : 10  sec                       Dead Interval       : 40  sec
Transit Delay   : 1   sec                       Retransmit Interval : 5   sec
Authentication  : Md5                           Link Speed          : 1000Mbps
Cost Configured : NA                            Cost Calculated     : 100
State/Type      : Point-to-point                Router Priority     : n/a
DR              : No                            BDR                 : No
Link LSAs       : 0                             Checksum Sum        : 0
```

- To trouble shoot you can use the ospf statistics command. The authentication errors should not increment this may point to a mismatch in passwords or configuration. A small number of authentication errors are expected during the initial configuration change as links are not configured simultaneously. Only link 1/1/1 for Switch C is shown here.

```
SwitchC# show ip ospf statistics int 1/1/1
OSPF Process ID 1 VRF default, interface 1/1/1 statistics  (cleared 3h46m45s ago)
================================================================================

Tx Hello Packets      : 1340        Rx Hello Packets      : 1321
Tx Hello Bytes        : 95532       Rx Hello Bytes        : 94272
Tx DD Packets         : 4           Rx DD Packets         : 5
Tx DD Bytes           : 360         Rx DD Bytes           : 428
Tx LS Request Packets : 0           Rx LS Request Packets : 1
Tx LS Request Bytes   : 0           Rx LS Request Bytes   : 72
Tx LS Update Packets  : 22          Rx LS Update Packets  : 18
Tx LS Update Bytes    : 3200        Rx LS Update Bytes    : 2428
Tx LS Ack Packets     : 10          Rx LS Ack Packets     : 14
Tx LS Ack Bytes       : 672         Rx LS Ack Bytes       : 944

Total Number of State Changes : 21
Number of LSAs                : 0
LSA Checksum Sum              : 0
Total Transmit Failures       : 0
Total OSPF Packets Discarded  : 20

Reason                        Packets Dropped
--------------------------------------------
Invalid type                  0
Invalid length                0
Invalid checksum              0
Invalid version               0
Bad or unknown source         0
Area mismatch                 0
Self-originated               0
Duplicate router ID           0
Interface standby             0
Total Hello packets dropped   0
  Network Mask mismatch       0
  Hello interval mismatch     0
  Dead interval mismatch      0
  Options mismatch            0
  MTU mismatch                0
  Neighbor ignored            0
Authentication errors         20
  Type mismatch               17
  Authentication failures     3
Wrong protocol                0
Resource failures             0
Bad LSA length                0
Bad DD packets                0
Others                        0

Total LSAs Ignored : 0
Bad Type           : 0
Bad Length         : 0
Invalid Data       : 0
Invalid Checksum   : 0
```

Task 4 – Configure VPC and test reachability (Optional)

- Configure VPC1

```
VPCS> ip 10.10.100.1/24 10.10.100.254
Checking for duplicate address...
PC1 : 10.10.100.1 255.255.255.0 gateway 10.10.100.254
```

- Check various Reachability .Here we check to Core Switch A

```
VPCS> ping 192.168.2.1

84 bytes from 192.168.2.1 icmp_seq=1 ttl=63 time=2.546 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=63 time=5.527 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=63 time=5.554 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=63 time=5.539 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=63 time=2.815 ms
```

- The reader can check further reachability as well as configure VPC2 to explore further.

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 A

```
SwitchA#
!
!Version ArubaOS-CX Virtual.10.07.0010
!export-password: default
hostname SwitchA
led locator on
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
!
!
ssh server vrf mgmt
vlan 1
interface mgmt
    no shutdown
    ip dhcp
interface lag 256
    no shutdown
    description to SwitchB_
    ip address 192.168.4.8/31
    lacp mode active
    ip ospf 1 area 0.0.0.0
    no ip ospf passive
    ip ospf network point-to-point
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 plaintext <your_password_here>
interface 1/1/1
    no shutdown
    mtu 9198
    description core link
    lag 256
interface 1/1/2
    no shutdown
    mtu 9198
    description core link
    lag 256
interface 1/1/3
    no shutdown
    mtu 9198
    description to SwitchC_
    ip address 192.168.4.0/31
    ip ospf 1 area 0.0.0.0
    no ip ospf passive
    ip ospf network point-to-point
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 plaintext <your_password_here>
interface loopback 0
    ip address 192.168.2.1/32
    ip ospf 1 area 0.0.0.0
!
!
router ospf 1
    router-id 192.168.2.1
    max-metric router-lsa on-startup
    passive-interface default
    graceful-restart restart-interval 300
    trap-enable
    area 0.0.0.0
https-server vrf mgmt
```

Switch B

```
!
!Version ArubaOS-CX Virtual.10.07.0010
!export-password: default
hostname SwitchB
led locator on
```

```
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
!
!
!
!
!
!
ssh server vrf mgmt
vlan 1
interface mgmt
    no shutdown
    ip dhcp
interface lag 256
    no shutdown
    description to SwitchA
    ip address 192.168.4.9/31
    lacp mode active
    ip ospf 1 area 0.0.0.0
    no ip ospf passive
    ip ospf network point-to-point
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 plaintext <your_password_here>
interface 1/1/1
    no shutdown
    mtu 9198
    description core link
    lag 256
interface 1/1/2
    no shutdown
    mtu 9198
    description core link
    lag 256
interface 1/1/3
    no shutdown
    mtu 9198
    description to SwitchC_
    ip address 192.168.4.4/31
    ip ospf 1 area 0.0.0.0
    no ip ospf passive
    ip ospf network point-to-point
interface 1/1/3
    no shutdown
    mtu 9198
    description to SwitchC_
    ip address 192.168.4.4/31
    ip ospf 1 area 0.0.0.0
    no ip ospf passive
    ip ospf network point-to-point
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 plaintext <your_password_here>
interface loopback 0
    ip address 192.168.2.2/32
    ip ospf 1 area 0.0.0.0
!
!
router ospf 1
    router-id 192.168.2.2
    max-metric router-lsa on-startup
    passive-interface default
    graceful-restart restart-interval 300
    trap-enable
    area 0.0.0.0
https-server vrf mgmt
```

Switch C

```
SwitchC# show run
Current configuration:
!
!Version ArubaOS-CX Virtual.10.07.0010
!export-password: default
hostname SwitchC
led locator on
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
!
!
```

```
ssh server vrf mgmt
vlan 1,100,200
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/1
    no shutdown
    mtu 9198
    description to SwitchA
    ip address 192.168.4.1/31
    ip ospf 1 area 0.0.0.0
    no ip ospf passive
    ip ospf network point-to-point
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 plaintext <your_password_here>
interface 1/1/2
    no shutdown
    mtu 9198
    description to SwitchB
    ip address 192.168.4.5/31
    ip ospf 1 area 0.0.0.0
    no ip ospf passive
    ip ospf network point-to-point
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 plaintext <your_password_here>
interface 1/1/8
    no shutdown
    no routing
    vlan access 100
interface 1/1/9
    no shutdown
    no routing
    vlan access 200
interface loopback 0
    ip address 192.168.2.3/32
    ip ospf 1 area 0.0.0.0
interface vlan 100
    ip address 10.10.100.254/24
ip ospf 1 area 0.0.0.0
    no ip ospf passive
interface vlan 200
    ip address 10.10.200.254/24
    ip ospf 1 area 0.0.0.0
    no ip ospf passive
!
!
router ospf 1
    router-id 192.168.2.3
    max-metric router-lsa on-startup
    passive-interface default
    graceful-restart restart-interval 300
    trap-enable
    area 0.0.0.0
https-server vrf mgmt
SwitchC#
```

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