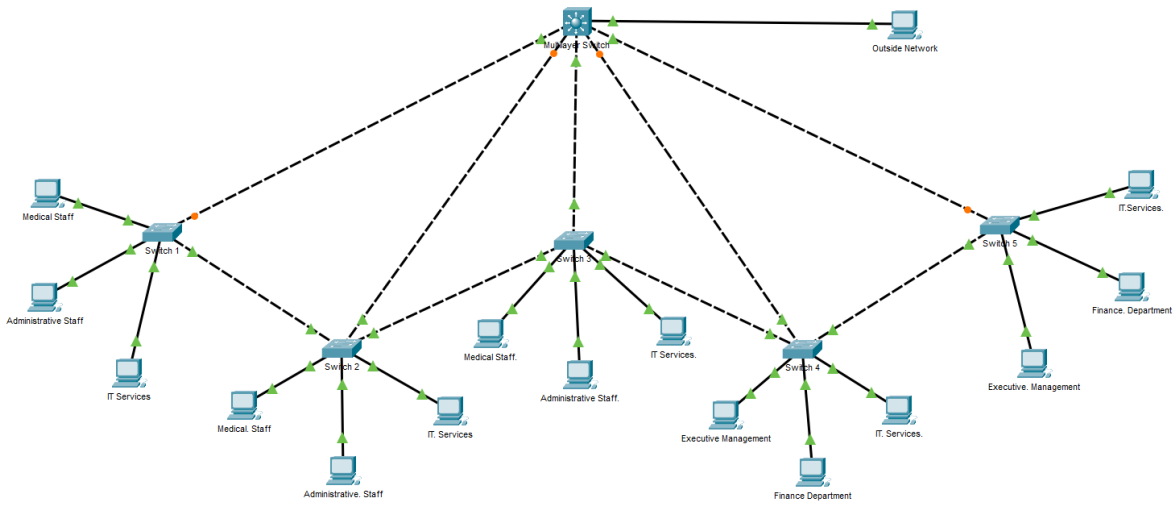
# Secure and Scalable LAN Design for Metro Health Hospital Headquarters


**Designed by:**

**Full Name:** Jamie Dempsey

**Student Number:** C00295144


Topology for the Hospital Headquarters Network:




## Description

To address Metro Health Hospital's requirements, I designed and prototyped a high-performance Local Area Network (LAN) that ensures secure, efficient, and reliable communication between departments while supporting critical operations.

# Requirement 1

## VLAN Configuration & Traffic Separation

VLANs were created for each department to isolate and manage traffic effectively. This ensures that traffic is restricted within its designated department, reducing unnecessary congestion across the network and improving security by controlling communication across departments.

```
VLAN Name                             Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/2
10   Executive_Management              active
20   Administrative_Staff              active    Fa0/3
30   Finance_Department                active
40   IT_Services_Department            active    Fa0/4
50   Medical_Staff                     active    Fa0/2
99   Management                        active
100  Native                            active
150  Voice                             active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

VLANs have been assigned to switch ports that are connected to PCs, limiting access control to safeguard communication to prevent traffic from entering unauthorised devices accessing department resources.

**Executive Management (VLAN 10)**: Dedicated to high-level management

**Administrative Staff (VLAN 20)**: For general administrative tasks

**Finance Department (VLAN 30)**: Handles sensitive financial data

**IT Services Department (VLAN 40)**: Manages technical communications

**Medical Staff (VLAN 50)**: Supports patient care and holds documentation

**Management (VLAN 99)**: Focuses on operations and manages communication

**Native VLAN (VLAN 100)**: Configured for any untagged traffic.

**Voice VLAN (VLAN 150)**: Created for VoIP traffic.

## Requirement 2

### Inter-VLAN Communication & External Connectivity

Inter-VLAN routing was established using the layer 3 capabilities of the multilayer switch, assigning each VLAN with a Switched Virtual Interface (SVI). SVI connects and routes traffic between devices, allowing traffic from one VLAN to be routed to another VLAN. Each SVI has a unique IP address corresponding to its subnet as VLAN 10 has an IP address of 192.168.10.1 to serve as its default gateway for devices in the subnet.

```
interface Vlan10
 mac-address 00e0.f9b6.6301
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 mac-address 00e0.f9b6.6302
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan30
 mac-address 00e0.f9b6.6303
 ip address 192.168.30.1 255.255.255.0
!
interface Vlan40
 mac-address 00e0.f9b6.6304
 ip address 192.168.40.1 255.255.255.0
!
interface Vlan50
 mac-address 00e0.f9b6.6305
 ip address 192.168.50.1 255.255.255.0
!
interface Vlan99
 mac-address 00e0.f9b6.6306
 ip address 192.168.99.1 255.255.255.0
!
interface Vlan100
 mac-address 00e0.f9b6.6307
 ip address 192.168.100.1 255.255.255.0
!
interface Vlan150
 mac-address 00e0.f9b6.6308
 ip address 192.168.150.1 255.255.255.0
```

To ensure the hospital network has access to external resources, a PC outside the network was introduced to simulate a connection to the internet, allowing devices to communicate beyond the local network. The connected switch port was assigned an IP address which enables the external device to communicate with devices inside the network.

## Requirement 3

## IP Addressing & DHCP Implementation

The hospital's network was set up using Dynamic Host Configuration Protocol (DHCP) on the multilayer switch to simplify and automate the process of assigning IP addresses, this helped create a structured and efficient network. DHCP is suitable for the hospital's network as it saves time and reduces the chances of any configuration errors. Each VLAN was assigned a unique /24 IPv4 subnet to ensure traffic segregation across the network. Each DHCP pool specifies the subnet for each department. The default router points back to the SVI IP, allowing PCs in the VLAN to communicate with other VLANs. The DNS server has been set to 8.8.8.8 (Google's public DNS server) for demonstration purposes.

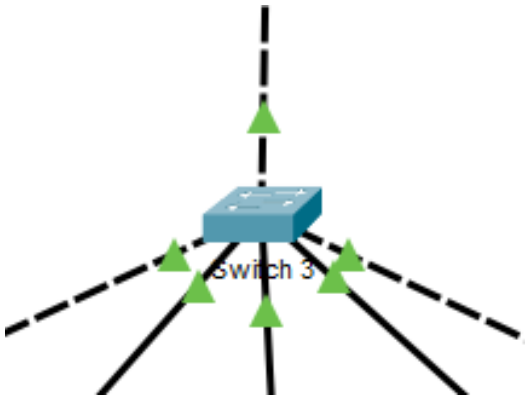
```
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp excluded-address 192.168.20.254
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.30.254
ip dhcp excluded-address 192.168.40.1 192.168.40.10
ip dhcp excluded-address 192.168.40.254
ip dhcp excluded-address 192.168.50.1 192.168.50.10
ip dhcp excluded-address 192.168.50.254

ip dhcp pool Executive_Management
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8
ip dhcp pool Administrative_Staff
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 8.8.8.8
ip dhcp pool Finance_Department
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 8.8.8.8
ip dhcp pool IT_Services_Department
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 8.8.8.8
ip dhcp pool Medical_Staff
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
 dns-server 8.8.8.8
```

The first 10 addresses in each subnet (.1 to .10) were excluded from each DHCP pool to reserve them for availability for other critical network devices. The last valid address in each subnet (.254) was reserved as the default gateway for each department's VLAN.

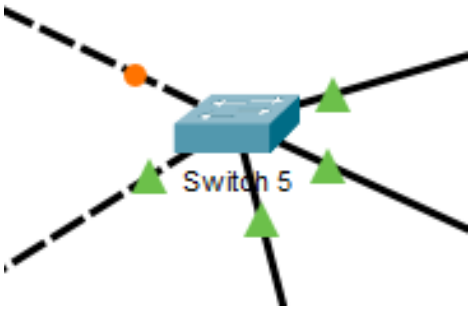
# Requirement 4

## Network Redundancy

To ensure constant availability and decrease any unexpected downtime on the hospital's network, redundancy has been established. Multiple paths for traffic have been formed throughout the topology with each layer 2 and 3 switches being allocated with several link connections, maintaining a persistent flow of data in the event of any link failures.




Spanning Tree Protocol (STP) has been automatically enabled on the network, preventing loops as well as ensuring other paths are available in case of corruption. STP places alternative ports in a blocking state until they are needed, in most cases if the primary path for traffic fails. Broadcast storms, duplicate frames and MAC address table instability are all scenarios which are eliminated by the use of STP in the network.




An example of a switch port in a blocking state is seen as the orange dot.

# Requirement 5

## Security Measures

Security is crucial in any circumstance and without it, the network is at risk of a breach. To avoid unknown traffic entering the PC access ports and accessing sensitive data, only specific VLANs have been permitted to pass through, reducing the risk of authorised department traffic. All unused switch ports have been set administratively down so that no authorised devices can be connected, ensuring no edits can be made.

Configuration of a secret password was implemented on all switches to access privileged EXEC mode. The password was set up as cisco for demonstration purposes as ideally, this isn't a very secure password. A banner MOTD was established for every switch upon login to prevent any unauthorized access and inform users of the policy. Password encryption was enabled to protect all plaintext passwords from exposure to unauthorised personnel, stored in configurations.

Secure Remote Access (SSH) has been enabled for all layer 2 and 3 switches. SSH is essential to have a secure login for administrators, allowing them to manage the network remotely without the exposure of login credentials to any attackers. A successful login is shown below.