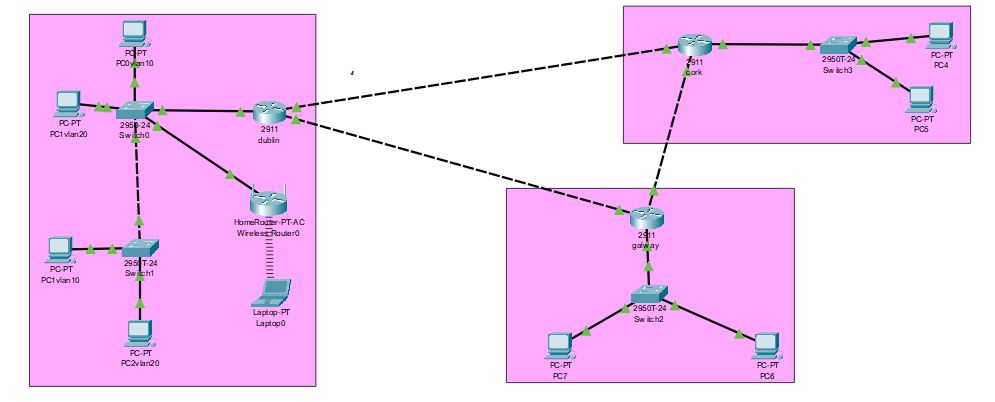
Emerald Retail



Alise Aleksane

C00296656

**Requirement 1 -Inter-Vlan routing**

Since the headquarter was going to be a router I decide to do the router on stick method as it would be easier to configure rather than a mls. This method meant that both Vlan can be configure on a one interface by using sub interface to communication with each other seamlessly.

**Requirement 2-IP**

I gave each vlan its own Ip range based on how many users were needed to be supported. I set up dhcp on the headquarter router so it could automically hand out Ip address to devices on the network. This made managing devices easier especially If more device were to be added on the network that dhcp could assign an Ip address instead of manually assigning it.

I also had to set up a range of Ip address for the Cork and Galway branch office. I did this on the headquarter router using dhcp pool. Then on the branch office I used the command Ip helper address to enable dhcp relay. This allows the branch office to receive Ip address from the headquarter dhcp pool easier. I also had to configure static routes to ensure that each router had ipv4 connection through dhcp.

Ipv6

My dhcp for ipv6 didn’t not work but I did make a dhcp pool on the headquarter router and used the address prefix length and I used ipv6 unicast routing to ensure that ipv6 Ip could make it to destination. Then I assign the ipv6 address to the port the branches offices where connect to from the headquarters. I also created ipv6 pool on the branches offices

**Requirement 3-layer 2 security**

**Mac address attacks**

On each switch in the network I shut down all unused ports to prevent unauthorized access. To prevent against mac address attacks, I enabled port security and set up a limit of 2 mac address per port. This is to prevent flooding and block out unauthorized devices. I also configured sticky mac address for port security. I chose this because it dynamically learns and saves mac address to the port which prevents unauthorized device to connect to the network overall improving security. I chose to do restrict violation over shutdown because it allows the port to remain up while dropping a packet and generates a violation log which I found was more efficient than shutdown which disable the whole port.

**Vlan attacks**

i used 802.1 encapuslation to prevent vlan hopping.

**STP attacks**

I enable port fast and bpduguard this would prevent any delays by skipping past the listen and learning phrase. On the router I enable a default port fast. While on the port that are connected to end device like the pc. I add bpduguards so if it got any bpduguards message it would shut down the port. This prevent STP attacks by improving security and reduce loop risks.

**Dhcp attacks**

I enable dhcp snooping trust to router and switch. This allow the ports to be trusted and not allow rogue dhcp server sending fake Ip that could disrupt the network. I sent the limit to be 3 before the port shutdowns. This limits the amount of fake request before shutting port down.

**Arp attacks**

I enable Arp snooping trust onto port that were trusted to all packet to pass through which helps Arp spoofing. This would allow only trusted network devices can send Arp packets while untrusted device can’t because the port will drop the packet.

**Requirement 4-SSH**

**Username =alise or admin**

**Password=cisco**

I configured ssh on the headquarter router for the ports connecting to the branch offices router. I then used the Ip address that’s I assign to those port for the ssh access. I created a domain name on the headquarter router and generated a crypto key, which I put as 2048 as it would encrypt the data that would be sent. I set the user’s name as admin and alise as I needed two user and both user passwords are cisco I config the user on line vty 0 15 this would allow 16 remote users to access. Finally, I Transport input ssh to enabled ssh traffic.

**Requirement 5-static route**

Headquarters router

I have configured two static routes to cork and Galway



The Ip route is the network address address where it trying to get to the router then is the subnet mask and finally the next hop.

I did the same with the cork and Galway branch office but use the default router

And then the next hop

**Requirement 6-ip dhcp server**

I excluded address for each dhcp pool to reserve Ip address for each network so there wouldn’t be any collisions.

**Requirement 7-wireless**

I assign a range of Ip to the wireless client in the WAP. I change the default name to the SSID EmeraldHQ-Wifi and set up the secure access and I enable mac filtering. Sadly, I couldn’t figure out why it intervlan routing for the wireless device

**Additionally**

I added password to all the switches and router using class and then cisco and added a banner. Authorized user Access