BAHRIA UNIVERSITY, Karachi Campus

Department of Software Engineering

REPORT

Course Title: Computer Communication And Networks
Course Code: **CEL 223**
Course Instructor: Dr Osama **Class**: BSE- (A)
Lab Instructor: Engr. Asma Shaheen

PROJECT TITLE:

HOSPITAL MANAGEMENT SYSTEM

GROUP MEMBERS LIST:

S.NO	Enrollment	Name	Email
1	02-131212-075	Kashan Riaz	kashanriaz3@gmail.com
2	02-131212-069	Haseebullah	haseebullah1408@gmail.com
3	02-131212-020	Eima Nasir	eimanasir12@gmail.com

SUBMISSION DATE: 4th January 2023

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Introduction:

The Hospital Management System project, developed in Cisco Packet Tracer, integrates advanced network technologies such as Hierarchical Network Design, VLANs, Inter-VLAN Routing, DHCP, Port-Security, SSH, NAT Overload (PAT), ACLs, Site-to-Site IPsec VPN, WLAN setup, Static IPv4 Addressing, and Host Configurations. This comprehensive solution aims to enhance the efficiency and security of hospital operations by providing a robust and scalable network infrastructure. The system ensures logical network segmentation, secure remote access, dynamic IP address assignment, secure internet connectivity through NAT Overload, fine-grained traffic control with ACLs, and encrypted communication between different hospital locations. With a focus on seamless wireless connectivity, host configurations, and static IP assignments for critical devices, the project demonstrates the capabilities of Cisco Packet Tracer in creating a secure and resilient Hospital Management System that addresses the diverse needs of a modern healthcare facility.

1.2 Proposed Solution:

1.2.1. Basic Network Topology Design:

Application: Design a network infrastructure to connect different departments within the hospital, ensuring that each department has appropriate connectivity.

Implementation in Hospital Network: Plan and configure the network topology to connect departments like administration, patient care, and laboratories. Use routers and switches to create a hierarchical structure for efficient data flow.

1.2.2. VLAN Configuration:

Application: Implement VLANs to segregate network traffic between departments, enhancing security and network efficiency.

Implementation in Hospital Network: Create VLANs for different departments (e.g., administration, patient care, laboratories). Assign appropriate switch ports to each VLAN to ensure that devices within the same department share the same broadcast domain.

1.2.3. Routing Protocols:

Application: Configure dynamic routing protocols for communication between different departments.

Implementation in Hospital Network: Set up routing protocols (e.g., OSPF or EIGRP) to enable dynamic communication between routers in different hospital departments. This ensures efficient and automatic route selection.

1.2.4. Access Control Lists (ACLs):

Application: Use ACLs to control access to sensitive areas of the network and protect patient data.

Implementation in Hospital Network: Apply ACLs on routers or switches to control access to specific resources or limit communication between certain departments. This helps maintain the confidentiality and integrity of patient data.

1.2.5. DHCP (Dynamic Host Configuration Protocol):

Application: Set up DHCP servers to automatically assign IP addresses to devices in the hospital network.

Implementation in Hospital Network: Deploy DHCP servers to automate the IP address assignment process for devices in the hospital network. This ensures efficient IP management and reduces the likelihood of addressing conflicts.

1.2.6. Wireless Networking

Application: Configure a secure Wi-Fi network for hospital staff and guests.

Implementation in Hospital Network: Set up Wi-Fi access points, implement security protocols (WPA/WPA2), and create separate wireless networks for hospital staff and guests. This provides secure and controlled wireless access.

1.2.7 Inter-VLAN Routing:

Application: Implement routing between VLANs to enable communication between different hospital departments.

Implementation in Hospital Network: Configure inter-VLAN routing on routers to allow communication between devices in different VLANs. This ensures seamless connectivity while maintaining VLAN segmentation. 8. Security Features: Application: Configure basic security features, such as port security on switches, to protect against unauthorized access. Implementation in Hospital Network: Enable port security on switches to control which devices are allowed to connect to specific switch ports. This prevents unauthorized access and enhances network security.

1.3 Problem Statement:

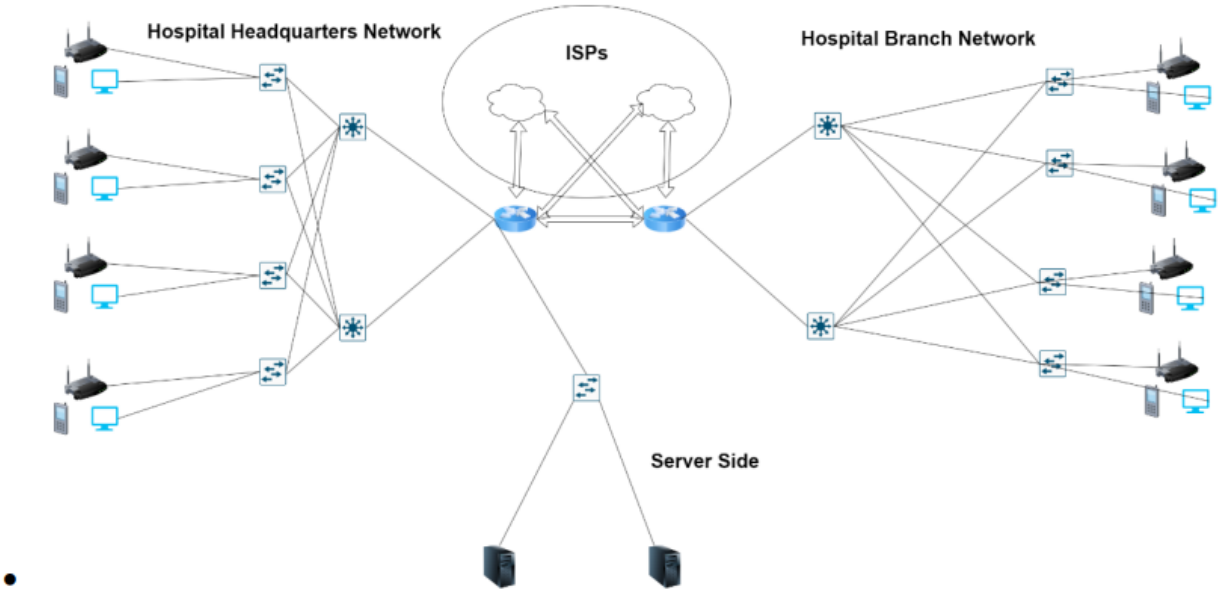
The smooth integration of technology is essential to improving patient care, increasing operational efficiency, and stimulating innovation in the dynamic field of healthcare. Acknowledging the urgent necessity of a dependable and cutting-edge infrastructure, we set out on an innovative path with our "Hospital Network System Design" project. We will use the Cisco Packet tracer and the technologies it offers to create a robust and efficient network system that can be used as a model for the real network used in the hospital.

1.4 Technologies Used:

- Cisco Packet Tracer

2. DESIGN DESCRIPTION

2.1. Work Flow Diagram:



2.2. Use Case Diagram:

2.3. Commands:

2.3.1. Assigning IP To Access Layer (Switch):

```
int gig1/0/1
no switchport
ip address 192.168.102.93 255.255.255.252
ex
do wr
```

2.3.2. Multi-layers Switch Initial Config:

```
en
config t
hostname BR-MultilayerSW1
enable password kashan
banner motd #Unauthorized Access not allowed!!!#
no ip domain lookup
line console 0
password kashan
login
exit
service password-encryption
ip domain name cisco.net
username admin password kashan
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit
do wr
```

2.3.3. OSPF Configuration:

```
ip routing
router ospf 10
network 192.168.101.128 0.0.0.31 area 0
network 192.168.101.160 0.0.0.31 area 0
network 192.168.101.192 0.0.0.31 area 0
network 192.168.101.224 0.0.0.31 area 0
network 192.168.102.0 0.0.0.31 area 0
network 192.168.102.32 0.0.0.31 area 0
network 192.168.102.96 0.0.0.3 area 0
ex
ip route 0.0.0.0 0.0.0.0 192.168.102.98
```

2.3.4. Router Initial Config:

```
en
```

```
config t
hostname BR-Router
enable password kashan
banner motd #Unauthorized Access not allowed!!!#
no ip domain lookup
line console 0
password kashan
login
exit
service password-encryption
ip domain name cisco.net
username admin password kashan
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit
do wr
```

2.3.5. Server Security:

```
int range fa0/3-24
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
ex
do wr
do sh port-security
```

2.3.6. Switch Initial Config:

```
en
config t
hostname BR-GWA-SW
enable password kashan
banner motd #Unauthorized Access not allowed!!!#
no ip domain lookup
line console 0
password kashan
login
exit
service password-encryption
```

2.3.7. VLAN Assignment Access Trunk ports:

```
vlan 130
name BR-GWA
exit
```

```
int range fa0/1-2
switchport mode trunk
exit
int range fa0/3-24
switchport mode access
switchport access vlan 130
```

2.3.8. VLAN Assignment MultiLayer:

```
vlan 80
vlan 90
vlan 100
vlan 110
vlan 120
vlan 130
int range gig1/0/2-7
switchport mode trunk
exit
```

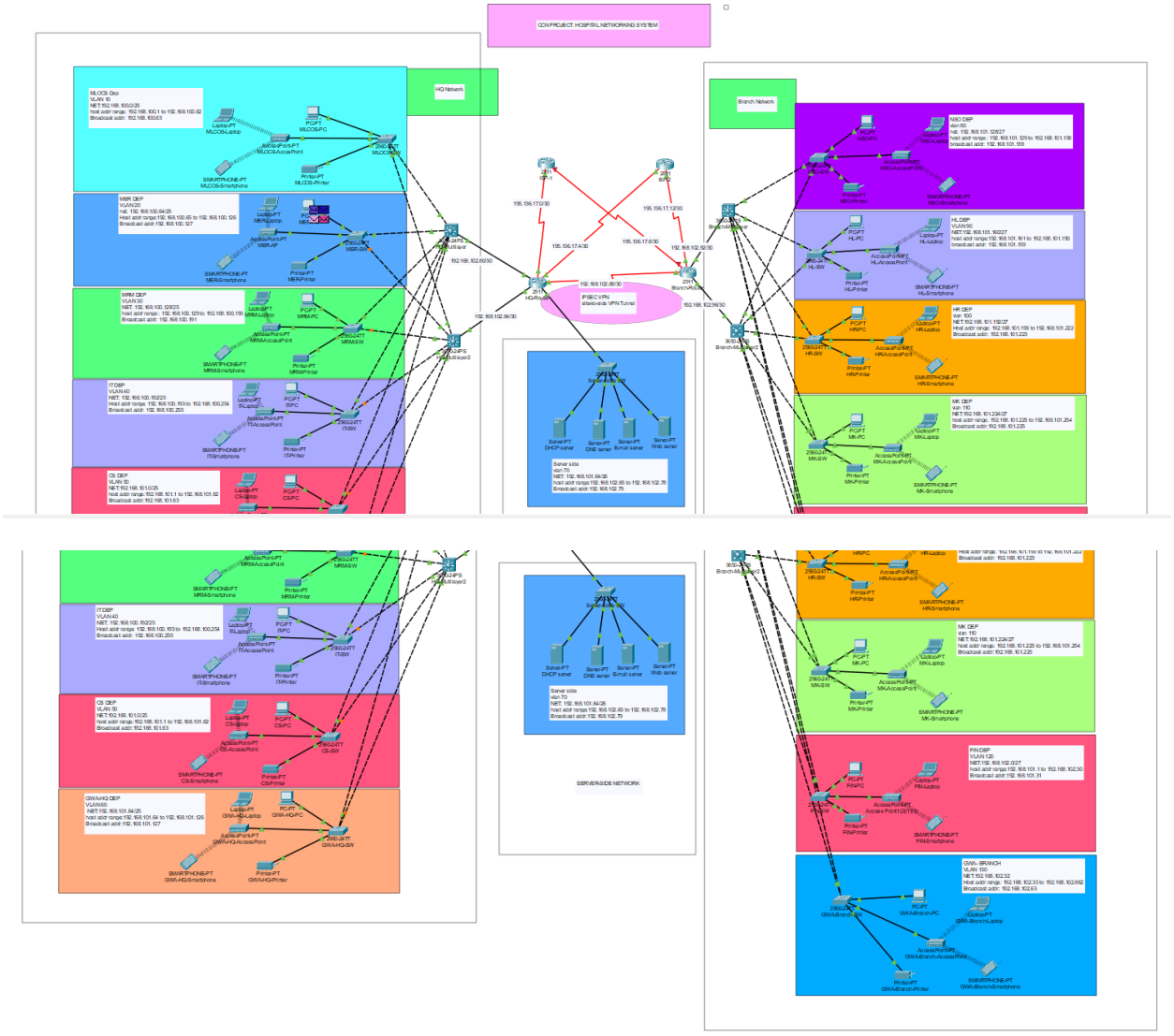
2.3.9. Setting IP on VLANS:

```
int vlan 80
ip address 192.168.101.129 255.255.255.224
ip helper-address 192.168.102.67
int vlan 90
ip address 192.168.101.161 255.255.255.224
ip helper-address 192.168.102.67
int vlan 100
ip address 192.168.101.193 255.255.255.224
ip helper-address 192.168.102.67
int vlan 110
ip address 192.168.101.255 255.255.255.224
ip helper-address 192.168.102.67
int vlan 120
ip address 192.168.102.1 255.255.255.224
ip helper-address 192.168.102.67
int vlan 130
ip address 192.168.102.33 255.255.255.224
ip helper-address 192.168.102.67
```

2.3.10. Router Configuration Of OSPF:

```
router ospf 10
network 195.136.17.4 0.0.0.3 area 0
network 195.136.17.12 0.0.0.3 area 0
ex
do wr
```

2.4. User Interface:



3. References:

- https://www.netacad.com/
- https://learningnetwork.cisco.com/
- https://community.cisco.com/
- https://www.academia.edu/39704348/SIMULATION_OF_AN_ENTERPRISE_NETWORK_WITH_THE_USE_OF_PACKET_TRACER_USING_VIRTUAL_LOCAL_AREA_NETWORK_VLAN_CONCEPT