**Hotel System Network Design Documentation**

**1. Project Overview**

The Hotel System Network Design project aims to establish a scalable, secure, and efficient network for a hotel consisting of four floors. Each floor is segmented into distinct VLANs to isolate traffic and optimize network performance. Advanced networking configurations such as Inter-VLAN routing, DHCP, SSH, ACL, PAT, and VPN are implemented to ensure seamless communication, security, and efficient data transmission across the network.

**2. Team Members**

* Mohamed Mustafa Mohamed
* Marwan Saad
* Tasneem Mohamed
* Abdallah Osama
* Ahmed Mohamed Yehya

**3. VLAN Creation and Port Assignment**

**Description**: Virtual Local Area Networks (VLANs) are used to segment network traffic into isolated, logical groups. Each VLAN corresponds to a department within the hotel, ensuring network efficiency and security.

**VLAN Configuration**:

* **First Floor**:
  + VLAN 60: Logistics (192.168.6.0/24)
  + VLAN 70: Store (192.168.7.0/24)
  + VLAN 80: Reception (192.168.8.0/24)
* **Second Floor**:
  + VLAN 30: Sales (192.168.3.0/24)
  + VLAN 40: HR (192.168.4.0/24)
  + VLAN 50: Finance (192.168.5.0/24)
* **Third Floor**:
  + VLAN 10: IT (192.168.1.0/24)
  + VLAN 20: Admin (192.168.2.0/24)
* **Fourth Floor**:
  + VLAN 100: Managers & Owners (192.168.100.0/24)

**Purpose**: VLANs are created to separate network traffic between different departments, improving network performance by reducing broadcast traffic and enhancing security by isolating sensitive data.

**4. Subnetting and IP Addressing**

**Description**: Subnetting involves dividing the overall network into smaller, more manageable subnetworks. Each VLAN is assigned its own subnet to avoid IP conflicts and better manage network traffic.

**Subnetting Plan**:

* **Subnet Mask**: /24 (255.255.255.0) for each VLAN.
* **IP Range**:
  + VLAN 60 Logistics: 192.168.6.0/24
  + VLAN 70 Store: 192.168.7.0/24
  + VLAN 80 Reception: 192.168.8.0/24
  + VLAN 30 Sales: 192.168.3.0/24
  + VLAN 40 HR: 192.168.4.0/24
  + VLAN 50 Finance: 192.168.5.0/24
  + VLAN 10 IT: 192.168.1.0/24
  + VLAN 20 Admin: 192.168.2.0/24
  + VLAN 100 Managers & Owners: 192.168.100.0/24

**Purpose**: Subnetting ensures efficient use of IP addresses, improves routing efficiency, and enhances network security by isolating network segments.

**5. Inter-VLAN Routing (Router on a Stick)**

**Description**: Inter-VLAN routing allows devices in different VLANs to communicate with each other. The "Router on a Stick" configuration uses a single physical router interface with subinterfaces for each VLAN.

**Configuration**:

* **Routers**: Core, Child, and Son.
* **Sub-Interfaces**: Created on one physical interface for each VLAN (e.g., Fa0/1.60 for VLAN 60).
* **Router-on-a-Stick Method**: Allows traffic from multiple VLANs to be routed via one interface using subinterfaces for each VLAN.

**Purpose**: Enables communication between different VLANs while keeping them logically separated.

**6. DHCP Server Configuration**

**Description**: The DHCP server is configured on the Core router, automating IP address assignment to devices within each VLAN.

**Configuration**:

* **Core Router**: Acts as the DHCP server.
* **IP Pool**: Defined for each VLAN (e.g., 192.168.6.10 to 192.168.6.254 for VLAN 60).

**Purpose**: DHCP automates the process of assigning IP addresses to hosts, reducing the need for manual configuration and ensuring efficient IP management.

**7. SSH Configuration for Secure Remote Access**

**Description**: Secure Shell (SSH) is configured on routers to allow secure, encrypted remote access for network administrators.

**Routers**:

* Core
* Child
* Son

**Security Features**:

* SSH version 2 enabled.
* Password and key-based authentication for secure access.

**Purpose**: SSH replaces less secure methods like Telnet, ensuring the confidentiality and integrity of management traffic.

**8. Switchport Security**

**Description**: Port security is configured on the third-floor switch to prevent unauthorized devices from connecting to the network.

**Configuration**:

* **Port**: fa0/2 on the 3rd-floor switch (VLAN 10, PC Test).
* **Security**: Limits the number of MAC addresses that can be associated with the port, blocking unauthorized devices.

**Purpose**: Enhances network security by restricting which devices can connect to specific switch ports.

**9. Host Device Configuration and Network Communication Testing**

**Description**: Each device within the network is assigned an IP address from its respective VLAN’s subnet. After configuration, connectivity tests are performed to verify that devices can communicate across VLANs and with external networks.

**Configuration**:

* IP addresses assigned dynamically through DHCP.
* Ping tests performed between VLANs to verify Inter-VLAN routing.

**Purpose**: Ensures that the network configuration is functional and that hosts can communicate with each other and access external resources.

**10. Telnet, OSPF, EIGRP, and VPN**

**Telnet Configuration**:

* Telnet access enabled on the **Serv** router for remote management.

**OSPF and EIGRP**:

* **OSPF**: Used for routing between internal networks.
* **EIGRP**: Configured for fast convergence and scalability.

**VPN**:

* **VPN Tunnel**: Established between **Child** and **Serv** routers with ISP in between, ensuring secure communication between remote networks.

**Purpose**: Telnet enables basic remote management, while OSPF and EIGRP manage internal routing. The VPN ensures secure communication between physically separated locations.

**11. PAT, ACL, and Console Configuration**

**PAT (Port Address Translation)**:

* Configured on **Son** and **Core** routers to allow multiple devices to share a single public IP address when accessing external networks.

**ACL (Access Control Lists)**:

* ACLs configured to control access between VLANs, allowing or denying traffic based on source and destination IPs and ports.

**Console Access**:

* **Fourth-floor router** configured for local management via console port.

**Purpose**: PAT optimizes the use of public IPs, ACLs provide traffic filtering, and console access allows direct device configuration.

**12. Port Channel and HSRP**

**Port Channel**:

* Four physical links between two multilayer switches are combined into one logical link, enhancing bandwidth and redundancy.

**HSRP (Hot Standby Router Protocol)**:

* Configured between two multilayer switches to provide router redundancy. In case the primary router fails, the backup router takes over, ensuring uninterrupted network service.

**Purpose**: Port Channel increases network bandwidth and redundancy, while HSRP ensures high availability and network resilience.

**13. Testing and Verification**

**Description**: Comprehensive testing is conducted to ensure the network is operating as designed.

**Tests**:

* **Ping Tests**: Verify connectivity between VLANs and to external networks.
* **SSH/Telnet Access**: Verify secure remote management functionality.
* **VPN Test**: Ensure secure communication between **Child** and **Serv** routers.
* **Switchport Security Test**: Verify unauthorized devices are blocked.

**Purpose**: Testing confirms the network’s stability, security, and functionality before deployment.

**Conclusion**

The Hotel System Network Design has been successfully implemented, meeting all requirements for VLAN segmentation, routing, security, and network management. With features like VPN, PAT, Port Channel, and HSRP, the network is highly secure, scalable, and reliable, ready to support the hotel's operations.