Project Title: Network Infrastructure Setup and Troubleshooting for a Small-Scale Data Center Simulation

Project Overview:

This project involved designing and deploying a network infrastructure that simulates a small-scale data center. The primary goal was to establish an efficient, reliable network using hardware switches and routers. The network setup was tested for performance, and connectivity issues were troubleshot by applying OSI (Open Systems Interconnection) model principles to isolate and resolve network disruptions. Additionally, the project includes comprehensive documentation of the deliverables and recommendations for future scalability of the network infrastructure.

Project Objectives:

1. **Design and deploy a simulated data center network:**
    a. Utilize hardware switches and routers to create a scalable network infrastructure.
    b. Set up different network segments for servers, workstations, and management systems.
2. **Troubleshoot connectivity issues:**
    a. Identify and resolve network disruptions by applying OSI model layers to diagnose problems.
3. **Document the project deliverables:**
    a. Produce detailed reports of network architecture, configurations, troubleshooting steps, and future scalability recommendations.

Tools and Technologies Used:

- **Hardware Devices:**
    - Cisco Routers
    - Cisco Switches
    - Network cables

    - Patch panels
- **Software Tools:**
    - Cisco Packet Tracer or GNS3 (for simulation)
    - Wireshark (for packet analysis)
    - Network Configuration Management Tools (e.g., SolarWinds)
- **Protocols:**
    - IP, TCP/IP, VLANs, OSPF, DHCP, DNS

Network Design and Implementation:

1. **Network Topology Design:**
    a. The network infrastructure was designed with a three-tier architecture:
        i. **Core Layer:** High-performance routers providing routing capabilities between different VLANs and subnets.
        ii. **Distribution Layer:** Switches that distribute the network load across various segments.
        iii. **Access Layer:** Switches connected to end-user devices like workstations, servers, and IoT devices.
    b. Key components include:
        i. Two routers for fault tolerance and load balancing.
        ii. Multiple Layer 2 and Layer 3 switches.
        iii. Servers segmented by VLANs for isolation and security.
2. **IP Addressing Scheme:**
    a. A private IP addressing scheme (e.g., 192.168.x.x/24) was used to assign IP addresses to devices in different subnets.
    b. Subnets were created based on departments (e.g., Administration, Finance, IT).
3. **Routing Configuration:**
    a. **Static Routing:** For simple network communication between subnets.
    b. **Dynamic Routing (OSPF):** Configured for automatic route updates between routers to ensure optimal routing paths.
4. **VLAN Configuration:**
    a. VLANs were set up for segmentation and security, isolating different network types (e.g., management, user, server).
5. **Network Security:**

    a. Basic security configurations were implemented, including setting up ACLs (Access Control Lists) and port security on switches to prevent unauthorized access.
6. **Server Configuration:**
    a. DNS and DHCP servers were configured for internal address resolution and automatic IP assignment.
    b. File servers were set up for network file sharing.
7. **Redundancy and High Availability:**
    a. Spanning Tree Protocol (STP) was enabled to prevent loops in the network.
    b. Hot Standby Router Protocol (HSRP) was configured to provide gateway redundancy.

Troubleshooting Methodology (OSI Model Application):

1. **Layer 1 (Physical Layer):**
    a. **Issue:** No connectivity between two switches.
    b. **Diagnosis:** Checked physical connections (cables, ports).
    c. **Solution:** Replaced faulty cables and ensured proper port configurations.
2. **Layer 2 (Data Link Layer):**
    a. **Issue:** Incorrect VLAN assignments leading to device communication failure.
    b. **Diagnosis:** Verified VLAN configurations on switches.
    c. **Solution:** Reconfigured VLANs on switches, ensured proper trunking, and checked switch port settings.
3. **Layer 3 (Network Layer):**
    a. **Issue:** Devices on different subnets unable to communicate.
    b. **Diagnosis:** Verified IP addresses and subnet masks.
    c. **Solution:** Corrected subnet masks and checked routing tables for correct static or dynamic routes.
4. **Layer 4 (Transport Layer):**
    a. **Issue:** Slow application performance.
    b. **Diagnosis:** Used Wireshark to analyze TCP handshakes and packet retransmissions.
    c. **Solution:** Identified congestion and bandwidth issues, adjusted QoS policies.
5. **Layer 7 (Application Layer):**
    a. **Issue:** DNS resolution failure.
    b. **Diagnosis:** Checked DNS server settings and logs.

c. **Solution:** Reconfigured DNS servers and ensured proper server connectivity.

Project Deliverables:

1. **Network Architecture Diagram:**
   a. A visual representation of the network design, including all routers, switches, and VLANs.
2. **Configuration Files:**
   a. Full configuration files for routers, switches, servers, and network devices.
3. **Troubleshooting Documentation:**
   a. Step-by-step guides on how issues were diagnosed and resolved, mapped to the OSI model layers.
4. **Testing and Validation Reports:**
   a. Reports showing the results of connectivity tests and performance benchmarks.
5. **Future Scalability Recommendations:**
   a. **Increased Redundancy:** Addition of extra routers or switches for load balancing.
   b. **Advanced Security Measures:** Implementing VPNs, IPS/IDS systems, and stronger firewall rules.
   c. **Bandwidth Management:** QoS policies and potential upgrades to network links to accommodate future growth.
   d. **Cloud Integration:** Considering hybrid cloud solutions for backup and disaster recovery.

Challenges and Solutions:

- **Challenge:** Network loops and broadcast storms.
  - **Solution:** Configured Spanning Tree Protocol (STP) to ensure that redundant paths did not cause network instability.
- **Challenge:** Routing table inconsistencies.
  - **Solution:** Used dynamic routing protocols (OSPF) to ensure accurate and efficient route propagation between routers.
- **Challenge:** Server DNS misconfigurations.
  - **Solution:** Rechecked DNS settings and manually added static entries to ensure name resolution.

Conclusion:

This project successfully established a small-scale data center network that is both reliable and scalable. The OSI model principles were invaluable for diagnosing and resolving network issues. By documenting the entire process and providing scalability recommendations, the network is poised for future growth with enhanced performance and security. The deployment not only reinforced theoretical knowledge but also provided practical experience in managing and troubleshooting real-world network infrastructures.