Case Study

Bank Branch Networking

Course Name: Computer Networks

Course Code: BCSE308L

Date: 13th October, 2025

Faculty: Dr. Babu E

Group Members

Anivesh Gupta - 23BCE0291

Yogita Agrahari - 23BCE2285

Abdhija Aryavalli - 23BCE0889

Mohamed Akif Mohamed Razeen - 23BCE2349

Bank Branch Networking

Introduction:

This case study is about building a secure and efficient computer network for a bank with 25 branches across Tamil Nadu. The main goal is to connect all the branches to the main head office and to each other in a way that is both fast and safe. We need to make sure all communications are secure, especially when dealing with sensitive financial information.

To make this happen, we've designed a network in Cisco Packet Tracer. We've used a technique called subnetting with IPv4 addresses to give each branch its own unique IP address range. For routing, which is how data finds its way through the network, we've chosen a protocol called OSPF. This is because OSPF is great for large networks and can handle changes very quickly, which is super important for a bank. Finally, to protect all the data, we're proposing a VPN, which creates a secure, encrypted tunnel for all communication between the branches and the head office.

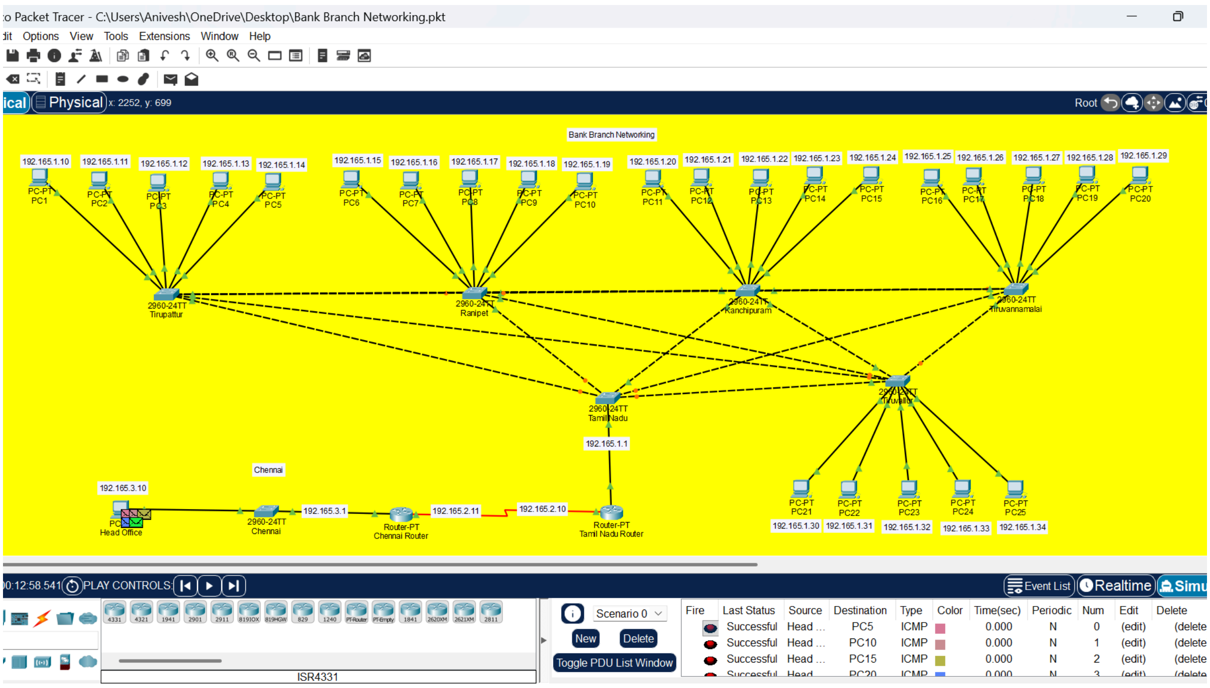
Expected Outcome:

By the end of this case study, you'll have a clear understanding of how to set up and manage a secure corporate network. Your group will create a presentation and a short report that covers the key details of our network design.

This will include:

- A diagram of the network topology you'll draw using Packet Tracer.
- A plan of the addressing scheme, showing how we've used subnetting.
- An explanation of why OSPF was chosen as the best routing protocol for this network.
- Details on how we're managing network traffic with flow and congestion control.
- An outline of one security measure, like a VPN, to protect the network.
- A recommendation for how the network can be scaled or upgraded in the future, for example, by migrating to IPv6.

Network diagram:



Addressing:

Used IPv4 for this project since the given address range is 192.165.1.0/24. IPv4 remains the most practical option for LANs and small to medium branch networks. IPv6 can be considered later for scalability, but within this network's size, IPv4 alone is sufficient.

IPv4 Addressing Details:

- Base network: **192.165.1.0/24**
- Total addresses: **256**
- Usable hosts: **254** (since 2 addresses are reserved for Network ID and Broadcast)
- Default subnet mask: **255.255.255.0**
- Prefix notation: **/24**

This network can be subdivided into smaller subnets to segregate traffic for different departments or VLANs (for example: Staff, Servers, ATMs, and Guest Wi-Fi).

Subnetting Calculation:

We will divide the `/24` network into four equal subnets using `/26` mask.

Subnet	Network ID	Prefix	Subnet Mask	Address Range	Usable Hosts	Broadcast
1	192.165.1.0	/26	255.255.255.192	192.165.1.0 – 192.165.1.63	62	192.165.1.63
2	192.165.1.64	/26	255.255.255.192	192.165.1.64 – 192.165.1.127	62	192.165.1.127
3	192.165.1.128	/26	255.255.255.192	192.165.1.128 – 192.165.1.191	62	192.165.1.191
4	192.165.1.192	/26	255.255.255.192	192.165.1.192 – 192.165.1.255	62	192.165.1.255

Addressing Hierarchy:

- Network Level: `192.165.1.0/24` – assigned to the site or branch.
- Subnet Level: Divided into four /26 networks, each representing a VLAN.
- Host Level: Individual devices (staff systems, ATMs, servers, etc.) are assigned unique IPs within their respective subnet.

Expected Outcome:

A structured IPv4 addressing scheme for the network `192.165.1.0/24` that provides segmentation for staff, servers, ATMs, and guest users, ensuring efficient routing and security isolation.

Routing:

For this network, OSPF (Open Shortest Path First) has been selected as the routing protocol.
OSPF is a dynamic link-state routing protocol that efficiently manages large and scalable networks like a bank with 25 branches spread across Tamil Nadu.

Reasons for choosing OSPF:

1. **Scalability:** OSPF can handle large and hierarchical networks better than RIP, which is limited to 15 hops.
2. **Faster Convergence:** When a link fails, OSPF quickly recalculates routes using Dijkstra's algorithm, minimizing downtime — crucial for financial transactions.
3. **Cost-based Routing:** OSPF selects paths based on link cost (bandwidth and reliability), ensuring optimal data flow between branches and the head office.
4. **VLSM Support:** It supports **Variable Length Subnet Masking**, allowing flexible IP address allocation for each branch subnet.
5. **Security:** OSPF supports **authentication** (MD5 or plain text) between routers, preventing unauthorized routing updates.

Hence, OSPF ensures the bank's inter-branch communication remains **efficient, reliable, and secure**.
Example: How Routing Happens in the Bank Network.
Let's say **Branch 1 (Vellore)** needs to send transaction data to the **Head Office (Tamil Nadu Hub)**.

1. Each branch router is connected to its own subnet, for example:
   - **Head Office (Router R0): 192.165.3.10/24**
   - **Branch 1 (Router R1 – Vellore): 192.165.2.10/24**
   - **Branch 2 (Router R2 – Tirupattur): 192.165.1.10/24**
   - **Branch 3 (Router R3 – Ranipet): 192.165.1.17/24**
   - **Branch 4 (Router R4 – Kanchipuram): 192.165.1.21/24**
   - **Branch 5 (Router R5 – Tiruvannamalai): 192.165.1.26/24**
   - **Branch 6 (Router R6 – Tiruvallur): 192.165.1.31/24**
2. All routers run **OSPF** within a single **Area 0 (Backbone Area)**.
   This means every router exchanges link-state advertisements (LSAs) to learn the **entire network topology**.
3. When Branch 1 sends data to the Head Office:
   - The **R1 router** checks its **OSPF routing table**.
   - It calculates the **shortest path** to 192.165.3.10/24 (Head Office network) using **Dijkstra's algorithm**.
   - OSPF considers the **link cost** — for example, higher-bandwidth leased lines have lower cost values.
   - The packet travels via the path with the lowest total cost, for example, **R1 → Tamil Nadu Router → Head Office**.
4. If a link fails, OSPF automatically recalculates a new shortest path, ensuring **no downtime** for transactions.

Thus, routing in this network is **dynamic, cost-optimized, and self-healing**, ensuring that even if one branch link fails, communication continues seamlessly through alternate routes.

Control Mechanisms:

In a banking network where data accuracy and timely delivery are critical, **flow and congestion control mechanisms** play a major role in maintaining performance.

Flow Control:

- Prevents a fast sender (e.g., a core server) from overwhelming a slow receiver (e.g., branch terminal).
- Uses **TCP sliding window** mechanism to manage the amount of data sent before receiving an acknowledgment.
- Ensures no data loss during peak transaction hours.

Congestion Control:

- Prevents the network from becoming overloaded when multiple branches send heavy data traffic simultaneously.
- TCP uses algorithms like **Slow Start**, **Congestion Avoidance**, and **Fast Recovery** to dynamically adjust the sending rate.
- Routers can use **queuing techniques** such as **Priority Queuing (PQ)** or **Weighted Fair Queuing (WFQ)** to ensure time-sensitive banking data (like fund transfers) is processed first.

Together, these mechanisms guarantee **smooth, delay-free, and reliable communication**, even during high-traffic situations like salary days or bulk transactions.

Security:

To comprehensively secure the bank's network, a multi-layered security approach is implemented, centered around establishing a **Virtual Private Network (VPN)** to protect data in transit.

- **Data Encryption with IPsec VPN:** The core security measure is the use of IPsec site-to-site VPNs to create encrypted tunnels for all communications. This applies to data moving between the head office and all 25 branches, as well as between individual branches. By using a strong encryption standard like AES-256, all sensitive financial data is rendered unreadable to anyone who might intercept it, ensuring both confidentiality and integrity.
- **Secure Routing Updates:** Beyond protecting user data, the routing infrastructure itself is secured. OSPF authentication is implemented using MD5/HMAC-SHA protocols. This security measure ensures that only trusted, authorized routers can participate in the exchange of routing information, preventing malicious actors from injecting false routes and disrupting the network.
- **Network Isolation and Segmentation:** The network design incorporates several features to limit the potential impact of a security breach:
    - **Subnetting:** A dedicated subnetting scheme assigns a unique block of IP addresses to each branch. This isolates traffic and helps contain threats within a single segment, preventing them from easily spreading across the entire network.
    - **Topology Hiding:** Route summarization is used at Area Border Routers (ABRs) to obscure the detailed internal topology of one area from another. This limits the amount of network information an attacker can gather.
    - **LSA Filtering:** The use of stub areas restricts the propagation of certain types of Link-State Advertisements (LSAs), further reducing the network information available to potential attackers.

Application Layer:

The Application Layer provides services that enable user-level communication across the bank’s 25 branches and head office. It supports essential protocols for web access, email, file transfer, and network management.

Required Protocols:

- **HTTP/HTTPS:** For secure web-based banking and administrative access.

- **DNS:** For translating domain names to IP addresses.
- **SMTP/IMAP:** For internal and external email communication.
- **SFTP:** For secure transfer of reports and backups.
- **DHCP & NTP:** For automatic IP allocation and time synchronization across all devices.

Security Measures:

- Use **HTTPS, SFTP, and SMTPS** to ensure data encryption and confidentiality.
- Implement **firewalls and access controls** to restrict unauthorized use.
- Apply **multi-factor authentication (MFA)** for sensitive systems.
- Enable **DNSSEC** to protect DNS queries.
- Regularly **update and patch** all application services.

Future-proofing:

To ensure the network can support the bank's long-term growth and technological evolution, the primary future-proofing strategy is a planned **migration to IPv6 via a dual-stack implementation**. This approach is supported by the network's inherently scalable design.

- **Dual-Stack IPv6 Transition:** A dual-stack network allows both IPv4 and IPv6 to run concurrently on the same devices and infrastructure. This strategy is recommended because it provides a seamless and gradual transition path, allowing new services to be deployed on IPv6 while legacy systems continue to operate on IPv4 without disruption. This migration will address the eventual exhaustion of IPv4 addresses and position the bank to take advantage of IPv6's enhanced features. For routing in the new environment, the plan includes deploying OSPFv3, the version of OSPF designed for IPv6.
- **Inherent Scalability of the Current Design:** The current network was built with future growth in mind:
    - **Scalable Routing Protocol:** OSPF was explicitly chosen for its high scalability, which allows the network to easily expand beyond the current 25 branches without degrading performance.
    - **Hierarchical Structure:** The network is organized into a backbone area (Area 0) and multiple stub areas. This modular, hierarchical design simplifies management and allows for easy expansion in the future by adding new branches or areas without a complete redesign.
    - **Robust Traffic Management:** The implementation of advanced queuing mechanisms like Priority Queuing (PQ) and Weighted Fair Queuing (WFQ) ensures that the network can effectively manage increased traffic loads as the bank's operations grow.

Conclusion:

We have designed a scalable, structured addressing scheme that ensures unique IP subnets for all 25 branches plus head office, and supports effective route summarization.

The 192.165.0.0/16 private block with /24 subnets per site strikes a balance between simplicity, expansion capability, and administrative ease.
Our approach aligns well with the selected routing protocol (OSPF) and supports summarization, which reduces routing table size and enhances network performance.
The design is secure and future-ready, allowing new branches or services to be added with minimal reconfiguration.

Additionally, essential application-layer protocols such as HTTPS, DNS, and SMTP have been integrated to ensure reliable and secure user-level communication across all branches.

Overall, the proposed solution meets the bank’s needs for reliable inter-branch connectivity, efficient network management, and secure data exchange.

Introduction - by Anivesh Gupta

Addressing - by Abdhija Aryavalli

Routing - by Yogita Agrahari

Control Mechanisms - by Yogita Agrahari

Security - by Mohamed Akif Mohamed Razeen

Application Layer - by Anivesh Gupta

Future-proofing - by Mohamed Akif Mohamed Razeen

Conclusion - by Abdhija Aryavalli