Hospital System Network Design

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 branch hospital was designed to share the workloads with the headquarters hence it contains the following departments; Nurses & Surgery Operations (NSO), Hospital Labs (HL), Human resource (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 was 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 to 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 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 carry 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.

Technologies Implemented

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Subnetting and IP Addressing.
7. Configuring Inter-VLAN Routing on the Multilayer switches (Switch Virtual Interface).
8. Configuring Dedicated DHCP Server device to provide dynamic IP allocation.
9. Configuring SSH for secure Remote access.
10. Configuring OSPF as the routing protocol.
11. Configuring NAT Overload (Port Address Translation PAT).
12. Configuring Site-to-Site IPsec VPN.
13. Configuring standard and extended Access Control Lists ACL.
14. Configuring switchport security or Port-Security on the switches.
15. Configuring WLAN or wireless network (Cisco Access Point).
16. Host Device Configurations.
17. Configuring ISP routers.
18. Test and Verifying Network Communication.