Design and Implementation of a Small Office Network

Ahmed Yousry - Ather Ahmed – Malak Ossama – Ahmed Ali – Abdelmegiud Azab

***Abstract***— This report outlines the design, implementation, and testing of a small office network. The project is divided into three key phases: planning and design, configurations, and testing, and final documentation.

In the first phase, the network requirements were identified, including the number of users, devices, and internet connectivity needs. A detailed network design was created, including topology diagrams, an IP addressing scheme, and a list of necessary devices.

The second phase focused on the initial configuration of Cisco switches and routers, where VLANs and IP addresses were configured to align with the network design. The third phase involved advanced configurations such as inter-VLAN routing and DHCP, followed by thorough network testing using tools like ping and traceroute to ensure proper connectivity and functionality.

Finally, all findings and configurations were compiled into a comprehensive report. This project showcases the importance of structured network planning, methodical configuration, and rigorous testing to ensure the successful deployment of a small office network.

# Introduction

In today's digital age, an efficient and well-structured network is essential for the smooth operation of any office environment. This report details the design, implementation, and testing of a small office network that meets the specific needs of a growing business. The objective of this project is to create a reliable, scalable, and secure network that supports a range of devices, ensures seamless communication between users, and provides consistent internet connectivity.

The project is divided into three phases: planning and design, configuration of basic and advanced network devices and testing them, and documentation. The network will be designed to support a specified number of users, devices such as computers, printers, and VoIP phones, and include configurations like VLANs for efficient traffic management and DHCP for dynamic IP addressing. Cisco switches and routers will be used to implement the core of the network infrastructure, ensuring both high performance and security.

This report will cover all aspects of the project, from the initial network design to the final configuration and testing results, providing a comprehensive overview of the process and the key decisions made along the way.

# Network Requirements

The network design for the small office is tailored to meet the business's specific requirements for user capacity, device integration, internet connectivity, and security. Initially, the network will support 72 users, primarily representing employee workstations. To accommodate typical internet usage, file transfers, VoIP calls, and cloud-based applications, a high-speed broadband connection with at least 100 Mbps of bandwidth is required, with a reliable Internet Service Provider (ISP) ensuring consistent uptime. The internal network must support gigabit speeds (1 Gbps) for fast data transfers between users, file servers, and other devices, while low latency is essential to ensure smooth VoIP services and minimize communication delays. The network is also designed for scalability, allowing for easy expansion as the business grows, with minimal reconfiguration required. Security will be enforced through VLAN segmentation, isolating sensitive resources like file servers from general user access. The network will employ a private IPv4 addressing scheme, assigning static IPs to servers and using DHCP to dynamically allocate IP addresses to user devices. Subnetting will be utilized to further segment the network based on different functions and roles, ensuring efficient IP management and traffic flow.

# Network Design

The network design for the small office aims to provide efficient, reliable, and secure connectivity to support 20 to 30 users, with scalability for future growth. The design includes a hierarchical structure, incorporating devices such as Cisco routers and switches, and uses VLANs to segment traffic for better management and security. The following design aspects were considered:

**1. Network Topology**

The network is built on a **star topology**, where all devices are connected through a central switch, allowing for straightforward management and troubleshooting. This topology is chosen for its simplicity and ease of expansion, ensuring scalability as the office grows.

* **Core Layer**: Consists of a central switch that interconnects the office’s routers, , and other essential devices.
* **Access Layer**: Includes additional switches that connect user workstations,

**2. IP Addressing Scheme**

A structured IP addressing scheme is implemented to ensure efficient management and minimize address conflicts.

* **Private IP Addressing**: The network will use the private address space **192.168.1.0/24**.
  + **Workstations**: Assigned dynamic IP addresses using DHCP within the range 192.168.1.50 to 192.168.1.150.
* **Subnetting**:
  + Subnetting is used to segment different network functions (IT, HR, Sales, Finance) for better management and security.
  + **Subnet 1**: 192.168.10.0/24 for IT
  + **Subnet 2**: 192.168.20.0/24 for HR.
  + **Subnet 3:** 192.168.30.0/24 for sales
  + **Subnet 4:** 192.168.40.0/24 for finance

**3. VLAN Configuration**

To improve security and performance, VLANs are used to segment traffic based on different office needs. This minimizes broadcast traffic and isolates sensitive resources from general network traffic.

* **VLAN 10 – IT Department**
* **VLAN 20 – HR department**
* **VLAN 30 – Sales department**
* **VLAN 40 – Finance department**

**4. Core Devices**

* **Router**: A Cisco router will be deployed to manage external connectivity to the internet and inter-VLAN routing. The router will handle NAT (Network Address Translation) for internet access, DHCP, and serve as the gateway for inter-VLAN communication.
* **Switches**: Cisco-managed switches will be used at both the core and access layers. These switches will support VLANs, ensuring traffic segmentation between different parts of the network.

**5. Network Diagram**

The network diagram provides a visual representation of the network’s layout, showing the central router, switches, connected devices, and the VLAN structure. The diagram illustrates how different devices connect to the network and the hierarchical design of the core and access layers.

* **Core Switch**: Directly linked to servers and access layer switches.

# Configurations and Testing

**Basic Configuration**

The basic configuration phase involved setting up the core network devices, including Cisco routers and switches, in alignment with the network design. The configurations were applied to enable IP connectivity, VLANs, and basic network functionalities.

**1. Router Configuration**

* **Hostname and Passwords**: The router was configured with a unique hostname, and secure passwords were set for privileged EXEC mode and console access.
* **Interface Configuration**: The router’s interfaces were configured with appropriate IP addresses to allow communication between subnets and VLANs.

**2. Switch Configuration**

* **VLAN Creation**: VLANs were created for different network segments, such as user devices, VoIP phones, and servers, to segment traffic.
* **Assigning Ports to VLANs**: Ports on the switch were assigned to their respective VLANs, ensuring that devices connected to specific ports are properly segmented.
* **Trunking**: Trunk ports were configured between switches and between the switch and the router to carry traffic for multiple VLANs

**Advanced Configuration and Testing**

The advanced configuration phase involved setting up inter-VLAN routing, refining the DHCP configurations, and testing the network to ensure full connectivity and performance.

**1. Inter-VLAN Routing**

* **Router on a Stick**: Inter-VLAN routing was implemented using the “Router on a Stick” method, where a single router interface handles multiple VLANs through sub-interfaces.

This configuration allows traffic to be routed between VLANs (e.g., users and servers) while maintaining traffic segregation.

**2. Advanced DHCP Configuration**

* **DHCP for VLANs**: The DHCP server was configured to handle multiple VLANs, ensuring that devices in different VLANs receive IP addresses from appropriate subnets.

**3. Testing and Troubleshooting**

* **Ping Testing**: Connectivity tests were conducted using the ping command to verify that devices in different VLANs could communicate and that inter-VLAN routing was functioning as expected.

Results confirmed that all VLANs could reach the gateway and communicate with each other where necessary.

* **Traceroute**: Traceroute tests were conducted to ensure that network paths were correctly configured and that there were no routing loops or delays.

The traceroute results showed proper path traversal and successful external connectivity.

* **DHCP Testing**: DHCP leases were tested by connecting various devices and confirming that they received IP addresses in the correct range according to their VLAN.
* **VLAN Testing**: Devices in separate VLANs were tested to ensure that communication was restricted based on ACL rules.
  + For example, devices in the VoIP VLAN were unable to communicate directly with user devices, but could access the internet and relevant servers.

**4. Network Performance Testing**

* **Speed Test**: Internal network speed was tested using gigabit-speed file transfers between devices to confirm that the network supports the required bandwidth.

**5. Troubleshooting**

* **DHCP Issues**: An initial issue was found with DHCP not assigning IP addresses to devices in the VoIP VLAN. This was resolved by verifying the DHCP pool and ensuring the correct VLAN tagging on trunk ports.
* **VLAN Trunking Issues**: Misconfigurations on the trunk ports caused some devices in different VLANs to lose connectivity. This was fixed by adjusting the allowed VLAN list and ensuring consistent trunking configurations across switches.

# Results

The design and implementation of the small office network successfully achieved the outlined goals of providing secure, scalable, and reliable connectivity for all office devices and users. The final configuration was tested thoroughly to verify performance, security, and functionality. The following are the key results from the project:

**1. Network Functionality**

* **IP Connectivity**: All devices, including workstations, servers, printers, and VoIP phones, successfully received IP addresses via DHCP or static assignments. The routing between VLANs was confirmed to work as expected.
* **Inter-VLAN Communication**: Devices in different VLANs communicated seamlessly where necessary (e.g., between user devices and servers)

**2. Network Performance**

* **Gigabit Network Speed**: The network successfully supported gigabit speeds between internal devices. Large file transfers between workstations and servers demonstrated that the network could handle the high bandwidth demands of the office.

**3. Testing Summary**

* **Ping and Traceroute**: All ping tests between VLANs and to external networks passed successfully, demonstrating correct routing and network setup. Traceroute results confirmed proper network path routing to internal and external destinations.
* **Internet Speed**: Speed tests on wired met the required standards for high-speed internet, validating the chosen bandwidth plan with the ISP.

**4. Troubleshooting**

* **DHCP Issues**: Initially, there were problems with DHCP not assigning IP addresses to devices in the VoIP VLAN. This issue was resolved by verifying DHCP pool configurations and VLAN tagging.
* **VLAN Trunking**: Some connectivity issues arose due to misconfigurations in VLAN trunking between switches. Adjusting trunk port settings resolved the issue, ensuring that traffic flowed correctly across VLANs.

# Conclusion

The design and implementation of the small office network met all the project’s objectives, providing a robust, secure, and scalable network infrastructure capable of supporting the office’s current and future needs. By employing a hierarchical structure with VLAN segmentation, the network ensures efficient traffic management and enhanced security across different departments and devices. The deployment of Cisco routers and switches, alongside reliable wireless access points, ensures optimal performance and connectivity throughout the office.

Key accomplishments include the successful configuration of inter-VLAN routing, dynamic IP addressing via DHCP, and comprehensive network testing using tools such as ping and traceroute. The network’s ability to handle voice, data, and wireless traffic without performance degradation was also validated, ensuring a high-quality user experience for both employees and guests.

In conclusion, the network is not only functioning as required but is also prepared for future growth. The design allows for easy expansion, with room to add more users, devices, and network segments as the office evolves. This project demonstrates the importance of a well-planned network infrastructure in enabling efficient business operations and ensuring long-term scalability and security.