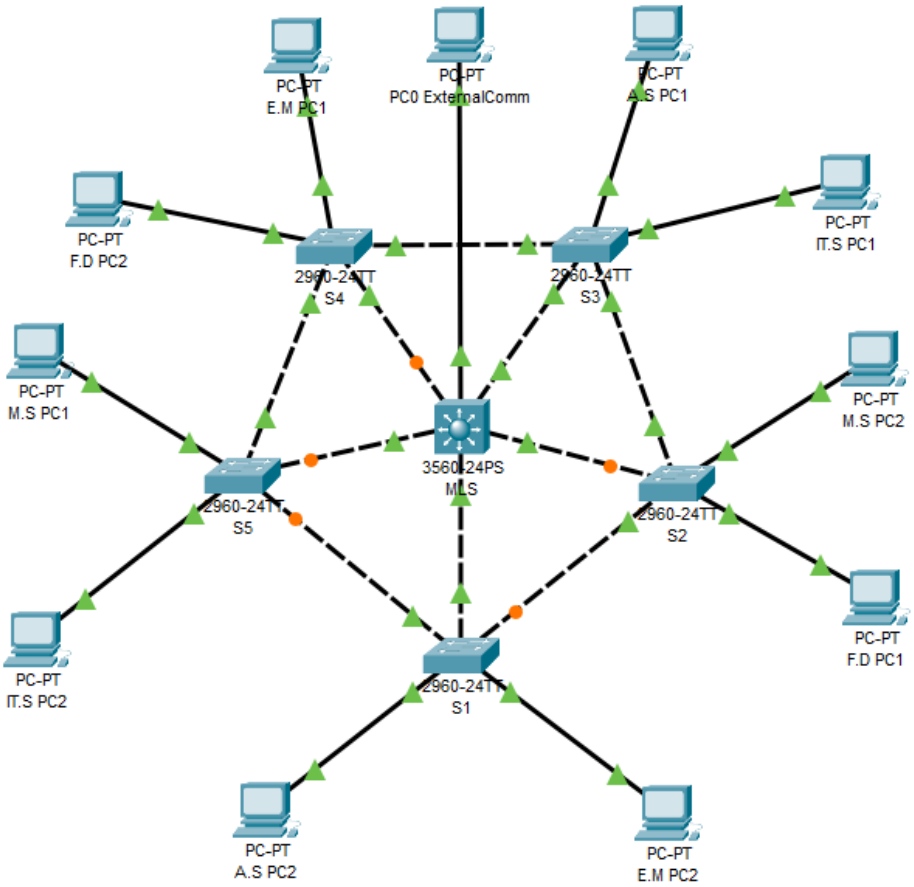
Mercy West Hospital

Introduction

In modern healthcare facilities, efficient and secure communication networks are essential for ensuring seamless operations and safeguarding sensitive patient data. This report provides an in-depth examination of the VLAN network deployed within our hospital, detailing its design, functionality, and role in supporting critical healthcare services. Key areas covered in this report include an overview of the network's architecture, its scalability to accommodate growth, the measures implemented to ensure a secure network within our hospital.



Img 1: Preview of the Network Setup

Inter-Vlan Communication and External Communication

Inter-Vlan Communication

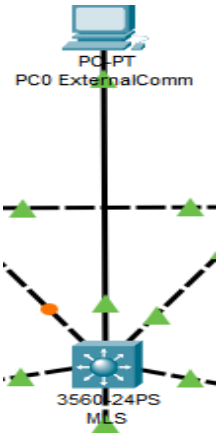
Inter-VLAN communication allows devices in separate VLANs to interact, enabling efficient and secure network operations. While VLANs isolate broadcast domains to enhance performance and security, inter-VLAN communication is necessary for sharing resources, such as servers or printers, and facilitating collaboration between departments. By routing traffic through a Layer 3 switch, inter-VLAN communication ensures controlled access and traffic management. It supports centralized resource access, secure cross-department interactions, optimized network performance, and scalability, making it a critical component in modern network design.

A multilayer switch allows devices in different VLANs to communicate by using virtual interfaces (SVIs) for each VLAN. It can both switch data within a VLAN (Layer 2) and route data between VLANs (Layer 3), allowing smooth and fast communication between them without needing a separate router.

External Communication

External communication allows VLANs to connect to the internet, cloud services, and remote networks, enabling essential functions such as browsing, software updates, cloud integration, VPN access, and external service connectivity. It ensures internal segmentation while supporting seamless interaction with external resources critical for business operations.

To allow VLANs to access things outside the network (like the internet), each VLAN is given a default gateway (usually a router or switch). This device changes the private IP addresses of devices in the VLAN to a public one using NAT. It also sends traffic between VLANs and outside networks, with security rules to control what can be accessed. This way, VLANs stay separate but can still connect to external resources.



Img1.1: External Communication Setup on the Network through an End Device.

Vlan Setup

Vlan 1		Default
		VLAN1 is the default vlan on most switches, where all ports are assigned unless changed. It's used for managing the switch, like for configuration. However, because it's the default, it's not recommended to use VLAN1 for important or sensitive traffic for security reasons.
Vlan 5		Unused
		An unused VLAN is a VLAN that has been created but is not assigned to any active ports or devices. It does not carry any traffic and is typically left dormant in the network configuration.
Vlan 10		Executive Management
Vlan 20		Administrative Staff
Vlan 30		Finance Department
Vlan 40		IT Services Department
Vlan 50		Medical Staff
Vlan 99	Native	
		The native VLAN handles untagged traffic on a trunk link between switches. It is the default VLAN for trunk ports and ensures compatibility with devices that don't support VLAN tagging, allowing smooth communication across trunk links.
Vlan 100		Management
		A management VLAN is used to separate network management traffic (such as for device configuration and monitoring) from regular data traffic. It improves security by isolating management access to devices like switches and routers.

IP Addressing and DHCPv4 Configuration

Using DHCP (Dynamic Host Configuration Protocol) in an inter-VLAN network allows devices in different VLANs to automatically receive IP addresses. It reduces manual configuration errors, improves scalability, and eases network administration by automating IP assignment.

This network is configured using a structured IP addressing to ease network management. Vlans are assigned a /24 subnet.

DHCP Dynamic Allocation:

The DHCP service is configured on the switch with specific ranges of IP addresses excluded to reserve for dynamic allocation.

For example: On the hospital's network, the current IP addresses excluded for Vlan 10 IP assignements would be 192.168.10.1 to 192.168.10.10.

Excluding such ip addresses ensure critical devices do not get assigned the same IP address as another critical device.

Security Measures

To ensure secure network connection and communication and also sensitive data within the hospital's network, several security measures have been integrated into this network:

- Password encryption :
    - Password Encryption on a Layer 2 or Layer 3 switch helps protect sensitive information by converting plain text passwords into encrypted formats.

        1. enable password 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
        2. username admin secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
        3. line con 0
           password 7 0822404F1A0A

- Secure Remote Access :
    - Secure remote access ensures encrypted communication for managing devices, protecting sensitive data from unauthorized access. It allows remote management, enhances security, controls access, and enables audit logging for monitoring actions.
    - SSH is enabled on vty lines for remote access.
        1. line vty 0 4

           login local

           transport input ssh
        2. line vty 5 15

           login local

           transport input ssh

Data Sheet (Vlan Brief)

		Port	Vlan	IP Address	Default Router	Mode
Switch 1	Switch 1 to MLS	Fa0/1	--------	----------	----------	Trunk
Switch 1	Switch 1 to Switch 2	Fa0/2	--------	----------	----------	Trunk
Switch 1	Switch 1 to Switch 5	Fa0/3	--------	----------	----------	Trunk
Switch 1	A.S PC 2	Fa0/4	Vlan 20	192.168.20.11	192.168.20.1	Access
Switch 1	E.M PC 2	Fa0/5	Vlan 10	192.168.10.11	192.168.10.1	Access
Switch 2	Switch 2 to MLS	Fa0/1	--------	----------	----------	Trunk
Switch 2	Switch 2 to Switch 1	Fa0/2	--------	----------	----------	Trunk
Switch 2	Switch 2 to Switch 3	Fa0/3	--------	----------	----------	Trunk
Switch 2	F.D PC 1	Fa0/4	Vlan 30	192.168.30.12	192.168.30.1	Access
Switch 2	M.S PC 2	Fa0/5	Vlan 50	192.168.50.11	192.168.50.1	Access
Switch 3	Switch 3 to MLS	Fa0/1	--------	----------	----------	Trunk
Switch 3	Switch 3 to Switch 2	Fa0/2	--------	----------	----------	Trunk
Switch 3	Switch 3 to Switch 4	Fa0/3	--------	----------	----------	Trunk
Switch 3	IT.S PC 1	Fa0/4	Vlan 40	192.168.40.11	192.168.40.1	Access
Switch 3	A.S PC 1	Fa0/5	Vlan 20	192.168.20.12	192.168.20.1	Access
Switch 4	Switch 4 to MLS	Fa0/1	--------	----------	----------	Trunk
Switch 4	Switch 4 to Switch 3	Fa0/2	--------	----------	----------	Trunk
Switch 4	Switch 4 to Switch 5	Fa0/3	--------	----------	----------	Trunk
Switch 4	E.M PC 1	Fa0/4	Vlan 10	192.168.10.12	192.168.30.1	Access
Switch 4	F.D PC 2	Fa0/5	Vlan 30	192.168.30.11	192.168.30.1	Access
Switch 5	Switch 5 to MLS	Fa0/1	--------	----------	----------	Trunk
Switch 5	Switch 5 to Switch 4	Fa0/2	--------	----------	----------	Trunk
Switch 5	Switch 5 to Switch 1	Fa0/3	--------	----------	----------	Trunk
Switch 5	M.S PC 1	Fa0/4	Vlan 50	192.168.50.11	192.168.50.1	Access
Switch 5	IT.S PC 2	Fa0/5	Vlan 40	192.168.40.12	192.168.40.1	Access
MLS	MLS to Switch5	Fa0/1	--------	----------	----------	Trunk
MLS	MLS to Switch1	Fa0/2	--------	----------	----------	Trunk
MLS	MLS to Switch2	Fa0/3	--------	----------	----------	Trunk
MLS	MLS to Switch3	Fa0/4	--------	----------	----------	Trunk
MLS	MLS to Switch4	Fa0/5	--------	----------	----------	Trunk