Example 1: Corporate LAN Design

Background and Objectives

A mid-sized company with around 500 employees is expanding and moving to a new office. The company has different departments: Finance, HR, Sales, Marketing, and IT. Each department has specific network requirements. The objective is to design a Local Area Network (LAN) that supports all these departments while ensuring security, scalability, and high availability.

Requirements

1. **Network Segmentation:**
    - Departments must be segmented into separate VLANs for security and traffic management.
    - Inter-VLAN routing should be allowed where necessary.
2. **Scalability:**
    - The network must be scalable to accommodate future growth in the number of employees or devices.
    - Support for additional VLANs and subnets without major redesigns.
3. **High Availability:**
    - Redundancy in the network design to ensure minimum downtime.
    - Critical servers and services should have redundant connections.
4. **Security:**
    - Implement security measures such as firewalls, intrusion detection/prevention systems, and VLAN segmentation.
    - Secure remote access for employees working from home.
5. **Performance:**
    - Ensure sufficient bandwidth for each department.
    - Prioritize traffic for critical services such as VoIP and video conferencing.

Design Overview

1. **Network Topology:**
    - **Core Layer:** A pair of high-performance core switches configured for redundancy using protocols like HSRP (Hot Standby Router Protocol) or VRRP (Virtual Router Redundancy Protocol).
    - **Distribution Layer:** Layer 3 switches at this level handle inter-VLAN routing and connect to the core switches.

- **Access Layer:** Layer 2 switches are used here, with each department connected to separate VLANs. These switches are connected to the distribution switches.

2. **VLAN Configuration:**
    - **VLAN 10:** Finance
    - **VLAN 20:** HR
    - **VLAN 30:** Sales
    - **VLAN 40:** Marketing
    - **VLAN 50:** IT
    - **VLAN 60:** Guest (for visitors needing internet access)

VLANs are assigned to different subnets, e.g., 10.10.10.0/24 for Finance, 10.10.20.0/24 for HR, etc.

3. **Routing and Switching:**
    - Inter-VLAN routing is handled at the distribution layer using Layer 3 switches.
    - OSPF (Open Shortest Path First) is used for routing between different network segments.
    - STP (Spanning Tree Protocol) is implemented to prevent loops in the network.
4. **Redundancy and High Availability:**
    - Dual core switches with link aggregation for high availability.
    - Redundant power supplies and UPS for critical networking equipment.
    - Use of dynamic routing protocols to provide failover capabilities.
5. **Security Measures:**
    - A firewall placed at the network edge for controlling incoming and outgoing traffic.
    - IDS/IPS systems to monitor and respond to potential threats.
    - VLAN ACLs (Access Control Lists) to control inter-VLAN traffic based on security policies.
    - VPN for secure remote access, with multi-factor authentication for added security.
6. **Performance Optimization:**
    - QoS (Quality of Service) policies to prioritize VoIP, video conferencing, and other critical services.
    - Gigabit Ethernet or higher bandwidth connections between core, distribution, and access layers.
    - Monitoring tools like SNMP (Simple Network Management Protocol) for real-time performance management.

Implementation and Testing

- **Phase 1:** Deploy core and distribution layer switches, configure VLANs, and test inter-VLAN routing.
- **Phase 2:** Connect access layer switches and end devices, configure ACLs and QoS policies.
- **Phase 3:** Implement security measures, set up VPN access, and deploy redundancy features.
- **Phase 4:** Conduct stress tests, failover tests, and performance monitoring.

Outcome

The LAN was successfully designed and implemented, meeting all requirements for security, scalability, and high availability. The network supports efficient communication between departments while ensuring that critical services remain uninterrupted even in the event of a hardware failure. The use of VLANs has enhanced security by segmenting traffic, and QoS policies have ensured that bandwidth-intensive applications run smoothly.

This design also allows for easy expansion as the company grows, with the ability to add more VLANs, devices, and subnets without major network overhauls.