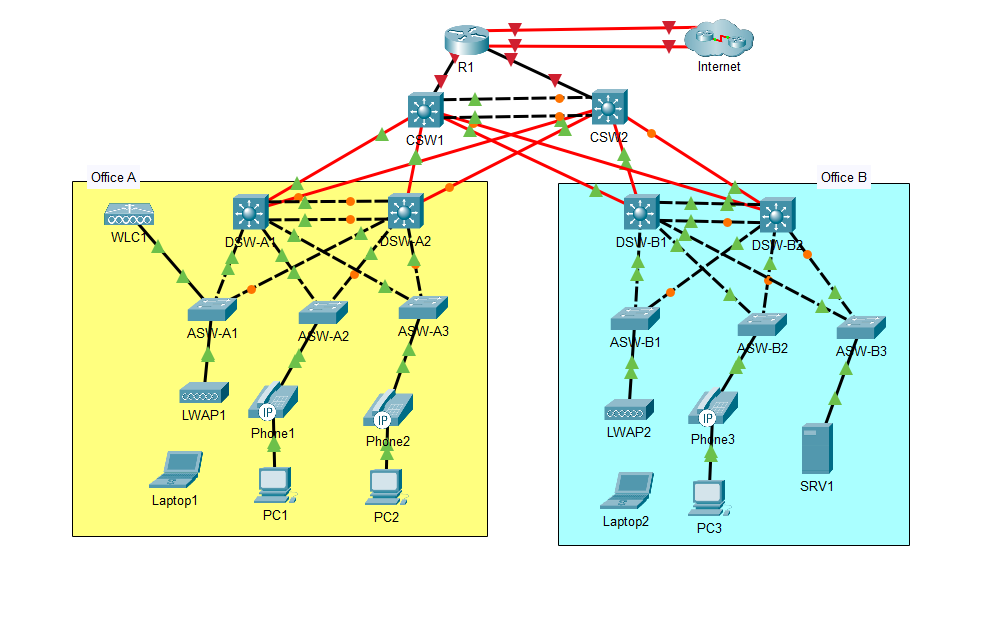
**PROJECT : NETWORK DESIGN OF THREE-TIER LAN USING CISCO PACKET TRACER**

**PROJECT DESIGN :**

A Three-Tier LAN with Two Office’s (A&B) connected to a Router with two (ISP) Redundancy routers with Internet.

**HIGH LEVEL DIAGRAM :**



**NETWORK DESIGN :**

1. Access layer : The Access Layer is the first tier, responsible for connecting end-user devices (such as computers and phones) to the network. These switches connect to the devices within the office LANs. Configured VLANs for different departments and functions .
2. Distribution layer: The Distribution Layer is the second tier, providing policy-based connectivity and controlling the boundary between the access and core layers. Configured VLAN interfaces on the distribution switches to route traffic between VLANs
3. Core layer : The Core Layer is the third tier, handling high-speed traffic between two offices (A&B), the core layer connects the two offices.
4. Dedicated VLAN is created for each department with respect to each office.
5. OSPF network protocol is implemented for communication between different locations

**CONNNECTIONS :**

**Router 1, CSW1 & CSW2**

|  |  |  |
| --- | --- | --- |
| **R1** | G0/0 | CSW1 G1/0/1 |
|  | G0/1 | CSW2 G1/0/1 |
|  | G0/0/0 | ISPA |
|  | G0/1/0 | ISPB |
| **CSW1** | G1/0/1 | R1 G0/0 |
| PortChannel1 | G1/0/2 | CSW2 G1/0/2 |
| G1/0/3 | CSW2 G1/0/3 |
|  | G1/1/1 | DSW-A1 G1/1/1 |
|  | G1/1/2 | DSW-A2 G1/1/1 |
|  | G1/1/3 | DSW-B1 G1/1/1 |
|  | G1/1/4 | DSW-B2 G1/1/1 |
| **CSW2** | G1/0/1 | R1 G0/0 |
| PortChannel1 | G1/0/2 | CSW1 G1/0/2 |
| G1/0/3 | CSW1 G1/0/3 |
|  | G1/1/1 | DSW-A1 G1/1/2 |
|  | G1/1/2 | DSW-A2 G1/1/2 |
|  | G1/1/3 | DSW-B1 G1/1/2 |
|  | G1/1/4 | DSW-B2 G1/1/2 |

**ASW-A1, ASW-A2, ASW-A3, ASW-B1, ASW-B2 & ASW-B3**

|  |  |  |
| --- | --- | --- |
| **ASW-A1** | G0/1 | DSW-A1 G1/0/1 |
|  | G0/2 | DSW-A2 G1/0/1 |
|  | F0/1 | LWAP1 |
|  | F0/2 | WLC1 |
| **ASW-A2** | G0/1 | DSW-A1 G1/0/2 |
|  | G0/2 | DSW-A2 G1/0/2 |
|  | F0/1 | Phone1 |
| **ASW-A3** | G0/1 | DSW-A1 G1/0/3 |
|  | G0/2 | DSW-A2 G1/0/3 |
|  | F0/1 | Phone2 |
| **ASW-B1** | G0/1 | DSW-A1 G1/0/1 |
|  | G0/2 | DSW-A2 G1/0/1 |
|  | F0/1 | LWAP2 |
| **ASW-B2** | G0/1 | DSW-A1 G1/0/2 |
|  | G0/2 | DSW-A2 G1/0/2 |
|  | F0/1 | Phone3 |
| **ASW-B3** | G0/1 | DSW-A1 G1/0/3 |
|  | G0/2 | DSW-A2 G1/0/3 |
|  | F0/1 | SRV1 |

**DSW-A1, DSW-A2, DSW-B1 & DSW-B2**

|  |  |  |
| --- | --- | --- |
| **DSW-A1** | G1/0/1 | ASW-A1 G0/1 |
|  | G1/0/2 | ASW-A2 G0/1 |
|  | G1/0/3 | ASW-A3 G0/1 |
| PortChannel1 | G1/0/4 | DSW-A2 G1/0/4 |
| G1/0/5 | DSW-A2 G1/0/5 |
|  | G1/1/1 | CSW1 G1/1/1 |
|  | G1/1/2 | CSW2 G1/1/1 |
| **DSW-A2** | G1/0/1 | ASW-A1 G0/2 |
|  | G1/0/2 | ASW-A2 G0/2 |
|  | G1/0/3 | ASW-A3 G0/2 |
| PortChannel1 | G1/0/4 | DSW-A1 G1/0/4 |
| G1/0/5 | DSW-A1 G1/0/5 |
|  | G1/1/1 | CSW1 G1/1/2 |
|  | G1/1/2 | CSW2 G1/1/2 |
| **DSW-B1** | G1/0/1 | ASW-B1 G0/1 |
|  | G1/0/2 | ASW-B2 G0/1 |
|  | G1/0/3 | ASW-B3 G0/1 |
| PortChannel1 | G1/0/4 | DSW-B2 G1/0/4 |
| G1/0/5 | DSW-B2 G1/0/5 |
|  | G1/1/1 | CSW1 G1/1/3 |
|  | G1/1/2 | CSW2 G1/1/3 |
| **DSW-B2** | G1/0/1 | ASW-B1 G0/2 |
|  | G1/0/2 | ASW-B2 G0/2 |
|  | G1/0/3 | ASW-B3 G0/2 |
| PortChannel1 | G1/0/4 | DSW-B1 G1/0/4 |
| G1/0/5 | DSW-B1 G1/0/5 |
|  | G1/1/1 | CSW1 G1/1/4 |
|  | G1/1/2 | CSW2 G1/1/4 |

**IPV4 CONNECTION:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Link** | **Subnet** | **Device** | **IP** |
| R1 <> ISPA | 203.0.113.0/30 | ISPA | 203.0.113.1 |
|  |  | R1 G0/0/0 | 203.0.113.2 |
| R1 <> ISPB | 203.0.113.4/30 | ISPB | 203.0.113.5 |
|  |  | R1 G0/1/0 | 203.0.113.6 |
| Mgmt A (VLAN99) | 10.0.0.0/28 | VIP | 10.0.0.1 |
|  |  | DSW-A1 V99 | 10.0.0.2 |
|  |  | DSW-A2 V99 | 10.0.0.3 |
|  |  | ASW-A1 V99 | 10.0.0.4 |
|  |  | ASW-A2 V99 | 10.0.0.5 |
|  |  | ASW-A3 V99 | 10.0.0.6 |
|  |  | WLC1 | 10.0.0.7 |

|  |  |  |  |
| --- | --- | --- | --- |
| Mgmt B (VLAN99) | 10.0.0.16/28 | VIP | 10.0.0.17 |
|  |  | DSW-B1 V99 | 10.0.0.18 |
|  |  | DSW-B2 V99 | 10.0.0.19 |
|  |  | ASW-B1 V99 | 10.0.0.20 |
|  |  | ASW-B2 V99 | 10.0.0.21 |
|  |  | ASW-B3 V99 | 10.0.0.22 |
| R1 <> CSW1 | 10.0.0.32/30 | R1 G0/0 | 10.0.0.33 |
|  |  | CSW1 G1/0/1 | 10.0.0.34 |
| R1 <> CSW2 | 10.0.0.36/30 | R1 G0/1 | 10.0.0.37 |
|  |  | CSW2 G1/0/1 | 10.0.0.38 |
| CSW1 <> CSW2 | 10.0.0.40/30 | CSW1 Po1 | 10.0.0.41 |
|  |  | CSW2 Po1 | 10.0.0.42 |
| CSW1 <> DSW-A1 | 10.0.0.44/30 | CSW1 G1/1/1 | 10.0.0.45 |
|  |  | DSW-A1 G1/1/1 | 10.0.0.46 |
| CSW1 <> DSW-A2 | 10.0.0.48/30 | CSW1 G1/1/2 | 10.0.0.49 |
|  |  | DSW-A2 G1/1/1 | 10.0.0.50 |
| CSW1 <> DSW-B1 | 10.0.0.52/30 | CSW1 G1/1/3 | 10.0.0.53 |
|  |  | DSW-B1 G1/1/1 | 10.0.0.54 |
| CSW1 <> DSW-B2 | 10.0.0.56/30 | CSW1 G1/1/4 | 10.0.0.57 |
|  |  | DSW-B2 G1/1/1 | 10.0.0.58 |
| CSW2 <> DSW-A1 | 10.0.0.60/30 | CSW2 G1/1/1 | 10.0.0.61 |
|  |  | DSW-A1 G1/1/2 | 10.0.0.62 |
| CSW2 <> DSW-A2 | 10.0.0.64/30 | CSW2 G1/1/2 | 10.0.0.65 |
|  |  | DSW-A2 G1/1/2 | 10.0.0.66 |
| CSW2 <> DSW-B1 | 10.0.0.68/30 | CSW2 G1/1/3 | 10.0.0.69 |
|  |  | DSW-B1 G1/1/2 | 10.0.0.70 |
| CSW2 <> DSW-B2 | 10.0.0.72/30 | CSW2 G1/1/4 | 10.0.0.73 |
|  |  | DSW-B2 G1/1/2 | 10.0.0.74 |
| Loopbacks | 10.0.0.76/32 | R1 L0 | 10.0.0.76 |
|  | 10.0.0.77/32 | CSW1 L0 | 10.0.0.77 |
|  | 10.0.0.78/32 | CSW2 L0 | 10.0.0.78 |
|  | 10.0.0.79/32 | DSW-A1 L0 | 10.0.0.79 |
|  | 10.0.0.80/32 | DSW-A2 L0 | 10.0.0.80 |
|  | 10.0.0.81/32 | DSW-B1 L0 | 10.0.0.81 |
|  | 10.0.0.82/32 | DSW-B2 L0 | 10.0.0.82 |
| PCs A (VLAN10) | 10.1.0.0/24 | VIP | 10.1.0.1 |
|  |  | DSW-A1 V10 | 10.1.0.2 |
|  |  | DSW-A2 V10 | 10.1.0.3 |
| Phones A (VLAN20) | 10.2.0.0/24 | VIP | 10.2.0.1 |
|  |  | DSW-A1 V20 | 10.2.0.2 |
|  |  | DSW-A2 V20 | 10.2.0.3 |
| PCs B (VLAN10) | 10.3.0.0/24 | VIP | 10.3.0.1 |
|  |  | DSW-B1 V10 | 10.3.0.2 |
|  |  | DSW-B2 V10 | 10.3.0.3 |

|  |  |  |  |
| --- | --- | --- | --- |
| Phones B (VLAN20) | 10.4.0.0/24 | VIP | 10.4.0.1 |
|  |  | DSW-B1 V20 | 10.4.0.2 |
|  |  | DSW-B2 V20 | 10.4.0.3 |
| Servers (VLAN30) | 10.5.0.0/24 | VIP | 10.5.0.1 |
|  |  | DSW-B1 V30 | 10.5.0.2 |
|  |  | DSW-B2 V30 | 10.5.0.3 |
| Wi-Fi (VLAN40) | 10.6.0.0/24 | VIP | 10.6.0.1 |
|  |  | DSW-A1 V40 | 10.6.0.2 |
|  |  | DSW-A2 V40 | 10.6.0.3 |

**CONFIGURATION :**

**PART-1 : Initial setup**

1.Configuring Hostname as displayed in the High level diagram as R1, CSW1, CSW2, DSW-A1, DSW-A2, DSW-B1, DSW-B2, ASW-A1, ASW-A2, ASW-A3, ASW-B1, ASW-B2 & ASW-B3

2. Configuring the enable secret kushankumar on each router/switch. Used type 9 hashing in CSW1,CSW2 available other network nodes used type 5 hashing

3. Configuring the user account cisco with secret ccna on each router/switch. Used type 9 hashing in CSW1,CSW2 available other network nodes used type 5 hashing

4. Configure the console line to require login with a local user account. Set a 30-minute inactivity timeout. Enable synchronous logging.

Command used for PART 1 :

* enable algorithm-type scrypt secret kushankumar
* username cisco algorithm-type scrypt secret ccna
* line console 0
* login local
* exec-timeout 30
* logging synchronous

**PART-2 : Configuring VLAN’s and Layer-2 Etherchannel**

1. In Office A, configuring a Layer-2 EtherChannel named PortChannel1 between DSW-A1 and DSW-A2 using a Cisco-proprietary protocol. Both switches should actively try to form an Ehterchannel.(Use PAgP)

Commad:

* int range g1/0/4-5
* Channel-group 1 mode desirable
* Show command show ether-channel summary

1. In Office B, configure a Layer-2 EtherChannel named PortChannel1 between DSW-B1 and DSW-B2 using an open standard protocol. Both switches should actively try to form an EtherChannel.(Use LACP)

Commad:

* int range g1/0/4-5
* Channel-group 1 mode active
* Show command show ether-channel summary

3. Configuring all links between Access and Distribution switches, including the EtherChannels, as trunk links.

a. Explicitly disable DTP on all ports.

b. Setting each trunk’s native VLAN to VLAN 1000 (unused).

c. In Office A, allow VLANs 10, 20, 40, and 99 on all trunks.

d. In Office B, allow VLANs 10, 20, 30, and 99 on all trunks.

Command:

###For DSW-A1, DSW-A2

* interface range g1/0/1-3
* switchport mode trunk
* switchport nonegotiate
* switchport trunk native vlan 1000
* switchport trunk allowed Vlan 10,20,40,99
* interface po1
* switchport mode trunk
* switchport nonegotiate
* switchport trunk native vlan 1000
* switchport trunk allowed Vlan 10,20,40,99

###For ASW-A1, ASW-A2, ASW-A3

* interface range g0/1-2
* switchport mode trunk
* switchport nonegotiate
* switchport trunk native vlan 1000
* switchport trunk allowed vlan 10,20,40,99

###For DSW-B1, DSW-B2

* interface range g1/0/1-3
* switchport mode trunk
* switchport nonegotiate
* switchport trunk native vlan 1000
* switchport trunk allowed Vlan 10,20,30,99
* interface po1
* switchport mode trunk
* switchport nonegotiate
* switchport trunk native vlan 1000
* switchport trunk allowed Vlan 10,20,30,99

### FOR ASW-B1, ASW-B2, ASW-B3

* interface range g0/1-2
* switchport mode trunk
* switchport nonegotiate
* switchport trunk native vlan 1000
* switchport trunk allowed vlan 10,20,30,99

4. Configuring one of each office’s Distribution switches as a VTPv2 server. Use domain name CCNA.

a. Verify that other switches join the domain.

b. Configuring all Access switches as VTP clients.

Command:

### For Distribution switches DSW-A1 & DSW-B1

* Vtp domain CCNA
* Vtp version 2
* vtp mode server

### For All Access switches ASW-A1, ASW-A2, ASW-A3, ASW-B1, ASW-B2 & ASW-B3

* Vtp mode client

Show command : show Vtp status

5. In Office A, creating and naming the following VLANs on one of the Distribution switches. **Ensure that VTP propagates the changes.**

a. VLAN 10: PCs

b. VLAN 20: Phones

c. VLAN 40: Wi-Fi

d. VLAN 99: Management

Command:

###For DSW-A1

* Vlan 10
* name PCs
* Vlan 20
* name Phones
* Vlan 40
* name Wi-Fi
* Vlan 99
* name management

For checking whether the VTP propagates the Vlan data to all other Distribution and Access switches with show command : show Vlan brief

6. In Office B, creating and naming the following VLANs on one of the Distribution switches. Ensure that VTP propagates the changes.

a. VLAN 10: PCs

b. VLAN 20: Phones

c. VLAN 30: Servers

d. VLAN 99: Management

Command:

###For DSW-B1

* Vlan 10
* name PCs
* Vlan 20
* name Phones
* Vlan 30
* name servers
* Vlan 99
* name management

7. Configuring each Access switch’s access port.

a. LWAPs will not use FlexConnect

b. PCs in VLAN 10, Phones in VLAN 20

c. SRV1 in VLAN 30

d. Manually configure access mode and explicitly disable DTP

Command :

### For ASW-A1 & ASW-B1

* int f0/1
* switchport mode access
* switchport nonegotiate
* switchport mode access vlan 99

### For ASW-A2,ASw-A3,ASW-B2

* interface f0/1
* switchport mode access
* switchport nonegotiate
* switchport access vlan 10
* switchport voice vlan 20

### For ASW-B3

* interface f0/1
* switchport mode access
* switchport nonegotiate
* Switchport mode access Vlan 30

8. Configuring ASW-A1’s connection to WLC1:

a. It must support the Wi-Fi and Management VLANs.

b. The Management VLAN should be untagged.

c. Disable DTP.

Command :

* int f0/2
* switchport mode trunk
* switchport nonegotiate
* switchport trunk allowed vlan 99,40
* switchport trunk native vlan 99

9. Administratively disable all unused ports on Access and Distribution switches.

Command :

### For DSW-A1,DSW-A2, DSW-B1, DSW-B2

* interface range g1/0/6-24,g1/1/3-4
* shutdown

### For ASW-A2,ASW-A3, ASW-B1, ASW-B2, ASW-B3

* interface range f0/2-24
* shutdown

Show command: show interface status

**PART-2 : IP Addresses, Layer -3 Etherchannel & HSRP**

1. Configuring the following IP addresses on R1’s interfaces and enable them:

a. G0/0/0: DHCP client (which is connected to ISP A )

b. G0/1/0: DHCP client(which is connected to ISP B )

c. G0/0: 10.0.0.33/30 (Connected to CSW1)

d. G0/1: 10.0.0.37/30 (Connected to CSW2)

e. Loopback0: 10.0.0.76/32

Command :

* interface range g0/0/0,g0/1/0
* ip address dhcp
* no shutdown
* interface g0/0
* ip address 10.0.0.33 255.255.255.252
* no shutdown
* interface g1/0
* ip address 10.0.0.37 255.255.255.252
* no shutdown
* interface loopback 0
* ip address 10.0.0.76 255.255.255.255
* no shutdown

2. Enabling IPv4 routing on all Core and Distribution switches.

Command :

* Ip routing

3. Creating a Layer-3 EtherChannel between CSW1 and CSW2 using a Cisco-proprietary protocol. Both switches should actively try to form an EtherChannel. Configuring following IP addresses:

a. CSW1 PortChannel1: 10.0.0.41/30

b. CSW2 PortChannel1: 10.0.0.42/30

Command :

###For CSW1

* interface range g1/0/2-3
* no switchport
* channel-group 1 mode desirable
* interface port-channel1
* ip addresss 10.0.0.41 255.255.255.252

###For CSW2

* interface range g1/0/2-3
* no switchport
* channel-group 1 mode desirable
* interface port-channel1
* ip addresss 10.0.0.42 255.255.255.252

show command : show etherchannel summary

4. Configuring the following IP addresses on CSW1. Disabling all unused interfaces.

a. G1/0/1: 10.0.0.34/30 (Connected to R1)

b. G1/1/1: 10.0.0.45/30 (Connected to DSW-A1)

c. G1/1/2: 10.0.0.49/30 (Connected to DSW-A2)

d. G1/1/3: 10.0.0.53/30 (Connected to DSW-B1)

e. G1/1/4: 10.0.0.57/30 (Connected to DSW-B2)

f. Loopback0: 10.0.0.77/32

Command:

### For CSW1

* interface g1/0/1
* no switchport
* ip address 10.0.0.34 255.255.255.252
* interface g1/1/1
* no switchport
* ip address 10.0.0.45 255.255.255.252
* interface g1/1/2
* no switchport
* ip address 10.0.0.49 255.255.255.252
* interface g1/1/3
* no switchport
* ip address 10.0.0.53 255.255.255.252
* interface g1/1/4
* no switchport
* ip address 10.0.0.57 255.255.255.252
* interface loopback 0
* ip address 10.0.0.77 255.255.255.255
* interface range g1/0/4-24
* shutdown

5. Configuring the following IP addresses on CSW2. Disabling all unused interfaces.

a. G1/0/1: 10.0.0.38/30 (Connected to R1)

b. G1/1/1: 10.0.0.61/30 (Connected to DSW-A1)

c. G1/1/2: 10.0.0.65/30 (Connected to DSW-A2)

d. G1/1/3: 10.0.0.69/30 (Connected to DSW-B1)

e. G1/1/4: 10.0.0.73/30 (Connected to DSW-B2)

f. Loopback0: 10.0.0.78/32

Commnad :

###For CSW2

* interface g1/0/1
* no switchport
* ip address 10.0.0.38 255.255.255.252
* interface g1/1/1
* no switchport
* ip address 10.0.0.61 255.255.255.252
* interface g1/1/2
* no switchport
* ip address 10.0.0.65 255.255.255.252
* interface g1/1/3
* no switchport
* ip address 10.0.0.69 255.255.255.252
* interface g1/1/4
* no switchport
* ip address 10.0.0.73 255.255.255.252
* interface loopback 0
* ip address 10.0.0.78 255.255.255.255
* interface range g1/0/4-24
* shutdown

6. Configuring the following IP addresses on DSW-A1:

a. G1/1/1: 10.0.0.46/30

b. G1/1/2: 10.0.0.62/30

c. Loopback0: 10.0.0.79/32

Command :

* interface g1/1/1
* no switchport
* ip address 10.0.0.46 255.255.255.252
* interface g1/1/2
* no switchport
* ip address 10.0.0.62 255.255.255.252
* interface loopback0
* ip address 10.0.0.79 255.255.255.255

7. Configuring the following IP addresses on DSW-A2:

a. G1/1/1: 10.0.0.50/30

b. G1/1/2: 10.0.0.66/30

c. Loopback0: 10.0.0.80/32

Command :

* interface g1/1/1
* no switchport
* ip address 10.0.0.50 255.255.255.252
* interface g1/1/2
* no switchport
* ip address 10.0.0.66 255.255.255.252
* interface loopback0
* ip address 10.0.0.80 255.255.255.255

8. Configuring the following IP addresses on DSW-B1:

a. G1/1/1: 10.0.0.54/30

b. G1/1/2: 10.0.0.70/30

c. Loopback0: 10.0.0.81/32

Command :

* interface g1/1/1
* no switchport
* ip address 10.0.0.54 255.255.255.252
* interface g1/1/2
* no switchport
* ip address 10.0.0.70 255.255.255.252
* interface loopback0
* ip address 10.0.0.81 255.255.255.255

9. Configuring the following IP addresses on DSW-B2:

a. G1/1/1: 10.0.0.58/30

b. G1/1/2: 10.0.0.74/30

c. Loopback0: 10.0.0.82/32

Command :

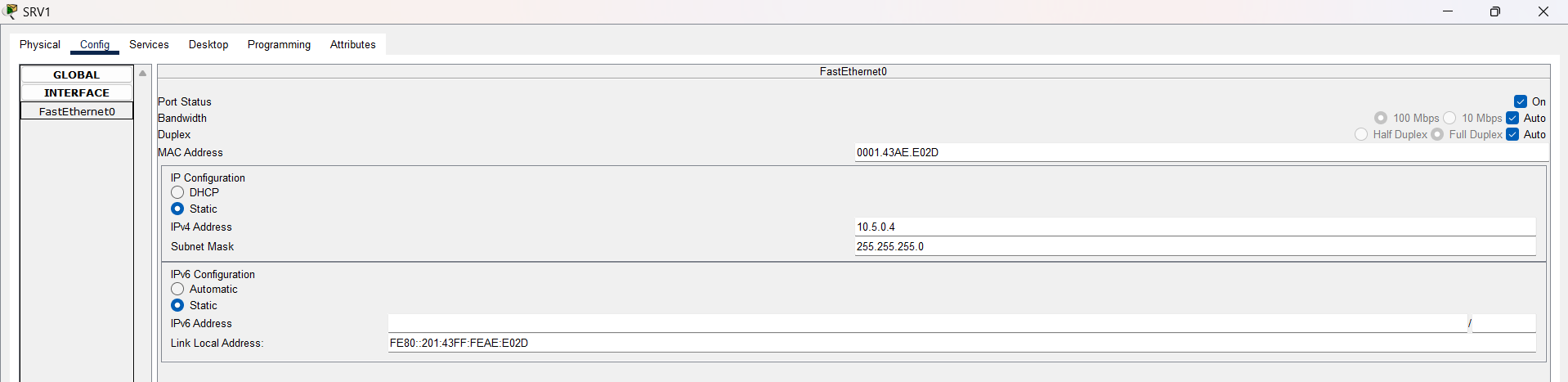
* interface g1/1/1
* no switchport
* ip address 10.0.0.58 255.255.255.252
* interface g1/1/2
* no switchport
* ip address 10.0.0.74 255.255.255.252
* interface loopback0
* ip address 10.0.0.82 255.255.255.255

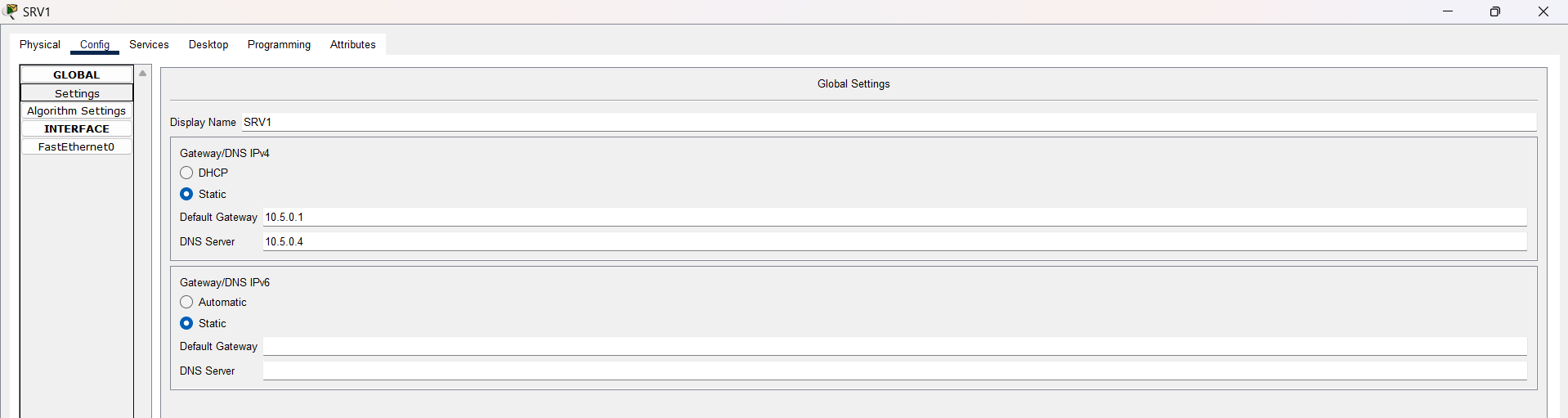
10. Manually configure SRV1’s IP settings:

a. Default Gateway: 10.5.0.1

b. IPv4 Address: 10.5.0.4

c. Subnet Mask: 255.255.255.0





11. Configuring the following management IP addresses on the Access switches (interface VLAN 99), and configure the appropriate subnet’s first usable address as the default gateway.

a. ASW-A1: 10.0.0.4/28

b. ASW-A2: 10.0.0.5/28

c. ASW-A3: 10.0.0.6/28

d. ASW-B1: 10.0.0.20/28

e. ASW-B2: 10.0.0.21/28

f. ASW-B3: 10.0.0.22/28

Command:

###For ASW-A1

* ip default-gateway 10.0.0.1
* interface vlan 99
* ip address 10.0.0.4 255.255.255.240

###For ASW-A2

* ip default-gateway 10.0.0.1
* interface vlan 99
* ip address 10.0.0.5 255.255.255.240

###For ASW-A3

* ip default-gateway 10.0.0.1
* interface vlan 99
* ip address 10.0.0.6 255.255.255.240

###For ASW-B1

* ip default-gateway 10.0.0.17
* interface vlan 99
* ip address 10.0.0.20 255.255.255.240

###For ASW-B2

* ip default-gateway 10.0.0.17
* interface vlan 99
* ip address 10.0.0.21 255.255.255.240

###For ASW-B3

* ip default-gateway 10.0.0.17
* interface vlan 99
* ip address 10.0.0.22 255.255.255.240

12. Configuring HSRPv2 group 1 for Office A’s Management subnet (VLAN 99). Make DSW-A1 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-A1.

a. Subnet: 10.0.0.0/28

b. VIP: 10.0.0.1

c. DSW-A1: 10.0.0.2

d. DSW-A2: 10.0.0.3

### For DSW-A1

* interface Vlan 99
* ip address 10.0.0.2 255.255.255.240
* standby version 2
* standby 1 ip 10.0.0.1
* standby 1 priority 105
* standby 1 preempt

### For DSW-A2

* interface Vlan 99
* ip address 10.0.0.3 255.255.255.240
* standby version 2
* standby 1 ip 10.0.0.1

13. Configure HSRPv2 group 2 for Office A’s PCs subnet (VLAN 10). Make DSW-A1 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-A1.

a. Subnet: 10.1.0.0/24

b. VIP: 10.1.0.1

c. DSW-A1: 10.1.0.2

d. DSW-A2: 10.1.0.3

### For DSW-A1

* interface Vlan 10
* ip address 10.1.0.2 255.255.255.240
* standby version 2
* standby 2 ip 10.1.0.1
* standby 2 priority 105
* standby 2 preempt

### For DSW-A2

* interface Vlan 10
* ip address 10.1.0.3 255.255.255.240
* standby version 2
* standby 2 ip 10.1.0.1

14. Configuring HSRPv2 group 3 for Office A’s Phones subnet (VLAN 20). Make DSW-A2 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-A2.

a. Subnet: 10.2.0.0/24

b. VIP: 10.2.0.1

c. DSW-A1: 10.2.0.2

d. DSW-A2: 10.2.0.3

### For DSW-A2

* interface Vlan 20
* ip address 10.2.0.3 255.255.255.240
* standby version 2
* standby 3 ip 10.1.0.1
* standby 3 priority 105
* standby 3 preempt

### For DSW-A1

* interface Vlan 20
* ip address 10.2.0.2 255.255.255.240
* standby version 2
* standby 3 ip 10.2.0.1

15. Configure HSRPv2 group 4 for Office A’s Wi-Fi subnet (VLAN 40). Make DSW-A2 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-A2.

a. Subnet: 10.6.0.0/24

b. VIP: 10.6.0.1

c. DSW-A1: 10.6.0.2

d. DSW-A2: 10.6.0.3

### For DSW-A2

* interface Vlan 40
* ip address 10.6.0.3 255.255.255.240
* standby version 2
* standby 4 ip 10.6.0.1
* standby 4 priority 105
* standby 4 preempt

### For DSW-A1

* interface Vlan 40
* ip address 10.6.0.2 255.255.255.240
* standby version 2
* standby 4 ip 10.6.0.1

16. Configure HSRPv2 group 1 for Office B’s Management subnet (VLAN 99). Make DSW-B1 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-B1.

a. Subnet: 10.0.0.16/28

b. VIP: 10.0.0.17

c. DSW-B1: 10.0.0.18

d. DSW-B2: 10.0.0.19

17. Configure HSRPv2 group 2 for Office B’s PCs subnet (VLAN 10). Make DSW-B1 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-B1.

a. Subnet: 10.3.0.0/24

b. VIP: 10.3.0.1

c. DSW-B1: 10.3.0.2

d. DSW-B2: 10.3.0.3

18. Configure HSRPv2 group 3 for Office B’s Phones subnet (VLAN 20). Make DSW-B2 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-B2.

a. Subnet: 10.4.0.0/24

b. VIP: 10.4.0.1

c. DSW-B1: 10.4.0.2

d. DSW-B2: 10.4.0.3

19. Configure HSRPv2 group 4 for Office B’s Servers subnet (VLAN 30). Make DSW-B2 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-B2.

a. Subnet: 10.5.0.0/24

b. VIP: 10.5.0.1

c. DSW-B1: 10.5.0.2

d. DSW-B2: 10.5.0.3

Command for step’s16-19

### For DSW-B1

* interface vlan 99
* ip address 10.0.0.18 255.255.255.240
* standby version 2
* standby 1 ip 10.0.0.17
* standby 1 priority 105
* standby 1 preempt
* interface vlan 10
* ip address 10.3.0.2 255.255.255.0
* standby version 2
* standby 2 ip 10.3.0.1
* standby 2 priority 105
* standby 2 preempt
* interface vlan 20
* ip address 10.4.0.2 255.255.255.0
* standby version 2
* standby 3 ip 10.4.0.1
* interface vlan 30
* ip address 10.5.0.2 255.255.255.0
* standby version 2
* standby 4 ip 10.5.0.1

### For DSW-B2

* interface vlan 99
* ip address 10.0.0.19 255.255.255.240
* standby version 2
* standby 1 ip 10.0.0.17
* interface vlan 10
* ip address 10.3.0.3 255.255.255.0
* standby version 2
* standby 2 ip 10.3.0.1
* interface vlan 20
* ip address 10.4.0.3 255.255.255.0
* standby version 2
* standby 3 ip 10.4.0.1
* standby 3 priority 105
* standby 3 preempt
* interface vlan 30
* ip address 10.5.0.2 255.255.255.0
* standby version 2
* standby 2 ip 10.5.0.1
* standby 2 priority 105
* standby 2 preempt

**PART 4 : Rapid Spanning Tree Protocol**

1. Configure Rapid PVST+ on all Access and Distribution switches.

a. Ensure that the Root Bridge for each VLAN aligns with the HSRP Active router by configuring the lowest possible STP priority.

b. Configure the HSRP Standby Router for each VLAN with an STP priority one increment above the lowest priority

Command:

### For DSWA1

* spanning-tree vlan 10,99 priority 0
* spanning-tree vlan 20,40 priority 4096

### For DSWA2

* spanning-tree vlan 20,40 priority 0
* spanning-tree vlan 10,99 priority 4096

### For DSWB1

* spanning-tree vlan 10,99 priority 0
* spanning-tree vlan 20,30 priority 4096

### For DSWB2

* spanning-tree vlan 20,30 priority 0
* spanning-tree vlan 10,99 priority 4096

2. Enable PortFast and BPDU Guard on all ports connected to end hosts (including WLC1). Perform the configurations in interface config mode.

Command:

### For ASW-A1

* interface f0/1
* spanning-tree portfast
* spanning-tree bpduguard enable
* interface f0/2
* spanning-tree portfast trunk
* spanning-tree bpduguard enable

### For ASW-A2, ASW-A3, ASW-B1, ASW-B2 & Asw-B3

* interface f0/1
* spanning-tree portfast
* spanning-tree bpduguard enable

Show Command: show spanning-tree, show spanning –tree detail

**PART 5 - Static and Dynamic Routing**

1. Configuring OSPF on R1 (LAN-facing interfaces) and all Core and Distribution switches (all Layer-3 interfaces).

a. Use process ID 1 and Area 0.

b. Manually configure each device’s RID to match the loopback interface IP.

c. On switches, use the network command to match the exact IP address of each interface.

d. On R1, enable OSPF in interface config mode.

e. Make sure OSPF is enabled on all loopback interfaces, too. Loopback interfaces should be passive.

f. Each Distribution switch’s SVIs (except the Management VLAN SVI) should be passive, too.

g. Configure all physical connections between OSPF neighbors to use a network type that doesn’t elect a DR/BDR. NOTE: This doesn’t work on the Layer-3 PortChannel interfaces between CSW1/CSW2. Leave them as the default network type

### For R1

* router ospf 1
* router id 10.0.0.76
* passive-interface loopback0
* interface loopback0
* ip ospf 1 area 0
* ip ospf network point-to-point

### For CSW1

* router ospf 1
* router id 10.0.0.77
* passive-interface loopback0
* network 10.0.0.41 0.0.0.0 area 0
* network 10.0.0.34 0.0.0.0 area 0
* network 10.0.0.45 0.0.0.0 area 0
* network 10.0.0.49 0.0.0.0 area 0
* network 10.0.0.53 0.0.0.0 area 0
* network 10.0.0.57 0.0.0.0 area 0
* network 10.0.0.77 0.0.0.0 area 0
* interface range g1/0/1,g1/1/1-4
* ip ospf network point-to-point

### For CSW2

* router ospf 1
* router id 10.0.0.78
* passive-interface loopback0
* network 10.0.0.42 0.0.0.0 area 0
* network 10.0.0.38 0.0.0.0 area 0
* network 10.0.0.61 0.0.0.0 area 0
* network 10.0.0.65 0.0.0.0 area 0
* network 10.0.0.69 0.0.0.0 area 0
* network 10.0.0.73 0.0.0.0 area 0
* network 10.0.0.78 0.0.0.0 area 0
* interface range g1/0/1,g1/1/1-4
* ip ospf network point-to-point

### For DSW-A1

* router ospf 1
* router id 10.0.0.79
* Passive-interface vlan 10
* Passive-interface vlan 20
* Passive-interface vlan 40
* passive-interface loopback0
* network 10.0.0.46 0.0.0.0 area 0
* network 10.0.0.62 0.0.0.0 area 0
* network 10.0.0.79 0.0.0.0 area 0
* network 10.1.0.2 0.0.0.0 area 0
* network 10.2.0.2 0.0.0.0 area 0
* network 10.0.0.2 0.0.0.0 area 0
* network 10.6.0.2 0.0.0.0 area 0
* interface range g1/1/1-2
* ip ospf network point-to-point

### For DSW-A2

* router ospf 1
* router id 10.0.0.80
* Passive-interface vlan 10
* Passive-interface vlan 20
* Passive-interface vlan 40
* passive-interface loopback0
* network 10.0.0.50 0.0.0.0 area 0
* network 10.0.0.66 0.0.0.0 area 0
* network 10.0.0.80 0.0.0.0 area 0
* network 10.1.0.3 0.0.0.0 area 0
* network 10.2.0.3 0.0.0.0 area 0
* network 10.0.0.3 0.0.0.0 area 0
* network 10.6.0.3 0.0.0.0 area 0
* interface range g1/1/1-2
* ip ospf network point-to-point

### For DSW-B1

* router ospf 1
* router id 10.0.0.81
* Passive-interface vlan 10
* Passive-interface vlan 20
* Passive-interface vlan 30
* passive-interface loopback0
* network 10.0.0.54 0.0.0.0 area 0
* network 10.0.0.70 0.0.0.0 area 0
* network 10.0.0.81 0.0.0.0 area 0
* network 10.3.0.2 0.0.0.0 area 0
* network 10.4.0.2 0.0.0.0 area 0
* network 10.5.0.2 0.0.0.0 area 0
* network 10.0.0.18 0.0.0.0 area 0
* interface range g1/1/1-2
* ip ospf network point-to-point

### For DSW-B2

* router ospf 1
* router id 10.0.0.82
* Passive-interface vlan 10
* Passive-interface vlan 20
* Passive-interface vlan 30
* passive-interface loopback0
* network 10.0.0.58 0.0.0.0 area 0
* network 10.0.0.74 0.0.0.0 area 0
* network 10.0.0.82 0.0.0.0 area 0
* network 10.3.0.3 0.0.0.0 area 0
* network 10.4.0.3 0.0.0.0 area 0
* network 10.5.0.3 0.0.0.0 area 0
* network 10.0.0.19 0.0.0.0 area 0
* interface range g1/1/1-2
* ip ospf network point-to-point

Show command: show ip ospf neighbour

2. Configure one static default route for each of R1’s Internet connections. They should be recursive routes.

a. Make the route via G0/1/0 a floating static route by configuring an AD value 1 greater than the default.

b. R1 should function as an OSPF ASBR, advertising its default route to other routers in the OSPF domain.

Command:

### For R1

* ip route 0.0.0.0 0.0.0.0 203.0.113.1
* ip route 0.0.0.0 0.0.0.0 203.0.113.5 2
* router ospf 1
* default-information originate

**PART 6 – Network Services : DHCP, DNS, NTP, SNMP, Syslog, FTP, SSH, NAT.**

1. Configure the following DHCP pools on R1 to make it serve as the DHCP server for hosts in Offices A and B. Exclude the first ten usable host addresses of each pool; they must not be leased to DHCP clients.

a. Pool: A-Mgmt

i. Subnet: 10.0.0.0/28

ii. Default gateway: 10.0.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

v. WLC: 10.0.0.7

b. Pool: A-PC

i. Subnet: 10.1.0.0/24

ii. Default gateway: 10.1.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

c. Pool: A-Phone

i. Subnet: 10.2.0.0/24

ii. Default gateway: 10.2.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

d. Pool: B-Mgmt

i. Subnet: 10.0.0.16/28

ii. Default gateway: 10.0.0.17

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

v. WLC: 10.0.0.7

e. Pool: B-PC

i. Subnet: 10.3.0.0/24

ii. Default gateway: 10.3.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

f. Pool: B-Phone

i. Subnet: 10.4.0.0/24

ii. Default gateway: 10.4.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

g. Pool: Wi-Fi

i. Subnet: 10.6.0.0/24

ii. Default gateway: 10.6.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

Command:

### For R1

* ip dhcp excluded-address 10.0.0.1 10.0.0.10
* ip dchp excluded-address 10.1.0.1 10.1.0.10
* ip dchp excluded-address 10.2.0.1 10.2.0.10
* ip dchp excluded-address 10.0.0.17 10.0.0.26
* ip dhcp excluded-address 10.3.0.1 10.3.0.10
* ip dhcp excluded-address 10.4.0.1 10.4.0.10
* ip dhcp excluded-address 10.6.0.1 10.6.0.10
* ip dhcp pool A-mgmt.
* network 10.0.0.0 255.255.255.240
* default-gateway 10.0.0.1
* domain-name jeremysitlab.com
* dns-server 10.5.0.4
* option 43 ip 10.0.0.7
* ip dhcp pool A-PC
* network 10.1.0.0 255.255.255.240
* default-gateway 10.1.0.1
* domain-name jeremysitlab.com
* dns-server 10.5.0.4
* ip dhcp pool A-Phone
* network 10.2.0.0 255.255.255.240
* default-gateway 10.2.0.1
* domain-name jeremysitlab.com
* dns-server 10.5.0.4
* ip dhcp pool B-mgmt
* network 10.0.0.16 255.255.255.240
* default-gateway 10.0.0.17
* domain-name jeremysitlab.com
* dns-server 10.5.0.4
* option 43 ip 10.0.0.7
* ip dhcp pool B-PC
* network 10.3.0.0 255.255.255.240
* default-gateway 10.3.0.1
* domain-name jeremysitlab.com
* dns-server 10.5.0.4
* ip dhcp pool B-Phone
* network 10.4.0.0 255.255.255.240
* default-gateway 10.4.0.1
* domain-name jeremysitlab.com
* dns-server 10.5.0.4
* ip dhcp pool Wi-Fi
* network 10.6.0.0 255.255.255.240
* default-gateway 10.6.0.1
* domain-name jeremysitlab.com
* dns-server 10.5.0.4

2. Configure the Distribution switches to relay wired DHCP clients’ broadcast messages to R1’s Loopback0 IP address

Command :

### For DSW-A1, DSW-A2

* interface Vlan 10
* ip helper-address 10.0.0.76
* interface vlan 20
* ip helper-address 10.0.0.76
* interface vlan 40
* ip helper-address 10.0.0.76
* interface vlan 99
* ip helper address 10.0.0.76

### For DSW-B1, DSW-B2

* interface Vlan 10
* ip helper-address 10.0.0.76
* interface vlan 20
* ip helper-address 10.0.0.76
* interface vlan 30
* ip helper-address 10.0.0.76
* interface vlan 99
* ip helper address 10.0.0.76

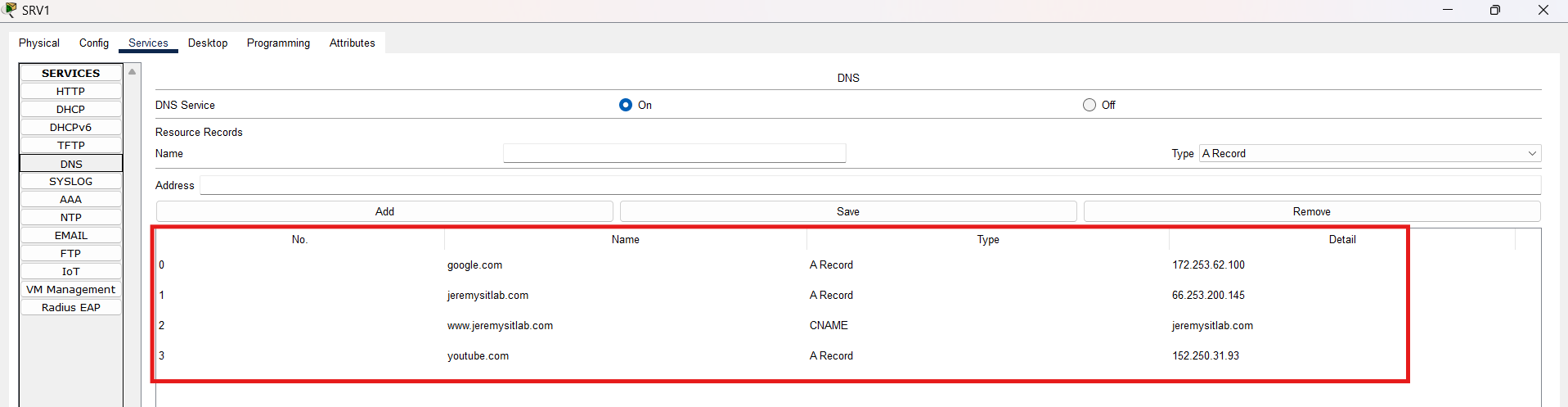
3. Configure the following DNS entries on SRV1:

a. google.com = 172.253.62.100

b. youtube.com = 152.250.31.93

c. jeremysitlab.com = 66.235.200.145

d. www.jeremysitlab.com = jeremysitlab.com



4. Configure all routers and switches to use domain name jeremysitlab.com and use SRV1 as their DNS server.

Command:

###For All Devices

* ip domain-name jerremysitlab.com
* ip name-server 10.5.0.4

5. Configure NTP on R1:

a. Make R1 a stratum 5 NTP server.

b. R1 should learn the time from NTP server 216.239.35.0

Command:

* ntp master 5
* ntp server 216.239.35.0

6. All Core, Distribution, and Access switches should use R1’s loopback interface as their NTP server.

a. Clients should authenticate R1 using key number 1 and the password ccna.

Command:

### For All Switches

* ntp authentication-key 1 md5 ccna
* ntp trusted-key 1
* ntp server 10.0.0.76 key 1

7. Configure the SNMP community string SNMPSTRING on all routers and switches. The string should allow GET messages, but not SET messages.

8. Configure Syslog on all routers and switches:

a. Send Syslog messages to SRV1. Messages of all severity levels should be logged.

b. Enable logging to the buffer. Reserve 8192 bytes of memory for the buffer.

Command:

### For All devices

* snmp-server community SNMPSTRING ro
* logging 10.5.0.4
* logging trap debugging
* logging buffered 8192

9. Use FTP on R1 to download a new IOS version from SRV1:

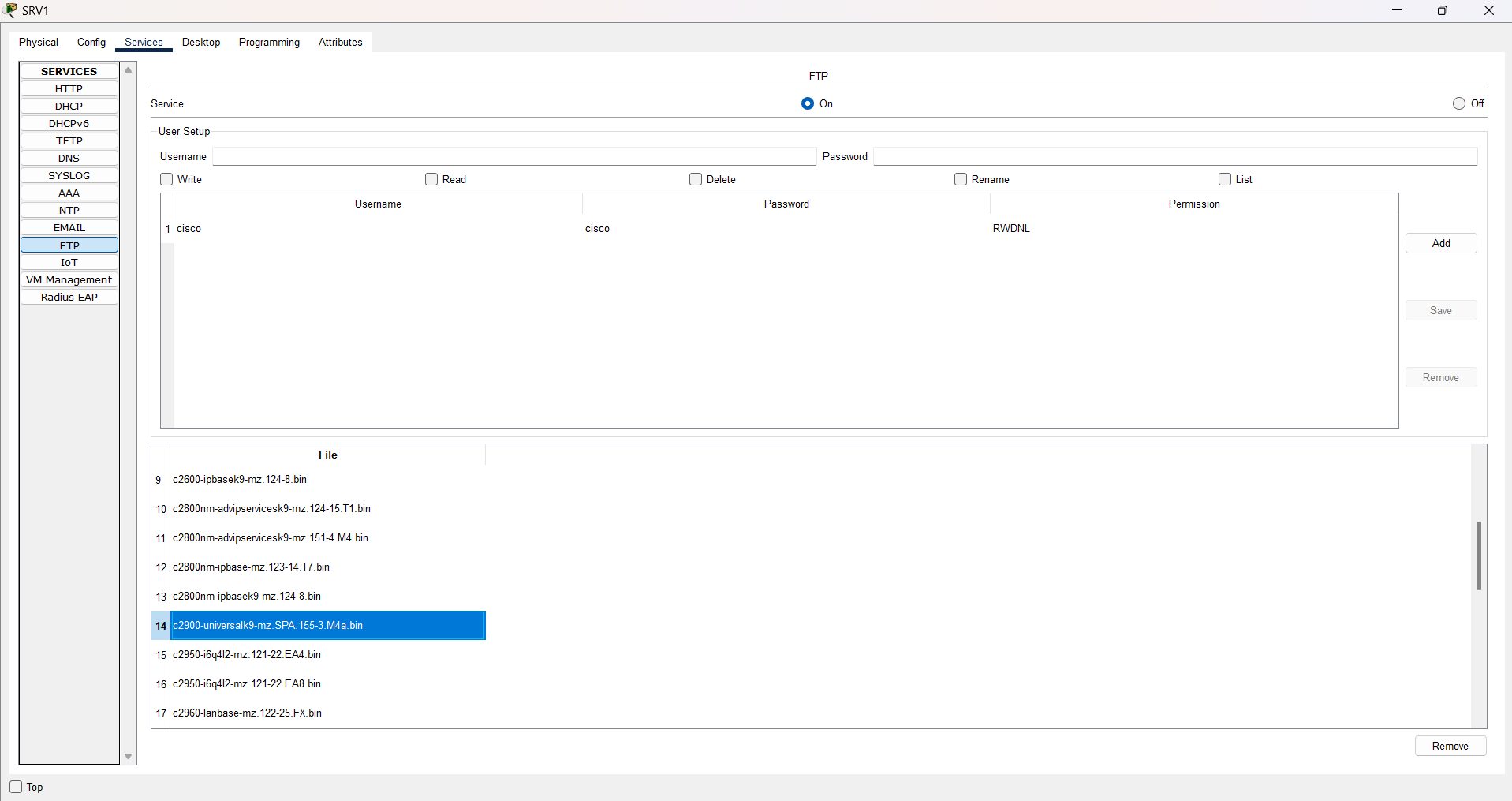
a. Configure R1’s default FTP credentials: username cisco, password cisco.

Command :

* ip ftp username cisco
* ip ftp password cisco

b. Use FTP to copy the file c2900-universalk9-mz.SPA.155-3.M4a.bin from SRV1 to R1’s flash drive.

c. Reboot R1 using the new IOS file, and then delete the old one from flash



* do copy ftp flash
* Address or name of remote host []? 10.5.0.4
* source filename []? c2900-universalk9-mz.SPA.155-3.M4a.bin
* Destination filename [c2900-universalk9-mz.SPA.155-3.M4a.bin]?
* Boot system flash:c2900-universalk9-mz.SPA.155-3.M4a.bin

### deleting the old flash

* R1#delete flash:c2900-universalk9-mz.SPA.151-4.M4.bin

Show command: show flash, show version

10. Configure SSH for secure remote access on all routers and switches.

a. Use the largest modulus size for the RSA keys.

b. Allow SSHv2 connections only.

c. Create standard ACL 1, only allowing packets sourced from Office A’s PCs subnet. Apply the ACL to all VTY lines to restrict SSH access.

d. Allow only SSH connections to the VTY lines.

e. Require users to log in with a local user account when connecting via SSH.

f. Configure synchronous logging on the VTY lines

Command:

* crypto key generate rsa
* 4096
* ip ssh version 2
* access-list 1 permit 10.1.0.0 0.0.0.255
* line vty 0 15
* access-class 1 in
* transport input ssh
* login local
* logging synchronous

11. Configure static NAT on R1 to enable hosts on the Internet to access SRV1 via the IP address 203.0.113.113.

Command :

* ip nat inside source static 10.5.0.5 203.0.113.113
* interface range g0/0/0,g0/1/0
* ip nat outside
* interface range g0/0-1
* ip nat inside

12. Configure pool-based dynamic PAT on R1 to enable hosts in the Office A PCs, Office A Phones, Office B PCs, Office B Phones, and Wi-Fi subnets to access the Internet.

a. Use standard ACL 2 to define the appropriate inside local address ranges in the following order:

i. Office A PCs: 10.1.0.0/24

ii. Office A Phones: 10.2.0.0/24

iii. Office B PCs: 10.3.0.0/24

iv. Office B Phones: 10.4.0.0/24

v. Wi-Fi: 10.6.0.0/24

b. Define a range of inside global addresses called POOL1, specifying the range 203.0.113.200 to 203.0.113.207 with a /29 netmask.

c. Map ACL 2 to POOL1 and enable PAT. Confirm that hosts can access the Internet by pinging jeremysitlab.com.

Command:

* access-list 2 permit 10.1.0.0 0.0.0.255
* access-list 2 permit 10.2.0.0 0.0.0.255
* access-list 2 permit 10.3.0.0 0.0.0.255
* access-list 2 permit 10.4.0.0 0.0.0.255
* access-list 2 permit 10.6.0.0 0.0.0.255
* ip nat pool POOL1 203.0.113.200 203.0.113.207 netmask 255.255.255.248
* ip nat inside source list 2 pool POOL1 overload

13. Disable CDP on all devices and enable LLDP instead.

a. Disable LLDP Tx on each Access switch’s access port (F0/1)

Command:

### For R1, Core switches, Distribution switches

* no cdp run
* lldp run

### For Access switches

* no cdp run
* lldp run
* interface f0/1
* no lldp transmit

**PART 7 - Security : ACLs and Layer-2 Security Features**

1. Configure extended ACL OfficeA\_to\_OfficeB where appropriate:

a. Allow ICMP messages from the Office A PCs subnet to the Office B PCs subnet.

b. Block all other traffic from the Office A PCs subnet to the Office B PCs subnet.

c. Allow all other traffic.

d. Apply the ACL according to general best practice for extended ACLs.

Command :

### For DSW-A1, DSW-A2 (Extended ACL as close to the source)

* ip access-list extended OfficeA\_to\_OfficeB
* permit icmp 10.1.0.0 0.0.0.255 10.3.0.0 0.0.0.255
* deny ip 10.1.0.0 0.0.0.255 10.3.0.0 0.0.0.255
* permit ip any any
* interface vlan 10
* ip access-group OfficeA\_to\_OfficeB in

2. Configure Port Security on each Access switch's F0/1 port:

a. Allow the minimum necessary number of MAC addresses on each port.

i. SRV1 does not use virtualization, so it uses a single MAC address.

b. Configure a violation mode that blocks invalid traffic without affecting valid traffic. The switches should send notifications when invalid traffic is detected.

c. Switches should automatically save the secure MAC addresses they learn to the running-config.

Command :

### For ASW-1, ASW-B1, ASW-B3

* interface f0/1
* switchport port-security
* switchport port-security violation restrict
* switchport port-security Mac-address sticky

### For ASW-A2, ASW-A3, ASW-B2

* interface f0/1
* switchport port-security
* switchport port-security maximum 2
* switchport port-security mac-address sticky
* switchport port-security violation restrict

3. Configure DHCP Snooping on all Access switches.

a. Enable it for all active VLANs in each LAN.

b. Trust the appropriate ports.

c. Disable insertion of DHCP Option 82.

d. Set a DHCP rate limit of 15 pps on active untrusted ports.

e. Set a higher limit (100 pps) on ASW-A1’s connection to WLC1.

Command:

### For ASw-A1

* ip dhcp snooping
* ip dhcp snooping vlan 10,20,40,99
* no ip dhcp snooping information option
* interfacae range g0/1-2
* ip dhcp snooping trust
* interface f0/1
* ip dhcp snooping limit rate 15
* interface f0/2
* ip dhcp snooping limit rate 100

### For ASW-A2, ASW-A3

* ip dhcp snooping
* ip dhcp snooping vlan 10,20,40,99
* no ip dhcp snooping information option
* interfacae range g0/1-2
* ip dhcp snooping trust
* interface f0/1
* ip dhcp snooping limit rate 15

### For ASW-B1, ASW-B2, ASW-B3

* ip dhcp snooping
* ip dhcp snooping vlan 10,20,30,99
* no ip dhcp snooping information option
* interfacae range g0/1-2
* ip dhcp snooping trust
* interface f0/1
* ip dhcp snooping limit rate 15

4. Configure DAI on all Access switches.

a. Enable it for all active VLANs in each LAN.

b. Trust the appropriate ports.

c. Enable all optional validation checks.

Command:

### For ASW-A1, ASW-A2, ASW-A3

* ip arp inspection vlan 10,20,40,99
* ip arp inspection validate src-mac dst-mac ip
* interface range g0/1-2
* ip arp inspection trust

### For ASW-B1, ASW-B2, ASW-B3

* ip arp inspection vlan 10,20,30,99
* ip arp inspection validate src-mac dst-mac ip
* interface range g0/1-2
* ip arp inspection trust

**PART 8 – IPv6**

1. To prepare for a migration to IPv6, enable IPv6 routing and configure IPv6 addresses on R1, CSW1, and CSW2:

a. R1 G0/0/0: 2001:db8:a::2/64

b. R1 G0/1/0: 2001:db8:b::2/64

c. R1 G0/0 and CSW1 G1/0/1: Use prefix 2001:db8:a1::/64 and EUI-64 to generate an interface ID for each interface.

d. R1 G0/1 and CSW2 G1/0/1: Use prefix 2001:db8:a2::/64 and EUI-64 to generate an interface ID for each interface.

e. CSW1 Po1 and CSW2 Po1: Enable IPv6 without using the ‘ipv6 address’ command.

Command

### For R1

* ipv6 unicast-routing
* interface g0/0/0
* ipv6 address 2001:db8:a::2/64
* interface g0/1/0
* ipv6 address 2001:db8:b::2/64
* interface g0/0
* ipv6 address 2001:db8:a1::/64 eui-64
* interface g0/1
* ipv6 address 2001:db8:a2::/64 eui-64

###For CSW1

* ipv6 unicast-routing
* interface g1/0/1
* ipv6 address 2001:db8:a1::/64 eui-64
* interface po1
* ipv6 enable

###For CSW2

* ipv6 unicast-routing
* interface g1/0/1
* ipv6 address 2001:db8:a2::/64 eui-64
* interface po1
* ipv6 enable

show commands: show ipv6 interface brief

2. Configure two default static routes on R1:

a. A recursive route via next hop 2001:db8:a::1.

b. A fully-specified route via next hop 2001:db8:b::1. Make it a floating route by configuring the AD 1 higher than default.

Command:

* ipv6 route ::/0 2001:db8:a::1
* ipv6 route ::/0 g0/1/0 2001:db8:b::1 2

**PART 9 : Wireless**

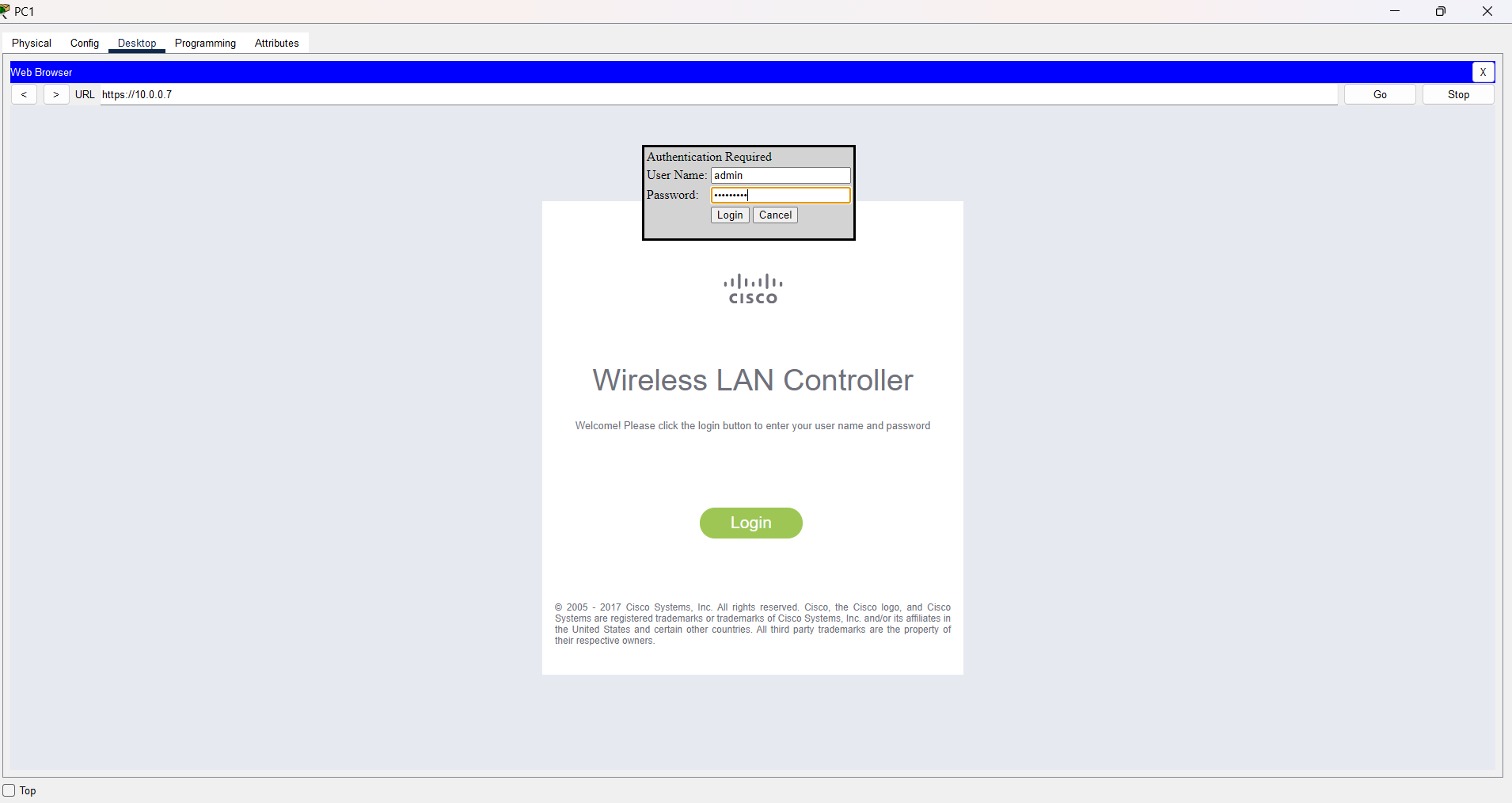
1. Access the GUI of WLC1 (https://10.0.0.7) from one of the PCs.

a. Username: admin

b. Password: adminPW12

-Access WLC using webserver IP address <https://10.0.0.7>

-Then login with user credentials



2. Configure a dynamic interface for the Wi-Fi WLAN (10.6.0.0/24)

a. Name: Wi-Fi

b. VLAN: 40

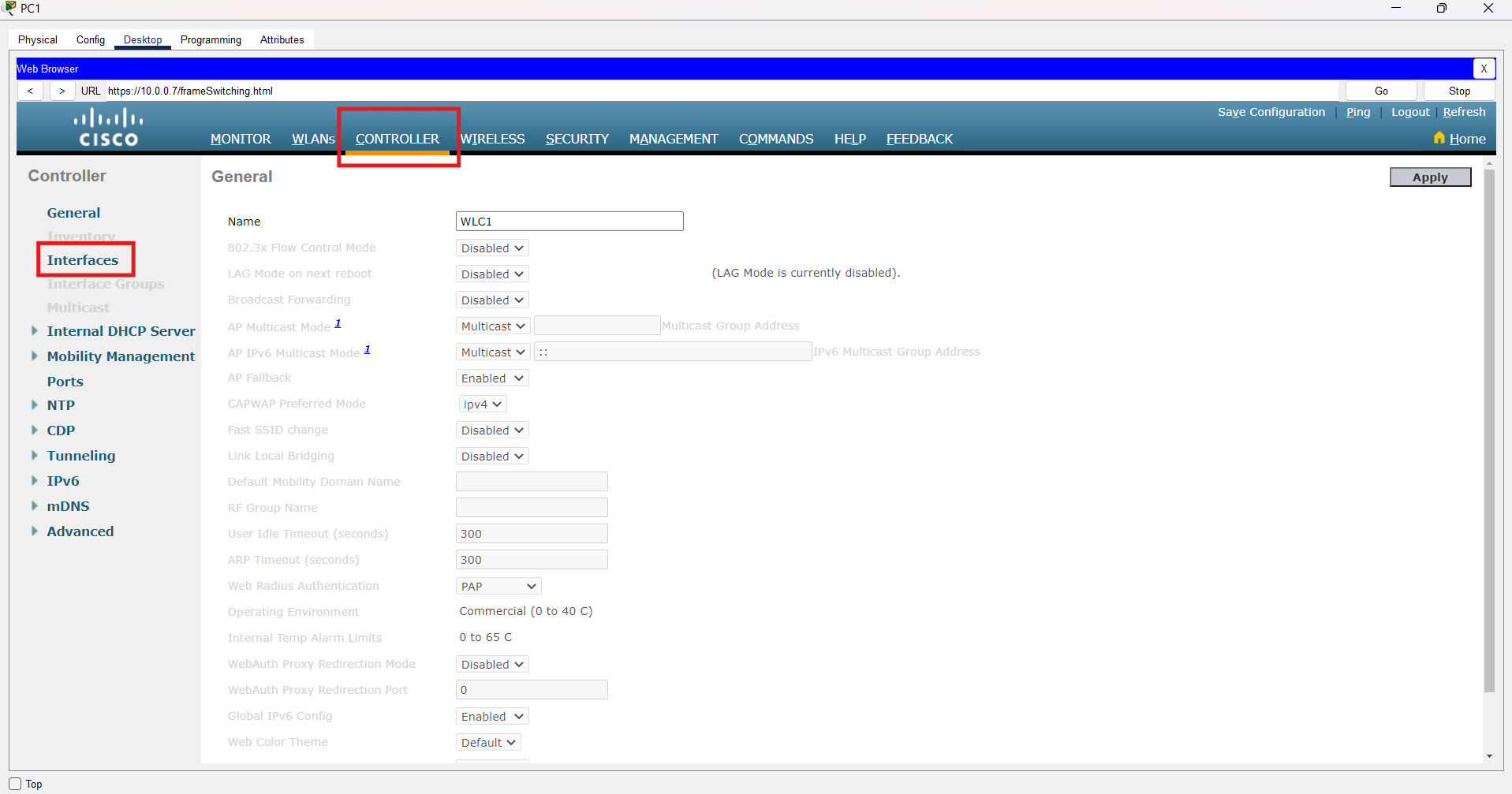
c. Port number: 1

d. IP address: .2 of its subnet

e. Gateway: .1 of its subnet

f. DHCP server: 10.0.0.76

-After Login in to WLC click on Controller tab and select the Interface as shown in Below picture



-To add Dynamic interface to the WLC Click on the New tab on the Right up side of the page.

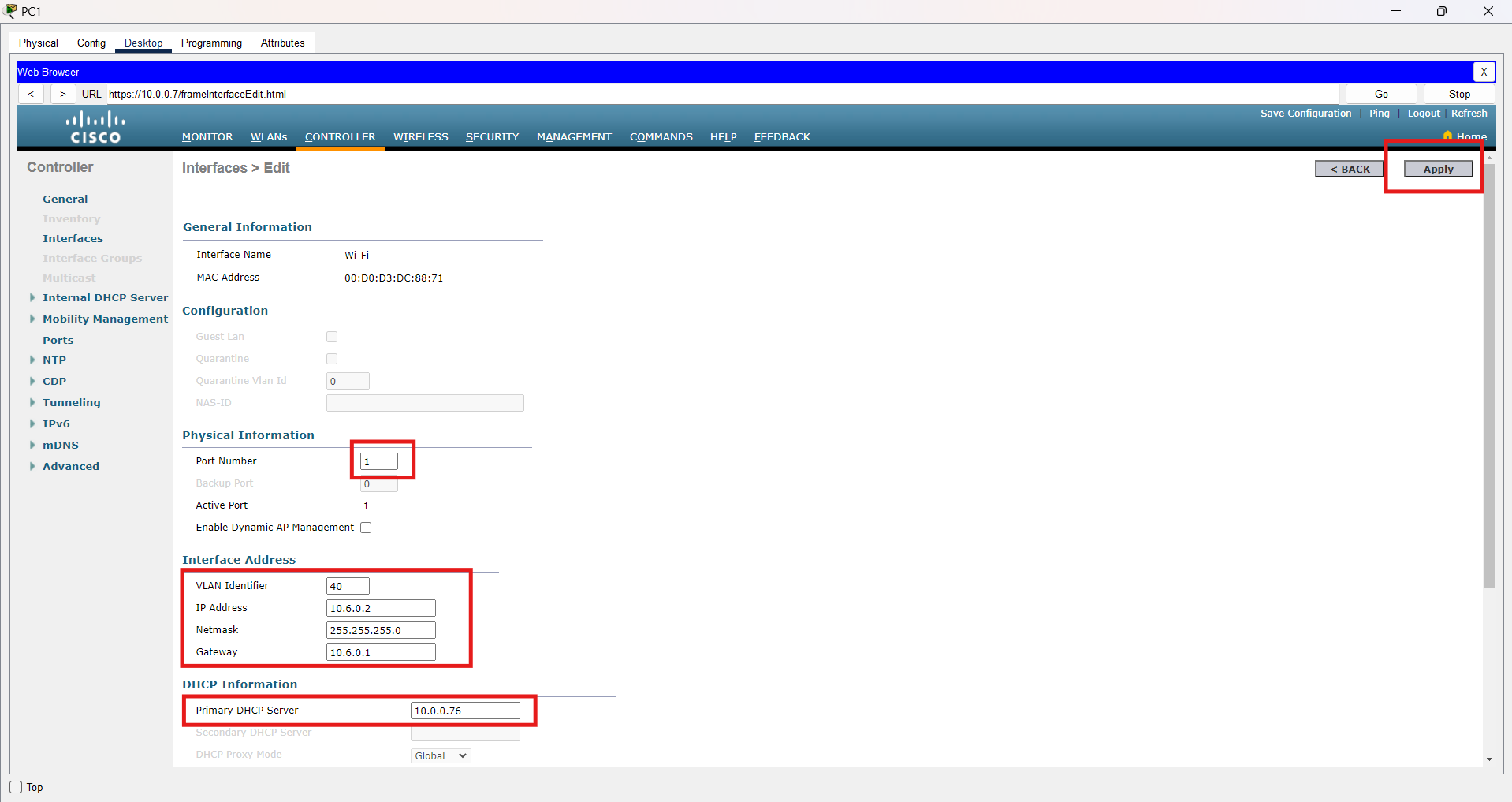
-Name the Dynamic interface as Wi-Fi and Vlan 40 (which is Wifi vlan)

-Then have to fill up the details of port number as 1 as it connected to physical port 1

-Fill the Interface details Vlan identifier to 40 and IP address of the WLC 10.6.0.2 Netmask 255.255.255.0 and Default gateway 10.6.0.1

-Mention the Primary DHCP server as 10.0.0.76 (R1 Loopback ) and click on Apply

- Give Save configuration to save the Wifi Configuration.



3. Configure and enable the following WLAN:

a. Profile name: Wi-Fi

b. SSID: Wi-Fi

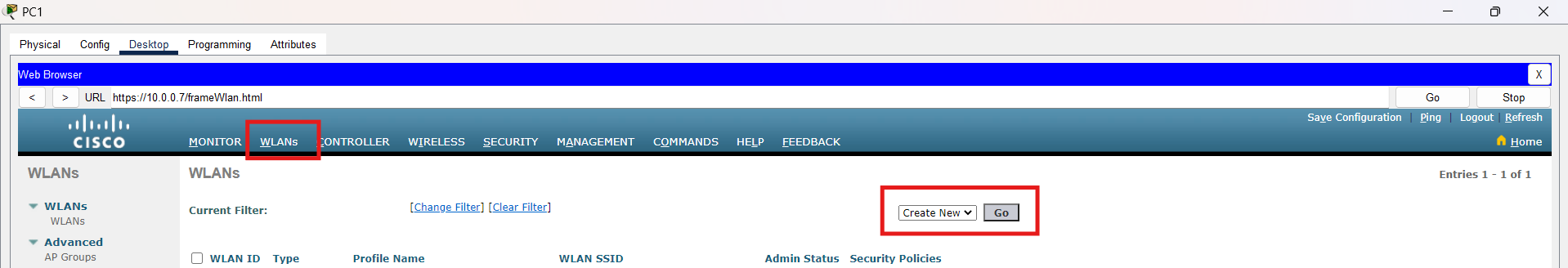
c. ID: 1

d. Status: Enabled

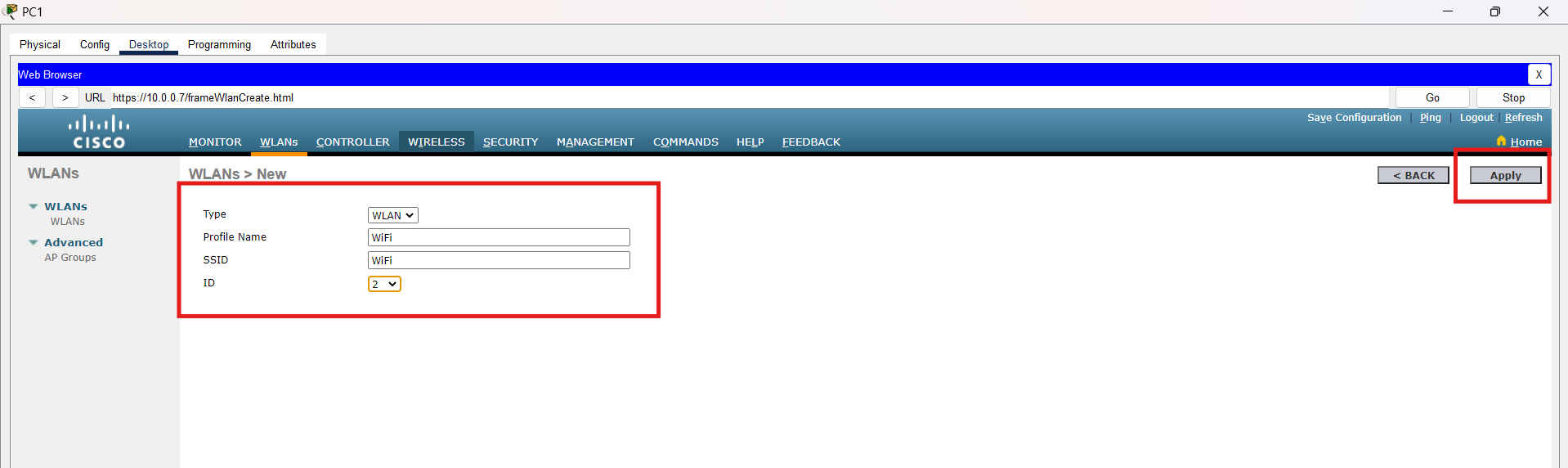
e. Security: WPA2 Policy with AES encryption, PSK of cisco123

Configuration :

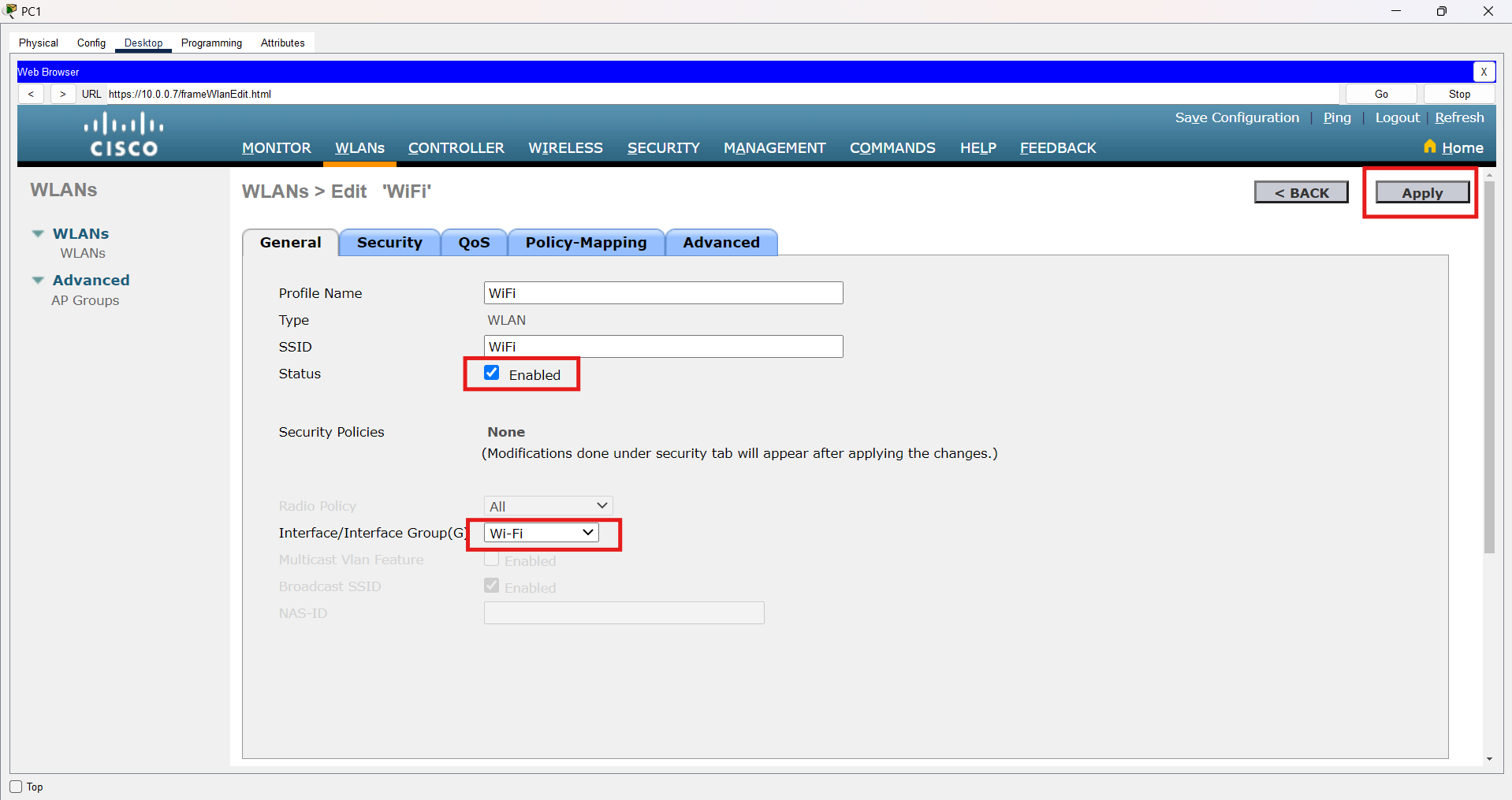
-To create a WLAN click on Create new and give go.



-Now Fill the Details below as shown Type –WLAN, Profile name –Wi-Fi, SSID-WiFi and Give apply.

-

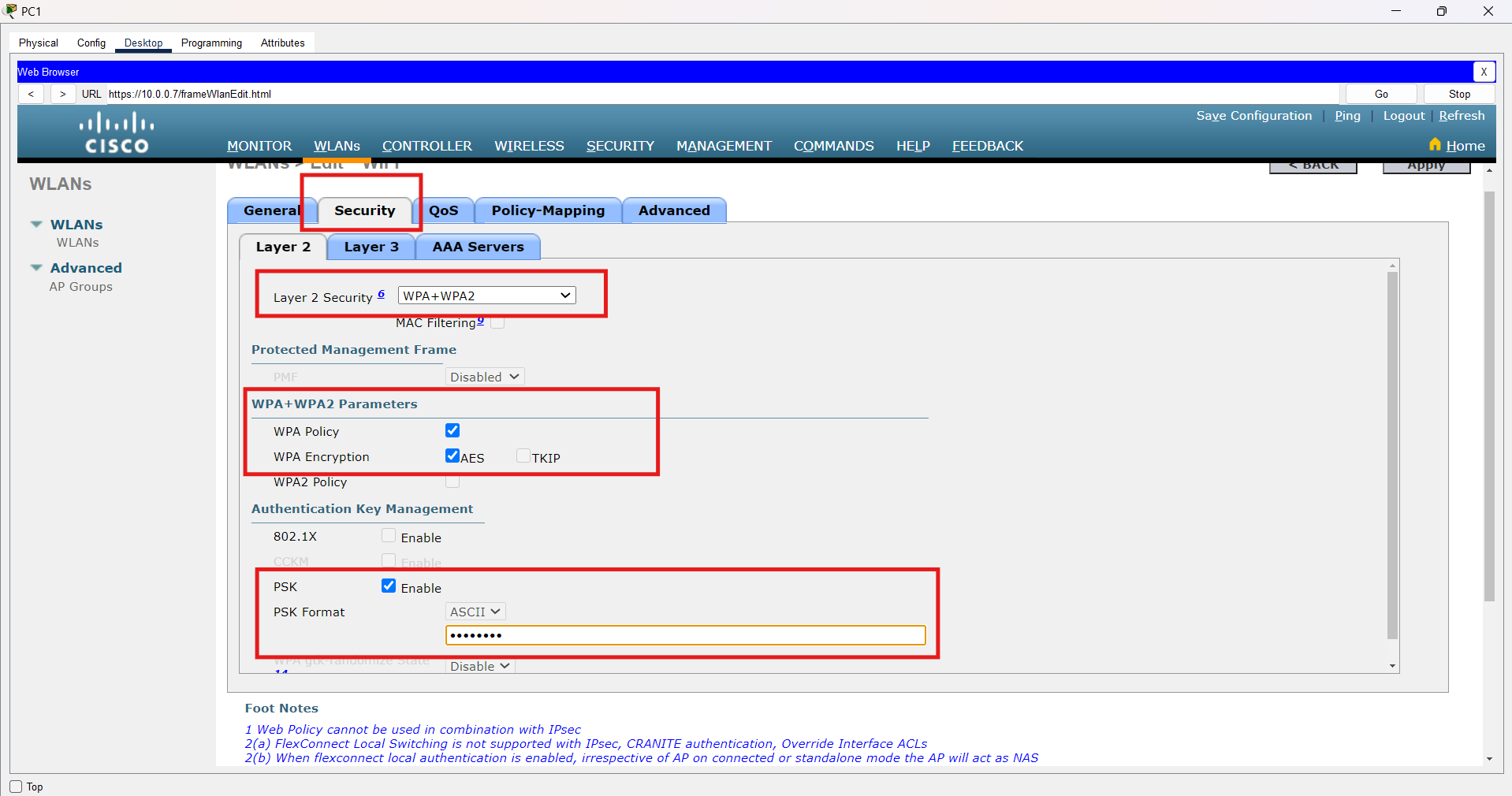
-In the tab General settings Click on the Enable check box to enable WLAN, This WLAN should use the Wifi interface change interface from Management to WiFi.



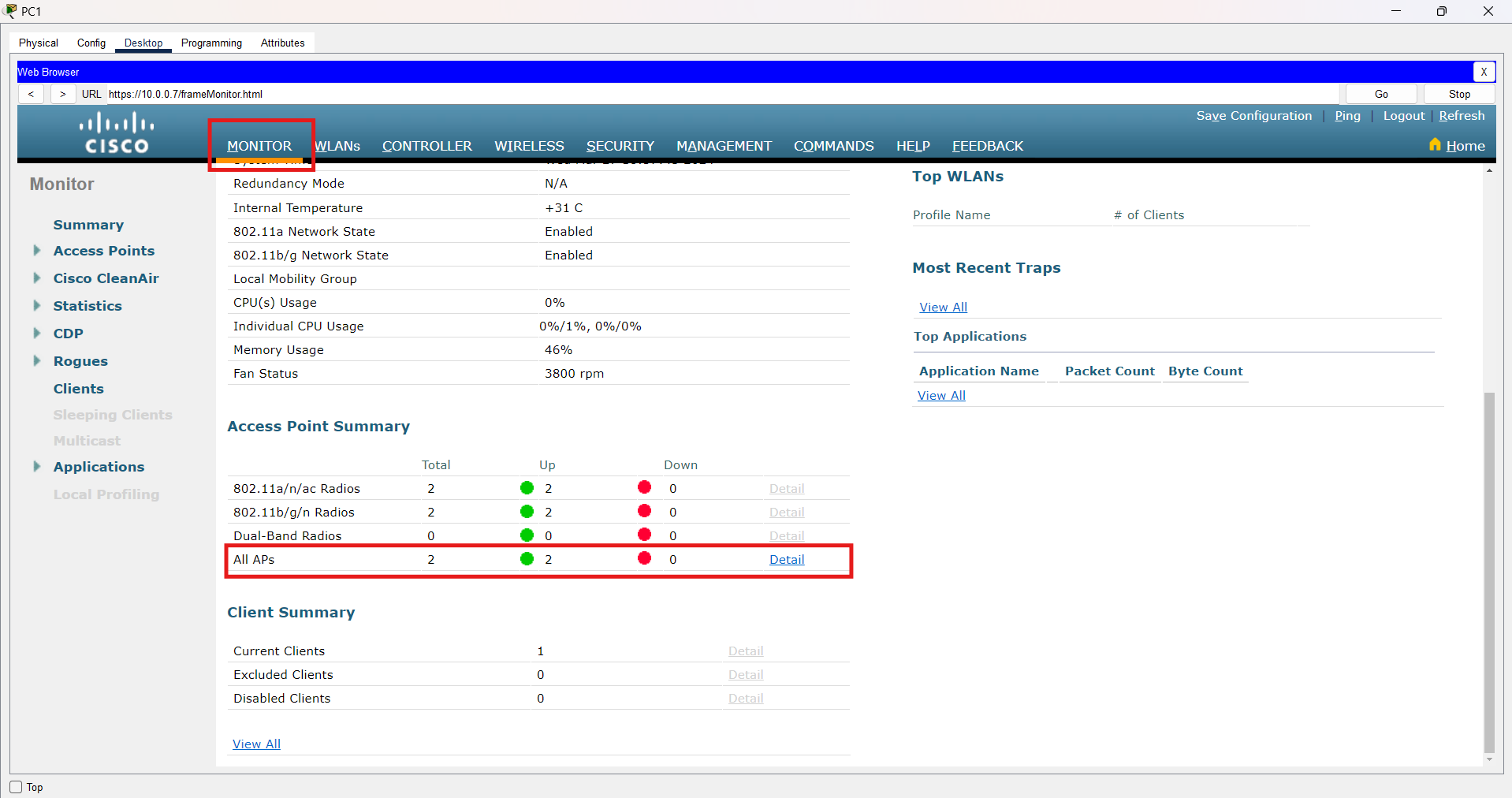
-Now go to the Security Tab, Enable WPA security from the Layer 2 security tab and select WPA+WPA2.

-Then click on WPA2 policy for encryption enable the AES check box and then enable Pre-shared key tab and configure as “cisco123”

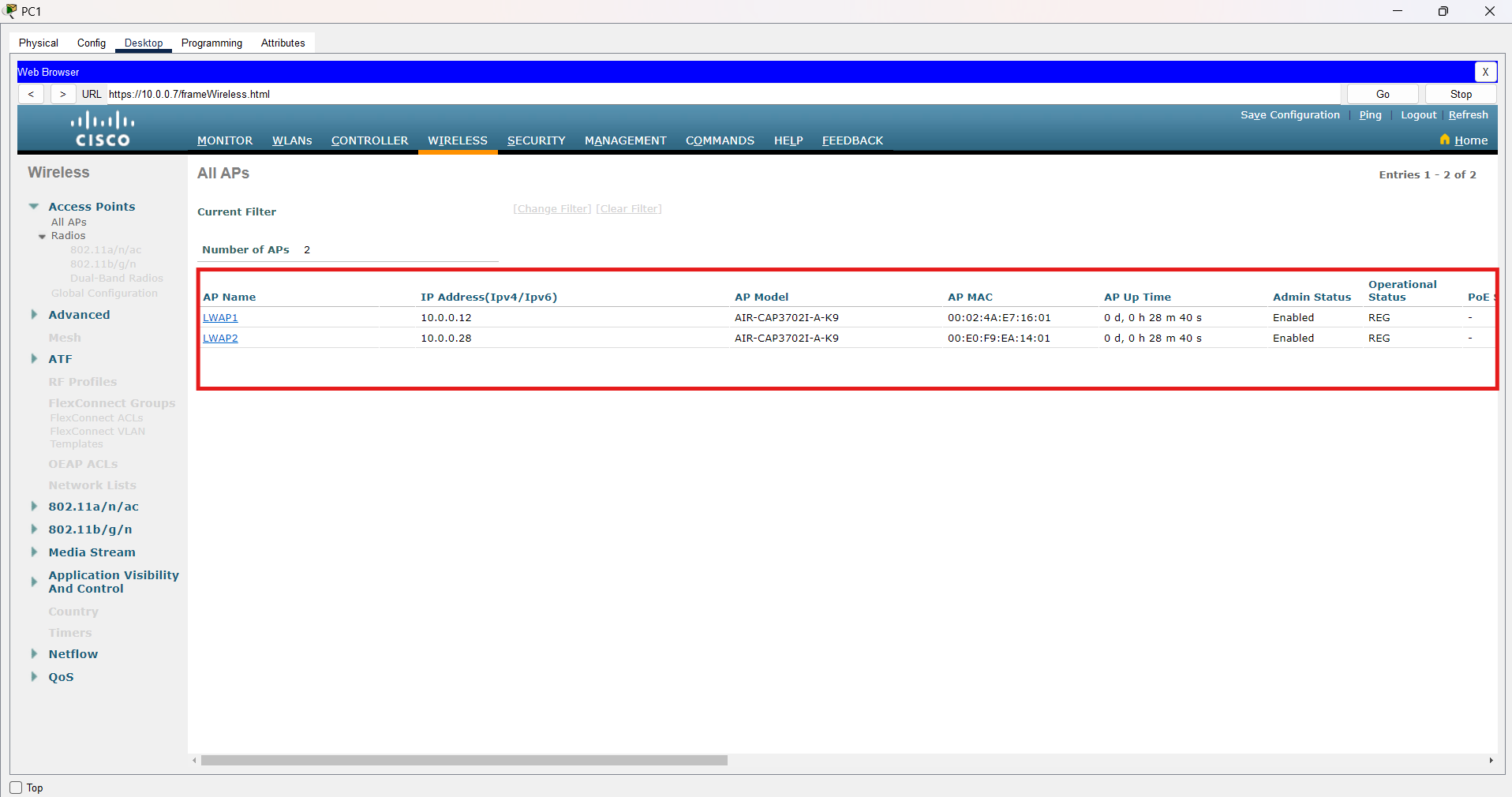
-Click on Apply and save configuration .



-After configuration Return to the Monitor screen and scroll down to Access Point summary click on all AP’s to show the Associated AP’s with WLC1.



-This is are the LWAP’s associated to WLC1.



4. Verify that both LWAPs have associated with WLC1.

Configuration:

-Specify the SSID:Wi-Fi, Enable WPA2PSK and give the PSK and finally select the Encryption type as AES.

