# Bank Network Topology Project Documentation

## Table of Contents



## Project Overview

This project involved designing and implementing a hierarchical network topology for a multi-floor bank building. The network spans four floors, housing

distinct departments such as Management, Finance, ICT, and a dedicated Server Room. The primary purpose was to create a robust, scalable, and secure infrastructure to support all banking operations with high availability and data integrity. Key objectives included establishing reliable communication across all floors and departments, enforcing secure access to network devices, automating IP address assignment via DHCP, segmenting the network using VLANs for each department, and implementing OSPF for dynamic and efficient routing between these segments.

## Network Requirements

To achieve the project's objectives for a multi-floor bank, the network design incorporated several core technologies:

- **Dynamic Routing (OSPF):** Open Shortest Path First (OSPF) was implemented as the interior gateway protocol to manage routing between the different subnets. Its fast convergence and scalability make it ideal for a dynamic environment where network paths may change, ensuring continuous connectivity between floors and departments.
- **VLAN Segmentation:** To enhance security and manageability, the network is logically segmented using Virtual Local Area Networks (VLANs). Each department (e.g., Management, Research, Marketing, Finance) is assigned a unique VLAN, isolating its traffic from other departments. This contains broadcast traffic and allows for granular security policies between segments.
- **DHCP for IP Allocation:** A centralized Dynamic Host Configuration Protocol (DHCP) server, located in the fourth-floor Server Room, is configured to automatically assign IP addresses to end-user devices in each department. This simplifies network administration, prevents IP address conflicts, and ensures devices receive the correct network configuration for their respective VLAN.

- **Secure Remote Access (SSH):** All network infrastructure devices (routers and switches) are configured for secure remote management using the Secure Shell (SSH) protocol. This encrypts administrative sessions, protecting login credentials and configuration commands from eavesdropping, thereby preventing unauthorized access.
- **Wireless Network per Department:** Each department is equipped with wireless access points (APs) broadcasting a unique SSID. This provides employees with secure and flexible wireless connectivity. The APs are configured to place wireless clients into the same VLAN as their wired counterparts, maintaining consistent network segmentation.
- **Port Security:** To prevent unauthorized device connections, port security is enabled on all user-facing switch ports. Using sticky MAC addressing, the switch port dynamically learns and locks to the MAC address of the first connected device. If an unauthorized device attempts to connect, the port is automatically shut down.
- **HTTP and Email Servers:** The network hosts dedicated internal servers for essential services, including HTTP (for an intranet portal) and email. These servers are located in a secure, dedicated VLAN in the Server Room to ensure reliable and controlled access for all employees.

## Network Design and Topology

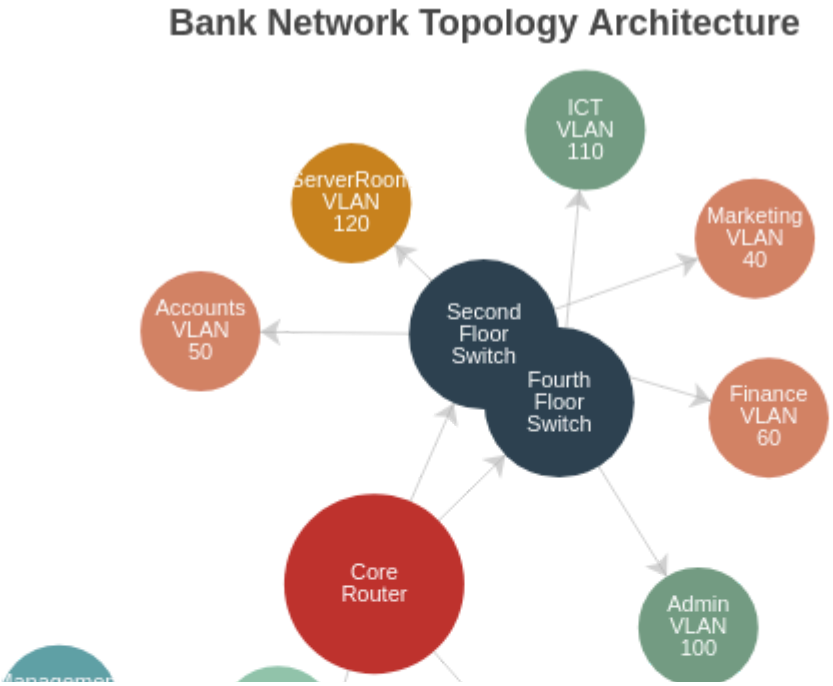
The network is architected using a hierarchical three-tier model (Core, Distribution, Access) physically organized across four floors. At the **core layer**, a high-performance router acts as the central backbone, responsible for high-speed packet switching between different parts of the network. It connects to four **distribution layer** switches, with one Layer 3 switch dedicated to each floor. These distribution switches manage inter-VLAN routing for all departments on their respective floors and run OSPF to share routing information with the core router and other distribution switches. The **access layer** consists of Layer

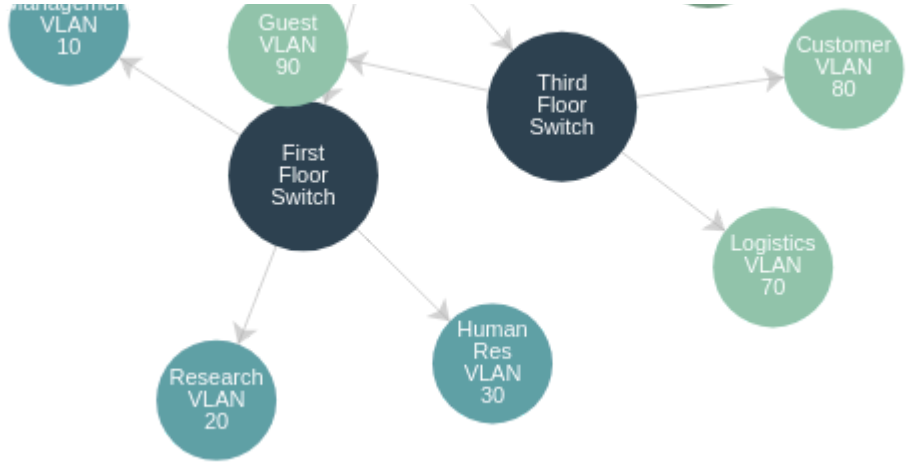
2 switches that provide direct network connectivity for end-user devices (computers, printers, APs) within each department.

The departmental layout is as follows:

- **First Floor:** Management (VLAN 10), Research (VLAN 20), Human Resources (VLAN 30).
- **Second Floor:** Marketing (VLAN 40), Accounts (VLAN 50), Finance (VLAN 60).
- **Third Floor:** Logistics (VLAN 70), Customer (VLAN 80), Guest (VLAN 90).
- **Fourth Floor:** Admin (VLAN 100), ICT (VLAN 110), Server Room (VLAN 120).

Inter-VLAN communication is handled by the Layer 3 distribution switches. Each switch has a Switched Virtual Interface (SVI) for every VLAN on its floor, which serves as the default gateway for devices in that VLAN. For example, when a user in the Marketing department (VLAN 40, Second Floor) needs to access the server in the Server Room (VLAN 120, Fourth Floor), the traffic is sent to the Second Floor distribution switch. This switch, having learned the route to the Server Room's subnet via OSPF, forwards the traffic to the core router, which then directs it to the Fourth Floor distribution switch and finally to the server. This design ensures efficient traffic flow and scalability.






# IP Addressing Plan

The IP addressing plan is systematically designed based on the bank's departmental and floor structure. The primary address spaces used are `192.168.10.0`, `192.168.11.0`, and `192.168.12.0`. Each department is allocated a unique `/26` subnet, providing 62 usable host addresses to accommodate both wired and wireless users. This segmentation ensures that each department operates within its own broadcast domain. The following tables, derived from the project's network address documentation, provide a comprehensive overview of the IP allocation. Additionally, the `10.10.10.0` network, subnetted with a `/30` mask, is reserved for point-to-point links connecting the core router to the distribution switches.

## First Floor

| Department (VLAN) | Network Address | Subnet Mask | Host Address Range | Broa Add |
|---|---|---|---|---|
| Management (VLAN 10) | 192.168.10.0 | 255.255.255.192/26 | 192.168.10.1 to 192.168.10.62 | 192.168 |

| Department (VLAN) | Network Address | Subnet Mask | Host Address Range | Broa Add |
|---|---|---|---|---|
| Research (VLAN 20) | 192.168.10.64 | 255.255.255.192/26 | 192.168.10.65 to 192.168.10.126 | 192.168 |
| Human Res (VLAN 30) | 192.168.10.128 | 255.255.255.192/26 | 192.168.10.129 to 192.168.10.190 | 192.168 |

## Second Floor

| Department (VLAN) | Network Address | Subnet Mask | Host Address Range | Broad Addr |
|---|---|---|---|---|
| Marketing (VLAN 40) | 192.168.10.192 | 255.255.255.192/26 | 192.168.10.193 to 192.168.10.254 | 192.168 |
| Accounts (VLAN 50) | 192.168.11.0 | 255.255.255.192/26 | 192.168.11.1 to 192.168.11.62 | 192.168 |
| Finance (VLAN 60) | 192.168.11.64 | 255.255.255.192/26 | 192.168.11.65 to 192.168.11.126 | 192.168 |

## Third Floor

| Department (VLAN) | Network Address | Subnet Mask | Host Address Range | Broad Addr |
|---|---|---|---|---|
| Logistics (VLAN 70) | 192.168.11.128 | 255.255.255.192/26 | 192.168.11.129 to 192.168.11.190 | 192.168 |
| Customer (VLAN 80) | 192.168.11.192 | 255.255.255.192/26 | 192.168.11.193 to 192.168.11.254 | 192.168 |
| Guest (VLAN 90) | 192.168.12.0 | 255.255.255.192/26 | 192.168.12.1 to 192.168.12.62 | 192.168 |

## Fourth Floor

| Department (VLAN) | Network Address | Subnet Mask | Host Address Range | Broad Addr |
|---|---|---|---|---|
| Admin (VLAN 100) | 192.168.12.64 | 255.255.255.192/26 | 192.168.12.65 to 192.168.12.126 | 192.168 |
| ICT (VLAN 110) | 192.168.12.128 | 255.255.255.192/26 | 192.168.12.129 to 192.168.12.190 | 192.168 |
| ServerRoom (VLAN 120) | 192.168.12.192 | 255.255.255.192/26 | 192.168.12.193 to 192.168.12.254 | 192.168 |

## Additional Network (Point-to-Point Links)

| Network Address | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|
| 10.10.10.0 | 255.255.255.252 | 10.10.10.1 to 10.10.10.2 | 10.10.10.3 |
| 10.10.10.4 | 255.255.255.252 | 10.10.10.5 to 10.10.10.6 | 10.10.10.7 |
| 10.10.10.8 | 255.255.255.252 | 10.10.10.9 to 10.10.10.10 | 10.10.10.11 |
| ... (and so on for all 14 links) | ... | ... | ... |

Data Source: Network Address Tables

A central DHCP server, located in the Server Room (VLAN 120), is configured with distinct scopes for each VLAN to automate IP address assignment. For instance, the scope for the Management department (VLAN 10) leases addresses from the `192.168.10.1` to `192.168.10.62` range. Critical infrastructure in the Server Room, such as the HTTP and Email servers, uses static IP addresses from the `192.168.12.192/26` subnet to ensure consistent accessibility.

## Device Configuration Summary

Each network device was meticulously configured to align with the hierarchical design and security requirements. The diagram below outlines the key configuration elements for the network's core, distribution, and access layers.

- **Core Router Configuration:** The router was given a hostname (e.g., `Core-Router`) and configured to run OSPF to exchange routes with the four floor-level distribution switches via `10.10.10.0/30` point-to-point links. Secure remote access was established by configuring SSH, generating RSA keys, and restricting VTY lines to SSH only. Encrypted passwords and a login banner were also implemented.
- **Layer 3 Switch Configuration:** Each floor's distribution switch was configured for inter-VLAN routing. For example, the First Floor switch was configured with VLAN 10 (Management), VLAN 20 (Research), and VLAN 30 (Human Res). Switched Virtual Interfaces (SVIs) were created for each VLAN to serve as the default gateway (e.g., SVI for VLAN 10 with IP `192.168.10.1/26`). The `ip helper-address` command was applied to each SVI, pointing to the DHCP server's IP in the Server Room (e.g., `192.168.12.194`) to facilitate DHCP relay.
- **Layer 2 Access Switch Configuration:** Access switches provide end-device connectivity. Ports were assigned to their respective departmental VLANs (e.g., ports for the Marketing department assigned to VLAN 40). Port security was enabled on user-facing ports with `switchport port-security mac-address sticky` and the violation mode set to `shutdown` to block unauthorized devices. Unused ports were disabled and moved to an isolated VLAN.
- **DHCP Server Configuration:** The central DHCP server in the Server Room (VLAN 120) was configured with separate IP pools for each departmental VLAN. For example, the pool for the Finance department (VLAN 60) was defined with the network `192.168.11.64/26`, a lease range of `192.168.11.65` to `192.168.11.126`, and the default gateway set to the SVI IP of VLAN 60.
- **Wireless Access Point Setup:** APs in each department were configured with a unique SSID (e.g., "Finance-WiFi") and connected to an access port assigned to the corresponding department's VLAN. This ensures wireless clients are placed in the correct network segment and receive an appropriate IP address from the DHCP server.

- **Server Configuration (HTTP & Email):** The internal HTTP and Email servers in the Server Room (VLAN 120) were assigned static IP addresses (e.g., `192.168.12.195` and `192.168.12.196`) from the `192.168.12.192/26` range for stable access. OSPF ensures these servers are reachable from all other VLANs.
- **Testing Commands and Verification:** Configuration was verified using a suite of commands. `show ip interface brief` checked interface status, `show vlan brief` confirmed VLAN assignments, and `show ip route` verified the OSPF routing table contained all subnets. End-to-end connectivity was tested using `ping` between different VLANs (e.g., from a device in Management to one in Logistics).

## Testing and Verification

A comprehensive testing phase was executed to validate the network's functionality, performance, and security against the project requirements.

- **Inter-VLAN and Inter-Floor Connectivity:** We verified that devices across different floors and departments could communicate. For instance, a PC in the Management VLAN (VLAN 10, `192.168.10.0/26`) on the first floor successfully pinged a device in the Logistics VLAN (VLAN 70, `192.168.11.128/26`) on the third floor. This confirmed that inter-VLAN routing, OSPF, and the core-distribution links were all functioning correctly.
- **DHCP Functionality:** We tested DHCP by connecting a client in the Accounts department (VLAN 50). The device successfully obtained an IP address from the `192.168.11.0/26` range, confirming that DHCPDISCOVER messages were correctly relayed from the second-floor switch to the central DHCP server on the fourth floor. This test was successfully repeated for multiple VLANs.

- **SSH Remote Access:** Secure access to all network devices was tested. From a workstation in the ICT department (VLAN 110), we successfully initiated SSH sessions to the core router and the distribution switches on each floor. An attempted Telnet connection was refused, confirming that only encrypted management access is permitted.
- **Server Access (HTTP and Email):** From a client PC in the Research department (VLAN 20), we accessed the internal web server by navigating to its static IP (e.g., `http://192.168.12.195`). The page loaded successfully. Similarly, email clients were configured to use the internal mail server, and test emails were sent and received between different departments, confirming service connectivity.
- **Port Security Test:** Port security was tested on an access switch in the Customer department. After connecting an authorized PC, we disconnected it and plugged in an unauthorized laptop. The switch port immediately entered an `err-disabled` state, which was verified using the `show interfaces status` command, confirming the shutdown violation mode was effective.
- **Use of Show Commands:** Throughout testing, verification commands were crucial. `show ip route ospf` on the core router confirmed that all 12 departmental subnets were learned dynamically. `show vlan brief` on access switches verified correct port-to-VLAN assignments (e.g., Admin staff ports in VLAN 100). `show ip ospf neighbor` confirmed adjacencies between the core router and floor switches.

## Security Implementation

A multi-layered security approach was implemented to protect the bank's network infrastructure and sensitive data.

- **Secure Remote Management (SSH):** All administrative access to routers and switches is restricted to SSH, which encrypts the entire session. This prevents eavesdropping on credentials and commands. Telnet was disabled, and strong, encrypted passwords were enforced for all access methods.
- **Port Security on Switches:** At the access layer, port security mitigates unauthorized physical access. By enabling sticky MAC addressing, switch ports are locked to the first device they see. Any attempt to connect a different, unauthorized device will cause the port to shut down, preventing network access and logging the violation.
- **Disabling Unused Ports:** All switch ports not in active use were administratively shut down and assigned to an unused, isolated "blackhole" VLAN. This simple but effective measure closes a common entry point for attackers by ensuring that unused network jacks are inactive.
- **Encrypted Passwords and Access Control:** The `service password-encryption` command was used to ensure all passwords stored in the device configurations are encrypted, not in plain text. Access to VTY lines can be further restricted with access control lists (ACLs), permitting SSH connections only from trusted subnets like the ICT department (VLAN 110).
- **VLAN Segmentation for Security:** The fundamental design of using VLANs for each department creates security boundaries. By default, traffic cannot cross from one VLAN to another without being processed by a Layer 3 device. This allows for the future implementation of ACLs on the distribution switches to control and filter inter-departmental traffic, such as restricting the Guest VLAN from accessing any internal corporate resources.
- **Wireless Security:** The wireless networks utilize WPA2/WPA3 encryption to protect all over-the-air traffic. By assigning each department its own SSID and VLAN, wireless traffic is segmented in the same manner as wired traffic, ensuring consistent security policies for all users.

# Challenges and Troubleshooting

During implementation, we encountered and resolved several configuration issues. A notable challenge involved a typo in a VLAN name on one of the distribution switches, which caused confusion during verification. More critically, inter-VLAN routing for the Research department (VLAN 20) initially failed. Using `show ip interface brief`, we discovered that the SVI for VLAN 20 on the first-floor switch had not been assigned an IP address. Assigning the correct gateway address (`192.168.10.65/26`) and enabling the interface resolved the issue.

Another issue arose when clients in the Finance department (VLAN 60) failed to receive IP addresses. We suspected a DHCP relay problem. By checking the configuration on the second-floor switch, we found the `ip helper-address` command was missing from the SVI for VLAN 60. Once we added the command pointing to the DHCP server, clients immediately began receiving correct IP configurations. This highlighted the importance of consistent configuration across all SVIs.

We also used verification commands proactively. When an OSPF adjacency failed to form between the core router and the third-floor switch, `show ip ospf neighbor` showed no active neighbors. Further investigation with `show ip ospf interface` revealed that the OSPF process was not enabled on the correct switch interface. Correcting the OSPF network statement brought the adjacency up, and routes were exchanged successfully. These experiences underscored the value of a systematic troubleshooting methodology, relying on commands like `show ip route`, `show vlan brief`, and `show running-config` to quickly diagnose and fix configuration errors.

# Conclusion

This project successfully culminated in the design and implementation of a robust, secure, and scalable network for a four-floor bank building. By leveraging a hierarchical architecture, we created a logical and efficient traffic flow, while VLANs provided necessary segmentation between diverse departments like Management, Finance, and ICT. The implementation of OSPF ensures dynamic and resilient routing, and a centralized DHCP server simplifies IP management across the entire enterprise. Key security measures, including SSH, port security, and traffic isolation via VLANs, establish a strong defensive posture for the bank's critical data and infrastructure.

The hands-on process of configuring routers and switches provided invaluable practical experience with Cisco IOS, covering inter-VLAN routing, OSPF, DHCP relay, and various security features. The meticulous planning of the IP addressing scheme and the troubleshooting of real-world configuration issues (such as missing helper addresses or incorrect SVI configurations) reinforced theoretical knowledge with practical problem-solving skills. The systematic use of verification commands proved essential for validating the configuration and ensuring end-to-end functionality.

In conclusion, the resulting network meets all specified objectives, providing a reliable foundation for the bank's operations. The design is inherently scalable, ready to accommodate future growth with ease. This project not only produced a functional enterprise network but also provided a deep, practical understanding of modern network design, implementation, and management principles.

## References


- Cisco Packet Tracer (Network simulation software used to design and test the topology).

- Cisco IOS Configuration Guides (for reference on configuring VLANs, OSPF, DHCP relay, SSH, and port security on Cisco devices).
- Networking course materials and textbooks (covering topics on network design principles, routing protocols, and security best practices).
- Network Address Tables (Project Documentation)