**CCNA v7 RSWE PT Skills Part-2**

**Part 1: Configure Switch Security**

**switch S1-1 or SW-A**

#### Step 1: Configure VLANs

Enable

Conf terminal

Vlan 10

Name users

Exit

Vlan 999

Name unused

Exit

#### Step 2: Configure active switch ports

Interface FastEthernet0/1

**switchport mode access**

**switchport access vlan 10**

**switchport port-security**

switchport port-security maximum 4

switchport port-security mac-address 00D0.D3DC.2825

**switchport port-security mac-address sticky**

**switchport port-security violation restrict**

**switchport port-security aging time 10**

**switchport port-security aging type inactivity**

spanning-tree portfast

spanning-tree bpduguard enable

**exit**

Interface FastEthernet0/2

**switchport mode access**

**switchport access vlan 10**

**switchport port-security**

switchport port-security maximum 4

**switchport port-security mac-address sticky**

**switchport port-security violation restrict**

**switchport port-security aging time 10**

spanning-tree portfast

spanning-tree bpduguard enable

**exit**

Interface FastEthernet0/3

**switchport mode access**

**switchport access vlan 10**

**switchport port-security**

switchport port-security maximum 4

**switchport port-security mac-address sticky**

**switchport port-security violation restrict**

**switchport port-security aging time 10**

spanning-tree portfast

spanning-tree bpduguard enable

**exit**

Interface FastEthernet0/4

**switchport mode access**

**switchport access vlan 10**

**switchport port-security**

switchport port-security maximum 4

**switchport port-security mac-address sticky**

**switchport port-security violation restrict**

**switchport port-security aging time 10**

spanning-tree portfast

spanning-tree bpduguard enable

**exit**

Interface FastEthernet0/5

**switchport mode access**

**switchport access vlan 10**

**switchport port-security**

switchport port-security maximum 4

**switchport port-security mac-address sticky**

**switchport port-security violation restrict**

**switchport port-security aging time 10**

spanning-tree portfast

spanning-tree bpduguard enable

**exit**

ip dhcp snooping

ip dhcp snooping vlan 10,999

ip arp inspection vlan 10,999

interface range f0/1 – 5

ip dhcp snooping limit rate 5

exit

interface g0/1

ip dhcp snooping trust

ip arp inspection trust

exit

#### Step 3: Secure unused switch ports

**interface range fa0/6 – 24**

**switchport mode access**

**switchport access vlan 999**

**shutdown**

**exit**

**interface *GigabitEthernet 0/2***

***shutdown***

***exit***

***exit***

**copy running-config startup-config**

### Part 2: Configure Addressing and DHCP

**Branch-101 or R-B-10**

#### Step 1: Configure and address a subinterface for the WLAN user network

En

Conf t

Interface G0/0/0.10

encapsulation dot1q 10

Ip address 192.168.10.1 255.255.255.0

no shutdown

exit

#### Step 2: Configure a DHCP pool for WLAN user network.

**ip dhcp excluded-address** 192.168.10.254

**ip dhcp excluded-address** 192.168.10.1

ip dhcp pool WLAN-hosts

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

dns-server 198.51.100.163

end

#### Step 3: Configure an interface as a DHCP client

Conf t

interface g0/0/1

ip address dhcp

no shutdown

end

copy running-config startup-config

### Part 3: Configure Static Routes

#### Step 1: Configure static routes on Central.

**On Central or R-1-A**

En

Conf t

Ip route 0.0.0.0 0.0.0.0 G0/0/2

Ip route 0.0.0.0 0.0.0.0 S0/1/0 10

Ipv6 route ::/0 2001:DB8:ACAD:A::2

Ipv6 route ::/0 2001:db8:acad:b::2 10

**ip route** 192.168.100.0 255.255.255.0 G0/0/2

**ip route** 192.168.100.0 255.255.255.0 S0/1/0 10

***ip route 192.168.10.0 255.255.255.0 GigabitEthernet0/0/2***

***ip route 192.168.10.0 255.255.255.0 Serial0/1/0 0 10***

**ip route** 192.168.3.0 255.255.255.0 S0/1/1

**ip route** 192.168.3.122 **255.255.255.255 *Serial0/1/1***

ipv6 route 2001:db8:acad:3::122/128 serial 0/1/1 fe80::2

**ipv6 unicast-routing**

exit

copy running-config startup-**config**

#### Step 2: Configure static routes on

#### **Branch-101 or R-B-10**

En

Conf t

Ip route 0.0.0.0 0.0.0.0 G0/0/1

Ip route 0.0.0.0 0.0.0.0 S0/1/0 10

Ipv6 route ::/0 2001:DB8:ACAD:C::1

Ipv6 route ::/0 2001:db8:acad:b::1 10

**ip route** 192.168.3.0 255.255.255.0 G0/0/1

**ip route** 192.168.3.0 255.255.255.0 S0/1/0 10

***ip route 192.168.10.0 255.255.255.0 GigabitEthernet0/0/0***

**ip route** 192.168.3.122 **255.255.255.255** 10.2.0.1

ipv6 route 2001:db8:acad:3::122/128 serial 0/1/0 fe80::2

**ipv6 unicast-routing**

exit

copy running-config startup-config

### Part 4: Configure a Wireless LAN using a Wireless LAN Controller.

### Refer 13.2 for detailed steps to configure...this section depends on individual….scores are varying 😉

#### Step 1: Configure a VLAN interface.

Click on Admin-host, Desktop->web browser

Enter https:// 192.168.100.254

admin/Cisco123

Controller tab->Interfaces-> new…

WLAN 10

10

DHCP 192.168.10.1

Gateway 192.168.10.1

IP 192.168.10.254/24

Press APPLY

#### Step 2: Configure a RADIUS server.

Security->new

172.16.1.100

RADsecret

#### Step 3: Configure a Wireless LAN.

WLANs->Create new in drop down and Go

WLAN 10 and configure the SSID as SSID-10

10

Click Apply

Goto security tab

WPA2 security policy and dot1x Authentication Key

Click on AAA, select radius server created

Advanced tab and scroll down to the Flexconnect sections. Activate FlexConnect Local Switching and FlexConnect Local Auth.

#### Step 4: Configure a DHCP scope for the management network.

Controller->Internal DHCP server->DHCP Scope

Name the DHCP scope Wired Admin.

b. Start the scope at address 192.168.100.240. End the scope at address 192.168.100.249.

c. Other information that is required can be found in the Addressing Table.

Network 192.168.100.0

Netmask 255.255.255.0

Default router 192.168.100.1

DNS 198.51.100.163

#### Step 5: Configure an SNMP server.

Management->SNMP->Trap receivers->new

a. Use the community name branch-wireless.

b. Use 172.16.1.100 as the server address.

#### Step 6: Configure the wireless host.

On laptop

Open PC Wireless->Profiles->New->

name **work net** for the profile and enter

Click Advance setup

Use enterprise authentication with a username of user1 and password of user1Pass.

When you are finished, click “Connect to Network.”

**Don’t use**

#spanning-tree portfast default

#spanning-tree portfast bpduguard default