PROJECT 9 - Financial Institution Network

Introduction

Jubilee Financial Services is a well-established finance service provider in South-Africa, which offers online finance solutions and services to its clients. The company operates in El Cabo, the country's capital city and is hosted within an eleventh-floor building. **The company primarily operates from the seventh to eighth floors** where **on each floor there are at least two departments**. The company has the following five departments within its main HQ:

- **7th Floor**
  - Human Resources (HR – 40 users + 40 phones)
  - Customer Service (CS – 40 users + 40 phones)
  - Marketing (MK – 40 users + 40 phones)

  One WiFi-AP

- 8th Floor
  - Legal Management (LM – 20 users + 20 phones)
  - Information Technology (IT – 20 users + 20 phones)

  One WiFi-AP

The design has been developed by **including LAN, WAN and external Server-Side Location** connected via appropriate **WAN technology** with prioritizing secure communication between the HQ and the external site. The **Server-Side Site (SSS) will host DHCP, DNS, WEB and EMAIL servers**. Also, the company is intending to subscribe to a **two ISPs (Safaricom and JTL)** to provide redundancy and load-balancing in terms of internet provisions. **The company has also purchased the following equipment**:

- **2 Cisco Catalyst 2911** Routers (one on the HQ and one for the SSS)
- **1 Gateway router catalyst 2811** (For HQ VoIP)
- **2 L3 Switches** (both on HQ)
- **6 Access switches** for departments

Due to Security requirements, it has been decided that **all five departments will be on a separate network segment within the same LAN**. **None of the servers is located within the LAN but will be hosted from an external site accessible via WAN connection**. The network security policy will comprehensively dictate the user access to the external site using ACLs and VPNs in order to enable secure communication considering security and network performance factors to safeguard Confidentiality, Integrity and Availability for data and communications.

Requirements

The company has emphasized high performance, redundancy, scalability and availability and hence you are required to provide a complete JFSL network infrastructure design and implementation.

- **Hierarchical design.** Use this model providing redundancy at every layer.
- **ISPs.** The network is also expected to connect to at least two ISP to provide redundancy and each router is connected to both ISPs.
- **WiFi.** Each department is required to have a wireless network for the users.
- **VoIP.** Each department should have IP phones and users in the department should be able to call to each other.
- **VLAN.** Each department should be in a different VLAN and different subnetwork. USE VLAN 120 for VoIP for the entire network.
- **Subnetting.** Allocate subnets to each department by carrying out the correct number of IP addresses on each case.
- **Basice Settings.** Configure basic device settings such as hostnames, console passwords, enable passwords, banner messages, encrypt all passwords and disable IP domain lookup.
- **Inter-VLAN Routing.** Devices in all departments are required to communicate with each other with the respective L3 Switch configured for interVLAN routing.
- **Core Switches.** The L3 Switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.
- **DHCP Server.** All devices in the networks (Except IP Phones) are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the Server-Side Site.
- **Cisco 2811 Router.** Ensure to have a router that can support telephony service as this device. The VoIP should be connected to any of the L3 switches at HQ.
- **Static Addressing.** Devices in the server room are to be allocated IP addresses statically.
- **Telephony Service.** Configure VoIP on the voice GW router and allocate dial numbers in format (4…).
- **Routing Protocol.** Use OSPF as the routing protocol to advertise routers both on the routers an L3 Switches.
- **Switchport security.** Configure port security for the server site department switch to allow **only one device** to connect to a switch port, an use the sticky method to obtain mac-address and violation mode shutdown.
- **SSH.** Configure SSH on all the Routers and L3 Switches, and also implement a simple Standard ACL on the line VTY to allow only the ICT department to carry out all remote administrative tasks using ssh.
- **NAT + ACL.** Configure PAT to use the respective outbound router interface IPv4 address, and implement the necessary ACL rule.
- **IPSec VPN + ACL.** Configure Site-to-Site IPSec VPN between the HQ router and the Server-Side Site router, and implement the necessary ACL rule.
- **Final test communication** for all the entire network.

Addressing

Network Address Allocation

Initial Conditions

- 192.168.20.0 /24 for Data
- 10.10.10.0 /24 for Voice
- 190.200.100.0 for public IP

7th Floor

- Human Resources (HR – 40 users + 40 phones)
- Customer Service (CS – 40 users + 40 phones)
- Marketing (MK – 40 users + 40 phones)

8th Floor

- Legal Management (LM – 20 users + 20 phones)
- Information Technology (IT – 20 users + 20 phones)

Note: VLAN Voice is unique for all ip phones, so the calculation is 40+40+40+20+20 = 160 phones.

Subnetting

7th Floor				
Name VLAN	**Network /mask**	**Host range**	**Default GW**	**Broadcast**
Human Resources	192.168.20.0 /26	20.1 – 20.62	192.168.20.1	192.168.20.63
Customer Service	192.168.20.64 /26	20.65 – 20.126	192.168.20.65	192.168.20.127
Marketing	192.168.20.128 /26	20.129 – 20.190	192.168.20.129	192.168.20.191
8th Floor				
Legal MGMT	192.168.20.193 /27	20.194 – 20.222	192.168.20.194	192.168.20.223
IT	192.168.20.224 /27	20.225 – 20.254	192.168.20.225	192.168.20.255
Server-Side Site				
Server-Side Site	192.168.21.0 /28	21.1 – 21.15	192.168.21.1	192.168.21.16
Voice GW				
VoIP	10.10.10.0 /24	10.1 – 10.254	10.10.10.1	10.10.10.255

Point-to-point Links

Point-to-Point links	
Link	**Network /Mask**
HQ-Router – HQ-L3-Switch1	192.168.21.16 /30
HQ-Router – HQ-L3-Swicth2	192.168.21.20 /30
HQ-Router – SafariCom-ISP	190.200.100.0 /30
HQ-Router – JTL-ISP	190.200.100.4 /30
SSS-Router – SafariCom-ISP	190.200.100.8 /30
SSS-Router – JTL-ISP	190.200.100.12 /30

DHCP Server's Pools

Department	Defaul Gateway	Start IP Addresss	Subnet Mask	Number of Devices
HR	192.168.20.1	192.168.20.5	255.255.255.192	50
CS	192.168.20.65	192.168.20.70	255.255.255.192	50
MK	192.168.20.129	192.168.20.130	255.255.255.192	50
LM	192.168.20.193	192.168.20.194	255.255.255.224	30
IT	192.168.20.225	192.168.20.226	255.255.255.224	30