**INDEX**

|  |  |
| --- | --- |
| **SRNO.** | **Content** |
| **1** | **Abstract** |
| **2** | **Introduction** |
| **3** | **Methodology Used** |
| **4** | **Objective** |
| **5** | **Network Requirements** |
| **6** | **Protocols used** |
| **7** | **Snapshot of Implementation Result** |
| **8** | **Advantages and Disadvantages** |
| **9** | **Conclusion** |

**Abstract**

In this project we will primarily focus on design and implementation of Bank Network using Cisco Packet Tracer (CPT). Security breach in the sector of banks is one of the most important concerns that needs to be addressed in the first place since loss of information can lead to huge losses to the bank overall. This project will help us curb such concerns by understanding the regulated flow of information/data. We will consider a bank which has its head offices located in big cities like Mumbai. The other small branches will be present in cities like Nashik, Pune, Nagpur, Kolhapur, Solapur.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Introduction**

In today’s interconnected world it is irrational to believe a computer network system is immune from an attack or think of it as too small to be considered as a predator by intruders to gain whatever advantage they need. Sometimes company owners deceived by thinking that company’s resource are not highly valued and hence, they are not worth to be targeted.

The reality is even at this moment companies are losing a significant amount money and wealth because of negligence or lack of awareness about the security issues. In this paper, we will primarily focus on designing and implementing a Bank Network using Cisco Packet Tracer (CPT). Security breach in the sector of banks is one of the most important concerns that need to be addressed in the first place since the loss of information can lead to huge losses to the bank overall. This paper will help us curb such concerns by understanding the regulated flow of information/data. We will consider a Bank with its head offices in big cities like Mumbai. The other small branches will be present in cities like Pune, Nagpur, Solapur, Kolhapur. These small branches in each state will be connected through LANs. Apart from this, VLANs and WANs will automatically be a part of the project networking since we are working on a Bank Network. Additionally, bank machines will be made available all around each city in specific to ensure better reach and reliable services to the people.

Employees use special software to access user accounts. The level of access to advanced resources within the bank varies from employee to employee based on several criteria, including the employee’s designation, the criticality and directories will be made available to all the employees to of the information, etc. The typical servers, mail, web, files, understand the flow of work within the bank.

**Methodology Used**

**Network Planning and Design**

The first step in the methodology was to design the banking network's architecture. The following elements were considered during the planning phase:

Network Requirements: A thorough analysis of the banking system's needs, including the number of branches, ATMs, data centers, and user traffic expectations, was conducted. This helped in defining the network’s size, devices, and structure.

Network Topology Selection: A hierarchical topology was chosen for the network, ensuring clear separation between the core, distribution, and access layers. This design allows efficient management of traffic between the central banking server, branch offices, and ATMs.

Subnetting and IP Addressing: The entire network was divided into smaller subnets, with each branch, ATM, and department assigned a unique subnet. This ensures effective use of IP addresses and facilitates better traffic management and security.

**Router and Static Routing Configuration**

Router Configuration: Cisco Packet Tracer was used to configure routers at each branch and in the central office. Static routes were manually set to ensure direct paths between branches and the central banking services.

Static Routing: Static routing was selected as it provides a predictable and secure way to route traffic. Routes were added by specifying the destination network, next-hop IP address, and interface for each router. This ensures control over data traffic across the banking network.

Routing Table Configuration: Each router’s routing table was manually updated with the necessary routes to ensure proper network communication. This included adding static routes for the head office, branches, and ATMs.

**Network Simulation in Cisco Packet Tracer**

Device Setup: All devices, including routers, switches, servers, ATMs, and end-user computers, were set up in Cisco Packet Tracer with appropriate IP addresses, subnet masks, and default gateways.

Link Establishment: Connections between devices were established using appropriate media, such as Ethernet or serial cables. All links were tested for connectivity using the Packet Tracer simulation environment.

**Documentation and Maintenance**

Network Documentation: All network configurations, including static routes, IP addressing, and device setups, were documented. This ensures the banking network can be scaled or modified in the future with minimal disruption.

Manual Updates: Given the static nature of the routing, future network changes, such as adding new branches or ATMs, require manual updates to routing tables. A detailed guide was prepared for future network administrators to handle such updates.

**Objective**

The primary objective of this project is to design and simulate a secure and efficient network infrastructure for a bank, connecting its head office in a major city with branches located in various regional cities using Cisco Packet Tracer. The project aims to achieve the following goals:

1. Establish Branch Connectivity: Implement LANs in each branch to ensure seamless communication between the head office and all branch offices.

2. Network Efficiency and Reliability: Design a network that supports high-speed data transfer and reliable connectivity, ensuring minimal downtime and efficient handling of banking operations.

3. Secure Communication: Integrate security protocols and configurations to protect sensitive banking data from potential threats and unauthorized access.

4. Scalability: Create a network infrastructure that can easily accommodate the bank’s future growth, allowing for the addition of more branches without compromising network performance.

5. Centralized Management: Enable centralized network management from the head office, facilitating easier control and monitoring of all branches.

6. Simulate Real-World Scenarios: Use Cisco Packet Tracer to simulate the network topology, verify its performance, and test real-world banking network operations such as data exchange, transactions, and internal communication.

This project aims to provide a scalable, secure, and efficient networking solution for the bank to streamline operations and ensure uninterrupted service delivery across its branch offices.

**Network Requirements**

1. **Devices and Components**:
   * **Router**: Used for inter-branch connectivity and routing between main branches and sub-branches.
   * **Switches**: Connects various departments within branches and server rooms.
   * **PCs**: Each department (e.g., IT Dept, Customer Dept, Loan Dept) has PCs.
   * **Servers**: Servers for handling branch-specific operations and services, including file sharing, online gateways, and central banking applications.
   * **ATMs**: Connected to branches, especially for the sub-branch in Nagpur.
   * **Peripherals**: IP cameras, home gateways, and sensor devices are connected for security and automation purposes.
2. **IP Addressing**:
   * **Static IP Addressing**: Each device (PC, server, etc.) is assigned a static IP address. Subnets are created for different branches and departments.
   * **Subnetting**: Logical segmentation of networks using different IP ranges for each department and branch.
3. **Routing Protocol**:
   * **Static Routing**: Routers are manually configured with static routes to direct traffic between branches.
4. **Security**:
   * **Firewall**: Protect the network from external threats (could be placed in the routers).
   * **Access Control Lists (ACLs)**: For restricting access to specific subnets or IP ranges.
   * **VPN**: (Optional) For secure communication between branches and HQ

Cisco Packet Tracer :

• for implementing this bank prototype, we have used Router-PT which has serial ports, So that it will be easy for us to connect to 5 branches we have also we have switches to connect to connect to all 5 cities with router.

• We can also configure every router and network with the IP address and tested whether the data transfer is successful or not.

• All the serial ports are assigned IP addresses so they can be recognized between the cities without confusion.

IP address:

|  |  |  |
| --- | --- | --- |
| **Branch** | **Ip Address** | **subnet mask** |
| Maharashtra | 192.168.1.2/192.168.2.1/ 192.168.3.2 192.168.2.2/192.168.5.2/ 192.168.6.1 192.168.6.2/192.168.7.2/ 192.168.8.2 | 255.255.255.0  255.255.255.0  255.255.255.0 |
| Mumbai | 192.168.1.1 | 255.255.255.0 |
| Nashik | 192.168.3.1 | 255.255.255.0 |
| Pune | 1.0.0.1 | 255.0.0.0 |
| Nagpur | 192.168.5.1 | 255.255.255.0 |
| Kolhapur | 192.168.7.1 | 255.255.255.0 |
| Solapur | 192.168.8.1 | 255.255.255.0 |

**Protocols Used**

**IPv4, IPv6, DHCP, DNS, and Static Routing Protocols Used in Routers:**

**Static Routing**: Static routing is a routing method in which network routes are manually configured on routers. Unlike dynamic routing protocols (such as OSPF or EIGRP), static routes do not change unless manually updated. Static routes are suitable for small networks or specific use cases where the routing path does not change often.

In static routing, the network administrator specifies the destination network, the subnet mask, and the next-hop address (the IP address of the next router in the path). While static routing is less flexible than dynamic routing, it is often more efficient and secure in smaller or simpler networks.

**IPv4 (Internet Protocol Version 4):**

IPv4 is the most widely used version of the Internet Protocol (IP) and is responsible for addressing and routing packets of data across a network. It uses a 32-bit address scheme, which allows for approximately 4.3 billion unique addresses. IPv4 addresses are typically written in dotted-decimal format, such as 192.168.1.1.

Routers forward packets between different networks based on their destination IPv4 addresses. IPv4 is connectionless and uses the best-effort delivery model, meaning it does not guarantee delivery, order, or integrity of packets.

**DHCP (Dynamic Host Configuration Protocol) Used in Servers**

DHCP is a network protocol used to automatically assign IP addresses and other network configuration settings (such as subnet mask, default gateway, and DNS server) to client devices on a network. In Cisco Packet Tracer, a server can be configured to act as a DHCP server, which dynamically provides IP addresses to client devices when they join the network.

Key Features:

IP Address Assignment: DHCP allows devices to automatically receive an IP address without requiring manual configuration. This simplifies network management, especially in large networks.

Lease Time: The IP address assigned by the DHCP server is leased for a specific period, after which the client must renew the lease.

Dynamic Allocation: The DHCP server automatically assigns IP addresses from a predefined range, ensuring efficient and collision-free distribution of addresses.

**DNS (Domain Name System) Used in Servers**

DNS is a network protocol used to resolve human-readable domain names (like www.example.com) into their corresponding IP addresses, which are required for network communication. In Cisco Packet Tracer, a server can be set up to function as a DNS server that maps domain names to IP addresses for client devices.

Key Features:

Domain Name Resolution: DNS allows users to access devices and websites using easy-to-remember names instead of IP addresses. The server translates domain names to IP addresses that routers can use to forward packets.

Caching: DNS servers can cache recent queries, which speeds up subsequent lookups for the same domain names.

Reverse Lookup: DNS also allows reverse lookups, where an IP address is mapped back to a domain name.

**HTTP/HTTPS (Hypertext Transfer Protocol/Secure) Used in Servers**

HTTP and HTTPS are protocols used to transfer web pages and resources over the internet or an internal network. In Cisco Packet Tracer, a server can be configured to act as a web server that serves web pages to clients using either HTTP or HTTPS.

Key Features of HTTP:

Web Page Delivery: HTTP is the foundation of data communication for the web. It enables web browsers to retrieve information from a web server in the form of web pages.

Stateless Protocol: HTTP is a stateless protocol, meaning each request from a client to a server is treated as an independent transaction without retaining session information.

Insecure Transmission: HTTP sends data in plain text, making it vulnerable to interception or tampering by attackers.

Key Features of HTTPS:

Encrypted Communication: HTTPS is a secure version of HTTP that uses SSL/TLS to encrypt the communication between the web server and the client, ensuring that the data exchanged cannot be intercepted or tampered with by unauthorized parties.

Authentication and Data Integrity: HTTPS ensures that users are connecting to the legitimate server (authentication) and that the data sent between the client and server remains unaltered (integrity).

Secure Web Browsing: HTTPS is used for secure web browsing, such as online banking, shopping, and any site that handles sensitive data.

In Cisco Packet Tracer, a server can be configured to host a web page using HTTP or HTTPS. Clients on the network can access these web pages using a web browser by typing the server's IP address or domain name (if a DNS server is also configured).

**VLAN and Ethernet Protocols Used in Switches**

1. Ethernet Protocol (IEEE 802.3): Ethernet is the primary communication protocol used in switches to transmit data between devices within the same local area network (LAN). Ethernet operates by forwarding data using frames that contain the necessary source and destination MAC addresses. Switches utilize these addresses to ensure data is delivered to the correct device within the network.

The basic structure of an Ethernet frame includes:

Preamble (for synchronization),

Destination MAC Address,

Source MAC Address,

Type/Length field,

Data payload,

Frame Check Sequence (FCS) for error checking.

2. VLAN (Virtual Local Area Network): A VLAN (Virtual Local Area Network) is a logical subdivision of a network, used to segment and isolate traffic for better management and security.

VLANs allow multiple networks to coexist on the same physical hardware, reducing the size of broadcast domains and improving network efficiency.

In switches, VLANs are created to separate traffic between different departments or groups within an organization. For instance, VLAN 10 could be assigned to the Sales department, and VLAN 20 to the IT department, ensuring that their traffic remains isolated despite sharing the same switch.

**Snapshot of Implementation Result**

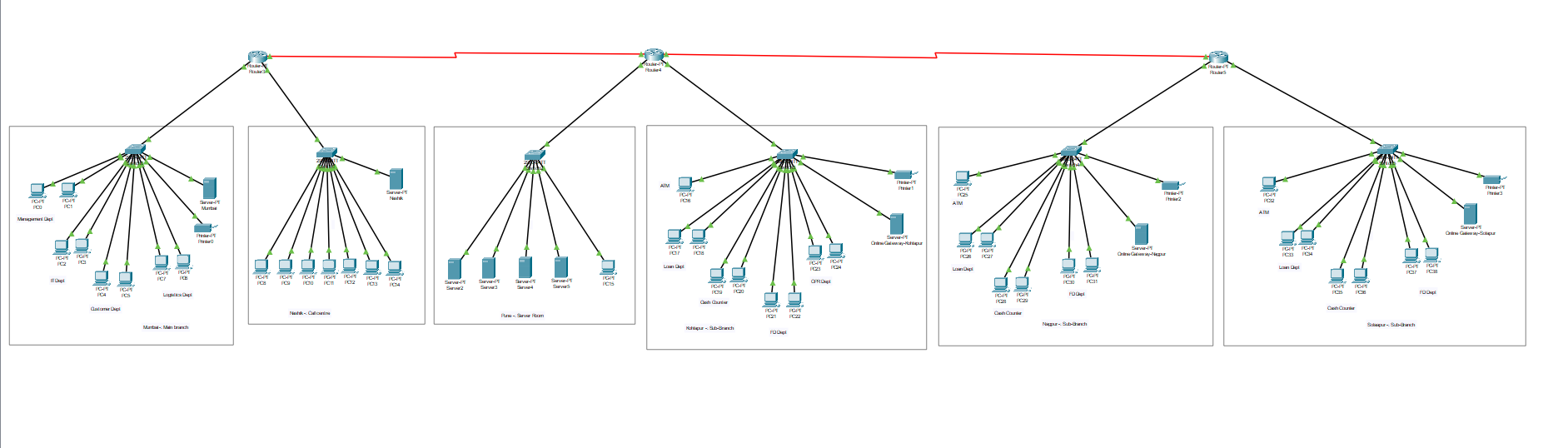
****

Figure 1 Bank Network tropology diagram

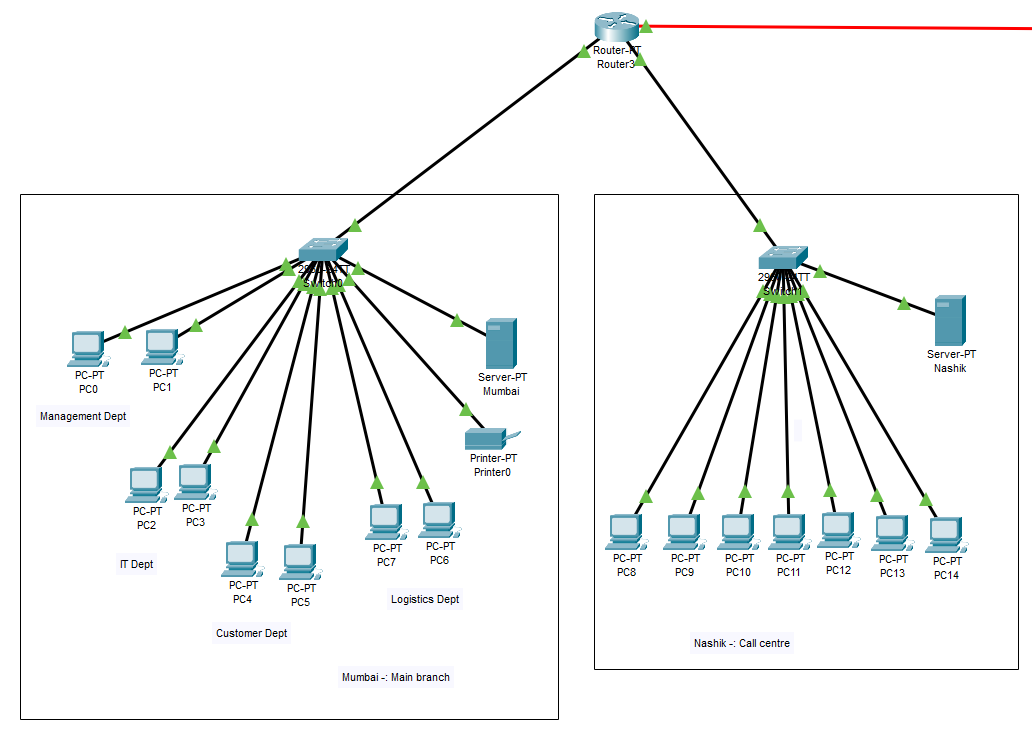
****

Figure 2 Mumbai and Nashik branch tropology diagram

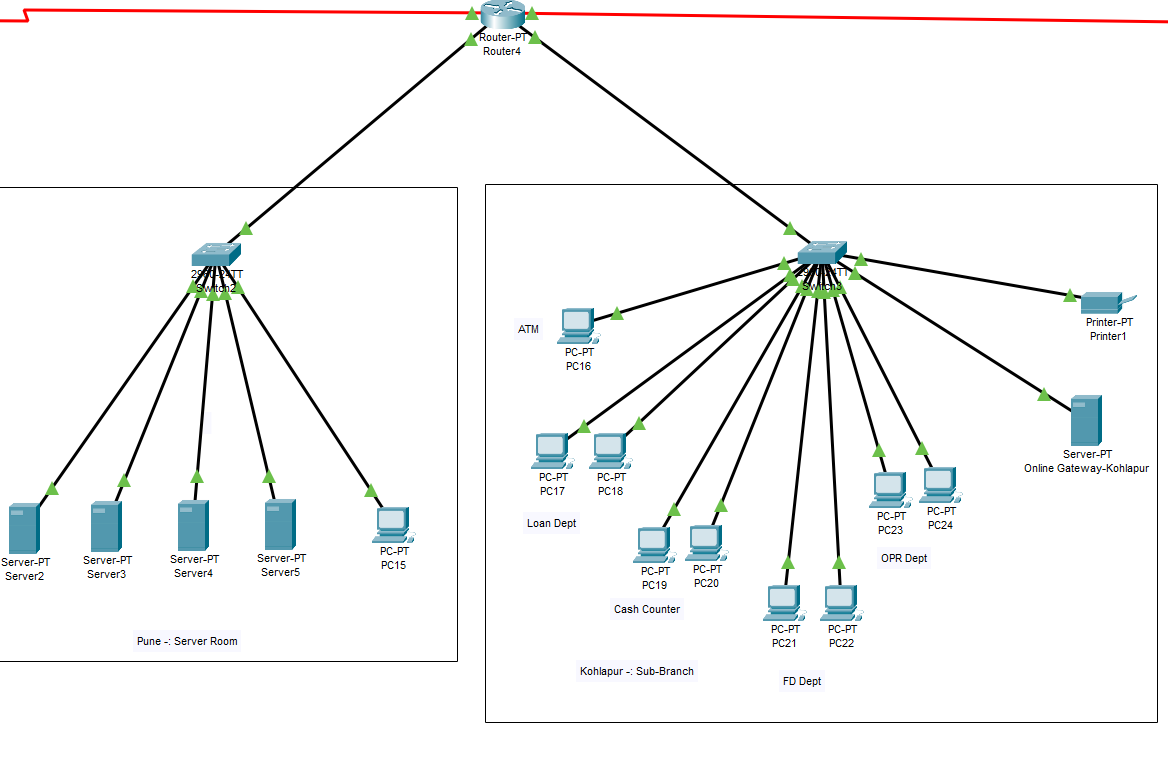
****

Figure 3 Pune server room and kolhapur branch tropology diagram

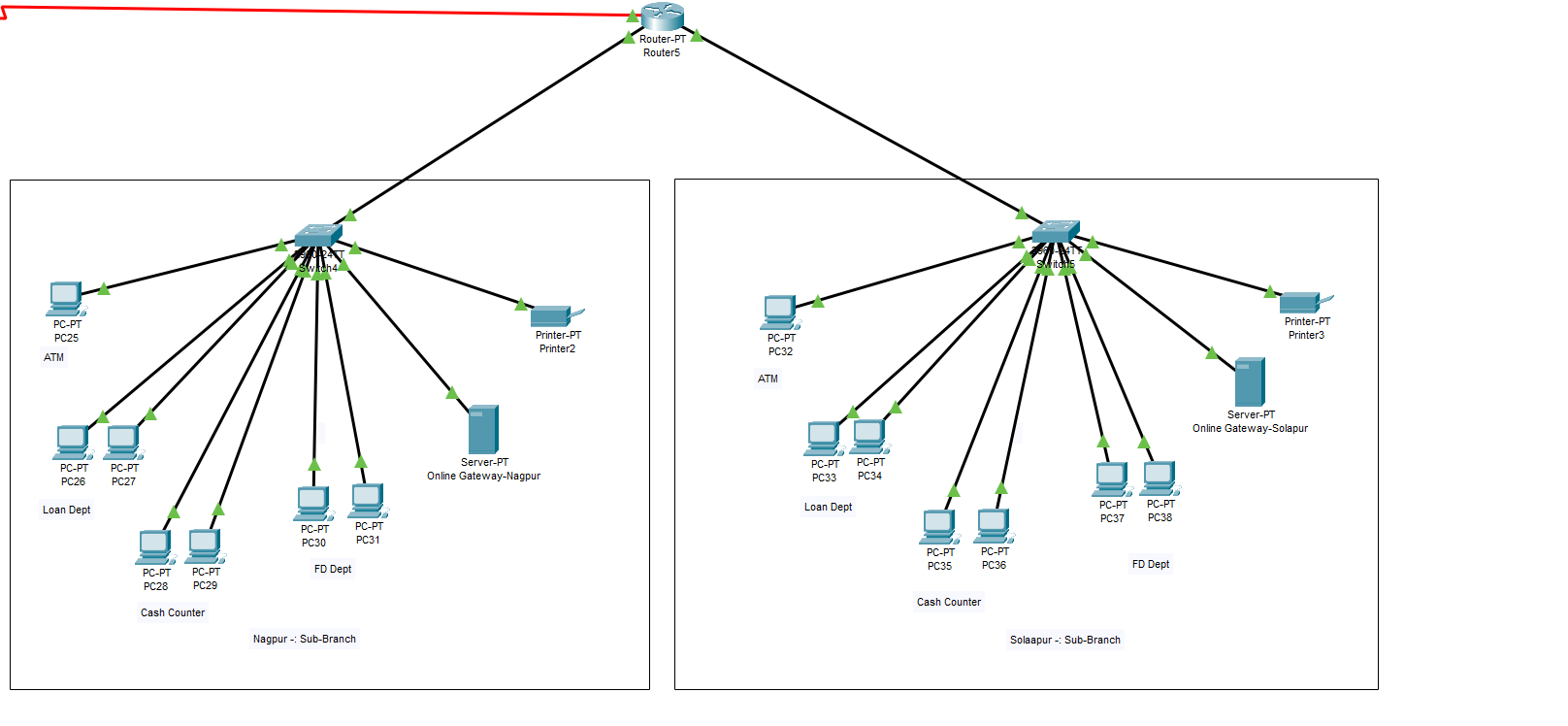
****

Figure 4 Nagpur and Solhapur Branch tropology diagram

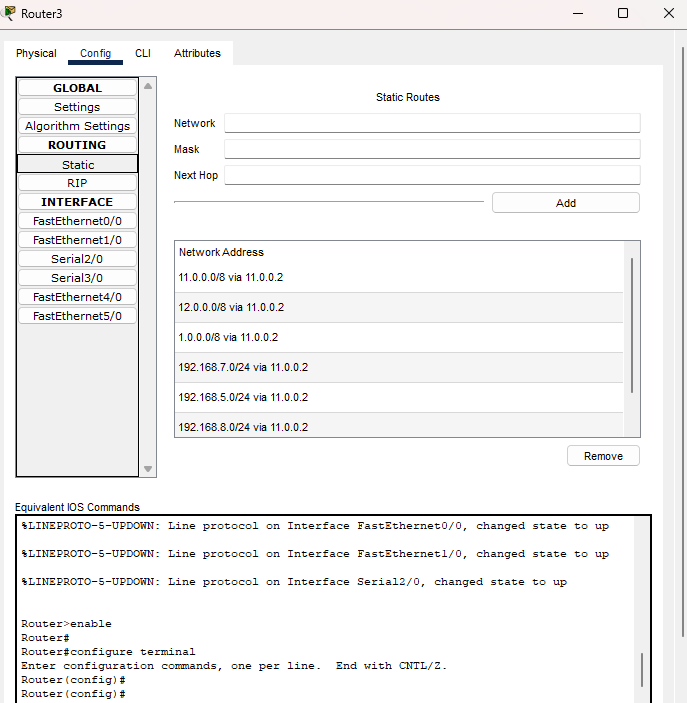


Figure 5 Router configuration

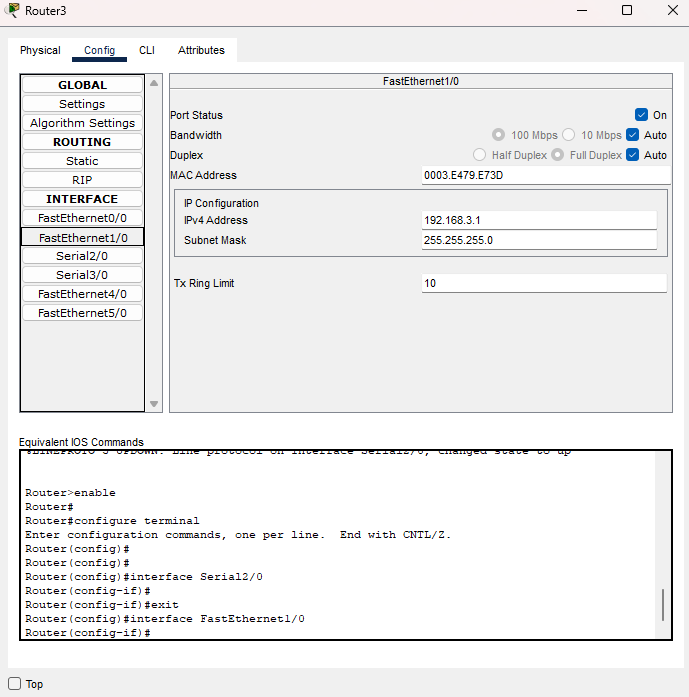


Figure 6 Router Configuration

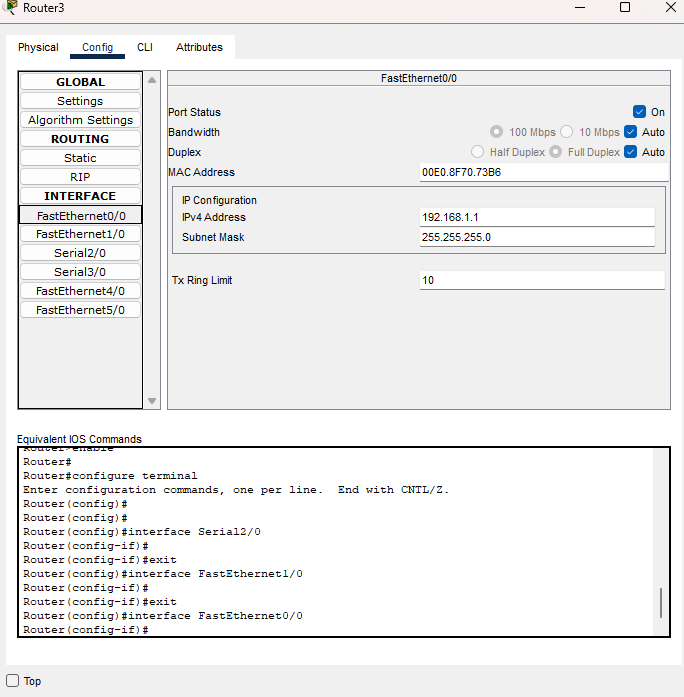
****

Figure 7 Router Configuration

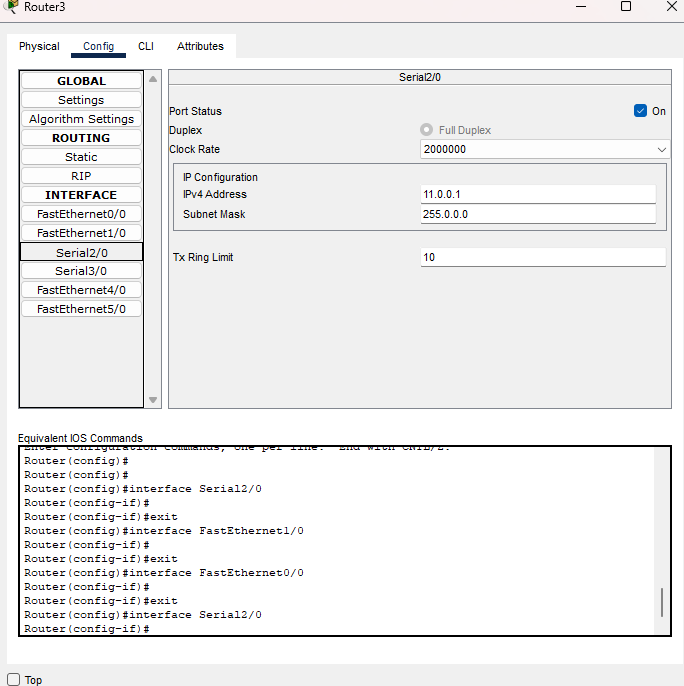
****

Figure 8 Router to outer connection

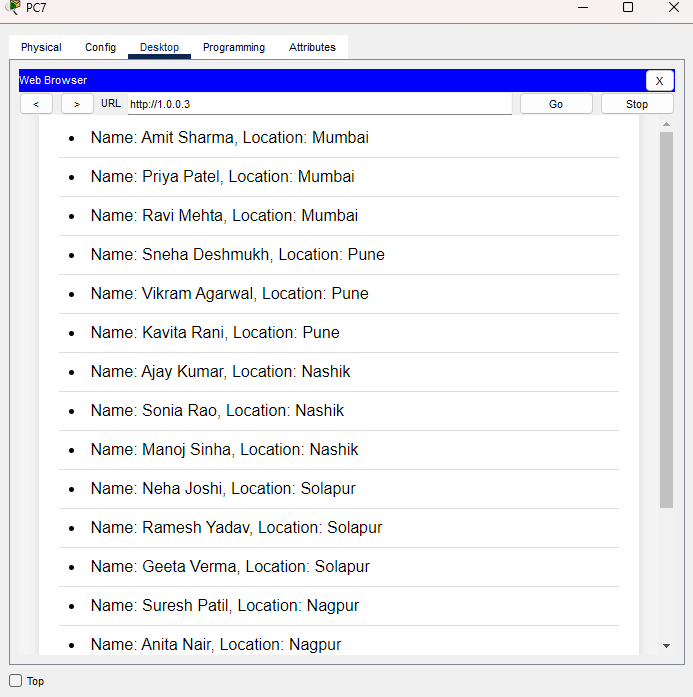
****

Figure 9 Pune Server room

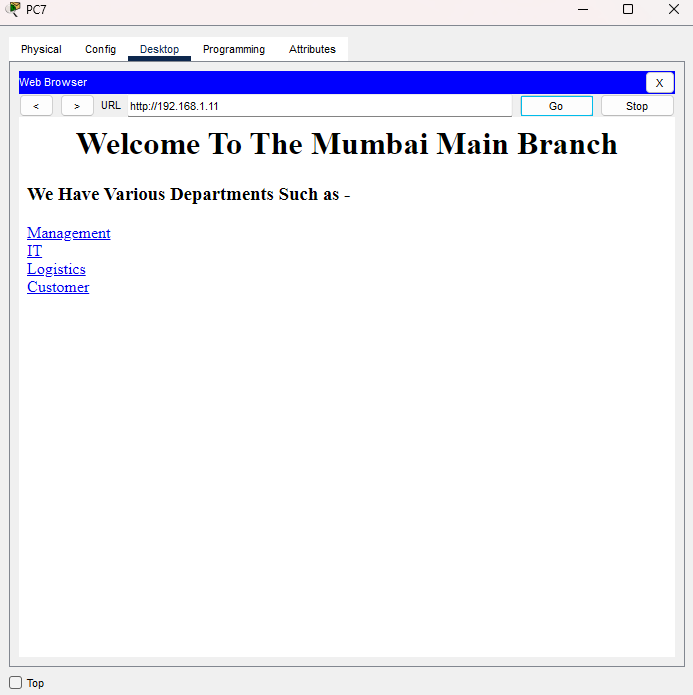
****

Figure 10 Main branch owerview

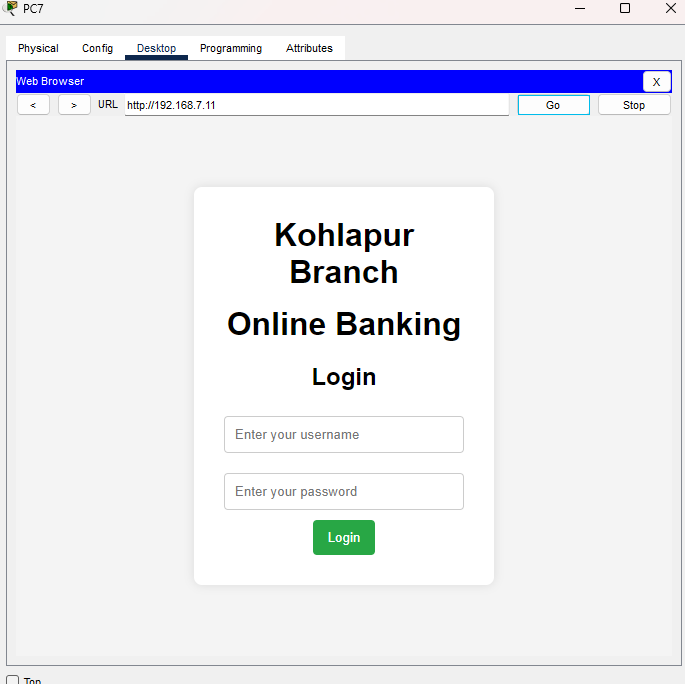
****

Figure 11 Sub Branches Owerview

**Advantages and Disadvantages**

Advantages:

1.Simplicity: Static routing is simple to implement and configure, especially for smaller networks with fewer routers, like in a banking network.

2. Predictability: With static routing, paths are fixed and predefined, making it easier to predict network behavior, which is crucial for maintaining security and reliability in banking systems.

3. Control: You have complete control over the routing paths, ensuring that data follows only trusted routes, important for sensitive financial transactions.

4. Low Overhead: Unlike dynamic routing protocols, static routing does not require routing updates or advertisements, reducing CPU and memory usage on routers.

5. Enhanced Security: Static routes are not subject to network disruptions caused by dynamic changes, reducing the risk of misconfigurations that could affect critical banking services.

Disadvantages:

1. Scalability Issues: As the network grows, manually configuring and maintaining static routes becomes impractical. In a large-scale banking network, static routing would require constant updates.

2. Lack of Redundancy: Static routes do not automatically reroute traffic in case of a network failure. This could be a significant issue in banking networks, where downtime can lead to financial losses.

3. Time-Consuming Maintenance: Any change in the network, such as adding or removing routers or links, requires manual reconfiguration of the routing tables.

4. No Load Balancing: Static routing cannot balance traffic load across multiple paths, which can lead to inefficiencies in bandwidth utilization in a banking network.

5. Risk of Misconfigurations: Manually setting routes increases the chance of human error, which can lead to security vulnerabilities or loss of network connectivity.

**Conclusion**

In this project, we successfully designed a **banking network infrastructure** using **Cisco Packet Tracer** with a focus on static routing to interconnect multiple branches across different cities. The network topology includes a **main branch in Mumbai** connected to sub-branches in **Nagpur**, **Nashik**, **Kolhapur**, **Solapur**, and a **central server room in Pune**. Each branch is assigned a unique IP addressing scheme with appropriate subnetting to ensure proper communication across all departments and branches.

Static routing was implemented to manually direct traffic between branches, ensuring efficient data flow and reliable connectivity. This method was chosen for its simplicity and control over routing paths, which is essential for the critical and secure operations of banking networks. The network also includes key security measures such as firewalls and access control lists (ACLs) to safeguard sensitive information.

This project demonstrates a robust, scalable, and secure network design suitable for banking operations, ensuring seamless communication and data sharing between branches while maintaining the highest levels of security.