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 CORE PRIMARY ROUTER**  enable  configure terminal  hostname MAIN-CORE-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 SECONDARY-CORE-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 |

|  |  |
| --- | --- |
| **FIRST MULTILAYER SWITCH**  enable  configure terminal  hostname M1-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 | **SECOND MULTILAYER SWITCH**  enable  configure terminal  hostname M2-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 | **ACCOUNT SWITCH**  enable  configure terminal  hostname ACCOUNT-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 |
| **MARKETING SWITCH**  enable  configure terminal  hostname MARKETING-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 | **ADMIN SWITCH**  enable  configure terminal  hostname ADMIN-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 | **PUBLIC RELATIONS SWITCH**  enable  configure terminal  hostname PUBLIC-RELATIONS-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 |
| **LOGISTIC SWITCH**  enable  configure terminal  hostname LOGISTIC-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 | **ICT SWITCH**  enable  configure terminal  hostname ICT-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 |
| **FINANCE SWITCH**  enable  configure terminal  hostname FINANCE-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 ROOM SWITCH**  enable  configure terminal  hostname SERVER-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 |

## Creating VLANs and assigning ports VLAN numbers.

## Subnetting and IP Addressing.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Floor** | **DEPARTMENT** | **NETWORK ID** | **GATEWAYS / STARTING IP** | **LAST IP / VLAN IP** | **BROADCAST ID** | **SUBNET MASK** |
| **1st Floor** | **SALES DEPARTMENT** | 172.16.1.0/26 | 172.16.1.1 | 172.16.1.62 | 172.16.1.63 | 255.255.255.192 |
| **MARKETING DEPARTMENT** | 172.16.1.64/26 | 172.16.1.65 | 172.16.1.126 | 172.16.1.127 | 255.255.255.192 |
| **2nd Floor** | **HR DEPARTMENT** | 172.16.1.128/26 | 172.16.1.129 | 172.16.1.190 | 172.16.1.191 | 255.255.255.192 |
| **LOGISTICS & STORE DEPARTMENT** | 172.16.1.192/26 | 172.16.1.193 | 172.16.1.254 | 172.16.1.255 | 255.255.255.192 |
| **3rd Floor** | **FINANCE DEPARTMENT** | 172.16.2.0/26 | 172.16.2.1 | 172.16.2.62 | 172.16.2.63 | 255.255.255.192 |
| **ACCOUNT DEPARTMENT** | 172.16.2.64/26 | 172.16.2.65 | 172.16.2.126 | 172.16.2.127 | 255.255.255.192 |
| **ADMIN DEPARTMENT** | 172.16.2.128/26 | 172.16.2.129 | 172.16.2.190 | 172.16.2.191 | 255.255.255.192 |
| **PUBLIC RELATIONS**  **DEPARTMENT** | 172.16.2.192/26 | 172.16.2.193 | 172.16.2.254 | 172.16.2.255 | 255.255.255.192 |
| **4th Floor** | **ICT DEPARTMENT** | 172.16.3.0/25 | 172.16.3.1 | 172.16.3.126 | 172.16.3.127 | 255.255.255.128 |
| **SERVER DEPARTMENT** | 172.16.3.128/28 | 172.16.3.129 | 172.16.3.142 | 172.16.3.143 | 255.255.255.240 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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.

## Configuring OSPF as the routing protocol.

## 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.