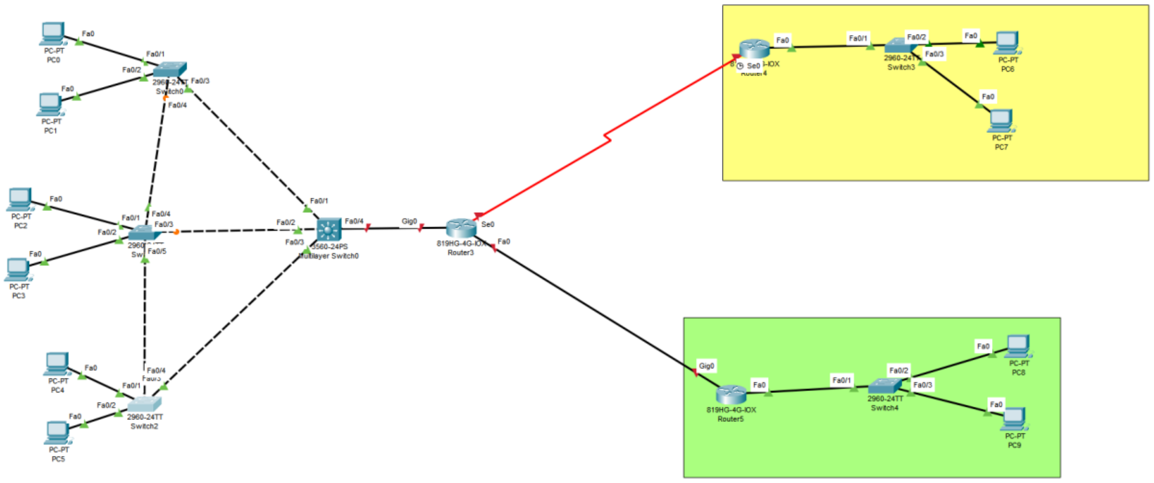
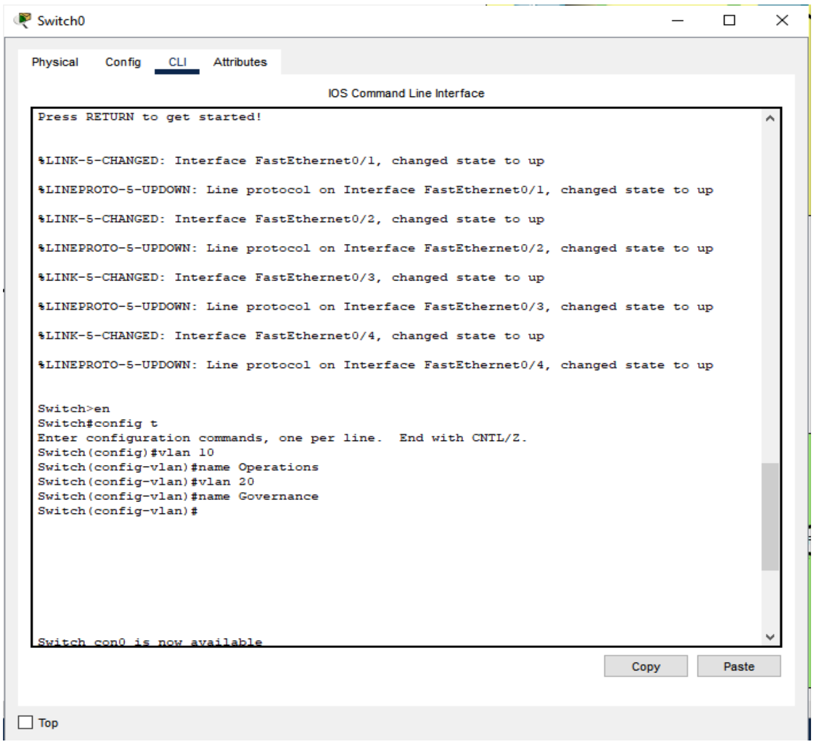
Routing and Wireless Concepts Report

This project is about creating a secure and reliable network for Emerald Retail Ltd, a company with a main office in Dublin and two branches in Cork and Galway. The goal is to build a working network that allows all location to communicate with each other. The network includes features like VLANs for better performance, IP addressing with DHCP, basic wireless access and security measures to protect the network.



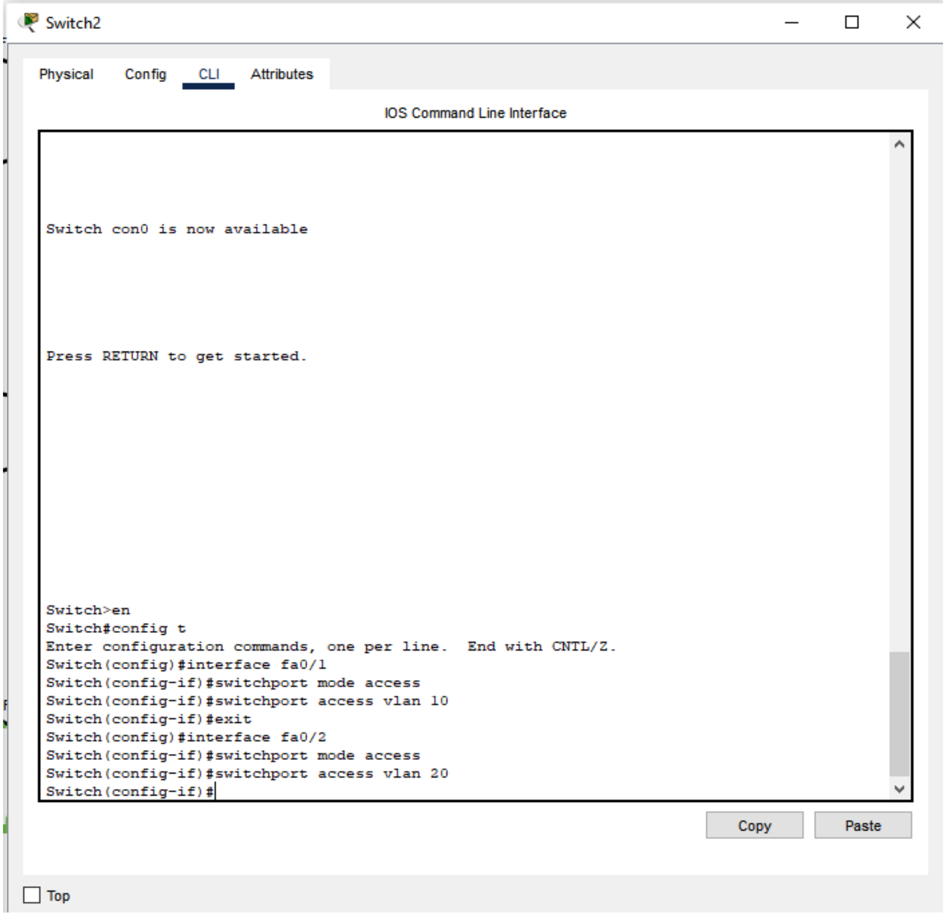
Requirement 1:

The first thing I did was make VLAN 10 and 20 on my three switches in the main office in Dublin and on the MLS. Without VLANs, all devices on a switch are on the same broadcast domain. With VLANs, you split the network into smaller, isolated groups, which reduces unnecessary traffic and improves performance.



```
Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up


Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Operations
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Governance
Switch(config-vlan)#







Switch con0 is now available
```

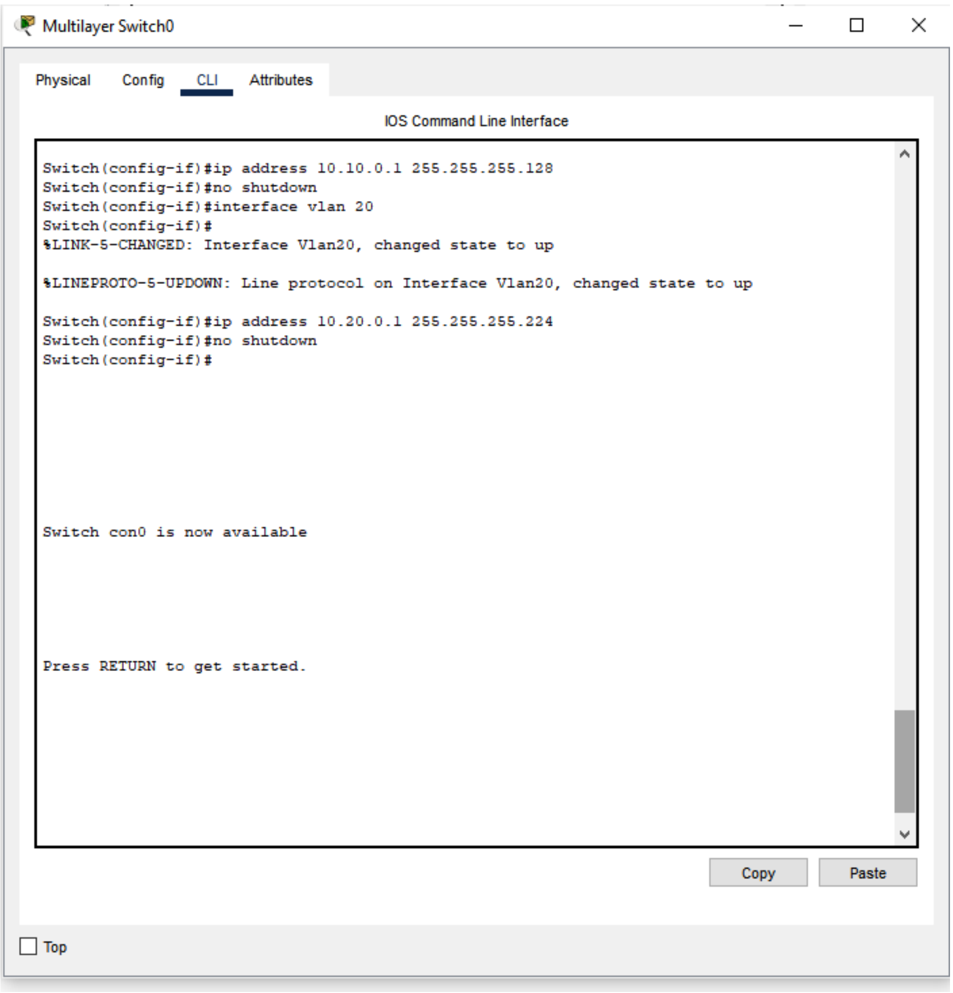
I then moved onto assigning VLANs to the PCs. I did this to separate the network into groups based on the departments. This improves security by limiting access between groups, reduces unnecessary traffic and helps manage the network more efficiently.



```
Switch con0 is now available



Press RETURN to get started.







Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
```

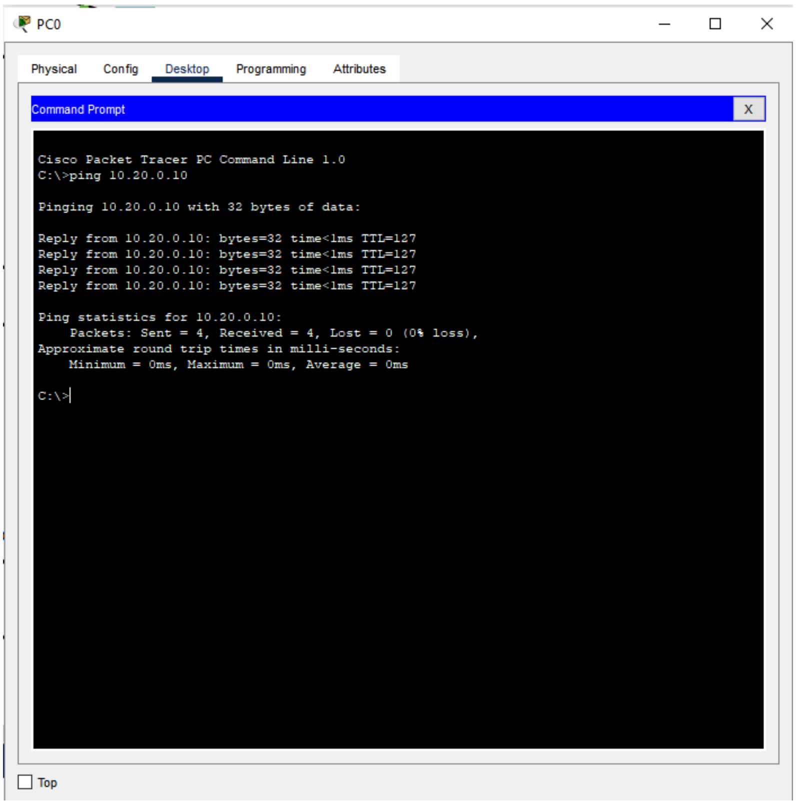
The next thing I did was set up trunk lines. Trunk lines are important because they allow multiple VLANs to communicate across different switches. By setting up trunk ports between the layer 2 switches and the multilayer switch, VLAN traffic can travel properly throughout the network. This is essential for enabling inter-VLAN routing and overall connectivity between devices in different VLANs.

Then I had to make the SVIs (Switched Virtual Interfaces) on the MLS. These are necessary in the network because the allow inter-VLAN communication through a multilayer switch. Each VLAN needs its own SVI with an IP address to act as the default gateway for devices within that VLAN. Without SVIs, devices in different VLANs wouldn’t be able to communicate with each other. In this network, SVIs were made for VLAN 10 and 20 to enable ip routing between the Operations and Governance departments.

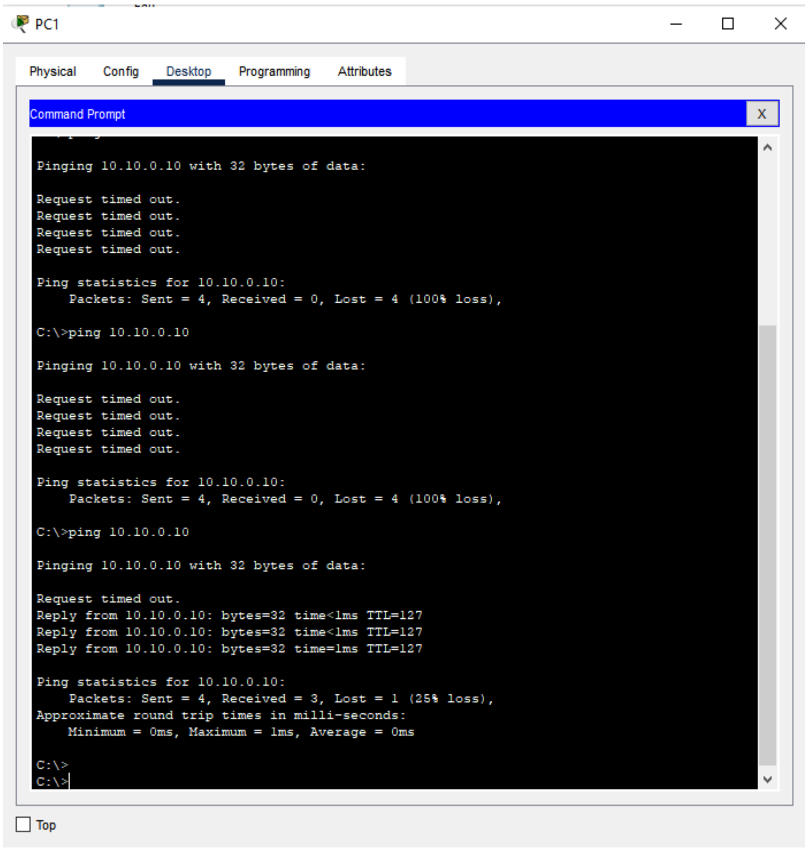


```
Switch(config-if)#ip address 10.10.0.1 255.255.255.128
Switch(config-if)#no shutdown
Switch(config-if)#interface vlan 20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

Switch(config-if)#ip address 10.20.0.1 255.255.255.224
Switch(config-if)#no shutdown
Switch(config-if)#








Switch con0 is now available






Press RETURN to get started.
```

I then decided to use static IP addresses first to make it easier to verify inter-VLAN routing and connectivity between devices without relying on DHCP configuration. Assigning static IPs also allowed me to quickly identify and fix any issues related to VLAN setup, trunking and routing before introducing DHCP into the network. I only assigned IPs to PC0 and PC1 and I was able to ping both PCs.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.20.0.10

Pinging 10.20.0.10 with 32 bytes of data:

Reply from 10.20.0.10: bytes=32 time<1ms TTL=127
Reply from 10.20.0.10: bytes=32 time<1ms TTL=127
Reply from 10.20.0.10: bytes=32 time<1ms TTL=127
Reply from 10.20.0.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.20.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



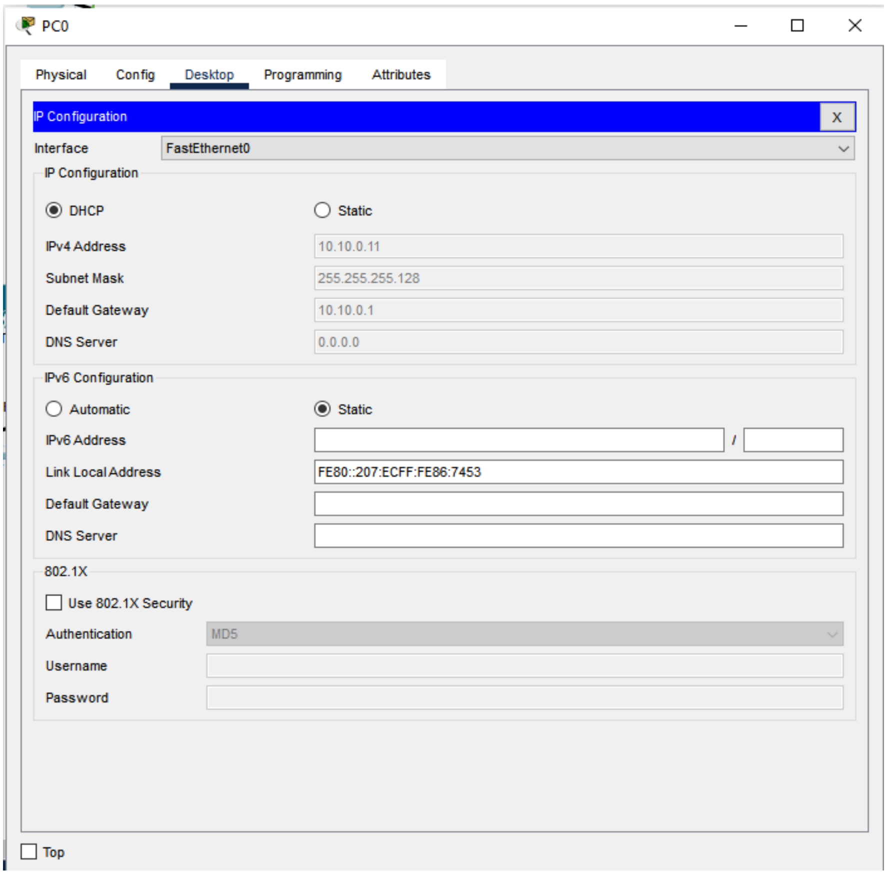
```
Pinging 10.10.0.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.10.0.10

Pinging 10.10.0.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.10.0.10

Pinging 10.10.0.10 with 32 bytes of data:

Request timed out.
Reply from 10.10.0.10: bytes=32 time<1ms TTL=127
Reply from 10.10.0.10: bytes=32 time<1ms TTL=127
Reply from 10.10.0.10: bytes=32 time=1ms TTL=127

Ping statistics for 10.10.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
C:\>
```

Requirement 2:

Each VLAN at the main office in Dublin was assigned a unique IP address range to ensure proper network segmentation. VLAN 10 (Operations) was given the subnet 10.10.0.0/25 and

VLAN 20 (Governance) was given 10.20.0.0/27. A DHCP server was configured on the multilayer switch to dynamically assign IP addresses within these ranges. 10 IP addresses were excluded to be reserved for default gateways and potential static devices, and all end devices in both VLANs successfully received IP addresses through DHCP, and all the PCs were able to ping each other.

Here is a screenshot of PC0 receiving an IP address through DHCP.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 10.10.0.11

Subnet Mask: 255.255.255.128

Default Gateway: 10.10.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::207:ECFF:FE86:7453

Default Gateway:

DNS Server:

802.1X

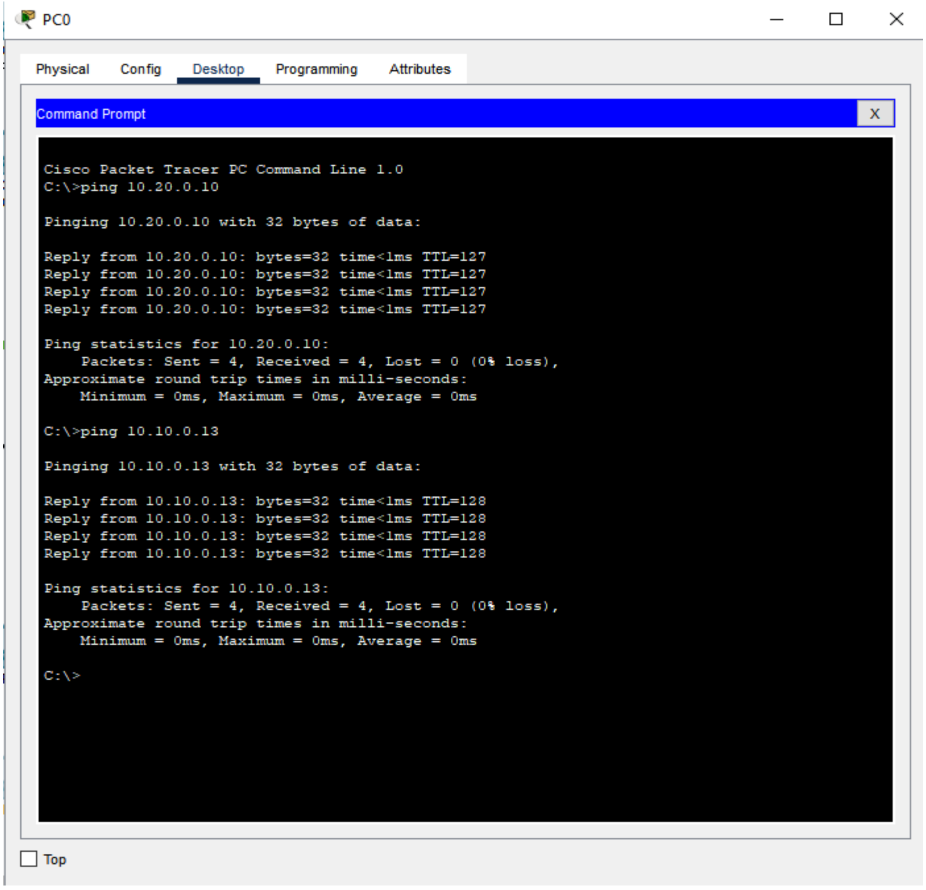
□ Use 802.1X Security

Authentication: MD5

Username:

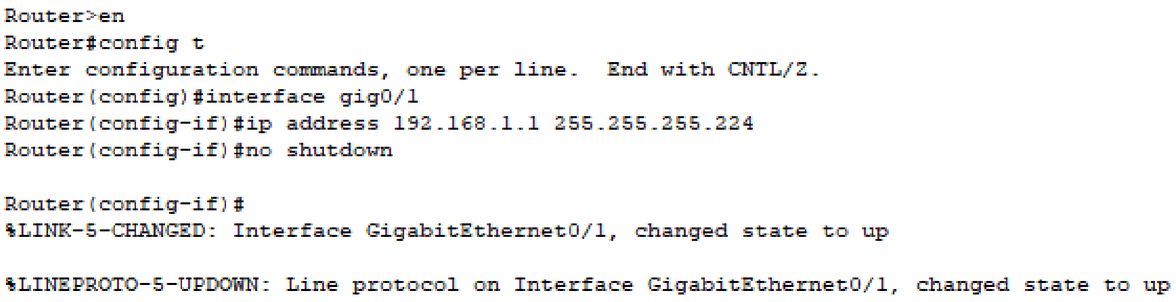
Password:

And here is a screenshot of PC0 pinging PC5 that has an IP address of 10.10.0.13

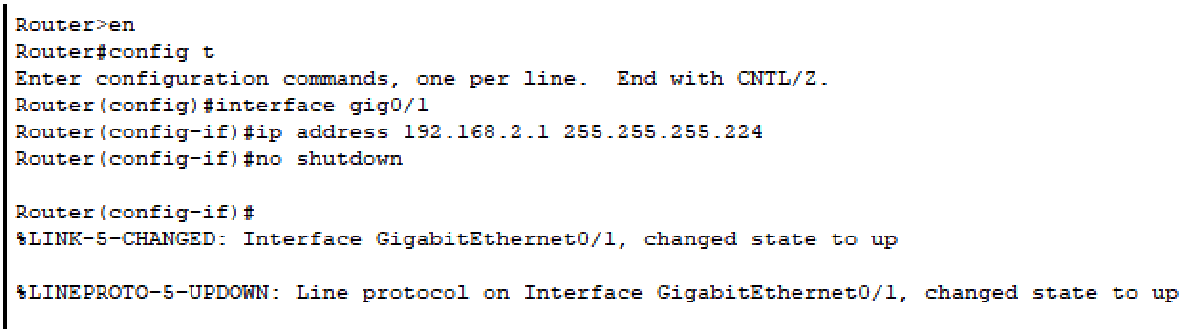


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.20.0.10

Pinging 10.20.0.10 with 32 bytes of data:

Reply from 10.20.0.10: bytes=32 time<1ms TTL=127
Reply from 10.20.0.10: bytes=32 time<1ms TTL=127
Reply from 10.20.0.10: bytes=32 time<1ms TTL=127
Reply from 10.20.0.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.20.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.10.0.13

Pinging 10.10.0.13 with 32 bytes of data:

Reply from 10.10.0.13: bytes=32 time<1ms TTL=128
Reply from 10.10.0.13: bytes=32 time<1ms TTL=128
Reply from 10.10.0.13: bytes=32 time<1ms TTL=128
Reply from 10.10.0.13: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.0.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Then the GigabitEthernet0/1 interfaces on the branch routers were configured with static IP addresses to serve as the default gateways. For the Cork branch, the interface was assigned with IP address 192.168.1.1 with a subnet mask of 255.255.255.224, and for the Galway branch, the interface was assigned with IP address 192.168.2.1 with the same subnet mask. The no shutdown command was used to activate the interfaces and enable communication between the branch routers and their connected devices.



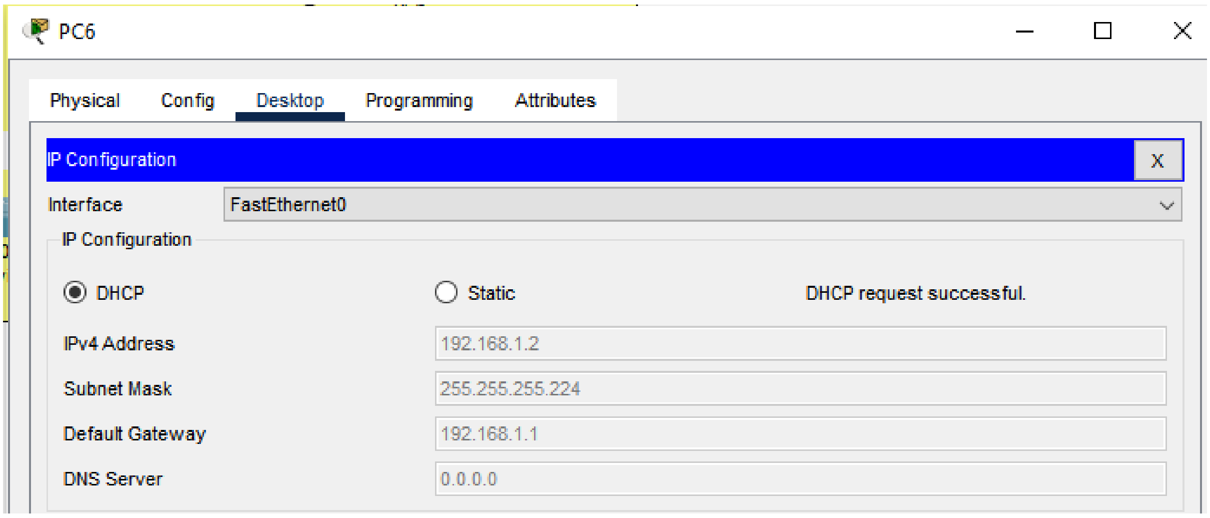
```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.224
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```



```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.224
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

To provide dynamic IP addressing for the Cork and Galway branch offices, a DHCP server was configured on the MLS. Since the DHCP server is not located locally at the branches, each branch router was configured with the ip helper-address command on its LAN interface. This allows the router to forward DHCP Discover messages from branch PCs to the MLS, where the DHCP pools for each branch are configured. To ensure the DHCP replies can return to the correct branches, static routes with next-hop IP addresses were added. On Router7, static routes were configured to reach Cork via 10.40.0.2 (Router8) and Galway via 10.50.0.2 (Router9). On the MLS, static routes were set using 10.30.0.2 (Router7’s IP) as next hop for both branch subnets.

Here are screenshots of my PCs on the branches successfully receiving an IPv4 address.



Interface FastEthernet0

IP Configuration

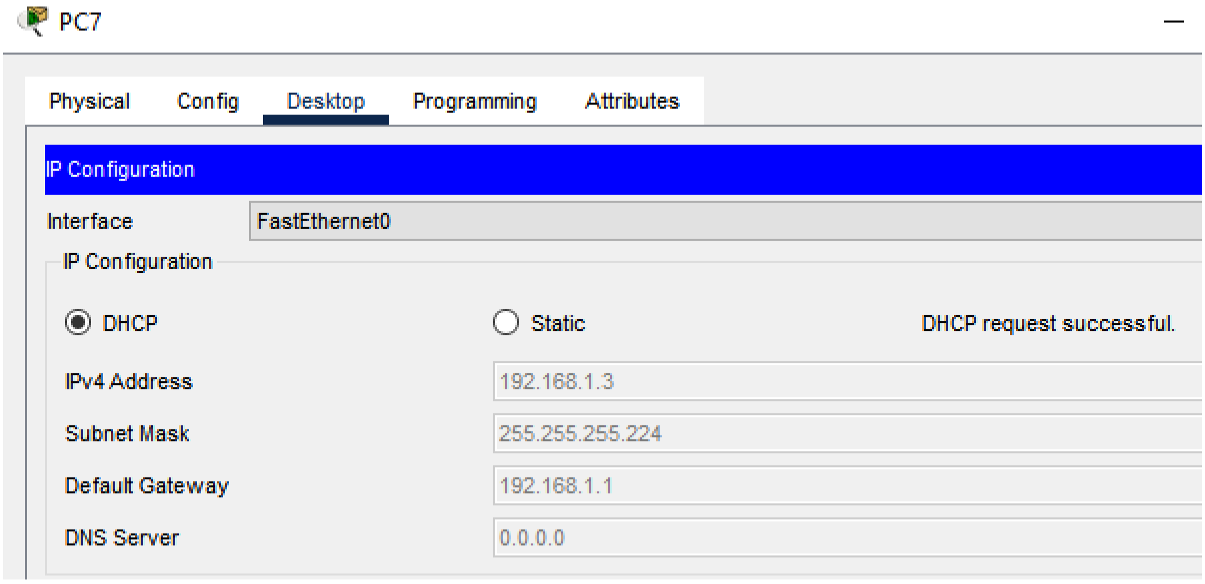
● DHCP ○ Static DHCP request successful.

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.224

Default Gateway 192.168.1.1

DNS Server 0.0.0.0



IP Configuration

Interface FastEthernet0

IP Configuration

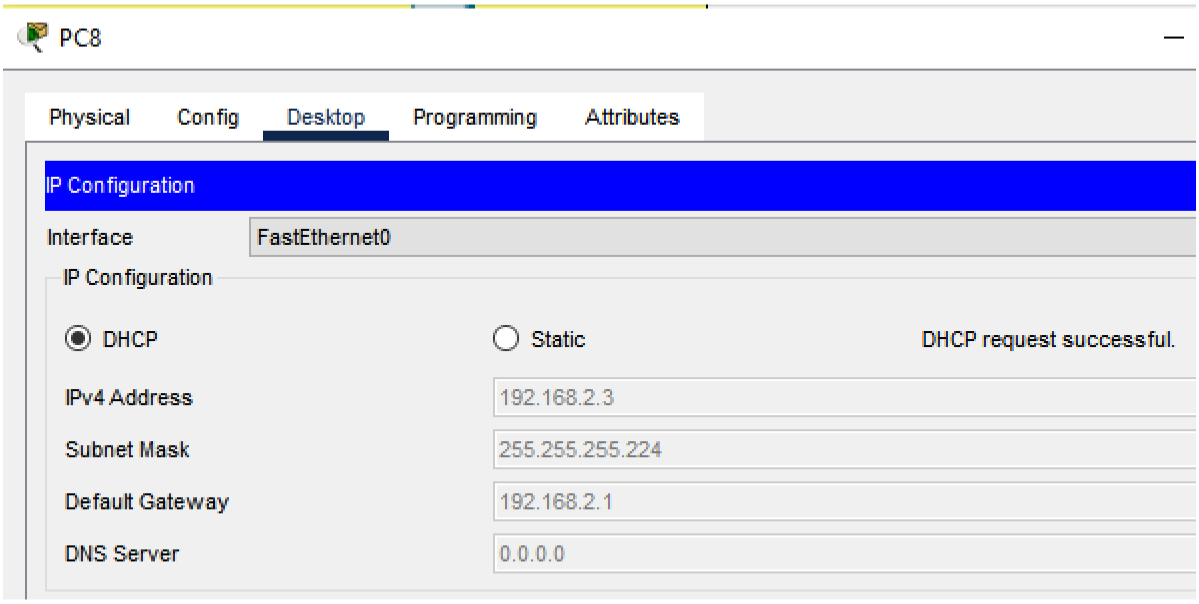
● DHCP ○ Static DHCP request successful.

IPv4 Address 192.168.1.3

Subnet Mask 255.255.255.224

Default Gateway 192.168.1.1

DNS Server 0.0.0.0



IP Configuration

Interface FastEthernet0

IP Configuration

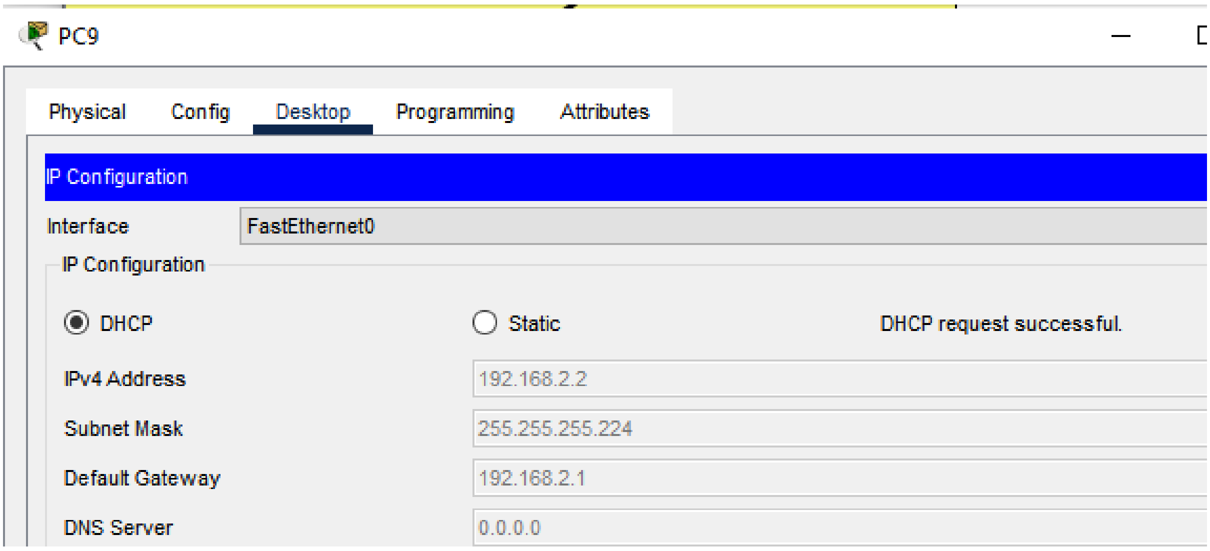
● DHCP ○ Static DHCP request successful.

IPv4 Address 192.168.2.3

Subnet Mask 255.255.255.224

Default Gateway 192.168.2.1

DNS Server 0.0.0.0



IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address 192.168.2.2

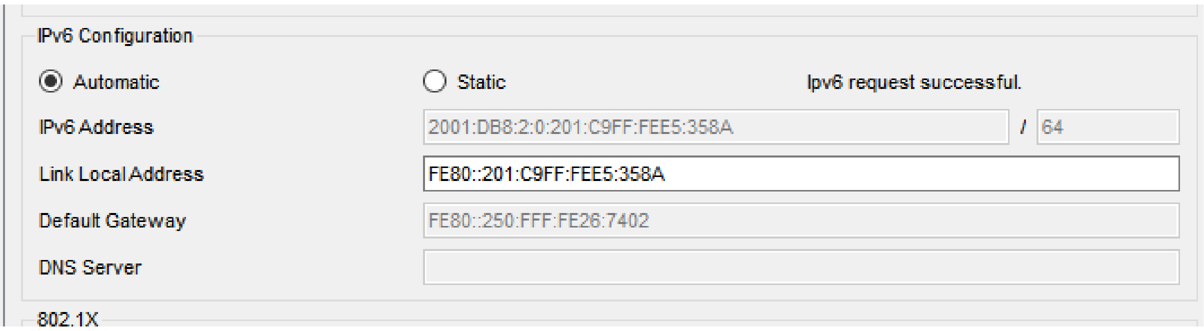
Subnet Mask 255.255.255.224

Default Gateway 192.168.2.1

DNS Server 0.0.0.0

For IPv6 configuration, I enabled IPv6 on both the Cork and Galway routers. Each router was assigned a unique IPv6, 2001:db8:1::/64 for Cork and 2001:db8:2::/64 for Galway. I configured the LAN interfaces (Gig0/1) on both routers with the addresses 2001:db8:1::1/64 for Cork and 2001:db8:2::1/64 for Galway and enabled IPv6 with the ipv6 enable command. On the PCs in each branch, I selected 'Automatic" in the IPv6 configuration settings to allow devices to use SLAAC. This allows both branches to support IPv6 communication, providing scalability.

Here is a screenshot of PC8 being able to receive and IPv6 address.



IPv6 Configuration

● Automatic ○ Static Ipv6 request successful.

IPv6 Address 2001:DB8:2:0:201:C9FF:FEE5:358A / 64

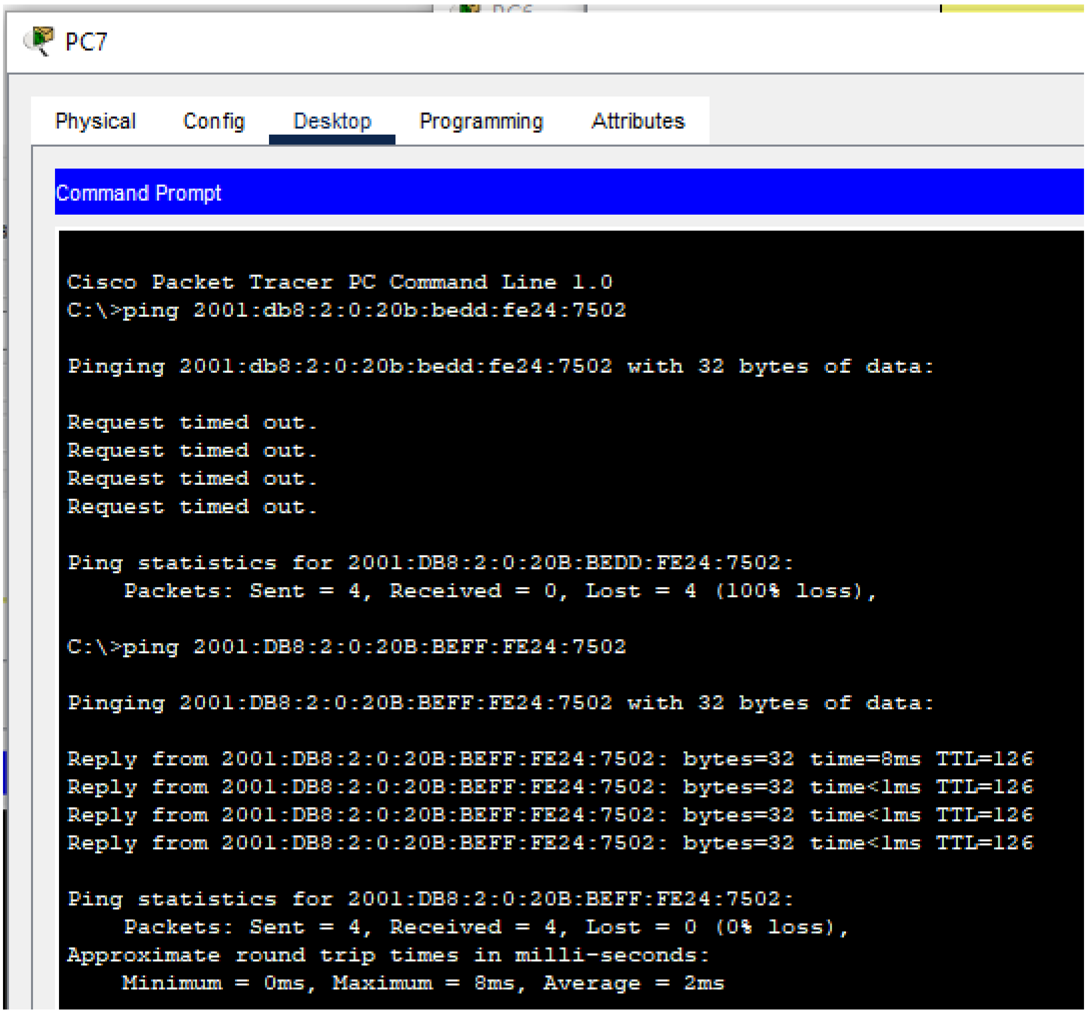
Link Local Address FE80::201:C9FF:FEE5:358A

Default Gateway FE80::250:FFF:FE26:7402

DNS Server

802.1X

And here is a screenshot of PC7 (Cork) being able to ping PC9 (Galway)

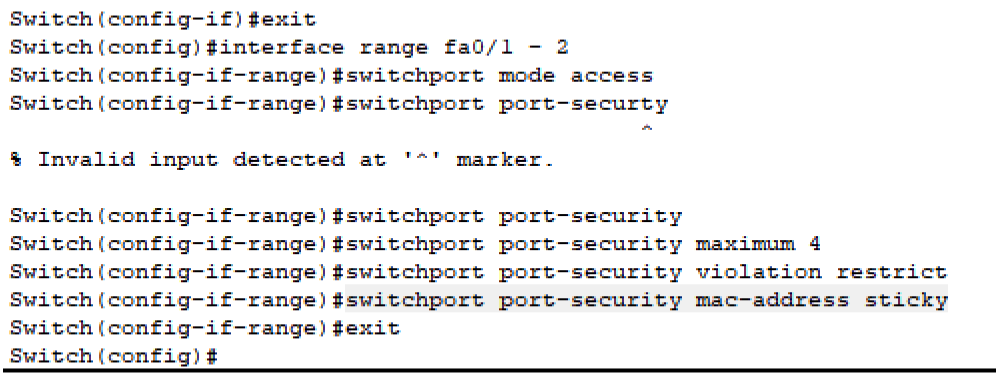


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:2:0:20b:bedd:fe24:7502

Pinging 2001:db8:2:0:20b:bedd:fe24:7502 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:2:0:20B:BEDD:FE24:7502:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 2001:DB8:2:0:20B:BEFF:FE24:7502

Pinging 2001:DB8:2:0:20B:BEFF:FE24:7502 with 32 bytes of data:

Reply from 2001:DB8:2:0:20B:BEFF:FE24:7502: bytes=32 time=8ms TTL=126
Reply from 2001:DB8:2:0:20B:BEFF:FE24:7502: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:2:0:20B:BEFF:FE24:7502: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:2:0:20B:BEFF:FE24:7502: bytes=32 time<1ms TTL=126

Ping statistics for 2001:DB8:2:0:20B:BEFF:FE24:7502:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

Requirement 3:

To prevent MAC table flooding attacks at the main office, port security was configured on all switches ports connected to the PCs. The maximum number of MAC addresses allowed per port was set to 4, ensuring that only 4 devices can be connected to each port. This prevents attackers from connecting multiple unauthorized devices or flooding the switch with fake MAC addresses to force it into flooding traffic across all ports. Additionally, the “sticky” MAC option was enabled so the switch learns and remembers the first connected device automatically, and the violation mode was set to “restrict” to block unauthorized devices without shutting down the port.

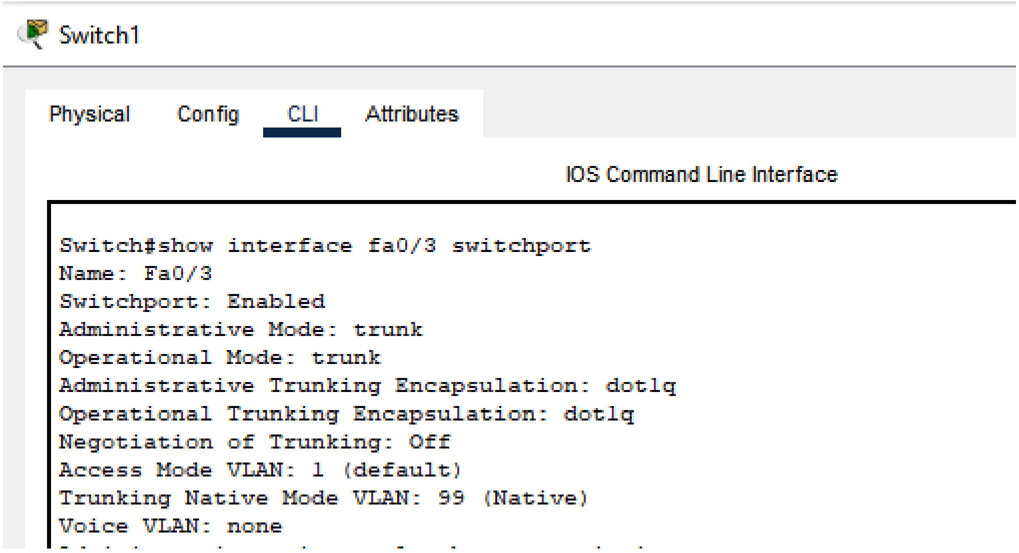
Here is a screenshot of Switch0



```
Switch(config-if)#exit
Switch(config)#interface range fa0/1 - 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-securty
                                             ^
% Invalid input detected at '^' marker.

Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 4
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#exit
Switch(config)#
```

To protect the network against VLAN hopping attacks, trunk ports between the MLS and layer 2 switched were configured with a native VLAN 99, which is not used for any active traffic. The switchport nonegotiate command was applied on all trunk interfaces to disable DTP (Dynamic Trunking Protocol). Access ports were set to access mode and assigned to the appropriate VLANs. These measures mitigate the risk of VLAN hopping within the network.

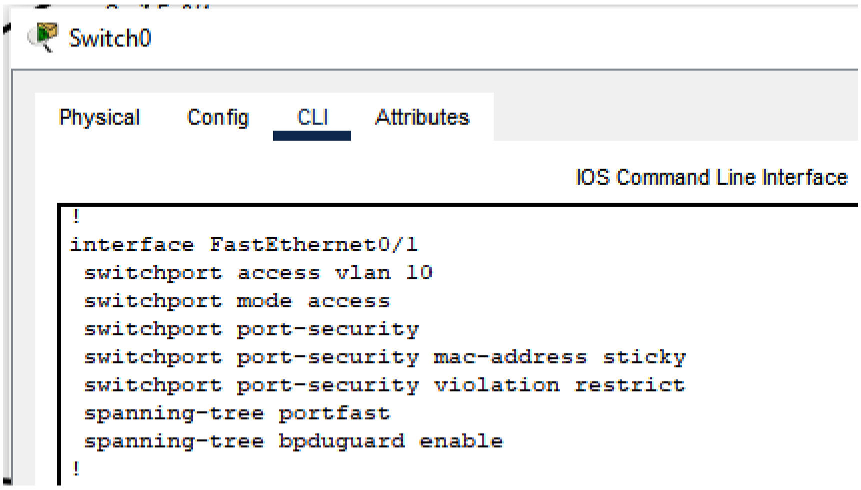
Here is a screenshot of Switch1 that shows it's in VLAN 99 and it's in trunk mode



```
Switch#show interface fa0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Native)
Voice VLAN: none
```

To protect the network against STP attacks, BPDU Guard was enabled on all access ports on the switches at the main office. This security feature prevents rogue switches from injecting malicious BPDUs into the network, which could cause traffic disruptions. With BPDU Guard enabled, any access port receiving an unexpected BPDU will automatically shut down.

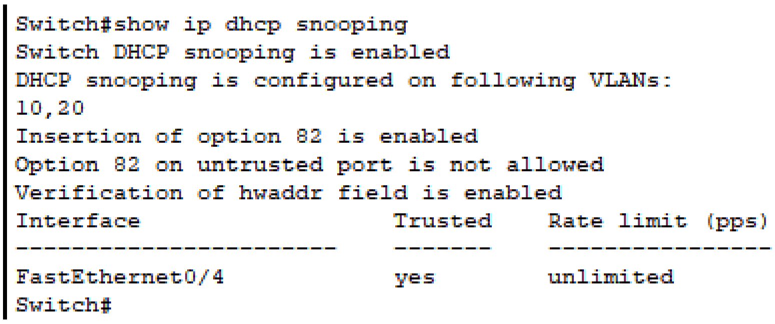
Here is a screenshot of Switch0, showing that BPDU was enabled.



```
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

To protect the network against DHCP attacks such as starvation and rogue server responses, DHCP snooping was implemented on all the switches. DHCP snooping was enabled globally and limited to VLANs 10 and 20. All the other ports remained untrusted by default, while only the ports going up to the MLS were configured as trusted using the ip dhcp snooping trust command. This ensures that only legitimate DHCP server at the MLS can issue IP addresses, while any unauthorized DHCP offers or acknowledgements from other devices are blocked. This configuration mitigates DHCP attacks on the network.

Here is a screenshot of Switch2 to show that DHCP snooping was configured



```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    --------   ----------------
FastEthernet0/4            yes        unlimited
Switch#
```

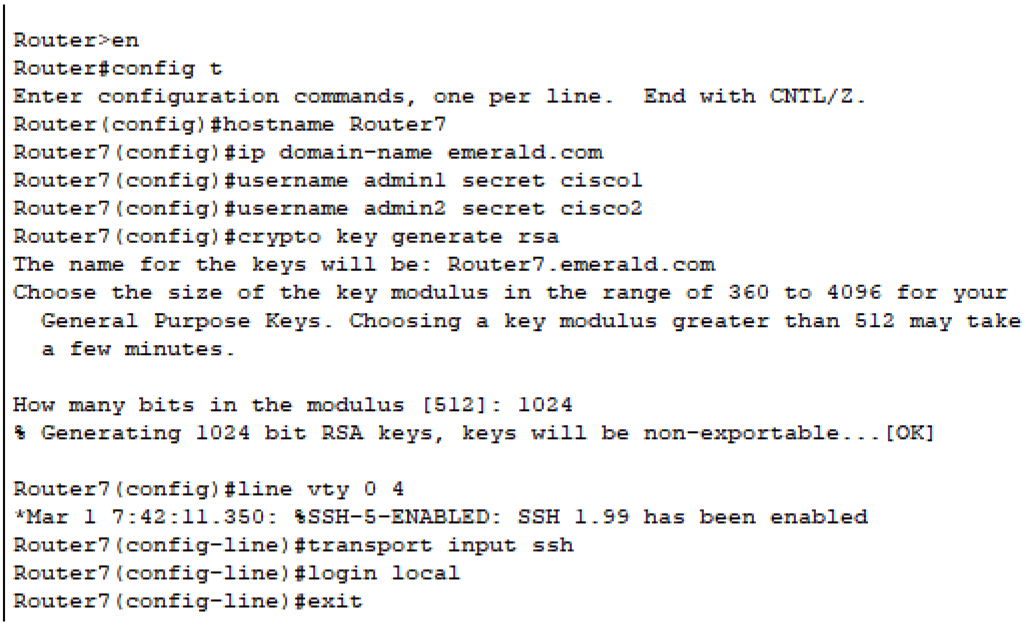
DAI was implemented on the network to protect against ARP spoofing, a common technique used by attackers to manipulate network traffic. By enabling DAI on VLANs 10 and 20, the switch monitors and verifies ARP messages against DHCP snooping. The ports going up to the MLS were marked as trusted, while all other ports were left untrusted to block any unauthorized ARP replied.

I also shut down unused ports on the switches and the MLS, and also assigned passwords. This would also be done on the switches on the branches.

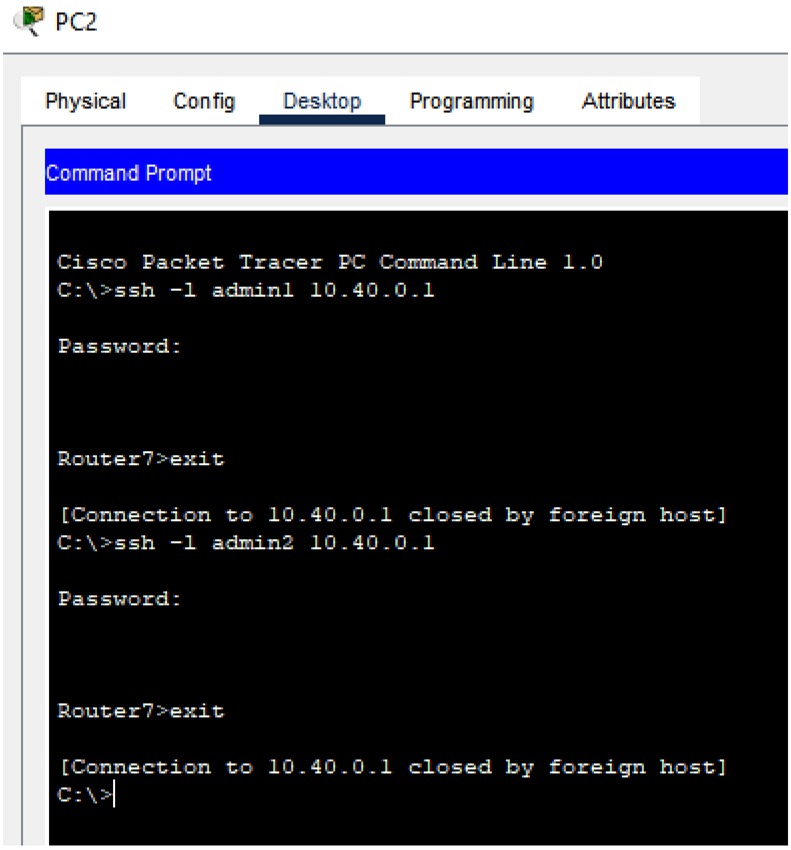
Requirement 4:

To secure remote administrative access to the headquarters' edge router (Router7), SSH was configured using local authentication. A domain name and crypto key were generated to enable SSH functionality, and two user accounts were created **admin1** with the password **cisco1** and **admin2** with the password **cisco2**. The router's vty lines were setup to accept

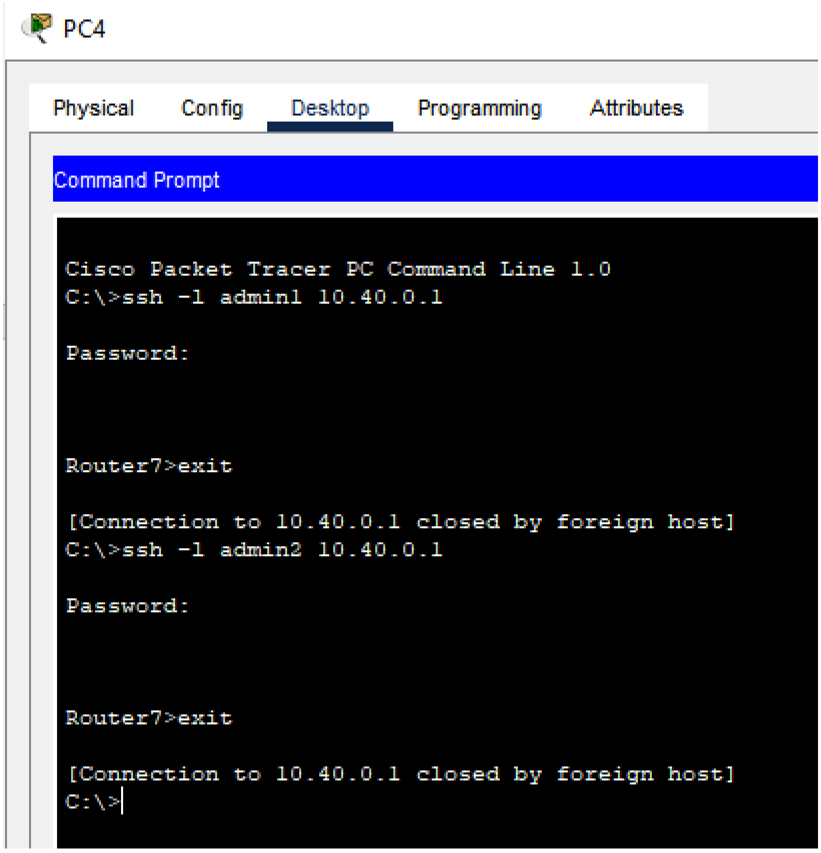
SSH input only, ensuring encrypted connections. The IP address of the router interface was used to establish successful SSH connections from the PCs, confirming secure remote management.



```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router7
Router7(config)#ip domain-name emerald.com
Router7(config)#username admin1 secret cisco1
Router7(config)#username admin2 secret cisco2
Router7(config)#crypto key generate rsa
The name for the keys will be: Router7.emerald.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router7(config)#line vty 0 4
*Mar 1 7:42:11.350: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router7(config-line)#transport input ssh
Router7(config-line)#login local
Router7(config-line)#exit
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin1 10.40.0.1

Password:



Router7>exit

[Connection to 10.40.0.1 closed by foreign host]
C:\>ssh -l admin2 10.40.0.1

Password:



Router7>exit

[Connection to 10.40.0.1 closed by foreign host]
C:\>
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin1 10.40.0.1

Password:



Router7>exit

[Connection to 10.40.0.1 closed by foreign host]
C:\>ssh -l admin2 10.40.0.1

Password:



Router7>exit

[Connection to 10.40.0.1 closed by foreign host]
C:\>
```

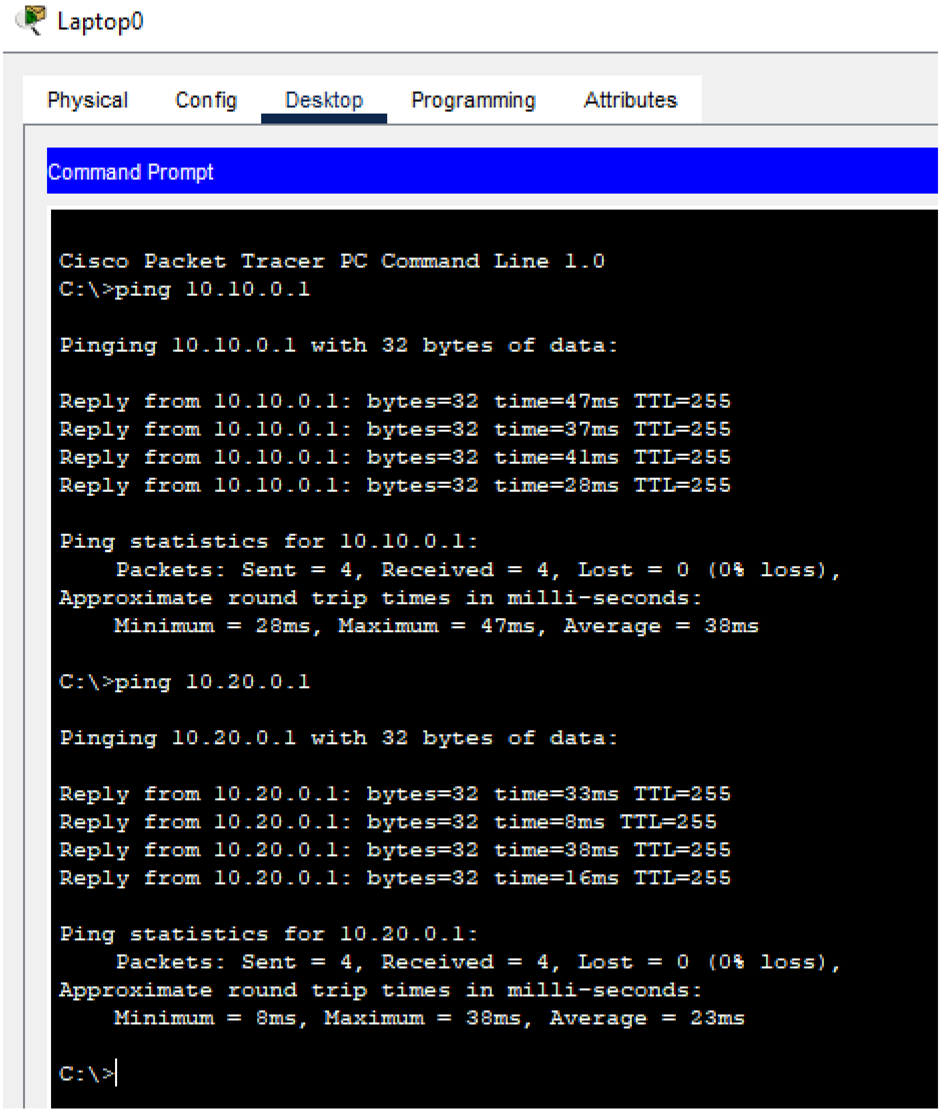
Requirement 6:

I also implemented floating static routes in my network, I configured two static routes to the same destination network, with different administrative distances to prioritize the primary paths. For example on Router 8 I created a primary static route to reach the 192.168.2.0/27 network (Galway) via the next hop IP 10.40.0.1 (Router7) which use the default administrative distance of 1. Then I configured a floating static route to the same destination network via 10.50.0.2 (Router9) but assigned it an administrative distance of 5, making it less preferred. This ensures the backup route will only be used if the primary path becomes unavailable.

Requirement 7:

To fulfill requirement 7, a basic wireless network was configured at the headquarters. An access point was configured with the SSID “EmeraldHQ-WiFi”, utilizing WPA2-PSK encryption with AES for secure wireless access. The wireless client was manually assigned an IP address from the 192.168.50.0/24 subnet, with a default gateway of 192.168.50.1. A new VLAN (VLAN 30) was created on the MLS to support wireless connectivity. Static routing was also added to enable wireless clients to have access to external networks. Wireless security was enhanced by disabling SSID broadcast.

Here is a screenshot of the laptop being able to ping the VLANs 10 and 20



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.0.1

Pinging 10.10.0.1 with 32 bytes of data:

Reply from 10.10.0.1: bytes=32 time=47ms TTL=255
Reply from 10.10.0.1: bytes=32 time=37ms TTL=255
Reply from 10.10.0.1: bytes=32 time=41ms TTL=255
Reply from 10.10.0.1: bytes=32 time=28ms TTL=255

Ping statistics for 10.10.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 47ms, Average = 38ms

C:\>ping 10.20.0.1

Pinging 10.20.0.1 with 32 bytes of data:

Reply from 10.20.0.1: bytes=32 time=33ms TTL=255
Reply from 10.20.0.1: bytes=32 time=8ms TTL=255
Reply from 10.20.0.1: bytes=32 time=38ms TTL=255
Reply from 10.20.0.1: bytes=32 time=16ms TTL=255

Ping statistics for 10.20.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 38ms, Average = 23ms

C:\>
```