Subash Subedi

[Email address]

Design and Implementation of a Hospital System Network Design (Project #7)

CCNA

Design and Implementation of a Hospital System Network Design (Project #7)

Melbourne Health Services is a well-established health provider in Australia, which offers health solutions and services to its clients. The institution operates in two locations within the same city, having the hospital headquarters 20km away from the branch hospital. Therefore, it has the following departments within its main headquarters Medical Lead Operation & Consultancy Services (MLOCS), Medical Emergency and Reporting (MER), Medical Records Management (MRM), Information Technology (IT), and Customer Service (CS). The hospital branch was designed to share the workload with the headquarters hence it contains the following departments: Nurses & Surgery Operations (NSO), Hospital Labs (HL), Human Resources (HR), Marketing (MK), and Finance (FIN). Each location is also expected to have a Guest/Waiting area (GWA) for patients or visitors.

So far, the network has been using third-party services to maintain its IT services. The senior management has decided to own their network infrastructure including Local Area Network (LAN), Wide Area Network (WAN), and a Server-Side site that is expected to be located separately at the headquarters and is connected to the HQ Router with an access switch. The server-side site will host the DHCP server, DNS Server, Web Server, and Email Server. The network is expected to be cost-effective and observes the information security rule of the CIA (Confidentiality, Integrity, and Availability).

The network is expected to have a hierarchical model with two already purchased Core routers (one at HQ and one Branch) each connecting two subscribed ISPs. Due to security requirements, it has been decided that all the departments will be on a separate network segment within the same local area network.

You have been hired as a network security engineer to design the network according to the requirements set by the senior management. You will consult an appropriate robust network design model to meet the design requirements. You will also implement Access Control Lists and Virtual Private Network (VPN) to enable secure communication considering security and network performance factors paramount to safeguarding Confidentiality, Integrity, and Availability of data and communication. The network security policy will comprehensively dictate the user's access to each site using Access Control List (ACL).

* Use Cisco Packet Tracer to design and implement the network solution.
* Use a hierarchical model providing redundancy in the network.
* Both HQ and Branch routers are expected to be connected using a serial connection.
* As mentioned earlier, for network cost-effectiveness, each site is expected to have one core router, two multilayer switches, and several access switches connecting each department.
* Each department is required to have a wireless network for the users.
* Every department in HQ is estimated to have around 60 users while in Branch it is estimated to be 30 users.
* Each department should be in a different VLAN and a different subnetwork.
* Provided a base network of 192.168.100.0 and carried out subnetting to allocate the correct number of IP addresses to each department.
* The company network is connected to the static, public IP addresses (Internet Protocol) 195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30, and 195.136.17.12/30 connected to the two Internet providers.
* Configure basic device settings such as hostnames, console password, enable password, banner messages, and disable IP domain lookup.
* Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
* The Multilayer switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.
* All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located in the server room.
* Devices in the server room are to be allocated IP addresses statically.
* Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
* Configure default static routing to enable routers and multilayer switches to forward any traffic that does not match routing table entries. Use next-hop IP addresses.
* Configure SSH in all the routers and layer three switches for remote login.
* Configure port-security for the server site department switch to allow only one device to connect to a switch port, use sticky method to obtain mac-address and violation mode shutdown.
* Configure the extended ACL rule together with site-to-site VPN (IPSec VPN) to create a tunnel and encrypt communication between HQ and the Branch network.
* Configure PAT to use the respective outbound router interface IPv4 address and implement the necessary ACL rule.
* Test Communication, ensure everything configured is working as expected.

Table of Contents

[Technologies Implemented 4](#_Toc200665003)

[1. Creating a network topology using Cisco Packet Tracer. Hierarchical Network Design. 4](#_Toc200665004)

[2. Connecting Networking devices with Correct cabling. 4](#_Toc200665005)

[3. Configuring Basic device settings. 4](#_Toc200665006)

[4. Creating VLANs and assigning ports VLAN numbers. 4](#_Toc200665007)

[5. Subnetting and IP Addressing. 4](#_Toc200665008)

[6. Configuring Inter-VLAN Routing on the Multilayer switches (Switch Virtual Interface). 4](#_Toc200665009)

[7. Configuring Dedicated DHCP Server device to provide dynamic IP allocation. 4](#_Toc200665010)

[8. Configuring SSH for secure Remote access. 4](#_Toc200665011)

[9. Configuring OSPF as the routing protocol. 4](#_Toc200665012)

[10. Configuring NAT Overload (Port Address Translation PAT). 4](#_Toc200665013)

[11. Configuring Site-to-Site IPsec VPN. 4](#_Toc200665014)

[12. Configuring standard and extended Access Control Lists ACL. 4](#_Toc200665015)

[13. Configuring switchport security or Port-Security on the switches. 4](#_Toc200665016)

[14. Configuring WLAN or wireless network (Cisco Access Point). 4](#_Toc200665017)

[15. Host Device Configurations. 4](#_Toc200665018)

[16. Configuring ISP routers. 4](#_Toc200665019)

[17. Test and Verifying Network Communication. 4](#_Toc200665020)

# Technologies Implemented

## Creating a network topology using Cisco Packet Tracer. Hierarchical Network Design.

## Connecting Networking devices with Correct cabling.

## Configuring Basic device settings.

|  |  |
| --- | --- |
| **MAIN HO PRIMARY ROUTER**  enable  configure terminal  hostname HO-PRIMARY-ROUTER  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **SECONDARY CORE PRIMARY ROUTER**  enable  configure terminal  hostname BRANCH-PRIMARY-ROUTER  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |
| **MAIN HO SECONDARY ROUTER**  enable  configure terminal  hostname HO-SECONDARY-ROUTER  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **SECONDARY CORE PRIMARY ROUTER**  enable  configure terminal  hostname BRANCH-SECONDARY-ROUTER  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |

|  |  |
| --- | --- |
| **PRIMARY HO MULTILAYER SWITCH**  enable  configure terminal  hostname PRIMARY-HO-MULTILAYER-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **PRIMARY BRANCH MULTILAYER SWITCH**  enable  configure terminal  hostname PRIMARY-BRANCH-MULTILAYER-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |
| **SECONDARY HO MULTILAYER SWITCH**  enable  configure terminal  hostname SECONDARY-HO-MULTILAYER-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **SECONDARY BRANCH MULTILAYER SWITCH**  enable  configure terminal  hostname SECONDARY-BRANCH-MULTILAYER-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |

|  |  |
| --- | --- |
| **MLCOS SWITCH**  enable  configure terminal  hostname MLCOS-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **NSO SWITCH**  enable  configure terminal  hostname NSO-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |
| **MER SWITCH**  enable  configure terminal  hostname MER-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **HL SWITCH**  enable  configure terminal  hostname HL-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |
| **MRM SWITCH**  enable  configure terminal  hostname MRM-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **HR SWITCH**  enable  configure terminal  hostname HR-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |
| **IT SWITCH**  enable  configure terminal  hostname IT-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **MK SWITCH**  enable  configure terminal  hostname MK-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |
| **CS SWITCH**  enable  configure terminal  hostname CS-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **FIN ROOM SWITCH**  enable  configure terminal  hostname FIN-ROOM-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |
| **GWA SWITCH**  enable  configure terminal  hostname GWA-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr | **BR-GWA SWITCH**  enable  configure terminal  hostname BR-GWA-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |
|  | **Server Side SWITCH**  enable  configure terminal  hostname Server-Side-SWITCH  do clock set 00:00:00 1 JANUARY 2025  banner motd $ ONLY AUTHORIZED ACCESS $  service password-encryption  enable secret cisco  username cisco secret cisco  no ip domain lookup  line console 0  motd-banner  password cisco  exec-timeout 5  login  exit  do wr |

## Creating VLANs and assigning ports VLAN numbers.

|  |  |
| --- | --- |
| **PRIMARY & SECONDARY HO MULTILAYER SWITCH**  enable  configure terminal  vlan 999  name NATIVE-VLAN  exit  vlan 210  name MLOCS-DEPARTMENT  exit  interface GigabitEthernet 1/0/1  description \*\*THIS IS TRUNK INTERFACE OF Medical Lead Operation & Consultancy Services (MLOCS) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 210  switchport nonegotiate  exit  vlan 240  name IT-DEPARTMENT  exit  interface GigabitEthernet 1/0/2  description \*\*THIS IS TRUNK INTERFACE OF Information Technology (IT) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 240  switchport nonegotiate  exit  vlan 260  name GWA-DEPARTMENT  exit  interface GigabitEthernet 1/0/3  description \*\*THIS IS TRUNK INTERFACE OF Guest/Waiting Area (GWA) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 260  switchport nonegotiate  exit  vlan 220  name MER-DEPARTMENT  exit  interface GigabitEthernet 1/0/4  description \*\*THIS IS TRUNK INTERFACE OF Medical Emergency and Reporting (MER) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 220  switchport nonegotiate  exit  vlan 230  name MRM-DEPARTMENT  exit  interface GigabitEthernet 1/0/5  description \*\*THIS IS TRUNK INTERFACE OF Medical Records Management (MRM) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 230  switchport nonegotiate  exit  vlan 250  name CS-DEPARTMENT  exit  interface GigabitEthernet 1/0/6  description \*\*THIS IS TRUNK INTERFACE OF Customer Service (CS) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 250  switchport nonegotiate  exit  do wr | **PRIMARY & SECONDARY BRANCH MULTILAYER SWITCH**  enable  configure terminal  vlan 999  name NATIVE-VLAN  exit  vlan 270  name NSO-DEPARTMENT  exit  interface GigabitEthernet 1/0/1  description \*\*THIS IS TRUNK INTERFACE OF Nurses & Surgery Operations (NSO) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 270  switchport nonegotiate  exit  vlan 280  name HL-DEPARTMENT  exit  interface GigabitEthernet 1/0/2  description \*\*THIS IS TRUNK INTERFACE OF Hospital Labs (HL) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 280  switchport nonegotiate  exit  vlan 290  name HR-DEPARTMENT  exit  interface GigabitEthernet 1/0/3  description \*\*THIS IS TRUNK INTERFACE OF Human Resources (HR) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 290  switchport nonegotiate  exit  vlan 300  name MK-DEPARTMENT  exit  interface GigabitEthernet 1/0/4  description \*\*THIS IS TRUNK INTERFACE OF Marketing (MK) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 300  switchport nonegotiate  exit  vlan 310  name FIN-DEPARTMENT  exit  interface GigabitEthernet 1/0/5  description \*\*THIS IS TRUNK INTERFACE OF Finance (FIN) DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 310  switchport nonegotiate  exit  vlan 320  name BR-GWA-DEPARTMENT  exit  interface GigabitEthernet 1/0/6  description \*\*THIS IS TRUNK INTERFACE OF BR-GWA DEPARTMENT \*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 320  switchport nonegotiate  exit  do wr |

|  |  |
| --- | --- |
| **MLCOS SWITCH**  enable  configure terminal  vlan 210  name MLOCS-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR MLOCS DEPARTMENT\*\*  switchport mode access  switchport access vlan 210  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 210  switchport nonegotiate  exit  interface vlan 210  description \*\*MLOCS DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.200.62 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.200.1  do wr | **NSO SWITCH**  enable  configure terminal  vlan 270  name NSO-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR Nurses & Surgery Operations (NSO) DEPARTMENT\*\*  switchport mode access  switchport access vlan 270  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 270  switchport nonegotiate  exit  interface vlan 270  description \*\*NSO DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.21.190 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.21.129  do wr |
| **MER SWITCH**  enable  configure terminal  vlan 220  name MER-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR MER DEPARTMENT\*\*  switchport mode access  switchport access vlan 220  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 220  switchport nonegotiate  exit  interface vlan 220  description \*\*MER DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.20.126 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.20.65  do wr | **HL SWITCH**  enable  configure terminal  vlan 280  name HL-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR Hospital Labs (HL) DEPARTMENT\*\*  switchport mode access  switchport access vlan 280  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 280  switchport nonegotiate  exit  interface vlan 280  description \*\*HL DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.21.254 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.21.193  do wr |
| **MRM SWITCH**  enable  configure terminal  vlan 230  name MRM-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR MRM DEPARTMENT\*\*  switchport mode access  switchport access vlan 230  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 230  switchport nonegotiate  exit  interface vlan 230  description \*\*MRM DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.20.190 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.20.129  do wr | **HR SWITCH**  enable  configure terminal  vlan 290  name HR-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR Human Resources (HR) DEPARTMENT\*\*  switchport mode access  switchport access vlan 290  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 290  switchport nonegotiate  exit  interface vlan 290  description \*\*HR DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.22.62 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.22.1  do wr |
| **IT SWITCH**  enable  configure terminal  vlan 240  name IT-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR IT DEPARTMENT\*\*  switchport mode access  switchport access vlan 240  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 240  switchport nonegotiate  exit  interface vlan 240  description \*\*IT DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.20.254 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.20.193  do wr | **MK SWITCH**  enable  configure terminal  vlan 300  name MK-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR Marketing (MK) DEPARTMENT\*\*  switchport mode access  switchport access vlan 300  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 300  switchport nonegotiate  exit  interface vlan 300  description \*\*MK DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.22.126 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.22.65  do wr |
| **CS SWITCH**  enable  configure terminal  vlan 250  name CS-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR CS DEPARTMENT\*\*  switchport mode access  switchport access vlan 250  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 250  switchport nonegotiate  exit  interface vlan 250  description \*\*CS DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.21.62 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.21.1  do wr | **FIN ROOM SWITCH**  enable  configure terminal  vlan 310  name FIN-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR Finance (FIN) DEPARTMENT\*\*  switchport mode access  switchport access vlan 310  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 310  switchport nonegotiate  exit  interface vlan 310  description \*\*FIN DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.22.190 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.22.129  do wr |
| **GWA SWITCH**  enable  configure terminal  vlan 260  name GWA-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR Guest/Waiting area (GWA) DEPARTMENT\*\*  switchport mode access  switchport access vlan 260  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 260  switchport nonegotiate  exit  interface vlan 260  description \*\*GWA DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.21.126 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.21.65  do wr | **BR-GWA SWITCH**  enable  configure terminal  vlan 320  name BR-GWA-DEPARTMENT  exit  vlan 999  name NATIVE-VLAN  exit  interface range FastEthernet 0/1-24  description \*\*ACCESS PORTS FOR BR-GWA DEPARTMENT\*\*  switchport mode access  switchport access vlan 320  no shutdown  exit  interface range GigabitEthernet 0/1-2  description \*\*TRUNK LINKS\*\*  switchport mode trunk  switchport trunk native vlan 999  switchport trunk allowed vlan 320  switchport nonegotiate  exit  interface vlan 320  description \*\*BR-GWA DEPARTMENT VLAN INTERFACE\*\*  ip address 172.16.22.254 255.255.255.192  no shutdown  exit  ip default-gateway 172.16.22.193  do wr |
|  | **Server Side SWITCH**  enable  configure terminal  vlan 999  name NATIVE-VLAN  exit  vlan 330  name SERVER-SIDE-NETWORK-DEPARTMENT  exit  interface range GigabitEthernet 1/0/1-13  description \*\*ACCESS PORTS FOR OF Server Side Network (SERVER) DEPARTMENT \*\*  switchport mode access  switchport access vlan 320  no shutdown  exit  do wr |

## Subnetting and IP Addressing.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **DEPARTMENT** | **NETWORK ID** | **GATEWAYS / STARTING IP** | **LAST IP / VLAN IP** | **BROADCAST ID** | **SUBNET MASK** |
| **HEAD**  **OFFICE** | **MEDICAL LEAD OPERATION & CONSULTANCY SERVICES (MLOCS) DEPARTMENT** | 172.16.200.0 | 172.16.200.1 | 172.16.200.62 | 172.16.200.63 | 255.255.255.192 |
| **MEDICAL EMERGENCY AND REPORTING (MER) DEPARTMENT** | 172.16.20.64 | 172.16.20.65 | 172.16.20.126 | 172.16.20.127 | 255.255.255.192 |
| **MEDICAL RECORDS MANAGEMENT (MRM) DEPARTMENT** | 172.16.20.128 | 172.16.20.129 | 172.16.20.190 | 172.16.20.191 | 255.255.255.192 |
| **INFORMATION TECHNOLOGY (IT) DEPARTMENT** | 172.16.20.192 | 172.16.20.193 | 172.16.20.254 | 172.16.20.255 | 255.255.255.192 |
| **CUSTOMER SERVICE (CS) DEPARTMENT** | 172.16.21.0 | 172.16.21.1 | 172.16.21.62 | 172.16.21.63 | 255.255.255.192 |
| **HO GUEST/WAITING AREA (GWA) DEPARTMENT** | 172.16.21.64 | 172.16.21.65 | 172.16.21.126 | 172.16.21.127 | 255.255.255.192 |
| **BRANCH** | **NURSES & SURGERY OPERATIONS (NSO) DEPARTMENT** | 172.16.21.128 | 172.16.21.129 | 172.16.21.190 | 172.16.21.191 | 255.255.255.192 |
| **HOSPITAL LABS (HL) DEPARTMENT** | 172.16.21.192 | 172.16.21.193 | 172.16.21.254 | 172.16.21.255 | 255.255.255.192 |
| **HUMAN RESOURCE (HR) DEPARTMENT** | 172.16.22.0 | 172.16.22.1 | 172.16.22.62 | 172.16.22.63 | 255.255.255.192 |
| **MARKETING (MK) DEPARTMENT** | 172.16.22.64 | 172.16.22.65 | 172.16.22.126 | 172.16.22.127 | 255.255.255.192 |
| **FINANCE (FIN) DEPARTMENT** | 172.16.22.128 | 172.16.22.129 | 172.16.22.190 | 172.16.22.191 | 255.255.255.192 |
| **Guest/Waiting area (GWA) DEPARTMENT** | 172.16.22.192 | 172.16.22.193 | 172.16.22.254 | 172.16.22.255 | 255.255.255.192 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **R1-ROUTER** | Gig 0/0/0 | 172.16.3.145 | 255.255.255.252 | M1-MULTILAYER-SWITCH  Gig 1/0/1 |
| Gig 0/0/1 | 172.16.3.154 | 255.255.255.252 | M2-MULTILAYER-SWITCH  Gig 1/0/1 |
| **R2-ROUTER** | Gig 0/0/0 | 172.16.3.149 | 255.255.255.252 | M1-MULTILAYER-SWITCH  Gig 1/0/2 |
| Gig 0/0/1 | 172.16.3.157 | 255.255.255.252 | M2-MULTILAYER-SWITCH  Gig 1/0/2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **M1-MULTILAYER-SWITCH** | Gig 1/0/1 | 172.16.3.146 | 255.255.255.252 | R1-ROUTER  Gig 0/0/0 |
| Gig 1/0/2 | 172.16.3.150 | 255.255.255.252 | R2-ROUTER  Gig 0/0/0 |
| **M2-MULTILAYER-SWITCH** | Gig 1/0/1 | 172.16.3.153 | 255.255.255.252 | R1-ROUTER  Gig 0/0/1 |
| Gig 1/0/2 | 172.16.3.158 | 255.255.255.252 | R1-ROUTER  Gig 0/0/2 |

## Configuring Inter-VLAN Routing on the Multilayer switches (Switch Virtual Interface).

## Configuring Dedicated DHCP Server device to provide dynamic IP allocation.

## Configuring SSH for secure Remote access.

|  |  |
| --- | --- |
| **MAIN HO PRIMARY ROUTER**  enable  configure terminal    ip domain-name sales.com  crypto key generate rsa    1024    ip ssh version 2  username cisco secret cisco  username admin secret admin    line vty 0 15  login local  transport input ssh  exit    ip ssh time-out 60  ip ssh authentication-retries 3  do wr | **SECONDARY CORE PRIMARY ROUTER**  enable  configure terminal  do wr |
| **MAIN HO SECONDARY ROUTER**  enable  configure terminal  do wr | **SECONDARY CORE PRIMARY ROUTER**  enable  configure terminal  do wr |

|  |  |
| --- | --- |
| **PRIMARY HO MULTILAYER SWITCH**  enable  configure terminal  do wr | **PRIMARY BRANCH MULTILAYER SWITCH**  enable  configure terminal  do wr |
| **SECONDARY HO MULTILAYER SWITCH**  enable  configure terminal  do wr | **SECONDARY BRANCH MULTILAYER SWITCH**  enable  configure terminal  do wr |

|  |  |
| --- | --- |
| **MLCOS SWITCH**  enable  configure terminal  do wr | **NSO SWITCH**  enable  configure terminal  do wr |
| **MER SWITCH**  enable  configure terminal    ip domain-name sales.com  crypto key generate rsa    1024    ip ssh version 2  username cisco secret cisco  username admin secret admin    line vty 0 15  login local  transport input ssh  exit    ip ssh time-out 60  ip ssh authentication-retries 3  do wr | **HL SWITCH**  enable  configure terminal  do wr |
| **MRM SWITCH**  enable  configure terminal  do wr | **HR SWITCH**  enable  configure terminal  do wr |
| **IT SWITCH**  enable  configure terminal  do wr | **MK SWITCH**  enable  configure terminal  do wr |
| **CS SWITCH**  enable  configure terminal  do wr | **FIN ROOM SWITCH**  enable  configure terminal  do wr |
| **GWA SWITCH**  enable  configure terminal  do wr | **BR-GWA SWITCH**  enable  configure terminal  do wr |
|  | **Server Side SWITCH**  enable  configure terminal  do wr |

## Configuring OSPF as the routing protocol.

|  |  |
| --- | --- |
| **MAIN HO PRIMARY ROUTER**  enable  configure terminal  do wr | **SECONDARY CORE PRIMARY ROUTER**  enable  configure terminal  do wr |
| **MAIN HO SECONDARY ROUTER**  enable  configure terminal  do wr | **SECONDARY CORE PRIMARY ROUTER**  enable  configure terminal  do wr |

|  |  |
| --- | --- |
| **PRIMARY HO MULTILAYER SWITCH**  enable  configure terminal  do wr | **PRIMARY BRANCH MULTILAYER SWITCH**  enable  configure terminal  do wr |
| **SECONDARY HO MULTILAYER SWITCH**  enable  configure terminal  do wr | **SECONDARY BRANCH MULTILAYER SWITCH**  enable  configure terminal  do wr |

|  |  |
| --- | --- |
| **MLCOS SWITCH**  enable  configure terminal  do wr | **NSO SWITCH**  enable  configure terminal  do wr |
| **MER SWITCH**  enable  configure terminal  do wr | **HL SWITCH**  enable  configure terminal  do wr |
| **MRM SWITCH**  enable  configure terminal  do wr | **HR SWITCH**  enable  configure terminal  do wr |
| **IT SWITCH**  enable  configure terminal  do wr | **MK SWITCH**  enable  configure terminal  do wr |
| **CS SWITCH**  enable  configure terminal  do wr | **FIN ROOM SWITCH**  enable  configure terminal  do wr |
| **GWA SWITCH**  enable  configure terminal  do wr | **BR-GWA SWITCH**  enable  configure terminal  do wr |
|  | **Server Side SWITCH**  enable  configure terminal  do wr |

## Configuring NAT Overload (Port Address Translation PAT).

## Configuring Site-to-Site IPsec VPN.

## Configuring standard and extended Access Control Lists ACL.

## Configuring switchport security or Port-Security on the switches.

## Configuring WLAN or wireless network (Cisco Access Point).

## Host Device Configurations.

## Configuring ISP routers.

## Test and Verifying Network Communication.