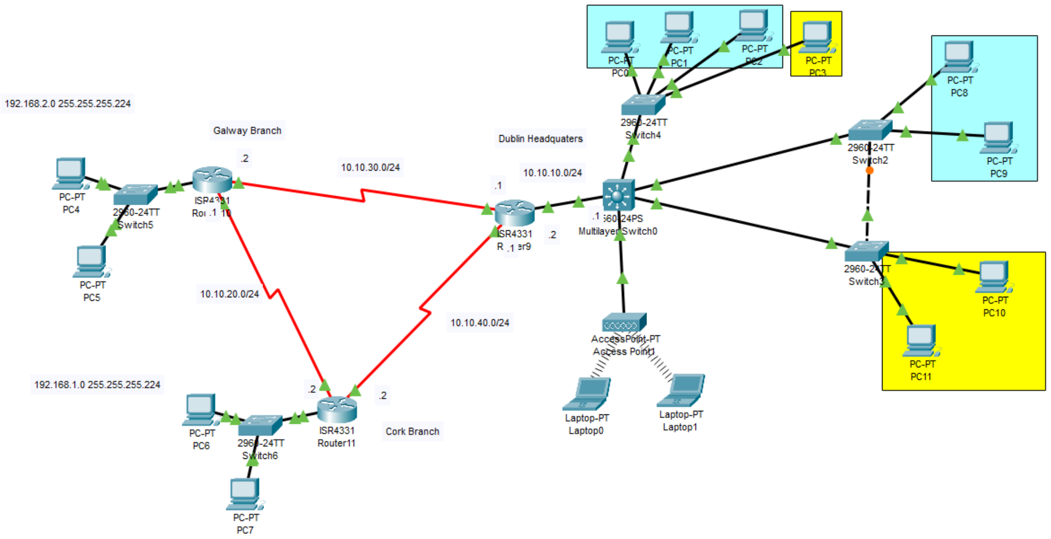
Emerald Retail Ltd

Prototype Company Internetwork Design



Adam Romanowicz

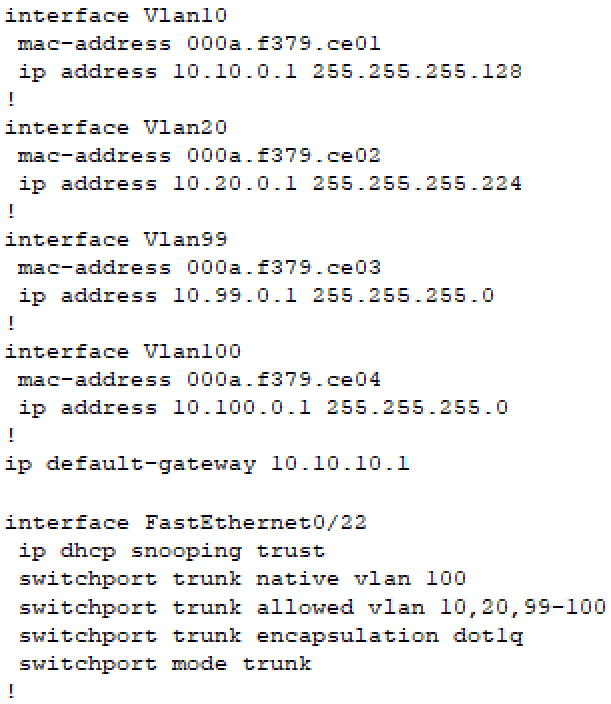
C00297492

IT Management

Requirement 1:

Inter-vlan communication is achieved through the Headquarter’s multi-layer switch using its SVIs which are the default gateway of each vlan. Vlan 10 can accommodate 126 hosts due to its /25 subnet mask however .1-.9 are reserved for future use. Vlan 20 can accommodate 30 hosts due to its /27 subnet mask with .1-.9 also reserved. These vlans are for operations staff and governance management respectively with these end users scattered across the headquarters. Manual configurated trunklines are included allowing both vlans to communicate with each other and a native vlan which is configured to vlan 100 for additional security while allowing untagged traffic to communicate with the network. Inter-departmental communication is also possible via the default-gateway on the MLS which sends traffic to the end router on the HQ.

MLS



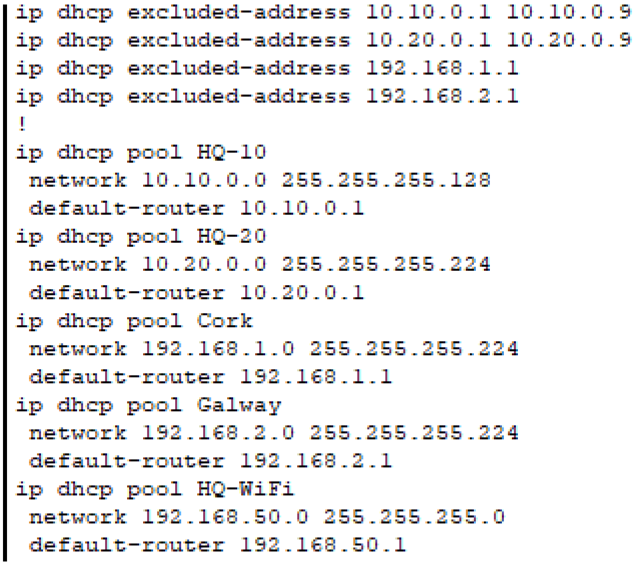
```
interface Vlan10
 mac-address 000a.f379.ce01
 ip address 10.10.0.1 255.255.255.128
!
interface Vlan20
 mac-address 000a.f379.ce02
 ip address 10.20.0.1 255.255.255.224
!
interface Vlan99
 mac-address 000a.f379.ce03
 ip address 10.99.0.1 255.255.255.0
!
interface Vlan100
 mac-address 000a.f379.ce04
 ip address 10.100.0.1 255.255.255.0
!
ip default-gateway 10.10.10.1

interface FastEthernet0/22
 ip dhcp snooping trust
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,99-100
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

Requirement 2:

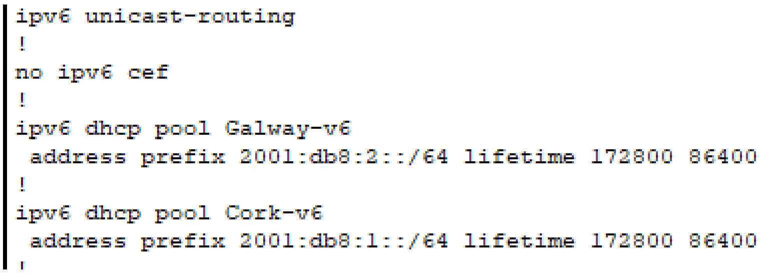
Each end user is assigned an ip dynamically using a DHCP server. IPv4 addresses are distributed from the MLS with 4 total pools set up (Operations, Governance, Cork, Galway). Cork and Galway have their default-gateway excluded from the DHCP pool to avoid assignment issues (Operations and governance is the same as explained above). Default-gateways for operations and governance are handled by the SVIs on the MLS while for Cork and Galway branches these default-gateways are set up on their respective end router. IPv6 is distributed from the HQ end router because the MLS does not support IPv6 DHCP pools however it can use IPv6 addresses. IPv6 is assigned only on routers and Cork and Galway branch end users for scalability of these offices in the future.

MLS



```
ip dhcp excluded-address 10.10.0.1 10.10.0.9
ip dhcp excluded-address 10.20.0.1 10.20.0.9
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool HQ-10
 network 10.10.0.0 255.255.255.128
 default-router 10.10.0.1
ip dhcp pool HQ-20
 network 10.20.0.0 255.255.255.224
 default-router 10.20.0.1
ip dhcp pool Cork
 network 192.168.1.0 255.255.255.224
 default-router 192.168.1.1
ip dhcp pool Galway
 network 192.168.2.0 255.255.255.224
 default-router 192.168.2.1
ip dhcp pool HQ-WiFi
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
```

HQ Router

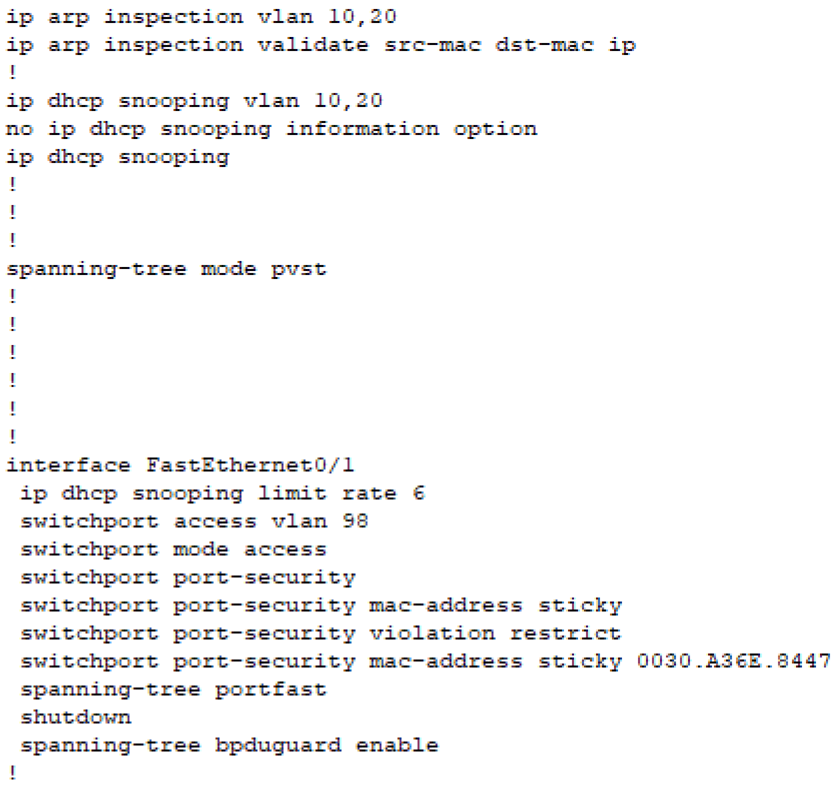


```
ipv6 unicast-routing
!
no ipv6 cef
!
ipv6 dhcp pool Galway-v6
 address prefix 2001:db8:2::/64 lifetime 172800 86400
!
ipv6 dhcp pool Cork-v6
 address prefix 2001:db8:1::/64 lifetime 172800 86400
!
```

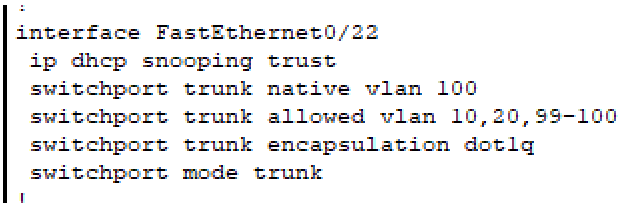
Requirement 3:

Headquarters security is of utmost importance therefore multiple layer 2 measures have been implemented to tackle this requirement. To prevent MAC table attacks port-security on every access port has been configured which includes a limit of 1 mac address per port with sticky dynamic configuration, the violation is set to restrict meaning the port does not shutdown upon unauthorized port use but it does log the record and alert administrators. All unused ports are set to a Void vlan that cannot travel across trunklines and are shutdown. These measures should make it harder for rogue agents to spam the mac table using macof. Vlan attacks are prevented by changing the native vlan to 100 (changing it from default) and ensuring the trunklines only allow verified vlan traffic to pass through; autotrunking is also turned off with every trunkline statically configured along with each access port having trunking turned off. STP attacks are prevented by using a combination of portfast and bpduguard; portfast disables access ports from being in the root switch election process and are always enabled while bpduguard prevents bpdu frames from entering these same access ports (disables the port if a bpdu frame enters). This ensures the topology of the network remains stable and not changed by rogue agents. DHCP attacks are mitigated via dhcp snooping global config which is set to check all dhcp frames on vlans 10 and 20; most ports are set to untrusted which block dhcp frames from entering with the trusted ports being configured on each port leaving the MLS and the ingress port of another switch coming from the MLS; each untrusted port also has a limiter of 6 dhcp frames. ARP spoofing attacks are prevented in a similar fashion as dhcp spoofing with all uplink ports to the default gateway being trusted; arp snooping checks the source mac, destination mac and the ip of frames.

MLS

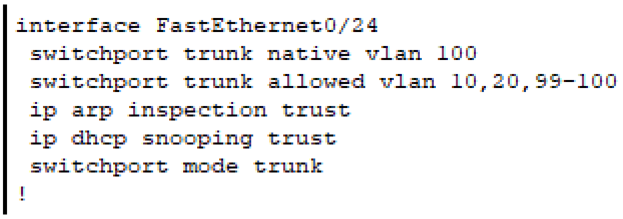


```
ip arp inspection vlan 10,20
ip arp inspection validate src-mac dst-mac ip
!
ip dhcp snooping vlan 10,20
no ip dhcp snooping information option
ip dhcp snooping
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/1
 ip dhcp snooping limit rate 6
 switchport access vlan 98
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0030.A36E.8447
 spanning-tree portfast
 shutdown
 spanning-tree bpduguard enable
!
```

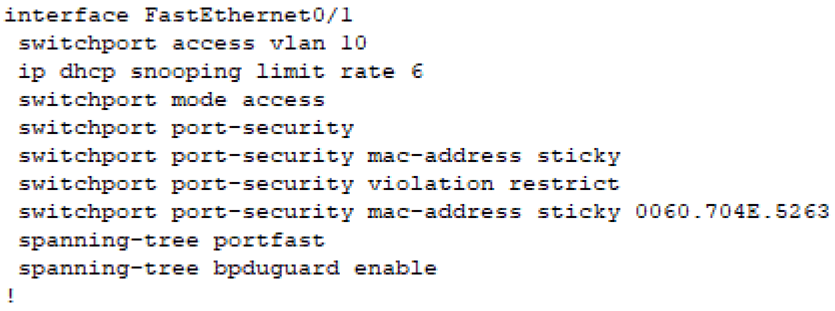


```
interface FastEthernet0/22
 ip dhcp snooping trust
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,99-100
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

HQ top-right switch



```
interface FastEthernet0/24
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,99-100
 ip arp inspection trust
 ip dhcp snooping trust
 switchport mode trunk
!
```

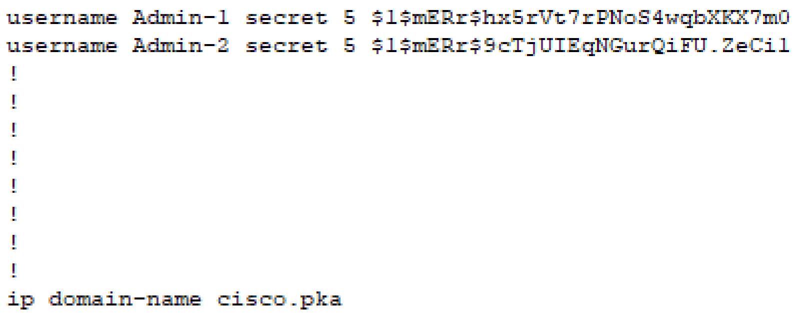


```
interface FastEthernet0/1
 switchport access vlan 10
 ip dhcp snooping limit rate 6
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.704E.5263
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

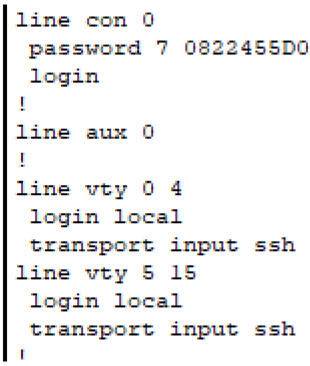
Requirement 4:

The headquarter's edge router is accessible via SSH and has 2 network administrator accounts set up and telnet disabled for additional hardening. Authentication is done locally however in later phases of the prototype this should be updated to having a authentication server using AAA for stronger security. Passwords are encrypted via service password-encryption and SSH traffic is encrypted via RSA. SSH management traffic is distributed on the management vlan 99 which is handled on the SVI in the MLS for further SSH scalability.

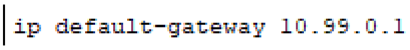
HQ Router



```
username Admin-1 secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username Admin-2 secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
!
!
!
ip domain-name cisco.pka
```

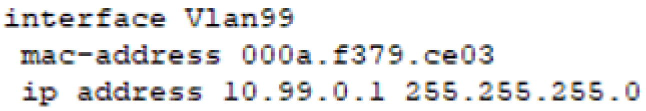


```
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
```



```
ip default-gateway 10.99.0.1
```

MLS

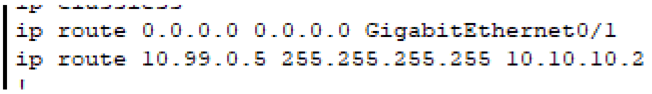


```
interface Vlan99
 mac-address 000a.f379.ce03
 ip address 10.99.0.1 255.255.255.0
```

Requirement 5:

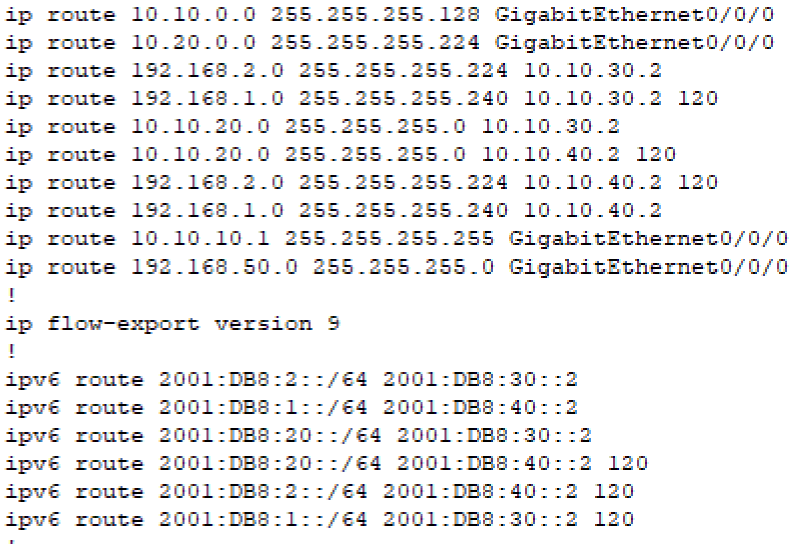
Inter-office communication is achieved via static routes set up on each router. The MLS is in a stub network configuration therefore it has a default route to its edge router. Each router then has a static route to its adjacent office via its shortest route and also a floating static route via its longer route (this is done for redundancy and availability); static and floating routes are also set up for each network between routers in case traffic is for the router rather than an end user. Static routes are also configured from the branch offices to the vlans within the HQ. Additionally, host routes are included which specifies the DHCP server. IPv6 routes are also included which are set up in a similar way excluding the HQ because this prototype does not include IPv6 addresses in the HQ networks.

MLS



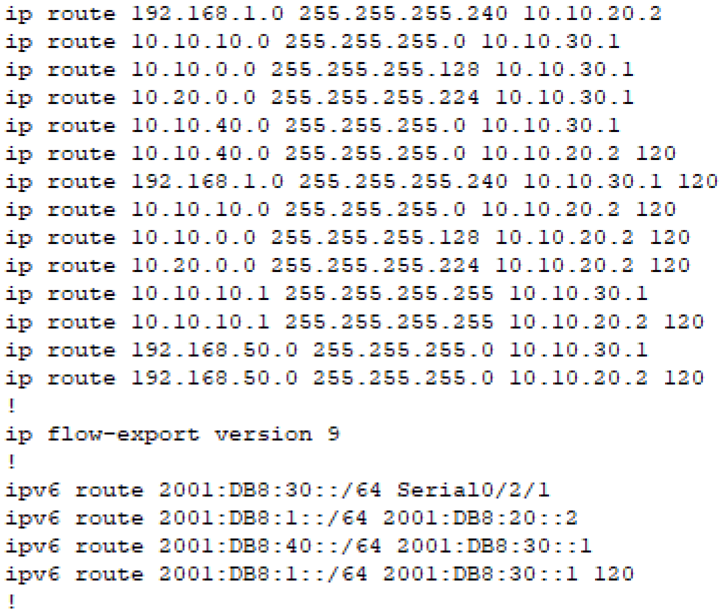
```
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
ip route 10.99.0.5 255.255.255.255 10.10.10.2
!
```

HQ Router



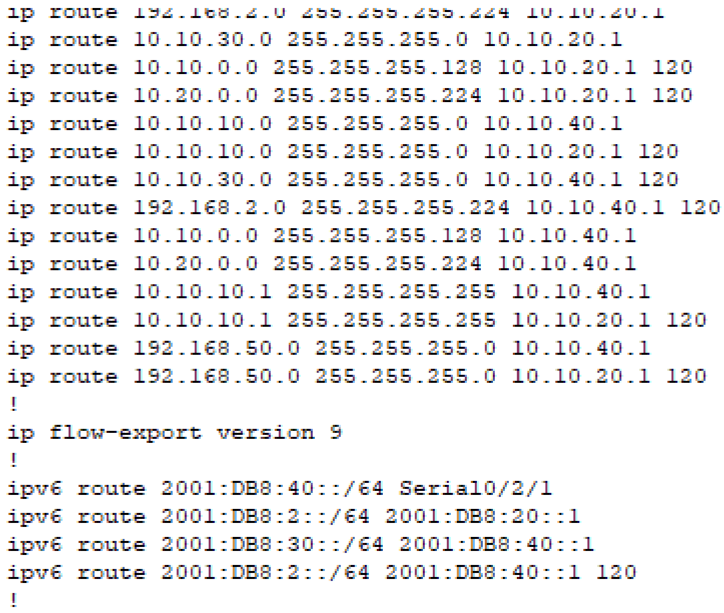
```
ip route 10.10.0.0 255.255.255.128 GigabitEthernet0/0/0
ip route 10.20.0.0 255.255.255.224 GigabitEthernet0/0/0
ip route 192.168.2.0 255.255.255.224 10.10.30.2
ip route 192.168.1.0 255.255.255.240 10.10.30.2 120
ip route 10.10.20.0 255.255.255.0 10.10.30.2
ip route 10.10.20.0 255.255.255.0 10.10.40.2 120
ip route 192.168.2.0 255.255.255.224 10.10.40.2 120
ip route 192.168.1.0 255.255.255.240 10.10.40.2
ip route 10.10.10.1 255.255.255.255 GigabitEthernet0/0/0
ip route 192.168.50.0 255.255.255.0 GigabitEthernet0/0/0
!
ip flow-export version 9
!
ipv6 route 2001:DB8:2::/64 2001:DB8:30::2
ipv6 route 2001:DB8:1::/64 2001:DB8:40::2
ipv6 route 2001:DB8:20::/64 2001:DB8:30::2
ipv6 route 2001:DB8:20::/64 2001:DB8:40::2 120
ipv6 route 2001:DB8:2::/64 2001:DB8:40::2 120
ipv6 route 2001:DB8:1::/64 2001:DB8:30::2 120
!
```

Galway Router



```
ip route 192.168.1.0 255.255.255.240 10.10.20.2
ip route 10.10.10.0 255.255.255.0 10.10.30.1
ip route 10.10.0.0 255.255.255.128 10.10.30.1
ip route 10.20.0.0 255.255.255.224 10.10.30.1
ip route 10.10.40.0 255.255.255.0 10.10.30.1
ip route 10.10.40.0 255.255.255.0 10.10.20.2 120
ip route 192.168.1.0 255.255.255.240 10.10.30.1 120
ip route 10.10.10.0 255.255.255.0 10.10.20.2 120
ip route 10.10.0.0 255.255.255.128 10.10.20.2 120
ip route 10.20.0.0 255.255.255.224 10.10.20.2 120
ip route 10.10.10.1 255.255.255.255 10.10.30.1
ip route 10.10.10.1 255.255.255.255 10.10.20.2 120
ip route 192.168.50.0 255.255.255.0 10.10.30.1
ip route 192.168.50.0 255.255.255.0 10.10.20.2 120
!
ip flow-export version 9
!
ipv6 route 2001:DB8:30::/64 Serial0/2/1
ipv6 route 2001:DB8:1::/64 2001:DB8:20::2
ipv6 route 2001:DB8:40::/64 2001:DB8:30::1
ipv6 route 2001:DB8:1::/64 2001:DB8:30::1 120
!
```

Cork Router

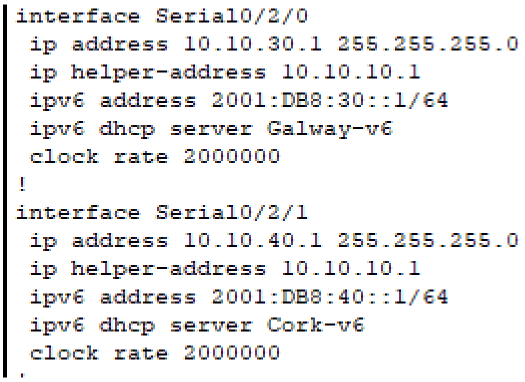


```
ip route 192.168.2.0 255.255.255.224 10.10.20.1
ip route 10.10.30.0 255.255.255.0 10.10.20.1
ip route 10.10.0.0 255.255.255.128 10.10.20.1 120
ip route 10.20.0.0 255.255.255.224 10.10.20.1 120
ip route 10.10.10.0 255.255.255.0 10.10.40.1
ip route 10.10.10.0 255.255.255.0 10.10.20.1 120
ip route 10.10.30.0 255.255.255.0 10.10.40.1 120
ip route 192.168.2.0 255.255.255.224 10.10.40.1 120
ip route 10.10.0.0 255.255.255.128 10.10.40.1
ip route 10.20.0.0 255.255.255.224 10.10.40.1
ip route 10.10.10.1 255.255.255.255 10.10.40.1
ip route 10.10.10.1 255.255.255.255 10.10.20.1 120
ip route 192.168.50.0 255.255.255.0 10.10.40.1
ip route 192.168.50.0 255.255.255.0 10.10.20.1 120
!
ip flow-export version 9
!
ipv6 route 2001:DB8:40::/64 Serial0/2/1
ipv6 route 2001:DB8:2::/64 2001:DB8:20::1
ipv6 route 2001:DB8:30::/64 2001:DB8:40::1
ipv6 route 2001:DB8:2::/64 2001:DB8:40::1 120
!
```

Requirement 6:

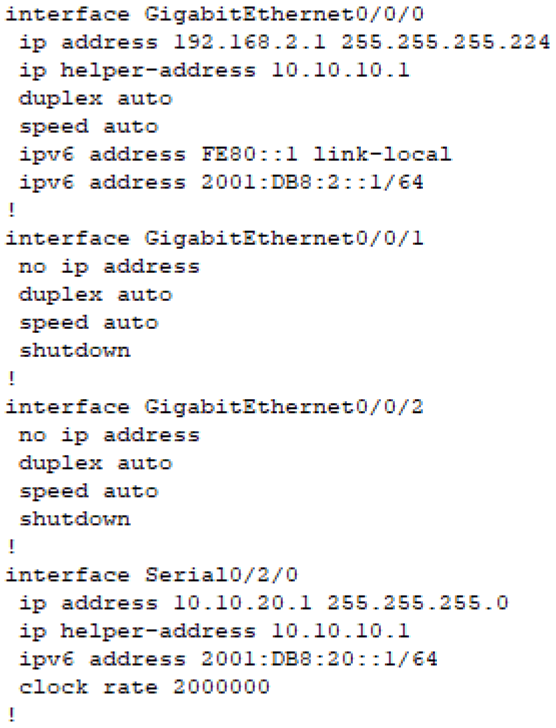
As stated above each branch office is assigned IPv4 address from the HQ MLS with 30 available addresses due to its /27 subnet mask. Cork is assigned 192.168.1.0 addresses while Galway is assigned 192.168.2.0 addresses. To reach the DHCP server helper addresses are configured on ports receiving client dhcp frames and this helper address is then reached via the host routes set up in the previous requirement. IPv6 is assigned from the HQ router DHCP pool interfaces that point towards that network and does not require helper/relay addresses because IPv6 uses neighbour discovery to locate the DHCP pool. The pool also does not specify the default gateway as IPv6 uses link local addresses as its default gateway.

HQ Router



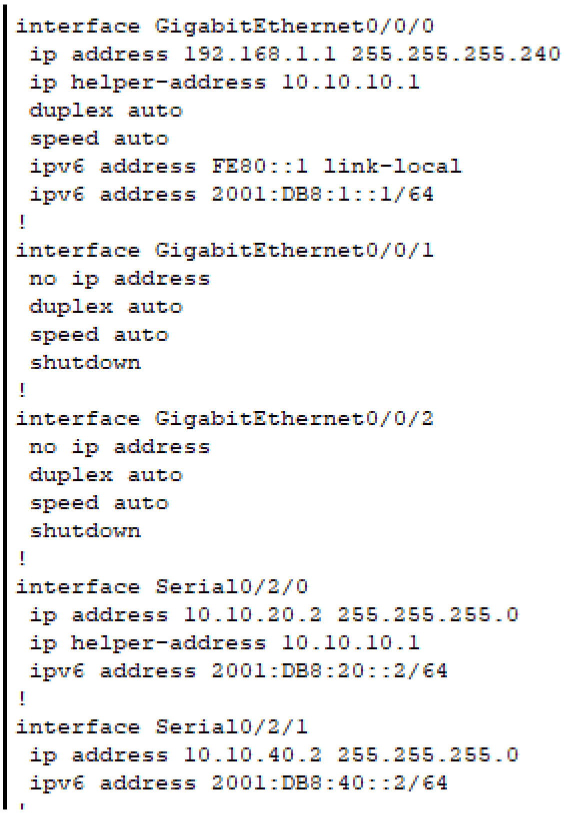
```
interface Serial0/2/0
 ip address 10.10.30.1 255.255.255.0
 ip helper-address 10.10.10.1
 ipv6 address 2001:DB8:30::1/64
 ipv6 dhcp server Galway-v6
 clock rate 2000000
!
interface Serial0/2/1
 ip address 10.10.40.1 255.255.255.0
 ip helper-address 10.10.10.1
 ipv6 address 2001:DB8:40::1/64
 ipv6 dhcp server Cork-v6
 clock rate 2000000
```

Galway Router



```
interface GigabitEthernet0/0/0
 ip address 192.168.2.1 255.255.255.224
 ip helper-address 10.10.10.1
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:2::1/64
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/2/0
 ip address 10.10.20.1 255.255.255.0
 ip helper-address 10.10.10.1
 ipv6 address 2001:DB8:20::1/64
 clock rate 2000000
!
```

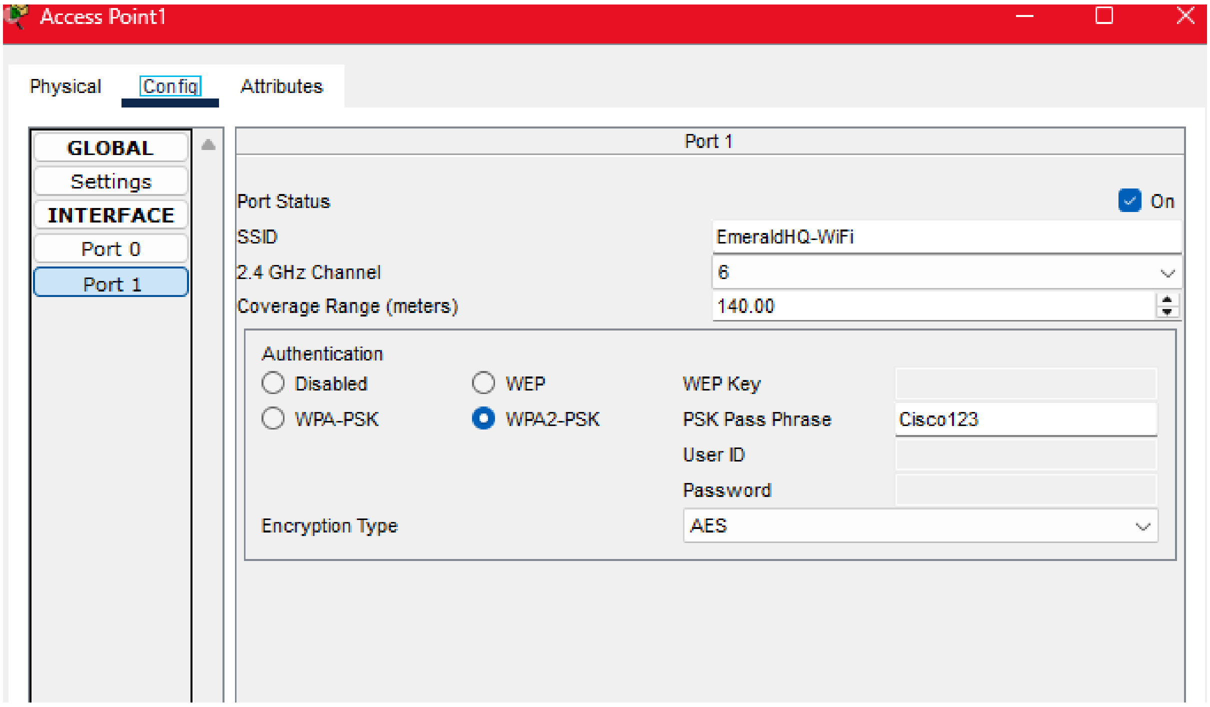
Cork Router



```
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.240
 ip helper-address 10.10.10.1
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:1::1/64
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/2/0
 ip address 10.10.20.2 255.255.255.0
 ip helper-address 10.10.10.1
 ipv6 address 2001:DB8:20::2/64
!
interface Serial0/2/1
 ip address 10.10.40.2 255.255.255.0
 ipv6 address 2001:DB8:40::2/64
!
```

Requirement 7:

A basic wireless network is included in this prototype which has been configured with WPA2 Enterprise security and a DHCP pool specifically for wireless clients has been set up on the MLS with the network 192.168.50.0/24. These clients can also access both vlans on the HQ network as well as communicating across branch offices. WPA3 is not supported by the access points available on Cisco Packet Tracer but should be used in real life application of this prototype as it is the most secure encryption method for WiFi at this moment. Disabling SSID broadcasting makes the network less accessible while providing little security therefore it is not included. Mac filtering is a “bandaid” solution for security and can easily be bypassed using mac spoofing tools and is also not included. Login passphrase is currently done locally but a AAA radius server should be considered. Default-gateway is on the MLS coming from the access point therefore considered its own network.



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 dhcp pool HQ-WiFi
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
!
```