

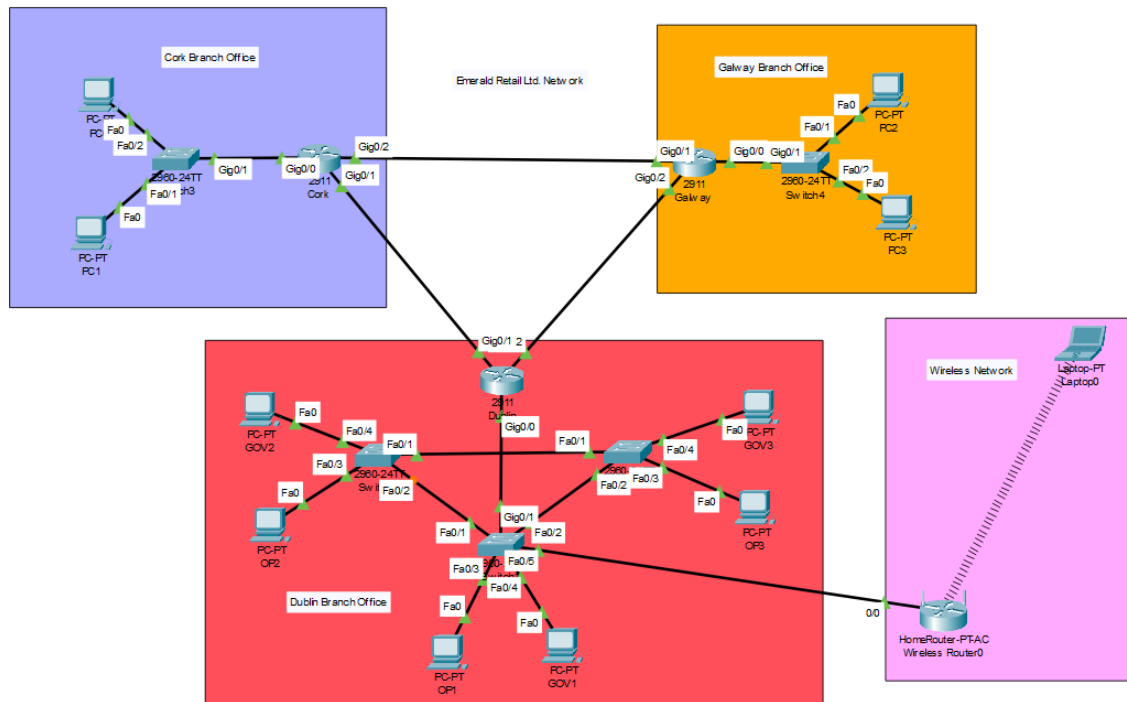
Emerald Retail Ltd.

Network Overview

The network will be designed for three main locations:

- Headquarters (Dublin): Given the larger size and more complex operations at the headquarters, I will implement more sophisticated network configurations here. This includes using VLANs for traffic segmentation and ensuring secure, high-performance inter-office communication.
- Branch Offices (Cork and Galway): The branch offices will have simpler network configurations, each with its own IP address range and dynamic IP allocation managed by the headquarters' DHCP server.

The main goal is to ensure that all locations can communicate with each other effectively while maintaining a high level of security and expansion for future needs.



Img1.1 – Network Overview

VLAN Configuration (Headquarters)

At the headquarters in Dublin, two VLANs are set up to segregate network traffic and improve both performance and security. These VLANs allow departments to work efficiently while ensuring sensitive data remains secure.

- Operations VLAN (VLAN 10):

- IP Range: 10.10.0.0/25

- Governance VLAN (VLAN 20):

- IP Range: 10.20.0.0/27

Communication Between VLANs: The two VLANs at the headquarters need to communicate with each other to ensure smooth collaboration. This is achieved through inter-VLAN routing, which is set up on the headquarters' router.

IP Addressing for Branch Offices

Each branch office (Cork and Galway) has its own IPv4 address range, with enough addresses for at least 30 devices. These addresses are dynamically assigned by the DHCP server located at the headquarters.

- Cork Branch:

- IPv4 Network: 192.168.1.0/27 (192.168.1.1 – 192.168.1.30)

- Galway Branch:

- IPv4 Network: 192.168.2.0/27 (192.168.2.1 – 192.168.2.30)

To future-proof the network, each branch also has its own unique IPv6 prefix:

- Cork Branch IPv6: 2001:db8:1::/64

- Galway Branch IPv6: 2001:db8:2::/64

The IPv6 addresses are dynamically assigned using DHCPv6.

Layer 2 Security Measures (Headquarters)

To protect the headquarters' network from potential vulnerabilities, several key security features will be implemented:

- Port-Security : To prevent attackers from overwhelming the switch's MAC table, limiting the number of MAC addresses allowed per port.
- 802.1Q Encapsulation : I configured 802.1Q VLAN tagging properly and use private VLANs to guard against VLAN hopping and double-tagging attacks.
- STP Protection: Root Guard and BPDU Guard will be used to prevent malicious Spanning Tree Protocol (STP) attacks, ensuring that the network topology remains stable and free from malicious disruptions.
- DHCP Snooping: To protect against rogue DHCP servers and DHCP starvation attacks.
- ARP Inspection: to prevent ARP spoofing, where attackers impersonate devices to intercept traffic.

Remote Access to Headquarters Edge Router

For secure remote management, network administrators will be able to access the headquarters' edge router using SSH (Secure Shell) with local authentication. This ensures that only authorized personnel can manage the router remotely, keeping the network secure.

Static Routing for Branch Office Communication

Because the headquarters and branch offices are on separate routers, static routes were configured to enable communication between them:

- Headquarters to Cork: Static route to the 192.168.1.0/27 network.
- Headquarters to Galway: Static route to the 192.168.2.0/27 network.
- Cork to Galway: Static route to the 192.168.2.0/27 network.
- Galway to Cork: Static route to the 192.168.1.0/27 network.

These static routes will ensure smooth communication between all locations.

Wireless Network Configuration (Headquarters)

To support mobile devices at the headquarters, a wireless network was set up with the following features:

- SSID: EmeraldHQ-WiFi
- Encryption: WPA2-PSK encryption for secure access.
- IP Address Range for Wireless Devices: 192.168.50.0/24

Wireless Network Security:

- SSID Broadcasting: Disabled to keep the network less visible to unauthorized users.
- MAC Filtering: Enabled to allow only approved devices to connect.

Wireless clients will be able to access both the Operations and Governance VLANs, thanks to inter-VLAN routing.

Expansion Considerations

The network is designed to be adaptable to support future growth within the company:

- IP Addressing: The current address scheme offers plenty of room for additional devices and locations in the future, both in IPv4 and IPv6.
- Network Expansion: The design allows for the easy addition of new VLANs, subnets, or devices as Emerald Retail Ltd. grows.
- Routing: Static routes can be adjusted as needed to accommodate new locations or network changes.

Conclusion

The proposed network design will provide Emerald Retail Ltd. with a secure, reliable, and efficient network to meet its current and future needs. The use of VLANs at the headquarters enhances both security and performance, while dynamic IP allocation and static routing ensure easy management and connectivity between the headquarters and branch offices. Layer 2 security measures, remote access configurations, and wireless network design further ensure a robust, secure environment.