Table of content

1.0 Network Design.....1
1.1 IP Addressing Scheme..... 1
1.2 Internet Service Providers (ISPs)..... 2
1.3 Wireless Network (Wi-Fi)..... 2
1.4 Voice over IP (VoIP)..... 2
1.5 Virtual Local Area Networks (VLANs)..... 2
1.6 Subnetting..... 2
1.7 Inter-VLAN Routing..... 2
1.8 Core Switches..... 3
1.9 Dynamic Host Configuration Protocol (DHCP) Server..... 3
1.10 Cisco 2811 Router..... 3
1.11 Static Addressing..... 3
1.12 Telephony Services..... 3
1.13 Routing Protocol..... 4
1.14 Switchport Security..... 4
1.15 Secure Shell (SSH)..... 4
1.16 Standard Access Control List (ACL) for SSH..... 4
1.17 Network Address Translation (NAT)..... 4
2.0 Implementation and Documentation..... 4
2.1 Network Layout..... 5
2.2 IP Addressing..... 5

1.0 Network Design

1.1 IP Addressing Scheme

The following IP address ranges have been allocated for the network:

- **192.168.20.0/24** for Data Network
- **10.10.10.0/24** for Voice Network
- **190.200.100.0/24** for Public IP Addresses

1.2 Internet Service Providers (ISPs)

The network will be connected to at least two ISPs for redundancy and failover purposes. This will ensure high availability and uninterrupted internet connectivity.

1.3 Wireless Network (Wi-Fi)

Each department will have wireless internet access provided through wireless access points (APs). The APs will be connected to the respective department's VLAN and will provide wireless connectivity to authorized devices.

1.4 Voice over IP (VoIP)

Each department will have IP phones, and users will be able to call each other within the organization using the VoIP system. The VoIP network will use the **10.10.10.0/24** subnet.

1.5 Virtual Local Area Networks (VLANs)

Each department will be assigned a separate VLAN and subnetwork. VLANs will be used to logically segment the network, providing better security, broadcast control, and network management.

1.6 Subnetting

The network will be divided into smaller subnets to accommodate the required number of devices in each department. Proper subnet planning and IP address allocation will be performed to ensure efficient use of available address space.

1.7 Inter-VLAN Routing

Multilayer switches will be configured for inter-VLAN routing, allowing devices in different VLANs and departments to communicate with each other. This will be achieved by configuring the multilayer switches with appropriate routing protocols and routing tables.

1.8 Core Switches

Multilayer switches will serve as the core switches, performing both switching and routing functions. These switches will be assigned IP addresses for management and routing purposes.

1.9 Dynamic Host Configuration Protocol (DHCP) Server

A dedicated DHCP server will be located in the server-side network. All devices in the network (except IP phones) will obtain their IP addresses dynamically from this DHCP server.

1.10 Cisco 2811 Router

A Cisco 2811 router will be used to support telephony services, ensuring compatibility with the VoIP system.

1.11 Static Addressing

Devices in the server room will be configured with static IP addresses for better control and management.

1.12 Telephony Services

VoIP services will be configured on the gateway router, and dial numbers will be allocated for the IP phones.

1.13 Routing Protocol

The Open Shortest Path First (OSPF) routing protocol will be used to advertise routes both on the routers and multilayer switches. OSPF will ensure dynamic routing and efficient path selection within the network.

1.14 Switchport Security

Port security will be configured on the server site department switch to allow only one device per switch port. The sticky method will be used to obtain the MAC address of the connected device, and the violation mode will be set to shutdown to prevent unauthorized access.

1.15 Secure Shell (SSH)

SSH will be configured on all routers and multilayer switches to allow secure remote login for administrative tasks.

1.16 Standard Access Control List (ACL) for SSH

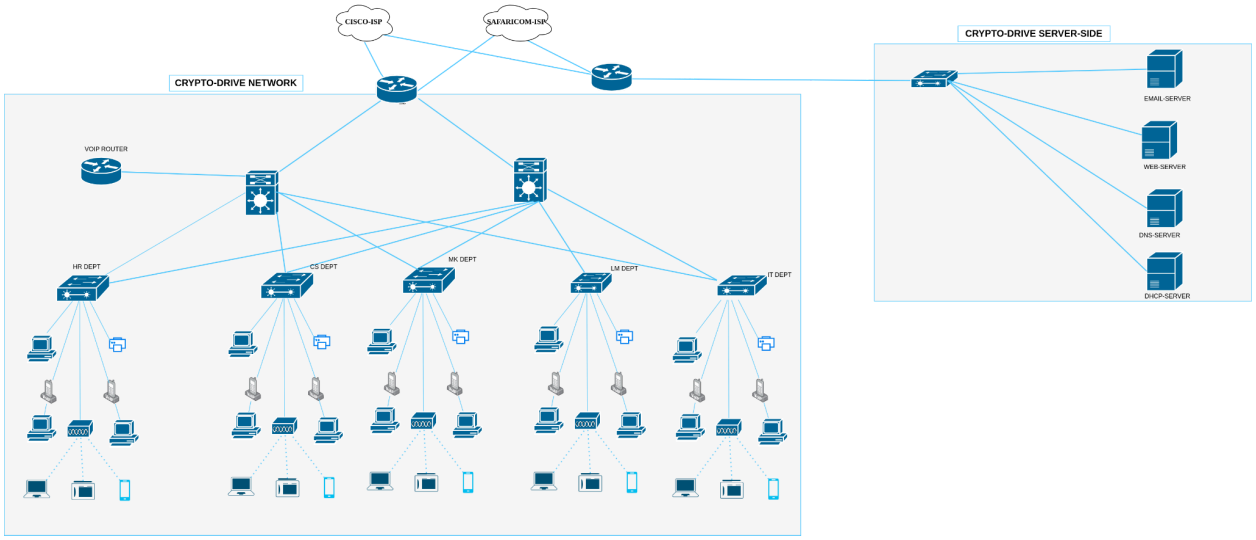
A standard ACL will be configured on the line VTY (virtual terminal lines) to restrict remote SSH access to the IT department only. This will enhance security by limiting administrative access to authorized personnel.

1.17 Network Address Translation (NAT)

Port Address Translation (PAT) will be configured on the outbound router interface to translate multiple internal IP addresses to a single public IP address. This will conserve public IP address usage and provide security by hiding the internal IP addresses from the public internet.

2.0 Implementation and Documentation

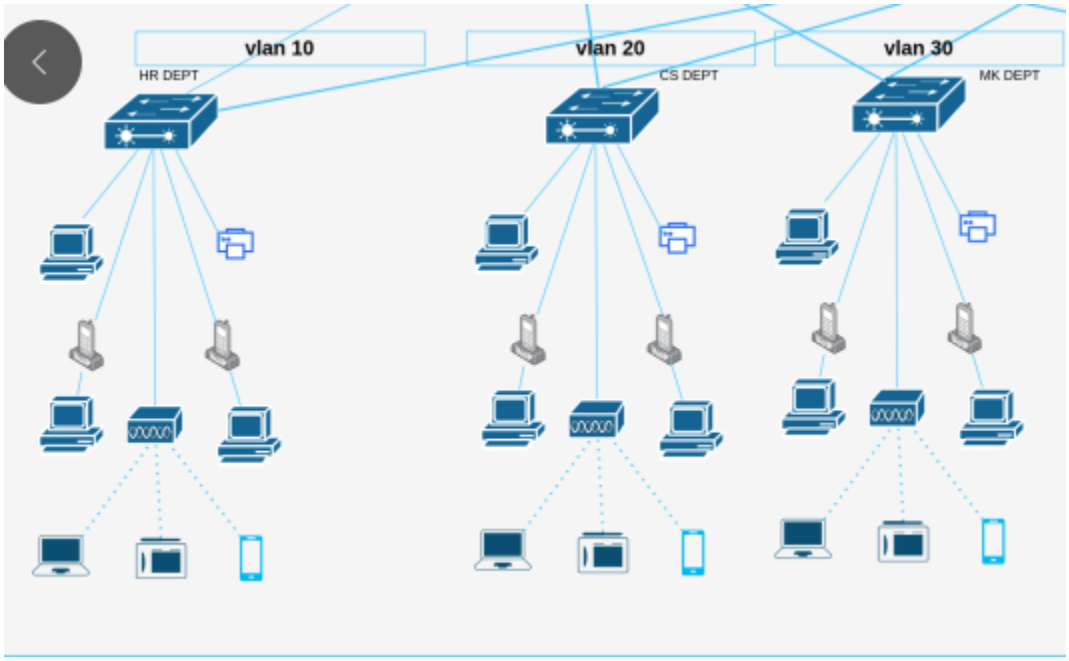
2.1 Network Layout



2.2 IP Addressing

1st Floor:

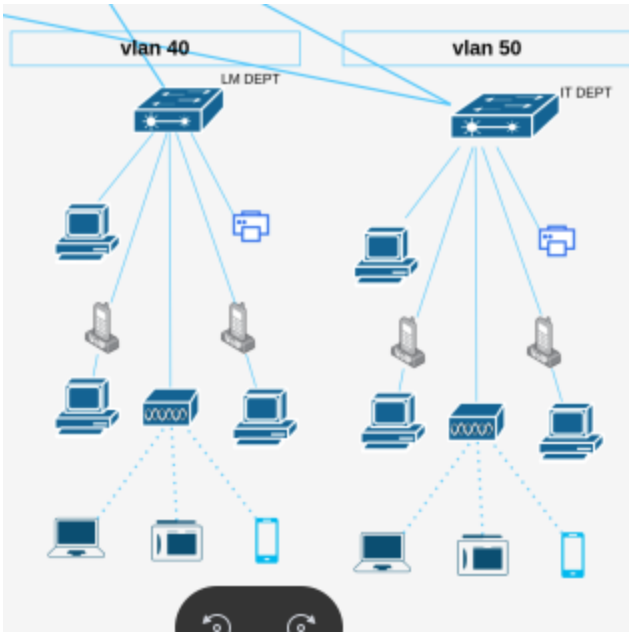
Have got three departments , HR, CS, and MK (which should accommodate a maximum of 40 members as per requirement)



VLAN ID	IP ADDRESS(SUBNET)	GATEWAY ADDRESS
10(HR)	192.168.20.0/26	192.168.20.1
20(CS)	192.168.20.64/26	192.168.20.65
30(MK)	192.168.20.128/26	192.168.20.129

2nd Floor:

Have got two departments; LM and IT (which should accommodate a maximum of 20 members as per the requirement)



VLAN ID	IP ADDRESS(SUBNET)	GATEWAY
40(LM)	192.168.20.192/27	192.168.20.193
50(IT)	192.168.20.224/27	192.168.20.225

NOTE: *Only the IT department should be able to ssh (access devices remotely)*

VOIP :

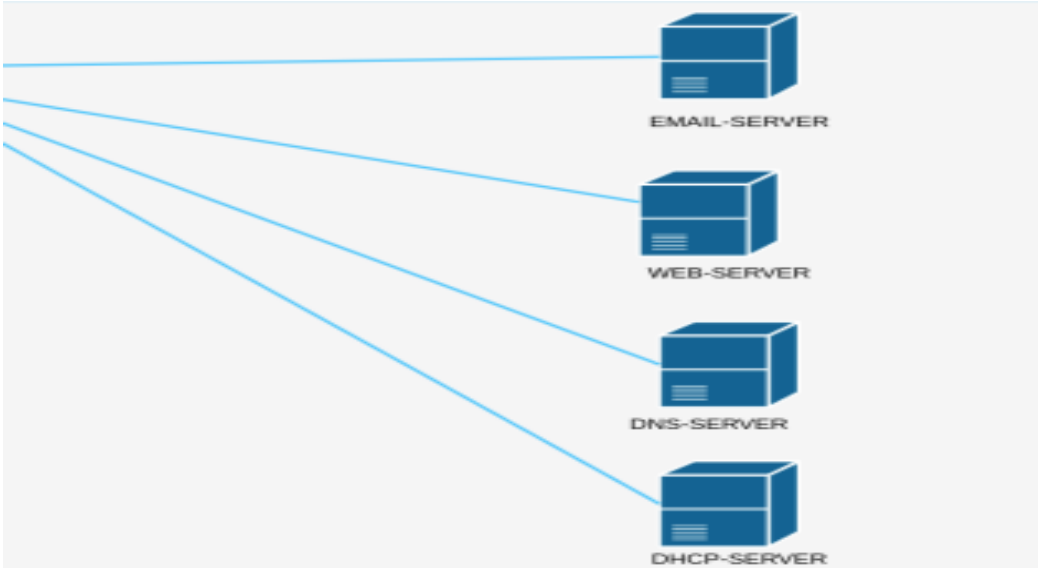
Operate independently on a 2811 router.

VLAN ID	IP ADDRESS(SUBNET)	GATEWAY
120	10.10.10.0/24	10.10.10.1

NOTE: *Line Number ranges from 401-410 across the department and each user have an association to the VOIP phones.*

Server Side:

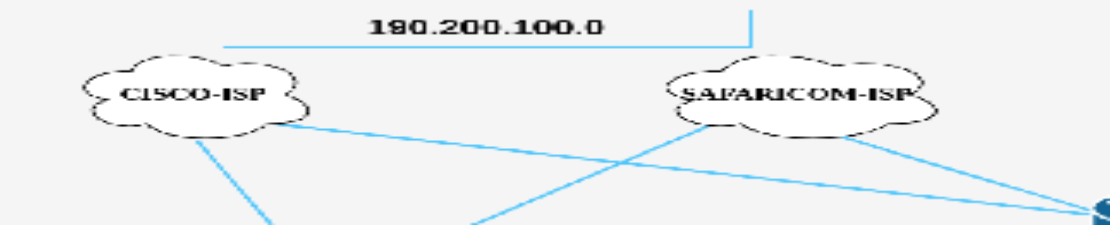
This also operates on isolated areas for security purposes. There are four servers; email server, web server, DNS server, and DHCP server.



IDENTITY	IP ADDRESS(SUBNET)
Server-Side-Network	192.168.21.0/28

Internet Service Provider (ISP) side:

The company has subscribed for two ISPs, i.e CISCO and SAFARICOM



ISPs	IP ADDRESS(SUBNET)	GATEWAYS
CISCO	190.200.100.0/30	190.200.100.1
	190.200.100.8/30	190.200.100.9
SAFARICOM	190.200.100.4/30	190.200.100.5
	190.200.100.12/30	190.200.100.13