

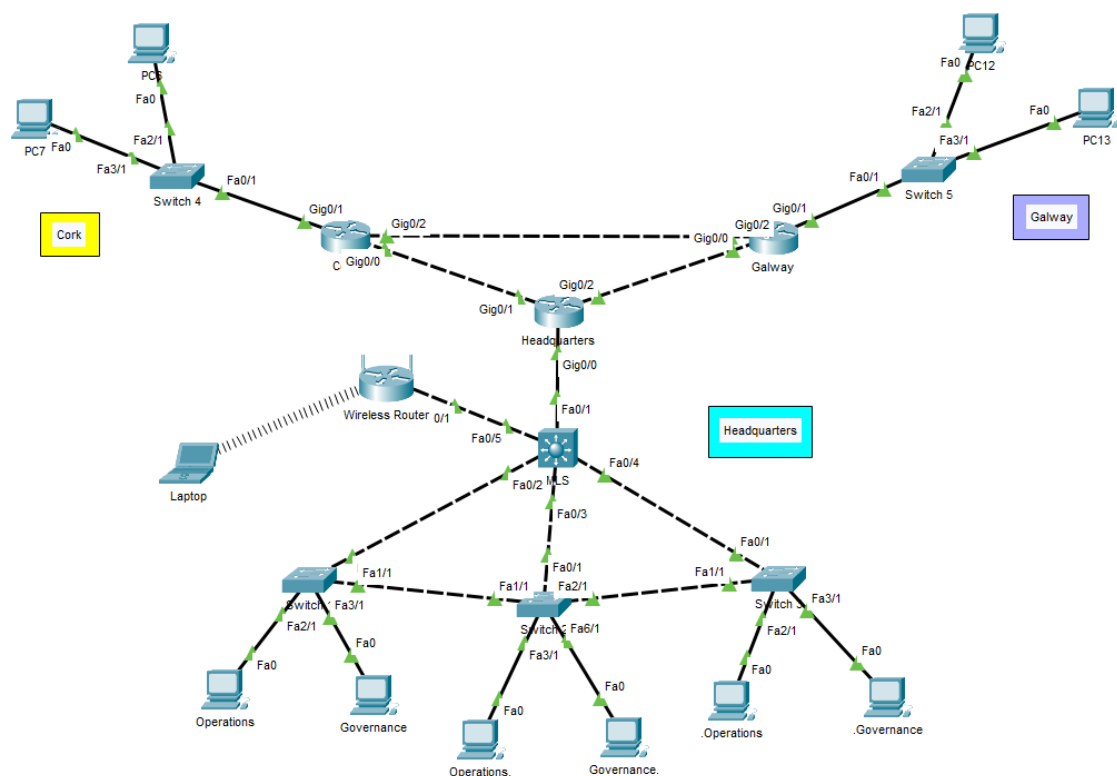
By: Jamie Dempsey

Student No: C00295144

Routing & Wireless Concepts Project 2025

As part of my studies in Cybercrime and IT Security, I was tasked with designing a secure and efficient internetwork for Emerald Retail Ltd, a growing Irish company with offices in Dublin, Cork, and Galway. The goal of this project was to create a scalable network that enables continuous communication between all locations, while also addressing security and reliability concerns. This involved setting up LANs, configuring VLANs, allocating IP addresses, and implementing strong security measures to protect against potential vulnerabilities. The result is a working prototype that meets the company's current needs and supports any future growth.

Topology



Requirement 1:

Headquarters VLAN Configuration & Inter-VLAN Routing

To meet the obligations of Emerald Retail Ltd's first requirement, I started by implementing the two specified VLANs on the headquarters network. A VLAN was created for the **Operations** department (VLAN 10), intended for the use of 100 users. Another VLAN was created for the **Governance** department (VLAN 20), intended for the use of 20 users. For better security and organisation, I also included a **Management** VLAN for network devices, a **Data** VLAN for user data, a **Voice** VLAN for VoIP services and also a **Native** VLAN for any untagged traffic throughout the network. I chose to implement these VLANs as they are essential for segmenting traffic, especially inside the headquarters. By separating the departments into their VLANs, I helped reduce unnecessary traffic between unrelated systems and limit the spread of potential threats. Without these VLANs, the network would pose a security risk, as all the traffic would be on the same domain and accessible.

VLAN	Name	Status
1	default	active
10	Operations	active
20	Governance	active
30	Voice	active
40	Data	active
50	Offline	active
99	Native	active
100	Management	active

I enabled inter-VLAN routing via the multi-layer switch (MLS) to allow for communication between the Operations and Governance VLANs. The MLS was a more efficient approach compared to a router, which would often be used for router on a stick, as the MLS can handle both layer 2 switching and layer 3 routing in one device, which will help reduce any latency and eliminate any unnecessary complexity, keeping it manageable and efficient.

Requirement 2:

VLAN IP Address & DHCP Allocation

For this requirement, I focused on setting up a scalable IP address system for Emerald Retail Ltd's network. Each VLAN and branch office (Cork & Galway) was given a unique IPv4 range to ensure appropriate segmentation.

VLAN 10 (Operations) was assigned the subnet **10.10.0.0/25** to allow for enough usable IPs for their 100 users. VLAN 20 (Governance) was given the subnet **10.20.0.0/27**, providing fewer usable IPs but enough for the 30 users.

For a more efficient approach to allocating dynamic IPs, I decided to set up a DHCP server on the MLS inside the headquarters network. The DHCP allocation means there's no need for individual static configuration and is a more secure option as it reduces the chance of collisions between subnets. DHCP pools were set up on the MLS for both VLANs and the two branches.

The Cork branch was assigned the subnet of **192.168.1.0/27**, and Galway was assigned **192.168.2.0/27**. Both these subnets are small and only support 30 usable IPs, but are appropriate for the size of our two branches.

The DHCP server may be located inside headquarters, but I set up DHCP relay agents on each branch office router. This allows devices inside those branches to still receive the dynamic IP addresses from headquarters, without needing a separate DHCP server for IP allocation on each branch.

Cork and Galway were also configured with IPv6 addresses to meet the standards of the requirement. Cork was assigned **2001:db8:1::/64**, and Galway was assigned **2001:db8:2::/64**. Since devices inside these branches needed IPv6 addresses, I used Stateless Address Autoconfiguration (SLAAC) to automatically generate the addresses for them. This approach was to accurately ensure that each device gets a unique and routable IP address.

```
ip dhcp pool Operations
network 10.10.0.0 255.255.255.128
default-router 10.10.0.1
dns-server 8.8.8.8
ip dhcp pool Governance
network 10.20.0.0 255.255.255.224
default-router 10.20.0.1
dns-server 8.8.8.8
```

```
ip dhcp pool Cork
network 192.168.1.0 255.255.255.224
default-router 192.168.1.1
dns-server 8.8.8.8
ip dhcp pool Galway
network 192.168.2.0 255.255.255.224
default-router 192.168.2.1
dns-server 8.8.8.8
```

Requirement 3:

Switch Security Measures

This requirement involved the implementation of layer 2 security measures on just the headquarters network. **NOTE:** These security measures would typically be applied to **ALL** switches (Cork & Galway) to ensure complete protection, but haven't been for the demonstration purposes of this project.

Common attacks that I've protected headquarters against are **MAC Table Attacks, VLAN Attacks, STP Attacks, DHCP Attacks, and ARP Spoofing.**

MAC Table Attacks – To prevent attackers from flooding the switch's MAC address tables, I enabled port security. This limits how many devices can connect to each port. Once I enabled port security on all the switches, I then implemented a few important features. Firstly, I set the maximum number of users at once to **4** to allow for an appropriate amount of communication. The *mac-address sticky* feature enables the switch to dynamically learn the MAC addresses even after a restart or downtime, ensuring only the authorized devices stay connected. I decided to implement the **restrict** violation mode as I felt it was the most appropriate approach to allow the network to still function smoothly even if a violation is detected. This ensures the network can still operate while the violation is already reported and being addressed.

```
interface FastEthernet3/1
  switchport access vlan 10
  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 000A.F362.0E64
```

Violation modes used for Port-Security

Switch Port Action during Port Security Violation	Protect	Restrict	Shutdown
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Disables the interface by putting it in an err-disabled state, discarding all traffic	No	No	Yes

VLAN Attacks – To stop attacks like VLAN hopping, where attackers would try to access other VLANs, I disabled trunking on unused ports and used VLAN Access Control Lists (VACLs) to control the communication between them.

STP Attacks – To protect the Spanning Tree Protocol (STP) from attacks that could cause network loops or reroute traffic, I enabled BPDU on all access ports. This will prevent rogue switches from sending BPDUs and disrupting the network's spanning tree topology. I also enabled Portfast, which allows the ports connected to clients to bypass STP for faster network connectivity.

DHCP Attacks – To prevent rogue DHCP servers and DHCP starvation attacks, where attackers try to exhaust the DHCP server's pool of IP addresses, I enabled DHCP snooping on my layer 2 switches themselves and for both VLANs 10 and 20. This feature filters out any unauthorised DHCP servers and ensures only the correct server can provide IP addresses.

```
ip dhcp snooping vlan 10,20
no ip dhcp snooping information option
ip dhcp snooping
```

ARP Spoofing – To protect against ARP spoofing, where attackers try to impersonate devices and capture traffic, I enabled Dynamic ARP Inspection (DAI) on VLANs 10 & 20. This checks ARP packets to ensure that they match the DHCP snooping database, preventing attackers from poisoning the ARP.

```
ip arp inspection vlan 10,20
```

By applying the above layer 2 security measures, I enhanced the protection of the network significantly from common attacks that could disrupt the everyday performance. These steps were essential to ensure confidentiality.

Requirement 4:

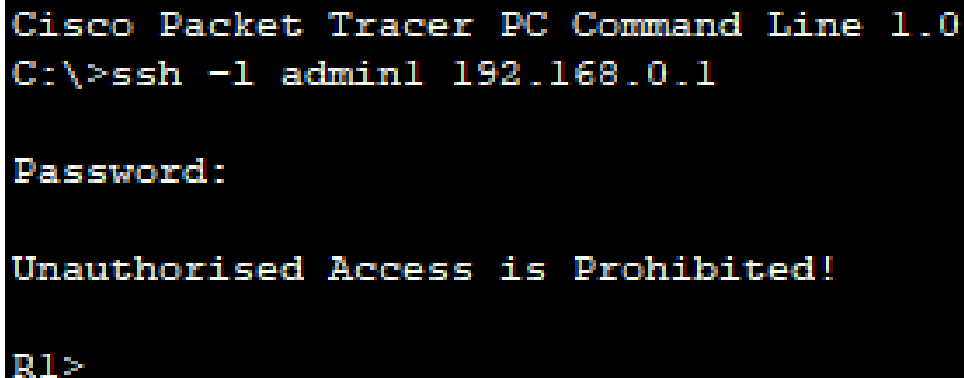
SSH Headquarters Router

To meet this requirement, I configured SSH on the headquarters router and set up local authentication to allow remote access for two administrators.

Firstly, I ensured that SSH was enabled on the router. I set the domain name to **headquarters.local** as it's required for the SSH key generation. The RSA keys were generated for the SSH encryption (2048 bits). Two administrator accounts were created and given **privilege level 15** to allow full access. The passwords for both accounts were set as **cisco** for demonstration purposes, but **NOTE:** they should be set as something stronger to enhance the security.

I then configured the router to use local authentication for SSH access, so the administrators can log in using their username and password. The router was set to accept SSH connections on the VTY lines of the router's interface.

I used SSH for a secure and encrypted remote access instead of Telnet, as SSH is much more secure. This feature ensures that only authorized administrators can remotely access the router to protect sensitive data.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin1 192.168.0.1

Password:

Unauthorised Access is Prohibited!

R1>
```

exec-timeout is for SSH sessions to timeout after **15 minutes** of inactivity.

```
line vty 0 4
  exec-timeout 15 0
```

Requirement 5:

Static Routes

For requirement 5, I configured static routes to allow for communication between headquarters, Cork and Galway. Since each branch has its own router and isn't connected, static routes are necessary to route any traffic.

I configured static routes on the headquarters router to reach the networks in both the Cork & Galway branches using **ip route** and a **next hop** address:

```
ip route 192.168.1.0 255.255.255.224 10.0.0.2  
ip route 192.168.2.0 255.255.255.224 10.0.0.6
```

The 1st route is traffic going to Cork from the HQ router.

The 2nd route is traffic going to Galway from the HQ router.

For Cork to reach Galway & headquarters, I added the following routes:

```
ip route 192.168.2.0 255.255.255.224 10.0.0.1  
ip route 192.168.0.0 255.255.255.224 10.0.0.1
```

The 1st route is traffic going to Galway from the Cork router.

The 2nd route is traffic going to HQ from the Cork router.

For Galway to reach Cork & headquarters, I added the following routes:

```
ip route 192.168.0.0 255.255.255.224 10.0.0.5  
ip route 192.168.1.0 255.255.255.224 10.0.0.5
```

The 1st route is traffic going to HQ from the Galway router.

The 2nd route is traffic going to Cork from the Galway router.

Since the branches are connected to different routers, static routes were the most straightforward approach. Static routes ensure that traffic between HQ and the branches, as well as between the branches themselves, is being forwarded through the appropriate routers. The **net-hop** address is the exact path that the traffic takes through the network until it reaches its destination.

Requirement 6:

DHCP IP Address Allocation

For requirement 6, I set up DHCP for Cork and Galway on the headquarters DHCP server (The MLS) to be able to dynamically assign IP addresses to the end devices. Each branch requires at least 30 usable addresses, so the DHCP server at HQ will manage IP address allocation for the two branches.

As I've already configured the MLS to act as a DHCP server, all I needed to do was create two new DHCP pools and assign the range of IP addresses.

```
ip dhcp pool Cork
  network 192.168.1.0 255.255.255.224
  default-router 192.168.1.1
  dns-server 8.8.8.8
ip dhcp pool Galway
  network 192.168.2.0 255.255.255.224
  default-router 192.168.2.1
  dns-server 8.8.8.8
```

The **network** section defines the range of IP addresses that the DHCP server can assign. The **default-router** is set to the branch router's IP address, which is used as the default gateway. The **dns-server** is assigned as Google's DNS.

Since the DHCP server is located at the headquarters and the Cork and Galway offices are remote, I configured DHCP relay (**IP Helper Address**) on both the Cork and Galway routers to forward the DHCP requests from the branch offices to the headquarters DHCP server and receive their address.

```
ip route 192.168.1.0 255.255.255.224 10.0.1.1 5
ip route 192.168.2.0 255.255.255.224 10.0.1.2 5
```

DHCP relay on the branch office routers, which are forwarding requests from the branch devices to the main server (headquarters), helps ensure consistency across the network. This provides a scalable and efficient solution for any future growth of the three networks, such as an expansion.

Requirement 7:

Configure Wireless Access Point (WAP)

For requirement 7, I configured a basic wireless network at headquarters to support wireless devices. The devices inside the wireless network also have access to the two VLANs (Operations & Governance) in inter-VLAN routing.

At headquarters, I configured a Wireless Access Point (WAP) to support wireless clients with secure access. I set the SSID as **EmeraldHQ-WiFi**, and the encryption was set at **WPA3** for secure access. Using **WPA3** is essential for the highest level of security for wireless access. There was also a DHCP pool created on the MLS for the wireless clients to use **192.168.50.0/24**.

```
ip dhcp pool Wireless
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1
dns-server 8.8.8.8
```

SSID Broadcasting was disabled to increase security and to prevent the network from being discovered easily. **MAC Filtering** was enabled to allow only authorised devices to connect to the network. The MAC address below belongs to the wireless laptop on the network. This is the ONLY MAC address as of current that can access the wireless network unless it's changed.

Wireless MAC Filter	
Wireless Port: 5G(1) v	
<input checked="" type="radio"/> Enabled <input type="radio"/> Prevent PCs listed below from accessing the wireless network	
<input checked="" type="radio"/> Permit PCs listed below to access wireless network	
Wireless Client List	
MAC 01:	00:05:5E:51:C6:D9

Additional: Password Protection

All devices inside the headquarters network have been assigned extra layers of security. **NOTE:** None of the devices in the Cork or Galway branches have been given these extra layers of security, but only for demonstration purposes of the prototype. **ALL** devices should typically always be password protected with encryption to ensure maximum security throughout the entirety of the network.

The headquarters has been secured with password protection for any attempt into **Privileged EXEC Mode, Global Configuration Mode** or **Line Console / Aux / VTY Mode**, as well as encryption of all passwords, including passwords for any of the SSH accounts.

```
service password-encryption
```

```
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password 7 0822455D0A16
```

```
username admin1 privilege 15 secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username admin2 privilege 15 secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
```

All switches and routers in the headquarters are configured with a banner MOTD upon any login attempt to configuration modes, including during SSH.

```
Unauthorized Access is Prohibited!
```

```
User Access Verification
```

```
Password:
```