Digital Egypt
Pioneers Initiative

رواد مصر الرقمية

DOCUMENTATION

HOSPITAL DATA MANAGEMENT NETWORK

Project Overview

Project Name:

Hospital Data Management Network

Purpose:

To establish a secure, scalable, and efficient network infrastructure for managing hospital operations, data storage, research, and patient care.

Scope:

The project covers 7 networks, ensuring secure communication across 61 PCs, 12 laptops, 19 servers, 7 tablets, 2 Access Points, 2 routers, and 6 switches.

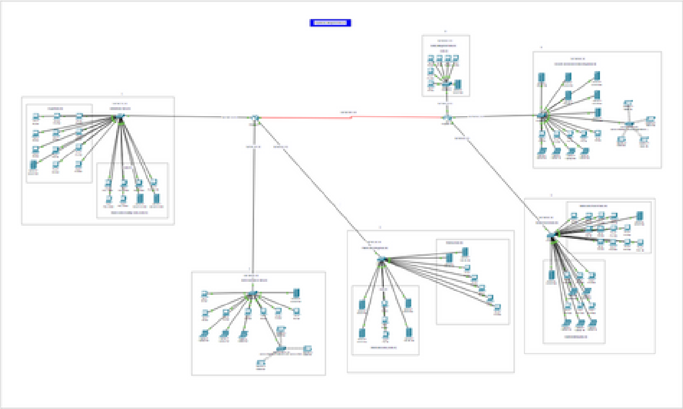
Team Members:

- **Yousuf Mahmoud Muhammad**
- **Ahmed Akram Atef**
- **Shaimaa Eid Abdelbaky**
- **Moaz Ahmed Abdelwahid**

Network Design and Architecture

Devices:

- 61 PCs
- 12 Laptops
- 19 Servers
- 7 Tablets
- 2 Access Points
- 2 Routers
- 6 Switches



Network IDs:

6 Networks for the 6 Switches:

1. **192.168.1.0/24**
2. **192.168.2.0/24**
3. **192.168.3.0/24**
4. **192.168.4.0/24**
5. **192.168.5.0/24**
6. **192.168.6.0/24**

1 Network for Router-to-Router

Connection:

- 192.168.10.0/30 (serial link between routers)

Detailed Network Descriptions

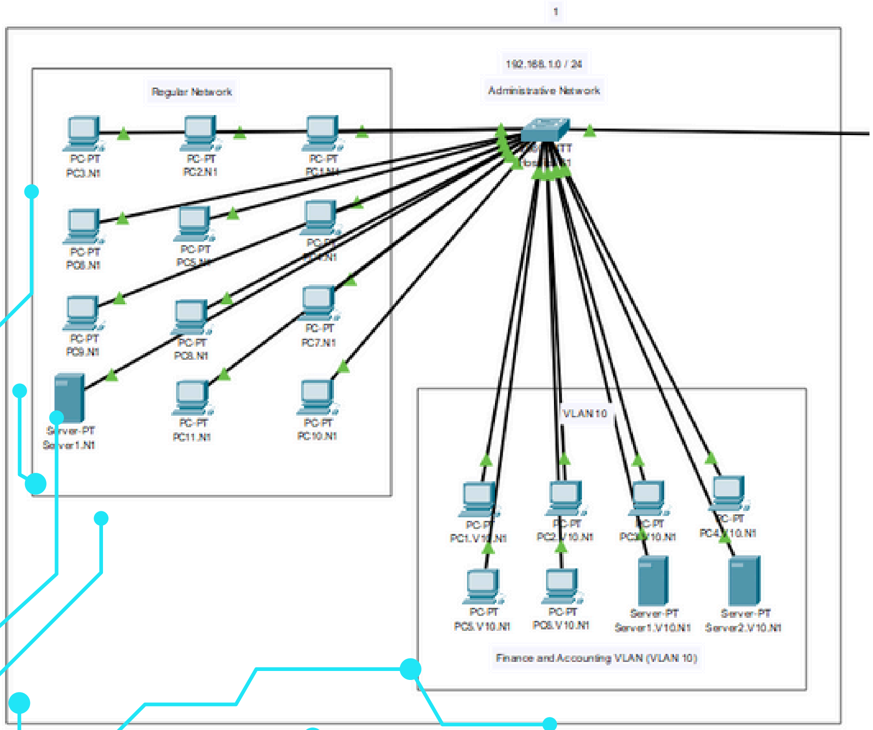
Network 1: Administrative Network (192.168.1.0/24)

Part 1: Administrative Segment

- **Devices: 11 PCs, 1 server.**
- **Role: Manages appointments, staff operations, and general administrative tasks.**

Part 2: Finance and Accounting VLAN (VLAN 10)

- **Devices: 6 PCs, 2 servers.**
- **Role: Handles financial transactions and hospital accounting with secure, isolated data.**

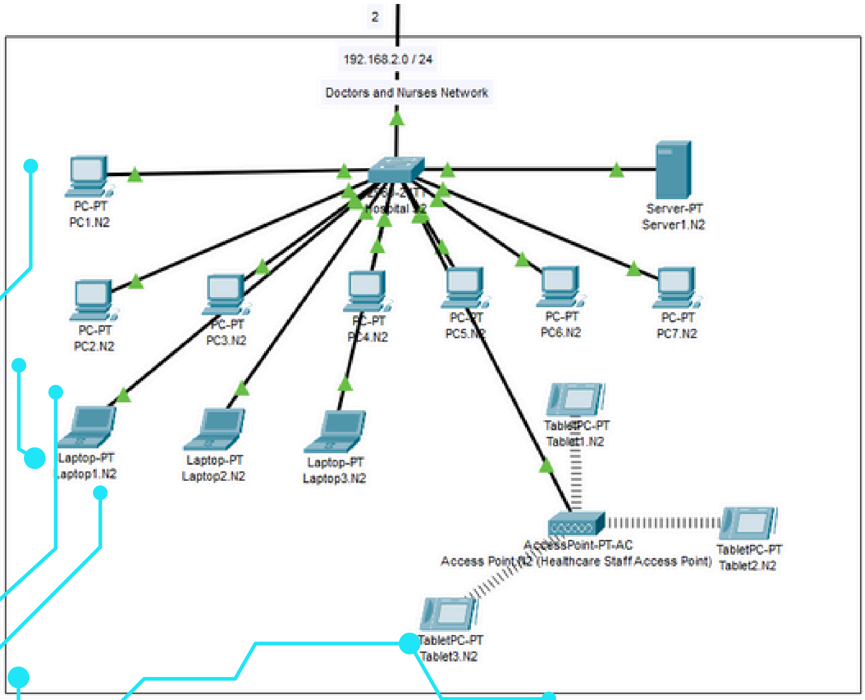


Detailed Network Descriptions

Network 2:
Doctors and Nurses Network
(192.168.2.0/24)

Devices: 7 PCs, 3 laptops, 1 server, 3 tablets, and an Access Point.

Role: Provides connectivity for doctors and nurses to access and update patient medical records. Tablets are connected via the Access Point using WPA2 PSK security to protect against unauthorized access.



Detailed Network Descriptions

Network 3:

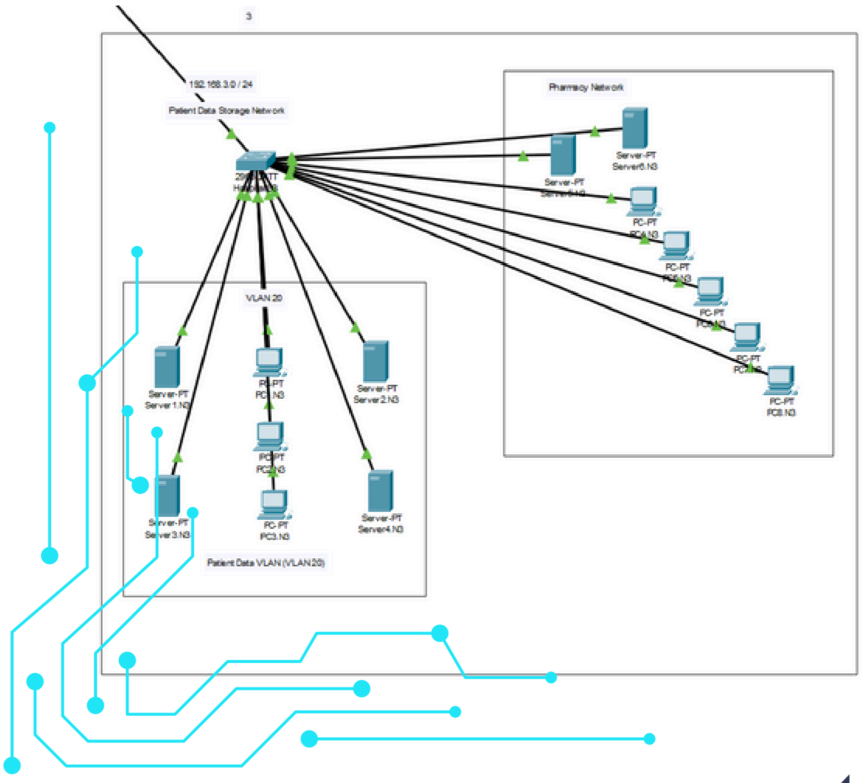
Patient Data and Pharmacy Network (192.168.3.0/24)

Part 1:

Patient Data Storage Network Devices: 3 PCs, 4 servers. Role: Stores and manages sensitive patient records.

Part 2:

Pharmacy Network Devices: 5 PCs, 2 servers. Role: Manages medication stock and medical orders. DHCP is enabled to allow easy addition of more devices.



Detailed Network Descriptions

Network 4:

Medical Devices and Health Monitoring Network (192.168.4.0/24)

Part 1:

Medical Devices Network

Devices: 12 PCs, 1 server.

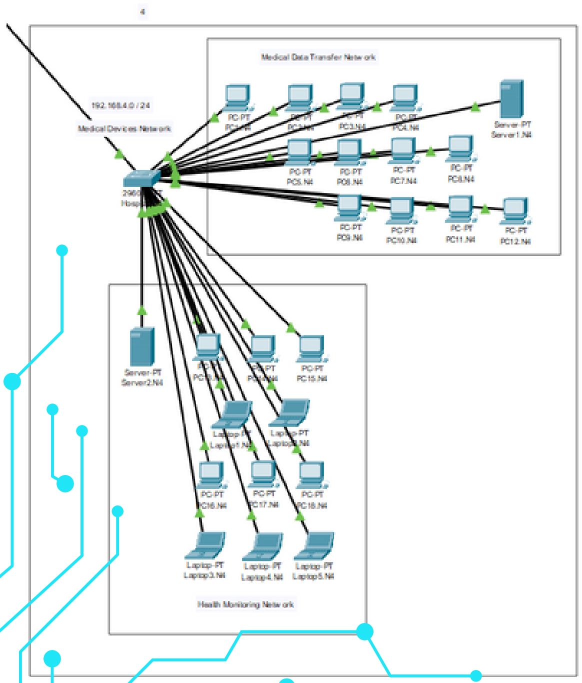
Role: Facilitates data transfer between medical devices and hospital computers for test analysis (e.g., X-rays, lab results).

Part 2:

Health Monitoring Network

Devices: 6 PCs, 5 laptops, 1 server, 3 tablets.

Role: Dedicated to real-time patient health monitoring systems. DHCP is enabled to allow easy management.

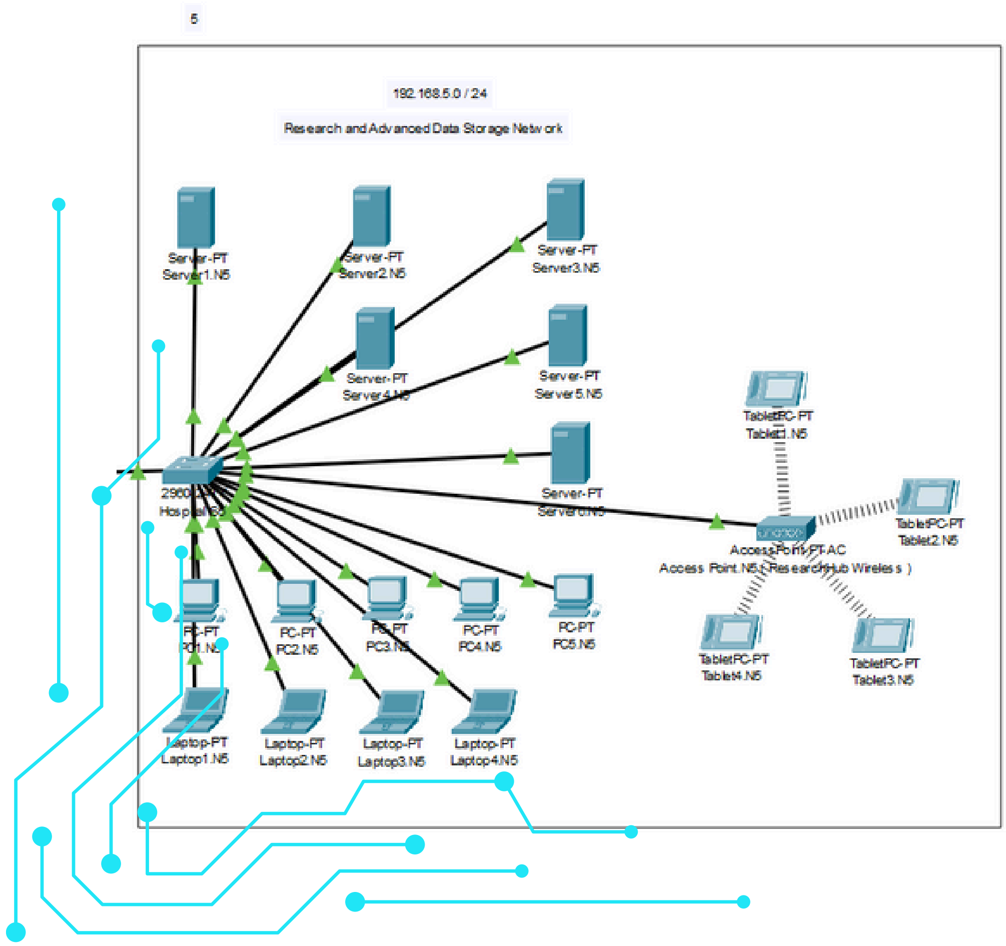


Detailed Network Descriptions

Network 5: Research and Advanced Data Storage Network (192.168.5.0/24)

Devices: 5 PCs, 4 laptops, 6 servers, 4 tablets, and 1 Access Point.

Role: Stores research data and large-scale hospital projects. The Access Point provides secure wireless access to the tablets using WPA2 PSK.



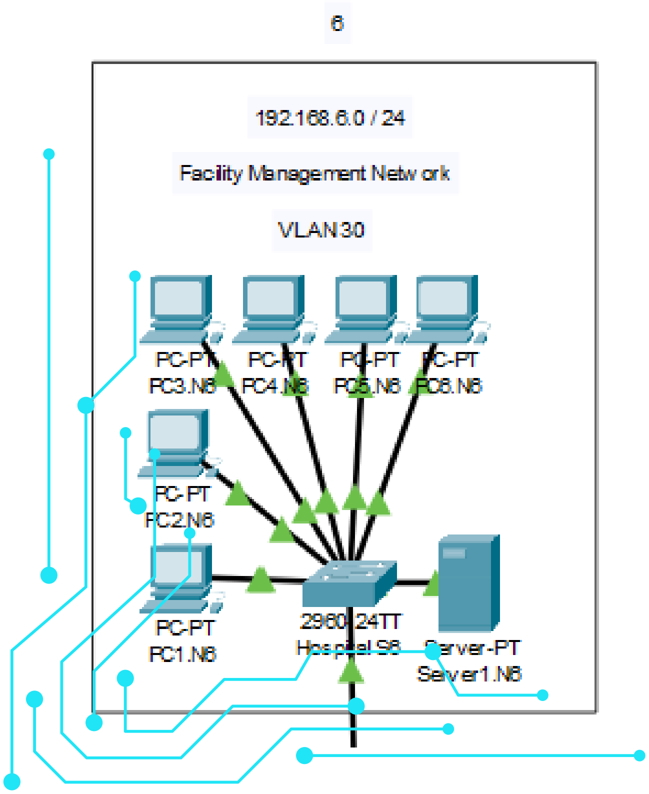
Detailed Network Descriptions

Network 6: Facility Management Network (192.168.6.0/24)

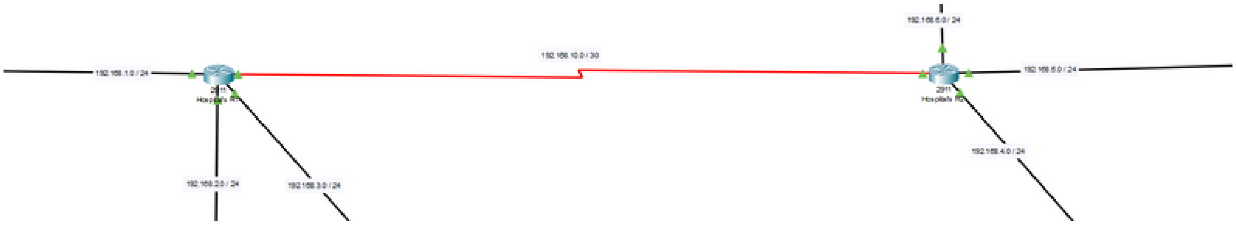
Devices: 6 PCs, 1 server.

VLAN: VLAN 30 (Facilities Management)

Role: Manages smart building systems such as lighting, air conditioning, and security systems like surveillance cameras. The network is segmented using VLAN 30 to ensure that the facility management devices are isolated for better performance and enhanced security. This segmentation helps to protect critical infrastructure from other network traffic, ensuring smooth and secure operation of the facility's systems.



Detailed Network Descriptions



Router-to-Router Network (192.168.10.0/30)

Devices: 2 routers.

Role: Manages the connection between Router R1 and Router R2 via a serial link. The IP addresses used are 192.168.10.1/30 (R1) and 192.168.10.2/30 (R2).

Detailed Configurations

- Router Configurations:

Each router is configured with IP addresses for the connected networks. R1 handles networks 1, 2, and 3, while R2 handles networks 4, 5 and 6, with a serial link between the two routers.

- Switch Configurations:

Switches are configured to manage traffic between PCs, servers, and other devices within each network.

DHCP Service: Servers are configured to provide DHCP services, each dedicated to its specific network for seamless IP assignment.

Security Features

Access Points: Each AP is configured with a unique SSID and WPA2 PSK security to protect against unauthorized access. Tablets connect securely to the network via SSID and password.

Scalability and Future Growth

The hospital network is designed to accommodate future growth, allowing for easy expansion by adding new devices, servers, or entire network segments. Additional security measures can be implemented as needed, and the network infrastructure can handle increased load as more departments are integrated.

Configuration for Switch:

```
# Enable privileged EXEC mode
enable

# Enter global configuration mode
configure terminal

# Change the hostname of the switch
hostname Hospital_Switch

# Set a welcome banner
banner motd # Welcome to Hospital's Network! #

# Create VLANs (if needed)
vlan 10
name Finance_VLAN
exit

# Assign ports to VLAN 10 (for sensitive data, if needed)
interface range Fa0/1 - Fa0/5
switchport mode access
switchport access vlan 10
exit

# Assign other ports to the default VLAN (if needed)
interface range Fa0/6 - Fa0/10
switchport mode access
switchport access vlan 1
exit

# Create VLAN 30
vlan 30
name FacilitiesManagement
exit

# Assign port Fa0/1 to VLAN 30 (for Facility Management - Router Port)(if needed)
interface Fa0/1
switchport mode access
switchport access vlan 30
exit

# Set the password for line console 0
line console 0
password [your_console_password]
login
exit

# Set the enable secret password
enable secret [your_enable_secret_password]

# Enable password encryption
service password-encryption

# Exit global configuration mode
exit

# Save the configuration
write memory
```

Switch Configuration Overview for Hospital Network

This configuration outlines the key steps taken to secure and organize the hospital's network switches for efficient management and enhanced security. Each switch is uniquely named, VLANs are created and assigned, and essential security measures like passwords and encryption are implemented. These changes are saved to ensure they remain active after a reboot.

Change Hostname: The switch's hostname is changed to Hospital_Switch_(N) to make identification easier, Each switch is named numerically (e.g., Hospital_Switch1, Hospital_Switch2) for easy identification and distinction between them.

Set a Welcome Banner: A message of the day (MOTD) banner is configured to display a welcome message when users access the switch.

Create and Assign VLANs: VLAN 10 is created for sensitive data (e.g., Finance VLAN). Ports are assigned to VLAN 10, while the remaining ports are assigned to the default VLAN (VLAN 1) if needed.

Set Console Password: A password is set for line console 0 to restrict unauthorized access via the console port.

Set Enable Secret Password: An enable secret password is configured for privileged EXEC mode, which is encrypted.

Enable Password Encryption: Password encryption is activated using service password-encryption, ensuring that all plain-text passwords are encrypted in the running configuration.

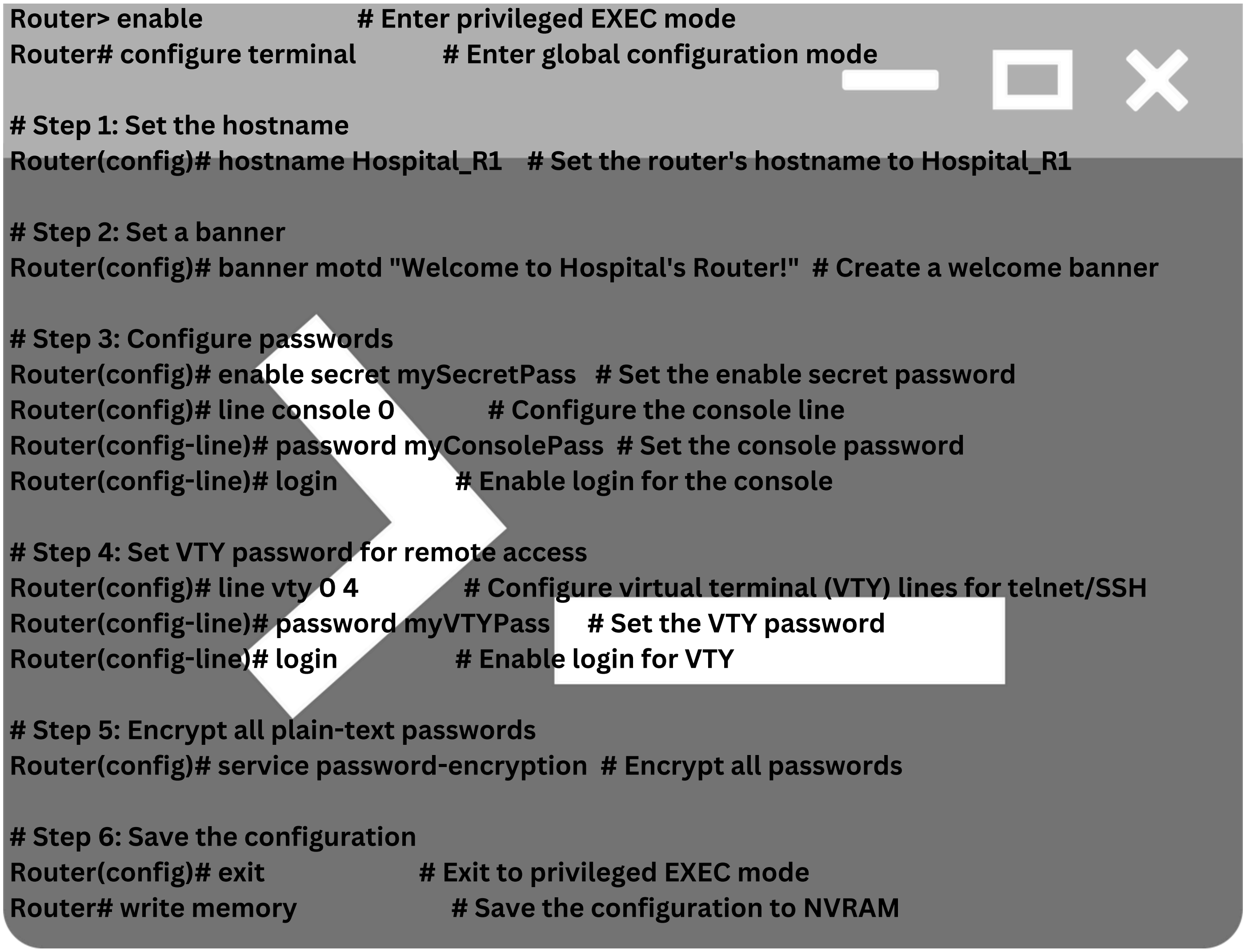
Save Configuration: The changes are saved to the switch’s memory using the write memory command, so they persist after a reboot.

Configuring the Switch for Access Point Connection

```
Switch> enable                    # Enter privileged EXEC mode
Switch# configure terminal           # Enter global configuration mode
Switch(config)# interface GigabitEthernet0/1  # Select the interface connected to the AP
Switch(config-if)# switchport mode access    # Set the port to access mode
Switch(config-if)# no shutdown            # Enable the port (turn it on)
```

This section shows the commands used to configure the switch for connecting to the Access Point (AP). The interface GigabitEthernet0/1 is set to access mode, ensuring the AP can connect to the network without VLAN tagging. The no shutdown command activates the port to allow traffic to flow between the switch and the AP.

The Router Configuration commands with comments explaining each step:

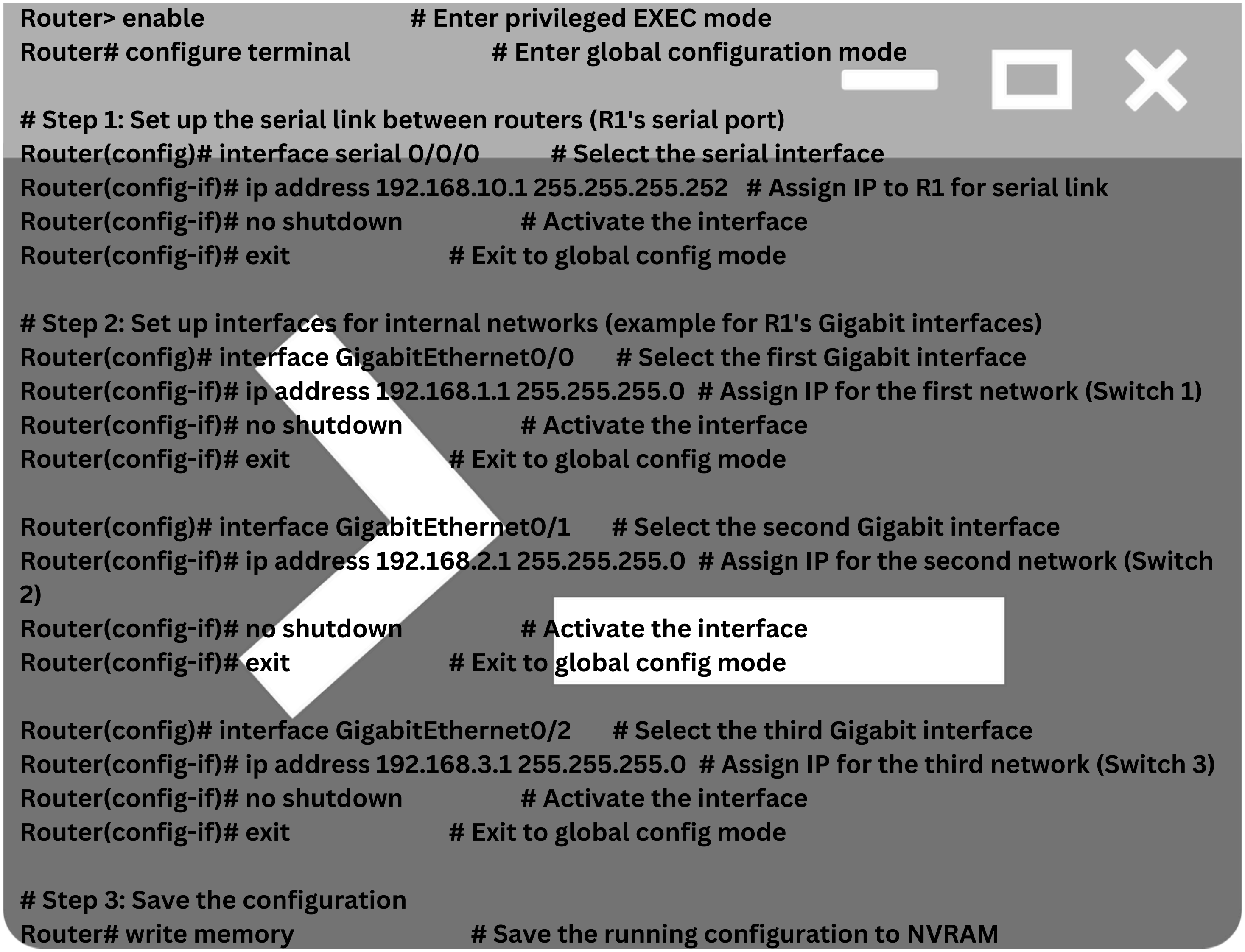


```
Router> enable                    # Enter privileged EXEC mode
Router# configure terminal            # Enter global configuration mode

# Step 1: Set the hostname
Router(config)# hostname Hospital_R1    # Set the router's hostname to Hospital_R1

# Step 2: Set a banner
Router(config)# banner motd "Welcome to Hospital's Router!"  # Create a welcome banner

# Step 3: Configure passwords
Router(config)# enable secret mySecretPass   # Set the enable secret password
Router(config)# line console 0             # Configure the console line
Router(config-line)# password myConsolePass  # Set the console password
Router(config-line)# login                 # Enable login for the console

# Step 4: Set VTY password for remote access
Router(config)# line vty 0 4               # Configure virtual terminal (VTY) lines for telnet/SSH
Router(config-line)# password myVTYPass     # Set the VTY password
Router(config-line)# login                 # Enable login for VTY

# Step 5: Encrypt all plain-text passwords
Router(config)# service password-encryption  # Encrypt all passwords

# Step 6: Save the configuration
Router(config)# exit                       # Exit to privileged EXEC mode
Router# write memory                       # Save the configuration to NVRAM
```

Explanation:

Hostname: Assigns a name to the router for easy identification.
Banner: Displays a welcome message when someone accesses the router.
Passwords: Secures the console, enable, and VTY lines with passwords.
Encryption: Encrypts all plain-text passwords to enhance security.
Save Configuration: Saves the running configuration to ensure it persists after a reboot.

Configuration for one of the Routers (R1), with examples for its four interfaces, including the serial link and the connections to the three switches.



```
Router> enable                         # Enter privileged EXEC mode
Router# configure terminal                  # Enter global configuration mode

# Step 1: Set up the serial link between routers (R1's serial port)
Router(config)# interface serial 0/0/0         # Select the serial interface
Router(config-if)# ip address 192.168.10.1 255.255.255.252   # Assign IP to R1 for serial link
Router(config-if)# no shutdown                 # Activate the interface
Router(config-if)# exit                     # Exit to global config mode

# Step 2: Set up interfaces for internal networks (example for R1's Gigabit interfaces)
Router(config)# interface GigabitEthernet0/0       # Select the first Gigabit interface
Router(config-if)# ip address 192.168.1.1 255.255.255.0  # Assign IP for the first network (Switch 1)
Router(config-if)# no shutdown                 # Activate the interface
Router(config-if)# exit                     # Exit to global config mode

Router(config)# interface GigabitEthernet0/1       # Select the second Gigabit interface
Router(config-if)# ip address 192.168.2.1 255.255.255.0  # Assign IP for the second network (Switch
2)
Router(config-if)# no shutdown                 # Activate the interface
Router(config-if)# exit                     # Exit to global config mode

Router(config)# interface GigabitEthernet0/2       # Select the third Gigabit interface
Router(config-if)# ip address 192.168.3.1 255.255.255.0  # Assign IP for the third network (Switch 3)
Router(config-if)# no shutdown                 # Activate the interface
Router(config-if)# exit                     # Exit to global config mode

# Step 3: Save the configuration
Router# write memory                        # Save the running configuration to NVRAM
```

Explanation:

Serial Interface (0/0/0): This connects Router R1 to Router R2 via a serial link. The IP address used is 192.168.10.1/30, and the interface is activated with no shutdown.

GigabitEthernet0/0: Connects R1 to Switch 1, which manages Network 192.168.1.0/24. The IP address 192.168.1.1 is assigned to R1 for this network.

GigabitEthernet0/1: Connects R1 to Switch 2, which manages Network 192.168.2.0/24. The IP address 192.168.2.1 is assigned.

GigabitEthernet0/2: Connects R1 to Switch 3, which manages Network 192.168.3.0/24. The IP address 192.168.3.1 is assigned.

write memory: This command saves the configuration changes to ensure that the setup is retained after a reboot.

"The configuration for Router R1 includes examples for its four interfaces: the serial link and connections to the three switches, while Router R2 has the same configuration but with different IP addresses."

"We configured the server to provide DHCP service, which allows it to automatically assign IP addresses to devices within its network. Each server is dedicated to its specific network, ensuring that the devices connected to that network receive appropriate configurations without conflicts. This setup enhances efficiency and management, as devices can join the network seamlessly without manual IP configuration. Additionally, the network is designed to be scalable, meaning it can easily accommodate future growth, such as adding more devices or expanding the network to include new segments, ensuring it remains functional and efficient as the needs of the organization evolve."

"We have configured each Access Point (AP) with a unique name (SSID) and password specific to its network, using WPA2 PSK for enhanced security. This setup allows devices, such as tablets, to connect easily by entering the SSID and password. By choosing WPA2 PSK, I ensure that only authorized devices can access the network, providing a secure wireless environment while allowing convenient access for users."

Passwords Configuration

Switches

Password (for line console and enable secret): hshs

Routers

Password (for line console and enable secret): hshshs

VTY (Virtual Terminal Lines)

Password: vthshs

Access Points Configuration

Access Point.N2 (Healthcare Staff Access Point)

Display Name: Access Point.N2

SSID: Healthcare Staff Access Point

PSK Pass Phrase: 999Hss##0101

Access Point.N5 (ResearchHub Wireless)

Display Name: Access Point.N5

SSID: ResearchHub Wireless

PSK Pass Phrase: !!HsS$::@#s%ps

Common Configuration for Both Access Points

Authentication: WPA2-PSK

Encryption Type: AES

5 GHz Channel: 112

Coverage Range (meters): 140.00

Hospital Data Management Network

- **Names of the Six Networks:**

1. **Administrative Network**
2. **Doctors and Nurses Network**
3. **Patient Data Storage Network**
4. **Medical Devices Network**
5. **Research and Advanced Data Storage Network**
6. **Facility Management Network**

- **Internal Sub-Network Names:**

Administrative Network:

Sub-Network 1: Finance and Accounting VLAN (VLAN 10)
Sub-Network 2: Regular Network
Patient Data Storage Network:

Sub-Network 1: Patient Data VLAN (VLAN 20)
Sub-Network 2: Pharmacy Network
Medical Devices Network:

Sub-Network 1: Medical Data Transfer Network
Sub-Network 2: Health Monitoring Network

- **Background on Packet Tracer**

Cisco Packet Tracer is a powerful network simulation tool used by professionals and students to design, configure, and troubleshoot complex network topologies. It offers a highly interactive environment where users can simulate real-world networking scenarios without the need for physical equipment. Developed by Cisco, Packet Tracer provides hands-on experience in configuring routers, switches, PCs, and other networking devices, making it an essential tool for learning networking concepts, designing scalable systems, and experimenting with network configurations.

In this project, Packet Tracer has been utilized to create a functional and comprehensive network model for a hospital environment. It allows us to test different network configurations, simulate device connections, and ensure proper communication between departments without the constraints of real-world hardware.

- **Background on the Hospital Data Management Project**

The Hospital Data Management Project is designed to address the growing need for efficient data flow, communication, and data storage in a hospital environment. Hospitals rely on a vast network of devices to ensure smooth operations, from administrative tasks to patient care. This project aims to create a secure, scalable, and well-organized network architecture that connects various departments, improves access to critical information, and supports essential hospital functions.

This network spans multiple departments, including:

Administration for managing patient appointments and hospital logistics.
Doctors and Nurses for accessing and updating patient medical records.
Patient Data Storage to safely store sensitive health information.
Medical Devices for transferring test results and other critical data.
Health Monitoring for real-time patient condition tracking.
Research and Advanced Data Storage for handling complex medical research and large datasets.
Facility Management to control hospital infrastructure, like lighting and security systems.
Each part of the network is carefully structured to ensure that the right devices and personnel have access to the data they need while maintaining high levels of security and flexibility for future growth.

By leveraging Packet Tracer, we are able to simulate this environment and ensure that the network performs reliably, is easily scalable, and can be protected from security threats.

Problem Facing the Hospital (Before)

Before implementing the Hospital Data Management Network, the hospital struggled with several operational inefficiencies and potential risks, including:

Disorganized Communication: Departments such as administration, medical staff, and research teams relied on separate systems, leading to poor communication and slower response times. This disconnection increased the risk of delays in critical decision-making, especially in emergencies.

Data Fragmentation: Patient records, test results, and research data were scattered across multiple devices and systems without centralized access. This disorganization made it challenging for healthcare providers to retrieve vital information quickly and accurately.

Security Risks: Without a unified network structure, sensitive data (such as patient health information and financial records) was vulnerable to breaches. The lack of proper security protocols increased the risk of unauthorized access, compromising both patient privacy and hospital integrity.

Limited Scalability: As the hospital expanded, the existing infrastructure could not support the growing number of devices or handle increased data flow. Each department operated in silos, making it difficult to integrate new systems without major disruptions.

Solution with the Hospital Data Management Network (After)

After implementing the Hospital Data Management Network, these challenges were effectively addressed:

Seamless Communication: The new network infrastructure connects all departments under a unified system, enabling seamless communication between administrative staff, medical professionals, and other teams. Data flows smoothly across all devices, allowing for faster decision-making and more efficient collaboration.

Centralized Data Management: By integrating all devices into a well-structured network, the hospital can now centrally manage patient records, medical tests, and research data. Medical staff can easily access critical information in real-time, improving patient care and ensuring that no data is lost or delayed.

Enhanced Security: The project ensures that sensitive information is protected through secure access points, passwords, and WPA2 encryption for wireless devices. Each department operates within its own network, preventing unauthorized access and securing patient health data and hospital financial records.

Scalability and Growth: The network is designed with scalability in mind. As the hospital grows, more devices, servers, and even new networks can be easily integrated without disrupting existing services. This flexibility ensures that the hospital can continue to expand while maintaining efficient operations.

Conclusion

The Hospital Data Management Network has revolutionized the hospital's infrastructure by streamlining communication, enhancing data access, and strengthening security measures. What was once a fragmented and inefficient system has been transformed into a unified, robust network that supports the hospital's daily operations and long-term goals. Designed to be scalable and adaptable, each network segment is equipped with dedicated servers and secure access points, ensuring seamless connectivity while protecting sensitive information. As the hospital continues to evolve and expand, this infrastructure is well-prepared to embrace new technologies and meet the growing demands of modern healthcare, positioning the hospital for future success.