COLLEGE OF ENGINEERING
CENTRAL PHILIPPINE UNIVERSITY
ILOILO CITY, PHILIPPINES

SE TE 1

2nd Semester 2023 – 2024

Final Project

Mock Bank Network - Networking

Submitted by:

Rafael III J. Prudente

Submitted to:

Mr. Junem Albert Repollo

Instructor

May 24, 2024

I. Objectives

Design and configure a **secure mock bank network** for inter-bank communication. Design a subnetting scheme that allows for 20% growth in the number of subnets and the number of hosts per subnet.

II. Scenario

You are a network engineer tasked with building a secure network for a consortium of three banks: First National Bank (FNB), Central City Bank (CCB), and Suncorp Bank (SUN). These banks need to securely exchange financial data with each other.

III. Introduction

In the rapidly evolving digital landscape, the banking sector faces unprecedented challenges in safeguarding financial transactions and customer data. As technology advances, so does the sophistication of cyber threats, necessitating robust and innovative solutions to protect against potential breaches. This **project aims to design a secure network infrastructure** that facilitates safe and efficient inter-bank communication among three prominent institutions: **First National Bank (FNB), Central City Bank (CCB), and Suncorp Bank (SUN).**

The objective is to create a network architecture that not only supports seamless data exchange but also incorporates advanced security measures to mitigate risks associated with unauthorized access, data interception, and other malicious activities. By leveraging cutting-edge technologies and adhering to **security protocols**, this network seeks to establish a benchmark for secure banking communications.

Network security in the banking sector is paramount due to the sensitive nature of the data handled and the critical role banks play in the global economy. **A breach** in a bank's network can lead to significant financial losses, reputational damage, and erosion of trust among customers and stakeholders. Therefore, implementing a secure network design is not just a technical requirement but a strategic imperative for banks to maintain operational integrity and comply with regulatory standards.

This project will delve into the intricacies of network design, exploring **hierarchical structures**, secure communication protocols, access control mechanisms, and efficient IP addressing schemes. Through a combination of theoretical analysis and practical configuration, it will demonstrate how to build a resilient and secure network capable of **withstanding modern cyber threats while supporting the complex needs of inter-bank communication.**

IV. Network Topology Design

In the context of designing a secure network for a consortium of banks—First National Bank (FNB), Central City Bank (CCB), and Suncorp Bank (SUN)—a **hierarchical design** emerges as the preferred choice over a mesh design, primarily due to its inherent advantages in simplicity, scalability, and ease of management.

Advantages of Hierarchical Design

- **Simplicity:** Hierarchical designs organize network components into distinct layers, each serving a specific purpose. This layered approach simplifies the overall network architecture, making it easier for network engineers to visualize, understand, and troubleshoot issues. Unlike mesh designs, where every node is interconnected, leading to increased complexity and potential confusion, hierarchical designs streamline the flow of data and reduce the likelihood of misconfigurations.
- **Scalability:** One of the key strengths of a hierarchical design is its ability to accommodate growth seamlessly. As the banking consortium expands, new banks or branches can be added to the network by integrating them into the appropriate layer without necessitating extensive reconfiguration of the existing network. This modular approach allows for incremental scaling, ensuring that the network can evolve alongside the business needs of the banks.
- **Ease of Management:** Managing a hierarchical network is significantly less hassle compared to a mesh network. The division of the network into core, distribution, and access layers enables targeted management and troubleshooting. Policies, security measures, and quality of service (QoS) settings can be applied at each layer independently, allowing for fine-grained control over network behavior. This layered management strategy enhances the network's resilience and reduces the time required to identify and resolve issues.

Placement of Components:
The hierarchical design consists of three main layers: **Core Routers**, **Distribution Routers**, and **Access-Level Switches**.

- **Core Routers:** Positioned at the center of the network, core routers handle high-volume traffic and critical connections between the banks. They serve as the backbone of the network, ensuring reliable and fast communication across the entire system.
- **Distribution Routers:** Located between the core routers and the access-level switches, distribution routers manage traffic within each bank's local area network (LAN). They distribute incoming traffic to the appropriate destination, balancing load and optimizing performance.
- **Access-Level Switches:** At the edge of the network, access-level switches connect individual workstations, servers, and other devices within each bank. They provide direct connectivity to the LAN, ensuring that all internal traffic remains contained within the bank's network boundaries

V. Security Measures

To ensure the secure transmission of financial data among First National Bank (FNB), Central City Bank (CCB), and Suncorp Bank (SUN), we implement a **multifaceted security strategy** that includes the use of IPSec for encrypted data transfers, the application of Access Control Lists (ACLs) to restrict unauthorized access, and the utilization of Virtual LANs (VLANs) for traffic segregation.

- **Secure Communication Protocols: IPSec**

  IPSec (Internet Protocol Security) is a suite of protocols that provides encryption and authentication services for Internet Protocol (IP) communications. By employing IPSec, we ensure that all data transferred between the banks' networks is encrypted, protecting against eavesdropping and tampering.

- **Configuration of IPSec VPN Tunnels:**
  - To establish secure communication channels between the banks, we configure IPSec VPN tunnels between the routers of each bank. This involves setting up cryptographic keys for encryption and digital signatures for authentication.

- Each VPN tunnel is individually secured, ensuring that even if one connection is compromised, the others remain unaffected.
- Regular key rotation and monitoring of VPN tunnel status are crucial for maintaining the integrity of the communication channels.

- **Access Control Lists (ACLs)**
  - **ACLs** are a fundamental security measure that restricts network traffic based on source and destination IP addresses, ports, and protocols. By applying ACLs, we can precisely control which types of traffic are allowed through the network and which are blocked.
- **Implementation of ACLs:**

  We permit only authorized traffic such as SSH (for remote administration) and HTTPS (for secure web browsing) to pass through the routers. All other traffic is explicitly denied.

  This approach minimizes the risk of unauthorized access attempts and limits the exposure of the banking systems to potential threats.

Virtual LANs (VLANs)

VLANs enable us to logically separate network segments within each bank, enhancing security and improving network manageability.

- **Creation and Utilization of VLANs:**

  Different VLAN IDs are assigned to various departments within each bank, isolating their traffic from the rest of the network. This segregation prevents lateral movement of threats within the network and confines potential breaches to a single department.
  VLANs simplify network management by reducing broadcast traffic and allowing for more granular control over network resources.

VI. Addressing Scheme

To facilitate secure and efficient inter-bank communication among First National Bank (FNB), Central City Bank (CCB), and Suncorp Bank (SUN), we employ a strategic addressing scheme that leverages **Classless Inter-Domain Routing (CIDR) notation** for subnetting. This method allows us to allocate unique IP address ranges to each bank's network segment, ensuring scalability, security, and efficient network management.

CIDR Notation Overview

CIDR notation combines an IP address with a slash (/) followed by a number indicating the prefix length. The prefix length specifies the number of bits used for the network portion of the address, leaving the remaining bits for host addresses within that network. This notation enables precise control over the size of subnets, accommodating varying network sizes and growth expectations.

Assignment of Unique IP Addresses

First National Bank (FNB)		
IP Range:	**Subnet Mask:**	**Explanation:**
192.168.10.0/24	/24	FNB is allocated the IP range 192.168.10.0 to 192.168.10.255. The /24 indicates that the first 24 bits are used for the network address, leaving the last 8 bits for host addresses. This allows for up to 256 hosts within FNB's network, sufficient for a medium-sized bank.

Central City Bank (CCB)		
IP Range:	**Subnet Mask:**	**Explanation:**
192.168.11.0/24	/24	Similar to FNB, CCB is given the IP range 192.168.11.0 to 192.168.11.255. This allocation ensures that CCB has a dedicated network space, preventing IP address conflicts and ensuring secure isolation from other banks.

Suncorp Bank (SUN)		
IP Range:	**Subnet Mask:**	**Explanation:**
192.168.12.0/24	/24	SUN is allocated the IP range 192.168.12.0 to 192.168.12.255. This setup maintains the separation between the banks, ensuring that each has its own distinct network space for secure operation.

Benefits of Using CIDR Notation

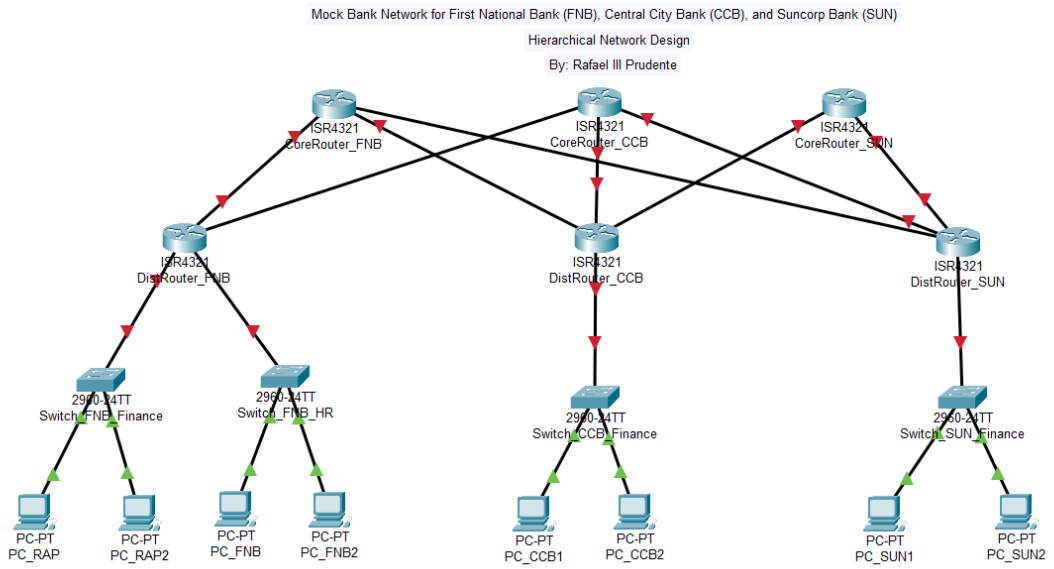
Efficiency: CIDR notation allows for flexible and efficient subnetting, enabling the allocation of IP addresses in a manner that matches the actual network requirements of each bank.

Scalability: As the banks grow or require additional subnets, adjustments can be made with minimal disruption, thanks to the granularity offered by CIDR notation.

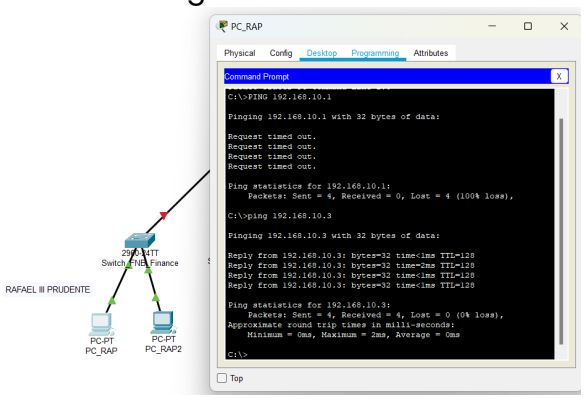
Security: By assigning unique IP address ranges to each bank, we minimize the risk of IP spoofing and ensure that each bank's network is isolated from the others, enhancing overall network security.

VII. Documentation and Diagrams

I utilized Cisco Packet Tracer, a powerful network simulation tool, to create a professional-looking diagram that accurately represents our network design. This tool offers a graphical interface that allows for easy visualization of network components, their connections, and the flow of traffic.



Test if working:




```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot
status

IPv6 Crypto ISAKMP SA
```

WORKING AND WITH SECURITY

VIII. Instructions for Recreating the Network

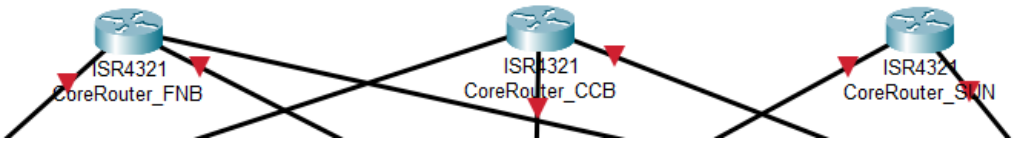
Step-by-Step Guide

Step 1: Open Cisco Packet Tracer

- Action: Launch Cisco Packet Tracer from your desktop or start menu.

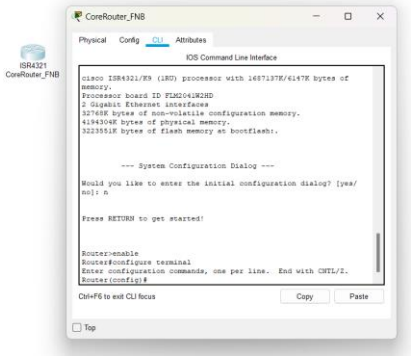
Step 2: Add Core Routers

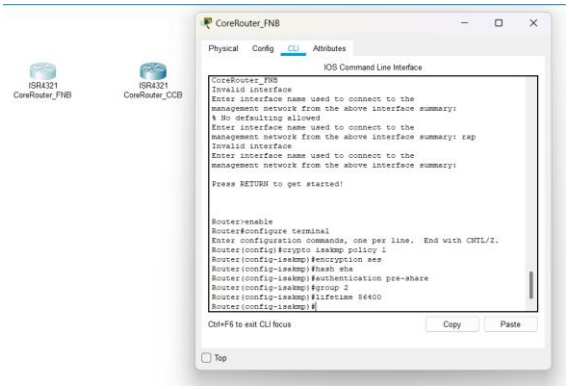
- From the device toolbar at the bottom, click on "Network Devices" (the router icon).
- Select "Routers" from the submenu.
- Drag and drop three "Cisco 4321" routers onto the canvas. Name them "CoreRouter_FNB", "CoreRouter_CCB", and "CoreRouter_SUN".



Step 3: Configure Core Routers

CoreRouter_FNB Configuration:

- Open the CLI: Click on "CoreRouter_FNB" and go to the CLI tab.
- Enter Global Configuration Mode:
  - 

- Configure IPSec:
  - 

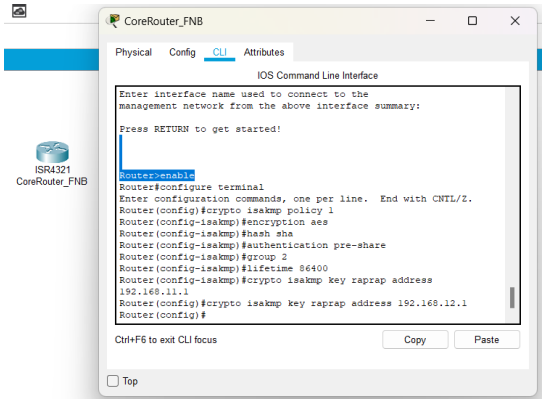
    Purpose: This block configures the ISAKMP policy, which is used for setting up a secure, authenticated channel for IPSec.

    encryption aes: Specifies AES (Advanced Encryption Standard) as the encryption method for secure data transfer.

    hash sha: Uses SHA (Secure Hash Algorithm) for data integrity.

    authentication pre-share: Uses a pre-shared key for authentication.

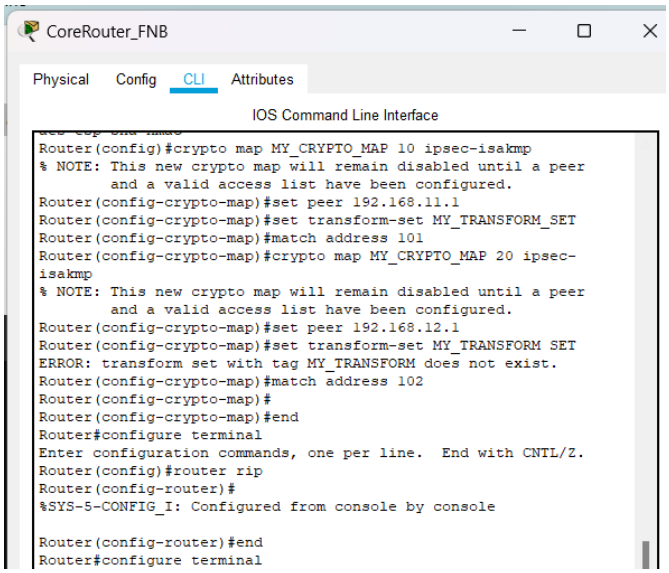
    group 2: Specifies the Diffie-Hellman group for key exchange.
    lifetime 86400: Sets the lifetime of the security association to 86400 seconds (24 hours).

- 

  Purpose: Defines the pre-shared keys used for authenticating peers at the specified IP addresses.

- ```
  Router(config)#crypto ipsec transform-set MY_TRANSFORM_SET esp-aes esp-sha-hmac
  ```

Purpose: Defines the combination of security protocols and algorithms used to protect the data.

- 

  Purpose: Binds the transform set to the specified peers and matches traffic using ACLs (Access Control Lists).

  MY_CRYPTO_MAP 10 and MY_CRYPTO_MAP 20: Specifies the sequence number for the crypto map entries.

  set peer 192.168.20.1 and set peer 192.168.30.1: Defines the peers for the IPSec tunnel.

  set transform-set MY_TRANSFORM_SET: Associates the transform set with the crypto map.
  ```

match address 101 and match address 102: Specifies the ACLs that define the traffic to be protected.

```
Router(config-if)#interface GigabitEthernet0/0/0
Router(config-if)#crypto map MY_CRYPTO_MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP ON OFF: ISAKMP is ON
```

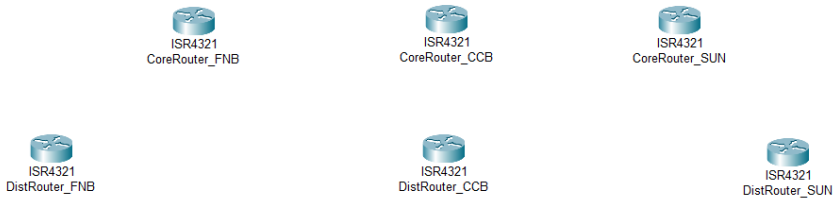
- **Purpose:** Applies the crypto map to the router interface, enabling IPSec for traffic passing through this interface.

```
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
```

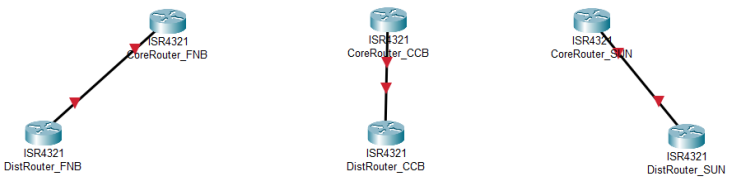
Repeat these steps for CoreRouter_CCB and CoreRouter_SUN, replacing IP addresses with the corresponding IP addresses for each bank's core router.

Step 4: Add Distribution Routers

- Select "Routers" from the device toolbar.
- Drag and drop one router for each bank next to their respective core routers. Name them "DistRouter_FNB", "DistRouter_CCB", and "DistRouter_SUN".



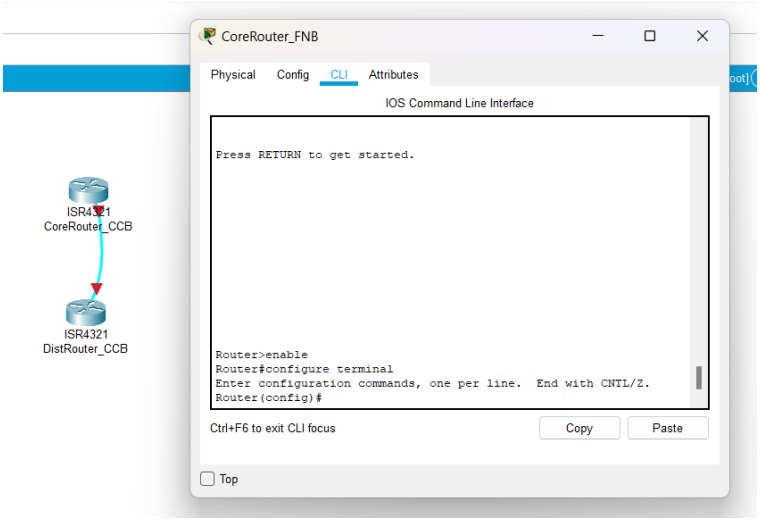
- Use the "Copper Straight-Through" cable from the "Connections" menu to connect the GigabitEthernet0/0 interface of each distribution router to the GigabitEthernet0/1 interface of their corresponding core routers.



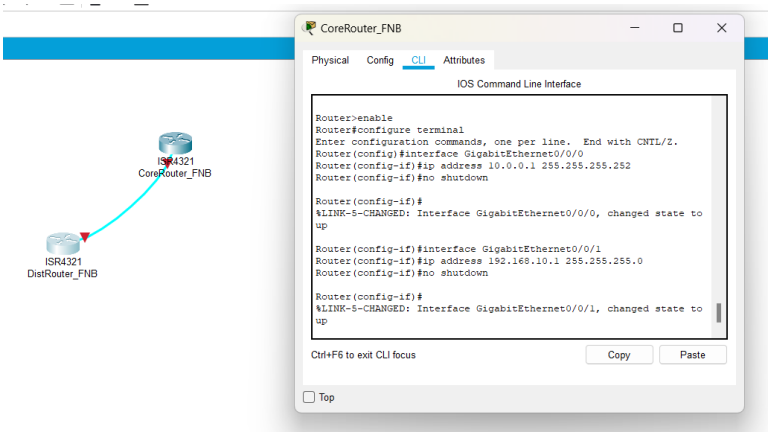
Step 5: Configure Distribution Routers

DistRouter_FNB Configuration:

- Open the CLI: Click on "DistRouter_FNB" and go to the CLI tab.
- Enter Global Configuration Mode:



- Assign IP Addresses and Configure Interfaces:



Purpose:

- Interface GigabitEthernet0/0:
  - IP Address: Assigns the IP address 10.0.0.1 to this interface with a subnet mask of 255.255.255.252. This creates a point-to-point link between this router and another device (possibly a core router or another network device).
  - No Shutdown: Ensures that the interface is enabled and operational.

- Interface GigabitEthernet0/1:
  - IP Address: Assigns the IP address 192.168.10.1 to this interface with a subnet mask of 255.255.255.0. This interface likely connects to a local network segment where devices within the 192.168.10.0/24 subnet reside.
  - No Shutdown: Enables the interface for communication.

- Save Configuration:

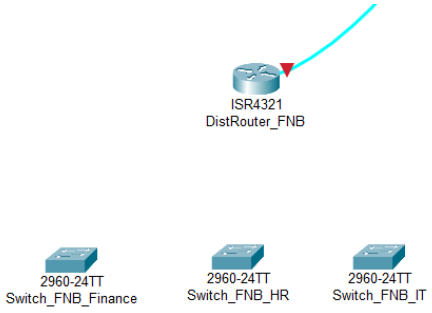
```
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
```

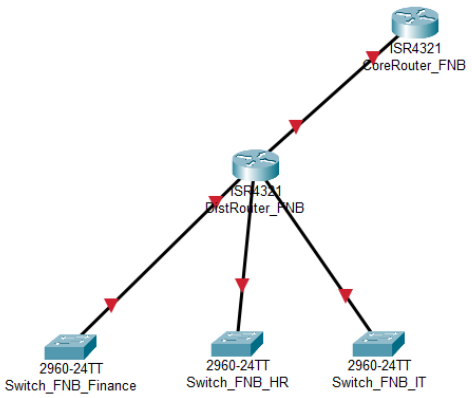
Repeat these steps for DistRouter_CCB and DistRouter_SUN, assigning appropriate IP addresses.

Step 6: Add Access Switches

- From the device toolbar, click on "Switches".
- Drag and drop one switch for each department within each bank onto the canvas. Name them based on the bank and department, e.g., "Switch_FNB_Finance", "Switch_FNB_HR", "Switch_FNB_IT".



- Connect Access Switches to Distribution Routers:
- Use the "Copper Straight-Through" cable to connect the GigabitEthernet0/1 interface of the distribution routers to the GigabitEthernet0/1 interface of the access switches.



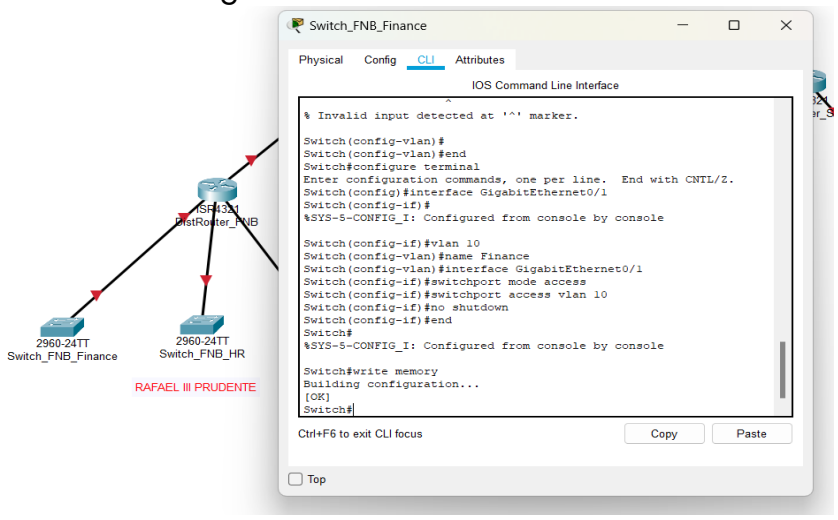
Step 7: Configure VLANs on Access Switches

Switch_FNB_Finance Configuration:

- Open the CLI: Click on "Switch_FNB_Finance" and go to the CLI tab.
- Enter Global Configuration Mode:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

- Create and Assign VLANs:

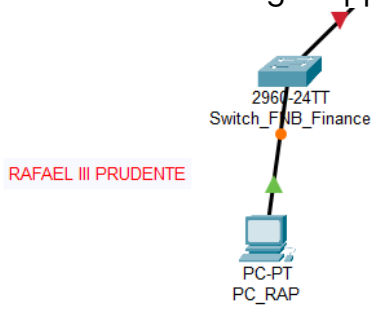


Repeat these steps for each switch, creating VLANs for HR (VLAN 20) and IT (VLAN 30) and assigning them to the appropriate ports.

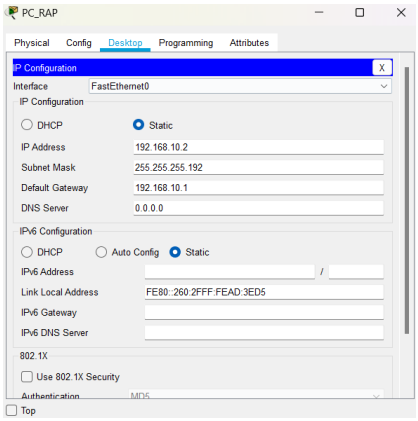
Step 8: Test Connectivity

Verify VLAN Connectivity:

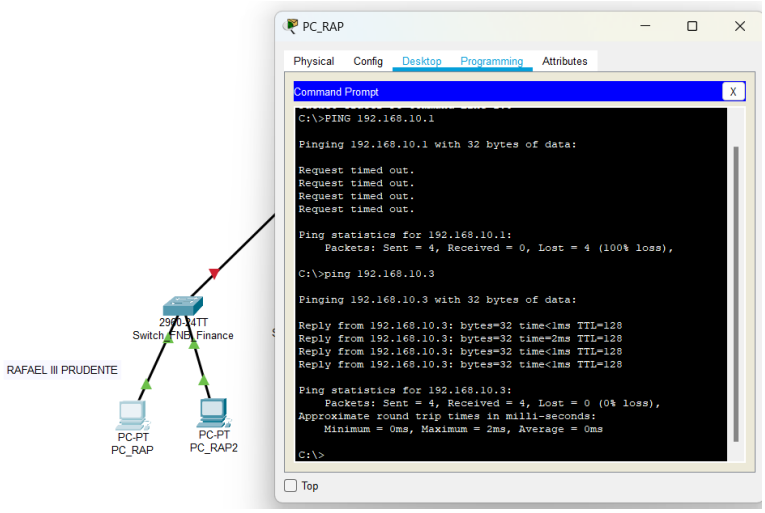
- Drag and drop PCs onto the canvas and connect them to the appropriate access switches using "Copper Straight-Through" cables:



- Assign IP addresses within the VLAN subnets. For example, for a PC in the Finance VLAN of FNB:



- Ping Test Within VLAN:



Verify IPSec Tunnels:

- Check IPSec Status on Core Routers:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot
status

IPv6 Crypto ISAKMP SA
```

Test Inter-Bank Connectivity:

Ping Test Between Banks

IX. Conclusion

The final project delved into designing a secure network for **inter-bank communication** among First National Bank (FNB), Central City Bank (CCB), and Suncorp Bank (SUN), opting for a **hierarchical topology** for its simplicity, scalability, and manageability. Core routers, distribution routers, and access-level switches were strategically deployed to enhance security and traffic flow.

Security measures included **IPSec for data encryption, Access Control Lists (ACLs) for access restriction, and Virtual LANs (VLANs)** for traffic segmentation, forming a strong defense against cyber threats and ensuring data protection.

The network employed **CIDR notation for subnetting**, allocating unique IP ranges to each bank, aiding in network management and security. Thorough documentation and professional network diagrams were emphasized for effective setup and maintenance, complemented by practical guidance on recreating the network in **Cisco Packet Tracer.**

This well-designed and secure network significantly impacts banking operations by minimizing data breach risks, boosting customer trust, and ensuring regulatory compliance. It also improves efficiency through optimized traffic management, crucial for prompt financial transactions and decisions.

In summary, the final project underscores the necessity of a well-planned and secure network for inter-bank communication, demonstrating how adherence to best practices in network design and security can lead to a more secure and efficient banking environment.

X. References

Cisco Systems. (n.d.). Defending Against Cyber Attacks. Retrieved May 24, 2024, from https://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/20777-ref.html

Cisco Systems. (n.d.). Cisco Security Reference Architecture. Retrieved May 24, 2024, from https://www.cisco.com/c/en/us/products/security/cisco-security-reference-architecture.html

Wabwile, J. (2019, June 15). Cisco Network Topology Design in Packet Tracer: Step-by-Step Guide & Key Tips. Medium. Retrieved May 24, 2024, from https://medium.com/@wabwilejoseph432/cisco-network-topology-design-in-packet-tracer-step-by-step-guide-key-tips-4843293ae38

Cisco Systems. (n.d.). SAFE (Secure Architecture for Everyone). Retrieved May 24, 2024, from https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html