Project Title:

Network Design for a Multi-Floor Hotel Using Cisco Packet Tracer

Ade Abujade

Overview

This project focuses on designing a functional and efficient network for a three-story hotel using Cisco Packet Tracer. The network will support both business operations and guest services while ensuring scalability, security, and ease of management. Each floor has distinct departments that need tailored connectivity and configurations based on their specific needs.

Objectives

- **Connectivity:** All devices communicate across VLANs and floors.
- **Secure Access:** SSH enables secure remote login.
- **Dynamic IP Allocation:** DHCP assigns IPs dynamically.
- **Port Security:** Unauthorized devices cannot access the IT network.
- **Scalable Design:** VLANs and OSPF allow future expansion.

Implementation Plan

Implementation Plan

1. Network Topology:

- **Routers:**
    - Use three routers: one for each floor.
    - Connect the routers using serial DCE cables with the following subnets:
        - **Router1 to Router2:** 10.10.10.0/30
        - **Router2 to Router3:** 10.10.10.4/30
        - **Router1 to Router3:** 10.10.10.8/30
- **Switches:**
    - Each floor will have one switch connected to its respective router.
- **Wireless Access Points:**
    - Place one wireless access point per floor to provide connectivity for laptops and phones.
- **Printers:**
    - Each department gets one printer connected to the respective VLAN.

2. VLAN Configuration:

- Assign unique VLANs for each department:
    - **First Floor:**
        - VLAN 10: Reception
        - VLAN 20: Store
        - VLAN 30: Logistics
    - **Second Floor:**
        - VLAN 40: Finance
        - VLAN 50: HR
        - VLAN 60: Sales/Marketing
    - **Third Floor:**
        - VLAN 70: IT
        - VLAN 80: Admin

3. Routing Protocol:

- Use OSPF for route advertisement across routers.
    - Assign each router to OSPF process 1 and use the appropriate network commands for advertising subnets.

4. DHCP Configuration:

- Configure each router as a DHCP server for its connected devices:
    - Define separate pools for each VLAN.
    - Assign gateway IPs for each VLAN.

5. SSH Configuration:

- Enable SSH on all routers for secure remote login:
    - Configure a username and password.
    - Generate RSA keys.
    - Enable SSH and disable Telnet.

6. Port Security for IT Department:

- Configure port security on the switch port connected to the IT department:
    - Allow only one MAC address (Test-PC).
    - Set violation mode to shutdown.

7. Test Remote Login:

- Connect a PC named Test-P to port fa0/1 in the IT department.
- Use this PC to test SSH connectivity to all routers.

1st Floor;

- Reception - VLAN 80, Network of 192.168.8.0/24
- Store - VLAN 70, Network of 192.168.7.0/24
- Logistics- VLAN 60, Network of 192.168.6.0/24

2nd Floor;

- Finance - VLAN 50, Network of 192.168.5.0/24
- HR - VLAN 40, Network of 192.168.4.0/24
- Sales - VLAN 30, Network of 192.168.3.0/24

3rd Floor;

- Admin - VLAN 20, Network of 192.168.2.0/24
- IT - VLAN 10, Network of 192.168.1.0/24