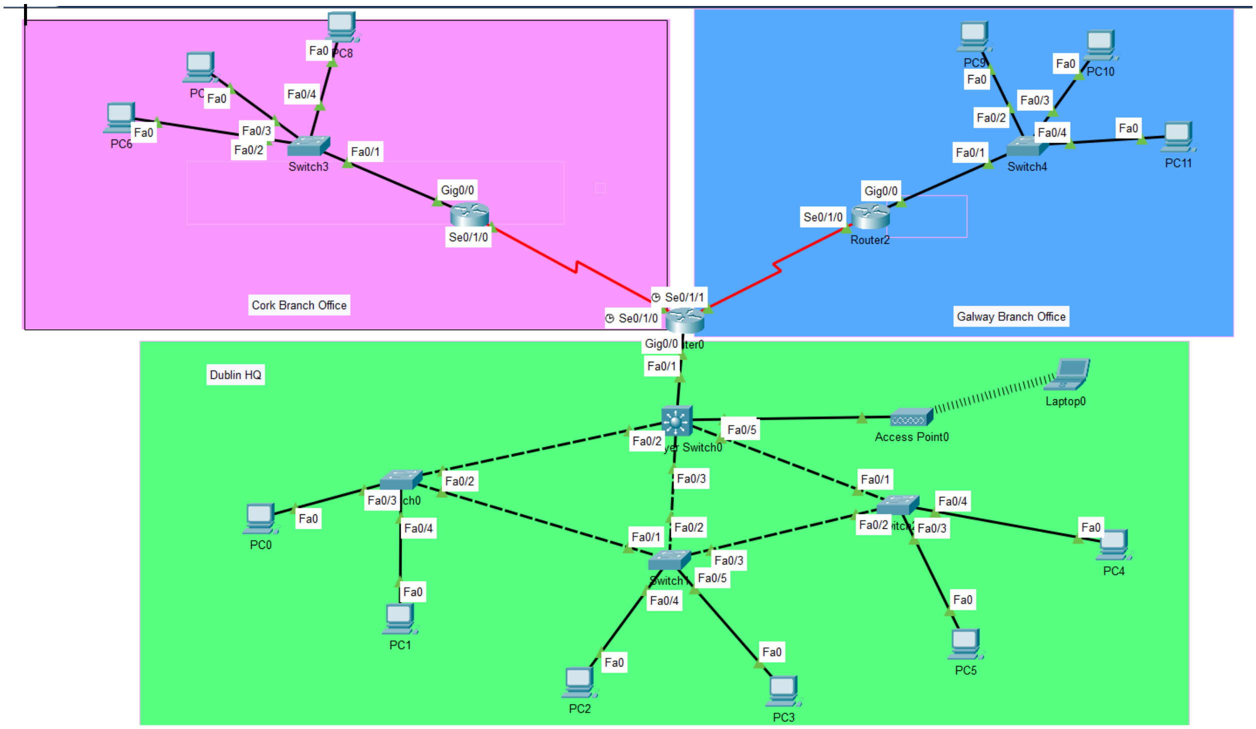
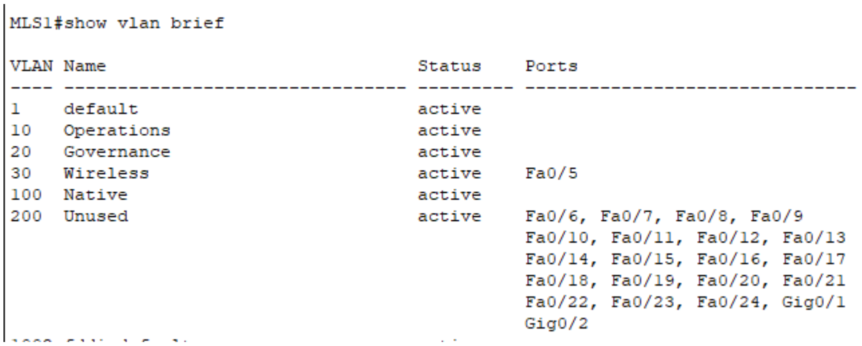
Routing & Wireless Concepts Project Documentation



I designed the above network prototype to fulfil the requirements of Emerald Retail Ltd, a growing Irish retail chain. In this project, I focused on seamless communication between the office headquarters in Dublin, and the two smaller branch offices in Cork and Galway. Other important aspects of this project were security, reliability and scalability.

Requirement 1:

In the headquarters, I have configured VLANs 10 (Operations) and 20 (Governance). These VLANs successfully segregate the traffic while also maintaining communication between all departments via inter-VLAN routing, configured on the Multi-Layer Switch. I also have a VLAN 30 (Wireless) to be used to route traffic to and from the Wireless Access Point and any connected devices, a VLAN 100 (Native) to ensure that traffic can travel through trunk ports, and a VLAN 200 (Unused) to assign all ports that are shutdown and currently not being used, for extra security.



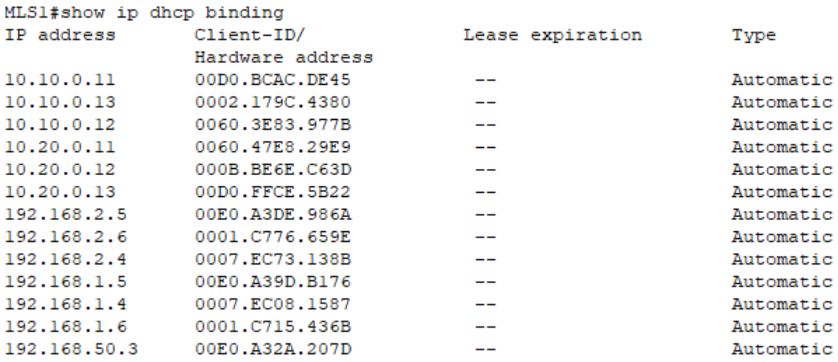
```
MLS1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   Operations                       active
20   Governance                       active
30   Wireless                         active    Fa0/5
100  Native                           active
200  Unused                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
```

Requirement 2:

Using the MLS as the DHCP server, I have dynamically assigned unique IPv4 addresses to all of the end devices on the network. The Operations VLAN uses the 10.10.0.0/25 prefix, and the Governance VLAN uses the 10.20.0.0/27 prefix.

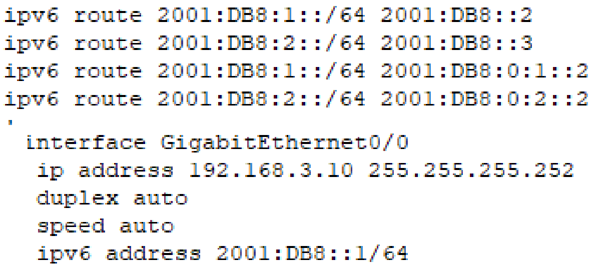
The Cork and Galway branch network also receive unique addresses from the MLS, using 192.168.1.0/27 and 192.168.2.0/27 prefixes respectively.

Wireless clients connecting through the Access Point also receive a unique IPv4 address using the MLS and the 192.168.50.0/24 prefix.

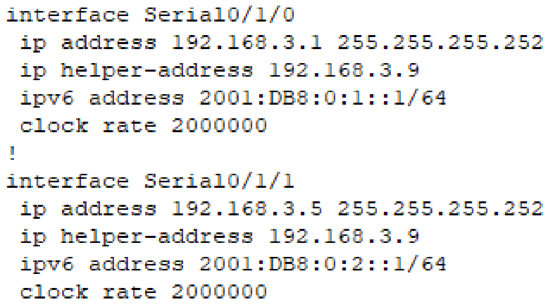


```
MLS1#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.10.0.11       00D0.BCAC.DE45           --                     Automatic
10.10.0.13       0002.179C.4380           --                     Automatic
10.10.0.12       0060.3E83.977B           --                     Automatic
10.20.0.11       0060.47E8.29E9           --                     Automatic
10.20.0.12       000B.BE6E.C63D           --                     Automatic
10.20.0.13       00D0.FFCE.5B22           --                     Automatic
192.168.2.5      00E0.A3DE.986A           --                     Automatic
192.168.2.6      0001.C776.659E           --                     Automatic
192.168.2.4      0007.EC73.138B           --                     Automatic
192.168.1.5      00E0.A39D.B176           --                     Automatic
192.168.1.4      0007.EC08.1587           --                     Automatic
192.168.1.6      0001.C715.436B           --                     Automatic
192.168.50.3     00E0.A32A.207D           --                     Automatic
```

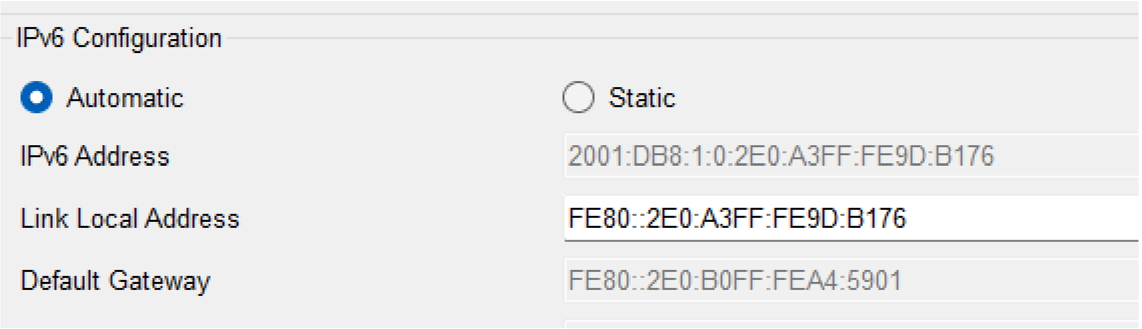
Using SLAAC, both branch networks have dynamic IPv6 addresses assigned to their end devices. I achieved this by enabling ‘ipv6 unicast-routing’ on all routers, and then assigning IPv6 addresses to all interfaces. I then configured ipv6 static routes to ensure smooth communication.



```
ipv6 route 2001:DB8:1::/64 2001:DB8::2
ipv6 route 2001:DB8:2::/64 2001:DB8::3
ipv6 route 2001:DB8:1::/64 2001:DB8:0:1::2
ipv6 route 2001:DB8:2::/64 2001:DB8:0:2::2
'
 interface GigabitEthernet0/0
  ip address 192.168.3.10 255.255.255.252
  duplex auto
  speed auto
  ipv6 address 2001:DB8::1/64
```



```
interface Serial0/1/0
 ip address 192.168.3.1 255.255.255.252
 ip helper-address 192.168.3.9
 ipv6 address 2001:DB8:0:1::1/64
 clock rate 2000000
!
interface Serial0/1/1
 ip address 192.168.3.5 255.255.255.252
 ip helper-address 192.168.3.9
 ipv6 address 2001:DB8:0:2::1/64
 clock rate 2000000
```



IPv6 Configuration

● Automatic ○ Static

IPv6 Address: 2001:DB8:1:0:2E0:A3FF:FE9D:B176

Link Local Address: FE80::2E0:A3FF:FE9D:B176

Default Gateway: FE80::2E0:B0FF:FEA4:5901

Requirement 3:

On all layer 2 switches, I have enabled various different security measures to protect the network.

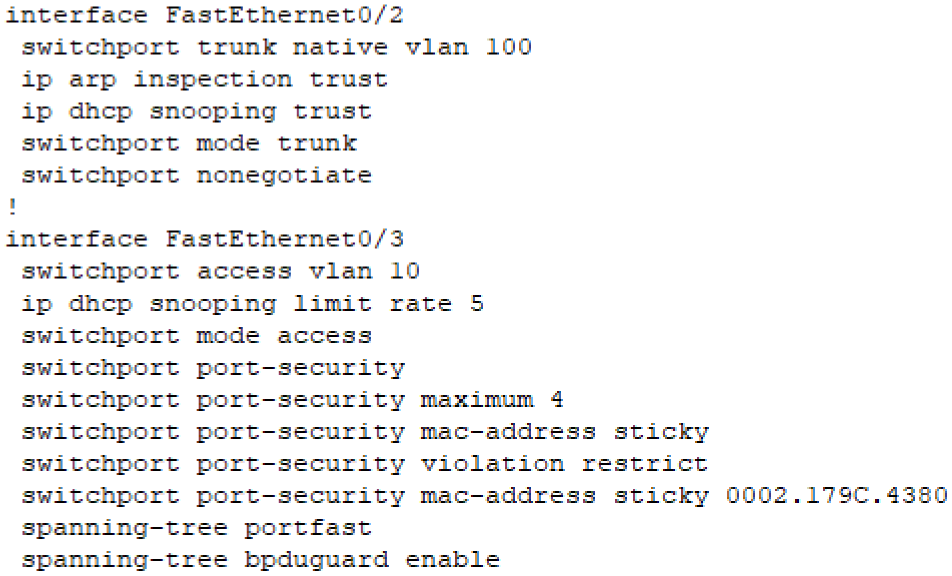
To prevent MAC Table and VLAN Attacks, port security is enabled on all access ports. I have a maximum of 4 mac addresses allowed to be learned on this ports, and they are ‘sticky’, meaning it dynamically learns the mac address of the first device that connects to that port, and remembers it even if the device is shut down. The violation mode on all of these ports is restrict, meaning if a mac address is detected outside of the four allowed addresses, packets will not be forwarded and the violation is logged.

To prevent STP attacks, spanning tree BPDU guard and portfast is also enabled on all access ports. This protects the spanning tree topology from malicious BPDUs that could potentially cause loops or reroute traffic.

To prevent DHCP attacks, DHCP snooping is enabled on all access ports to limit the amount of DHCP packets that can be sent. Trunk ports are marked as trusted ports, so that DHCP requests and addresses can be sent without interruptions.

To prevent ARP Spoofing, ARP inspection is enabled globally on the switch and then ‘ip arp inspection trust’ is enabled on the trunk ports to ensure effective population of the ARP table.

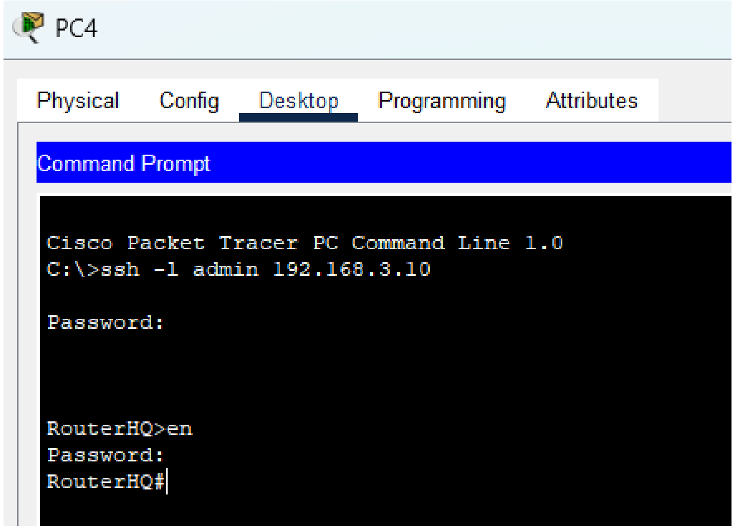
Below shows one of my layer 2 switches with FastEthernet0/2 being a trusted trunk port, and FastEthernet0/3 being an untrusted access port, and the security configurations to go along with that.



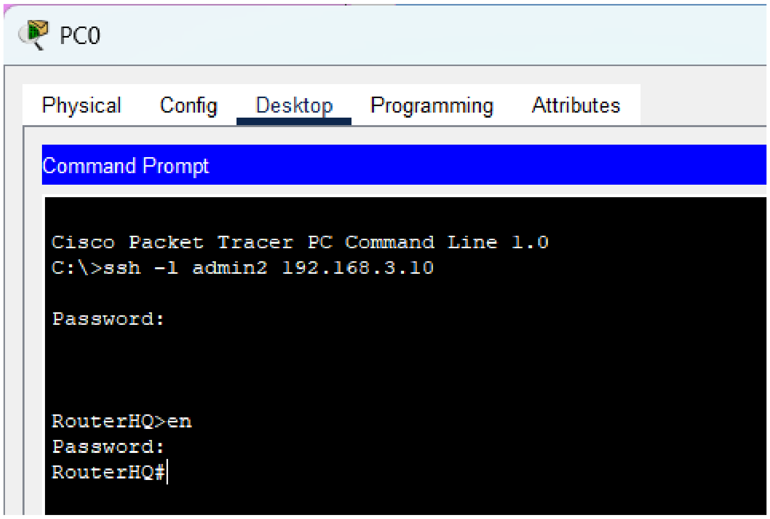
```
interface FastEthernet0/2
 switchport trunk native vlan 100
 ip arp inspection trust
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/3
 switchport access vlan 10
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0002.179C.4380
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Requirement 4:

I have successfully allowed two users to securely and remotely connect to the headquarters head router using SSH.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.3.10

Password:



RouterHQ>en
Password:
RouterHQ#
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin2 192.168.3.10

Password:



RouterHQ>en
Password:
RouterHQ#
```

Requirement 5:

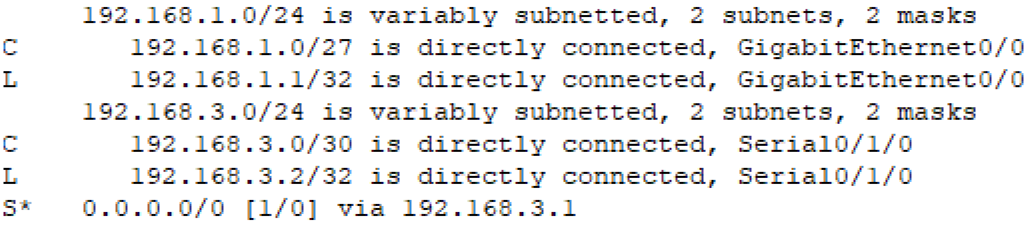
I have configured static routes between the main headquarters and the branch networks to ensure effective communication. My topology includes three routers connecting all three networks, so static routes are essential.

I used an IPv4 private addressing scheme using the 192.168.3.0/30 prefix on the router interfaces. I chose a /30 subnet as they are suitable for point-to-point networks, like connecting two routers.

```
     10.0.0.0/27 is subnetted, 2 subnets
S       10.10.0.0/27 [1/0] via 192.168.3.9
S       10.20.0.0/27 [1/0] via 192.168.3.9
     192.168.1.0/27 is subnetted, 1 subnets
S       192.168.1.0/27 [1/0] via 192.168.3.2
     192.168.2.0/27 is subnetted, 1 subnets
S       192.168.2.0/27 [1/0] via 192.168.3.6
     192.168.3.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.3.0/30 is directly connected, Serial0/1/0
L       192.168.3.1/32 is directly connected, Serial0/1/0
C       192.168.3.4/30 is directly connected, Serial0/1/1
L       192.168.3.5/32 is directly connected, Serial0/1/1
C       192.168.3.8/30 is directly connected, GigabitEthernet0/0
L       192.168.3.10/32 is directly connected, GigabitEthernet0/0
```

As seen from the HQ Routers routing table above, I have configured next-hop static routes to both branch networks and both VLANs in the HQ.

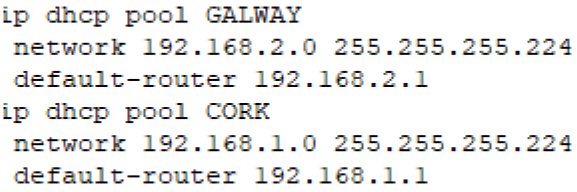
I also configured default routes on the routers for both branch networks, so they have a path back to the HQ.



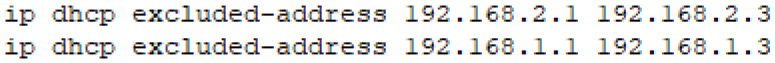
```
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, Serial0/1/0
L       192.168.3.2/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 192.168.3.1
```

Requirement 6:

Both branch networks have dynamic IPv4 addresses assigned by the DHCP server at the headquarters. This is possible because of the static routes connecting the headquarters to the branch networks.



```
ip dhcp pool GALWAY
 network 192.168.2.0 255.255.255.224
 default-router 192.168.2.1
ip dhcp pool CORK
 network 192.168.1.0 255.255.255.224
 default-router 192.168.1.1
```



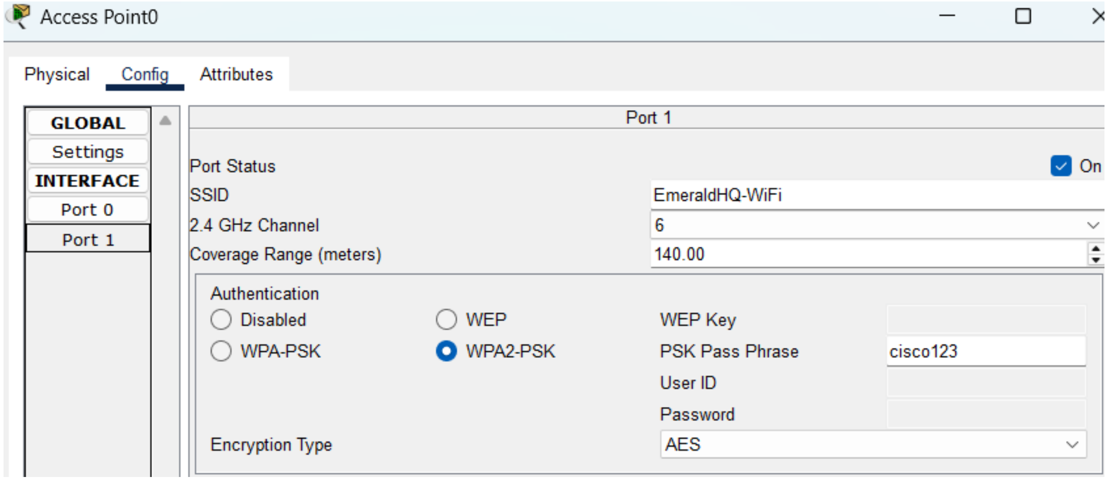
```
ip dhcp excluded-address 192.168.2.1 192.168.2.3
ip dhcp excluded-address 192.168.1.1 192.168.1.3
```

I have pools set up with the addressing scheme for both branch networks, and all end devices are successfully receiving IPv4 addresses.

Requirement 7:

Wireless clients can become a part of the network using the Wireless Access Point I have configured. All wireless clients receive a 192.168.50.0/24 IPv4 address via DHCP.

Clients connect to the network by choosing the correct SSID and providing the correct PSK.



Port 1

Port Status ☑ On

SSID: EmeraldHQ-WiFi

2.4 GHz Channel: 6

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

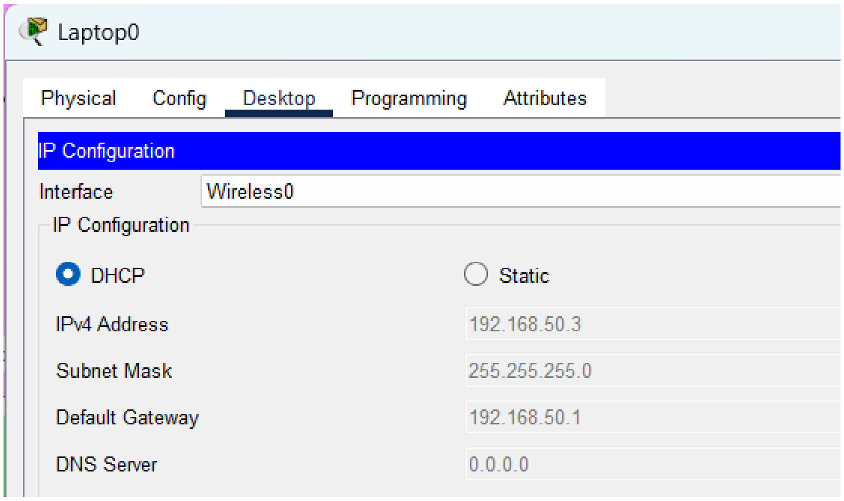
WEP Key:

PSK Pass Phrase: cisco123

User ID:

Password:

Encryption Type: AES



IP Configuration

Interface: Wireless0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.50.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.50.1

DNS Server: 0.0.0.0