Project Report

On

Computer Networking: Concepts

(CSE3751)

Secure and Scalable Bank Network

Submitted by:

Name1:Ashish Kumar Samantaray	Regd. No.:2241019278
Name2:Ruchi Rangada Kar	Regd. No.:2241011021
Name3:Shreya Mishra	Regd. No.:2241013173
Name4:Shaurya Singh	Regd. No.:2241019512

B. Tech. BRANCH 5th Semester (Section 022)

INSTITUTE OF TECHNICAL EDUCATION AND RESEARCH
(FACULTY OF ENGINEERING)
SIKSHA 'O' ANUSANDHAN (DEEMED TO BE UNIVERSITY),
BHUBANESWAR, ODISHA

Declaration

We, the undersigned students of B. Tech. of **Computer Science and Engineering** Department hereby declare that we own the full responsibility for the information, results etc. provided in this PROJECT titled "Secure and Scalable Bank Network" submitted to **Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar** for the partial fulfillment of the subject **Computer Networking: Concepts (CSE 3751)**. We have taken care in all respect to honor the intellectual property right and have acknowledged the contribution of othersfor using them in academic purpose and further declare that in case of any violation of intellectual property right or copyright we, as the candidate(s), will be fully responsible for the same.

Name1: Ashish Kumar Samantaray	Regd. No.:2241019278
Name2: Ruchi Rangada Kar	Regd. No.:2241011021
Name3: Shreya Mishra	Regd. No.:2241013173
Name4: Shaurya Singh	Regd. No.:2241019512

Date:

Place: **Bhubaneswar**

Abstract

In the modern banking sector, secure and scalable network infrastructure is vital to ensure seamless communication between branches and centralized operations. This paper presents the design and implementation of a secure and scalable banking network using Cisco Packet Tracer. The network interconnects four geographically dispersed branch offices with a centralized head office, hosting the Bank Management System (BMS) on a server accessible to authorized users. Dynamic routing using Open Shortest Path First (OSPF) protocol ensures reliable communication and adaptability to network topology changes.

To enhance operational efficiency, Dynamic Host Configuration Protocol (DHCP) services are configured at each branch to manage IP address allocation dynamically, reducing administrative overhead. Security is prioritized by implementing Access Control Lists (ACLs) on network routers to restrict unauthorized access to the centralized BMS server, ensuring the confidentiality and integrity of sensitive banking data. The proposed network is tested for functionality, including communication between branches, centralized server access, and enforcement of ACL policies.

The deliverables include a detailed network topology diagram, router configurations for OSPF, DHCP, and ACLs, and testing logs validating successful communication and security measures. This design emphasizes a scalable, secure, and efficient approach to managing banking networks, addressing critical requirements for adaptability, reliability, and security in financial institutions.

Contents

Introduction

The rapid advancements in technology and the growing complexity of financial operations necessitate robust, scalable, and secure network infrastructures in the modern banking sector. Efficient communication between distributed branch offices and a centralized head office is essential to ensure smooth transactions, data integrity, and operational reliability. This project focuses on designing and implementing a secure and scalable network model for a banking system using **Cisco Packet Tracer**.

The proposed network infrastructure connects four branch offices to a central head office, where the Bank Management System (BMS) server resides. Reliable communication across this architecture is achieved using **Open Shortest Path First (OSPF)**, a dynamic routing protocol that adapts to network topology changes and provides optimal path selection. Furthermore, **Dynamic Host Configuration Protocol (DHCP)** services are configured at each branch to automate IP address management, minimizing manual intervention and improving administrative efficiency.

Security remains a cornerstone of this design. To safeguard the centralized BMS server from unauthorized access, **Access Control Lists (ACLs)** are applied on network routers. These ACLs enforce stringent access policies, preventing branches designated with restricted access from reaching critical resources. Comprehensive testing, including connectivity verification and ACL enforcement validation, ensures that the network meets functional, security, and scalability requirements.

This report outlines the topology design, device configurations, and a detailed analysis of the network's performance, providing an integrative approach to addressing core networking challenges in financial institutions. The methodology, results, and testing logs collectively demonstrate how this design supports the dynamic, secure, and scalable infrastructure needed for modern banking environments.

Problem Statement

The problem at hand is the design and implementation of a **secure and scalable bank network** that ensures reliable communication between multiple branch offices and a centralized head office. The network needs to be configured using **Cisco Packet Tracer** and must meet the following key objectives:

1. **Four Branch Offices Connected to a Central Head Office**: The network should consist of four branch offices located in different cities, with each branch connected via a router to the **centralized head office**. The router setup needs to allow communication between the branches and the head office while maintaining scalability and ease of management.

2. **Centralized Bank Management System (BMS)**: The head office will host the **Bank Management System (BMS)** on a centralized server. Clients from the branch offices should be able to create accounts and access the system.

3. **Dynamic Routing for Reliable Communication**: Dynamic routing (OSPF) should be implemented on the routers to ensure that communication between all branches and the head office is resilient to network changes (such as device failures or network topology changes).

4. **DHCP Services for Client Devices**: Each branch should have a **DHCP service** to dynamically assign IP addresses to client devices such as computers and workstations.

5. **Access Control Lists (ACLs) for Security**: To ensure that only authorized devices have access to the centralized server at the head office, **Access Control Lists (ACLs)** should be configured on the routers. The ACLs will restrict unauthorized access from certain branches.

Objects to be considered for implementation:

- **Routers**: Five routers (one for each branch and one for the head office) will be needed to interconnect the networks.

- **Switches**: Each branch and head office will have a switch to connect the PCs and other devices.

- **PCs/Workstations**: These will be connected at each branch and the head office, allowing clients to access the Bank Management System.

- **Server**: A centralized server at the head office will host the Bank Management System (BMS).

- **Links**: WAN links between routers for inter-branch communication.

- **DHCP**: The routers will provide **DHCP services** for IP address assignment.

- **OSPF**: **Open Shortest Path First (OSPF)** protocol will be configured on the routers to facilitate dynamic routing.

- **ACL**: **Access Control Lists (ACLs)** will be implemented on the routers to restrict access to the centralized server.

II. Highlighting the Constraints (if any)

- **Device Limitations**: Cisco Packet Tracer may have limitations when it comes to the number of devices and certain advanced network protocols. While it supports OSPF, DHCP, and ACL configurations, it may not handle very large-scale network simulations as efficiently as other Cisco network simulation tools.

- **IP Address Range**: The problem is constrained by the need to use private IP address ranges (as specified in the IP addressing scheme). This limits the number of addressable devices in the network.

- **Security Considerations**: While ACLs will be implemented to restrict access, Packet Tracer does not fully emulate real-world security implementations, so further testing and fine-tuning on real hardware may be necessary.

- **Simulated Environment**: Given the simulated nature of Packet Tracer, certain real-world constraints, such as link bandwidth, network latency, and real-world hardware failures, cannot be fully replicated.

Methodology

The initial phase involved designing a robust and scalable network topology in Cisco Packet Tracer. The design ensured efficient connectivity between the head office and its branch offices while meeting all specified requirements. Key design features included:

1. **Central Head Office**:
   - The head office served as the central hub of the network, hosting the Bank Management System (BMS) on a server.
   - A router at the head office connected to the branch office routers via WAN links to enable communication across the network.

2. **Branch Offices**:
   - Four branch offices, each located in different cities, were incorporated into the topology.
   - Each branch was designed with a local area network (LAN) consisting of a router and two PCs for clients to access the BMS.
   - DHCP services were planned to enable dynamic IP management, simplifying client device configuration.

3. **Inter-Branch Connectivity**:
   - WAN links were designed using subnetted IP addresses (/30) to connect the head office router to each branch router.
   - Dynamic routing (OSPF) was chosen for adaptive and efficient inter-branch communication.

Additionally, the number of ports were increased and serial bus was brought into use by attaching the **HWIC-2T** Serial Interface at the back of the **router-1942.**

IP Addressing Scheme:

Network Segment	**Subnet**	**Device**	**IP Address**
Head Office	192.168.0.0/24	R0 (G0/0)	192.168.0.1
		Server	192.168.0.100
		PC0	192.168.0.101
		PC1	192.168.0.102
Branch 1	192.168.1.0/24	R1 (G0/0)	192.168.1.1
		PC2	DHCP
		PC3	DHCP
Branch 2	192.168.2.0/24	R2 (G0/0)	192.168.2.1
		PC4	DHCP
		PC5	DHCP
Branch 3	192.168.3.0/24	R3 (G0/0)	192.168.3.1
		PC6	DHCP
		PC7	DHCP
Branch 4	192.168.4.0/24	R4 (G0/0)	192.168.4.1
		PC8	DHCP
		PC9	DHCP
WAN Links (/30)		R0-R1 (S0/0/0)	10.0.1.1 / 10.0.1.2
		R0-R2 (S0/0/1)	10.0.2.1 / 10.0.2.2
		R0-R3 (S0/1/0)	10.0.3.1 / 10.0.3.2
		R0-R4 (S0/1/1)	10.0.4.1 / 10.0.4.2

The second phase involved configuring the routers, switches, and client PCs in the network. Key steps included:

1. **Router Configuration:**
   - The routers were configured to support OSPF dynamic routing, ensuring adaptive and reliable communication between the head office and branch offices.
   - DHCP services were implemented on branch routers, dynamically assigning IP addresses to client PCs within their respective subnets.
2. **Switch and PC Configuration:**
   - Switches were set up to connect client PCs and routers within each branch LAN.
   - PCs were configured to obtain IP addresses dynamically from the DHCP server running on the branch router.
3. **Access Control**:
   - Access Control Lists (ACLs) were configured on routers to secure the network.
   - ACLs ensured only authorized devices could access the centralized BMS server, restricting unnecessary or malicious traffic.

The final phase implemented specific CLI commands on routers to meet the project objectives:

1. **Dynamic Routing and DHCP**:
   - OSPF was configured on all routers to ensure dynamic routing.
   - DHCP pools were created on branch routers with excluded addresses for router interfaces and appropriate default gateways.
2. **Security through ACLs**:
   - ACL rules were applied to filter traffic and protect sensitive resources such as the BMS server.
3. **Verification and Testing**:
   - Network connectivity was verified using ping and traceroute commands.
   - ACL functionality was tested by attempting unauthorized access to the BMS server, ensuring restrictions were effectively enforced.

This structured approach ensured a secure and scalable network design, providing seamless connectivity and efficient operations for the bank’s branch offices.

Below is the code for CLI configuration of the headoffice Router (R0):

For WAN Links:

```
interface serial 0/0/0
ip address 10.0.1.1 255.255.255.252
no shutdown

interface serial 0/0/1
ip address 10.0.2.1 255.255.255.252
no shutdown

interface serial 0/1/0
ip address 10.0.3.1 255.255.255.252
no shutdown

interface serial 0/1/1
ip address 10.0.4.1 255.255.255.252
no shutdown
```

For OSPF Configuration:

```
router ospf 1
network 192.168.0.0 0.0.0.255 area 0
network 10.0.1.0 0.0.0.3 area 0
network 10.0.2.0 0.0.0.3 area 0
network 10.0.3.0 0.0.0.3 area 0
network 10.0.4.0 0.0.0.3 area 0
```

Similarly for R1,R2,R3,R4 (Branch Offices):

For WAN Interface:

```
interface serial 0/0/0
ip address 10.0.1.2 255.255.255.252
no shutdownip address 10.0.4.1 255.255.255.252
no shutdown
```

For DHCP Configuration:

```
ip dhcp pool Branch1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 8.8.8.8
```

For OSPF Configuration:

```
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 10.0.1.0 0.0.0.3 area 0
```

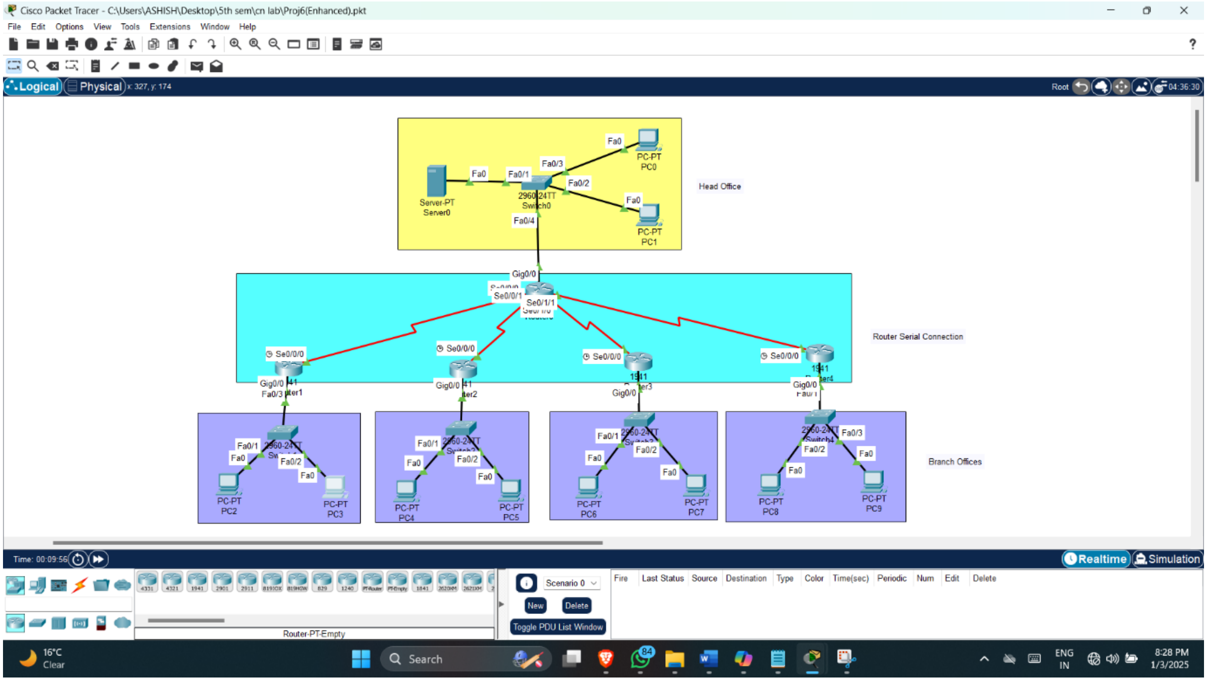
The steps for Router 1,2,3,4 were the similar as the branch offices were configured in a similar technique, configuring all of them with DHCP and OSPF. Moreover, the PCs in the branch offices were configured so as to receive the IPs via the DHCP instead of static configuration.

For ACL Configuraton in R0: (Branch 3 and 4 are restricted)

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 101 permit ip 192.168.2.0 0.0.0.255 any
access-list 101 deny ip any any
interface g0/0
ip access-group 101 in
```

Results & Interpretation

Network Topology:



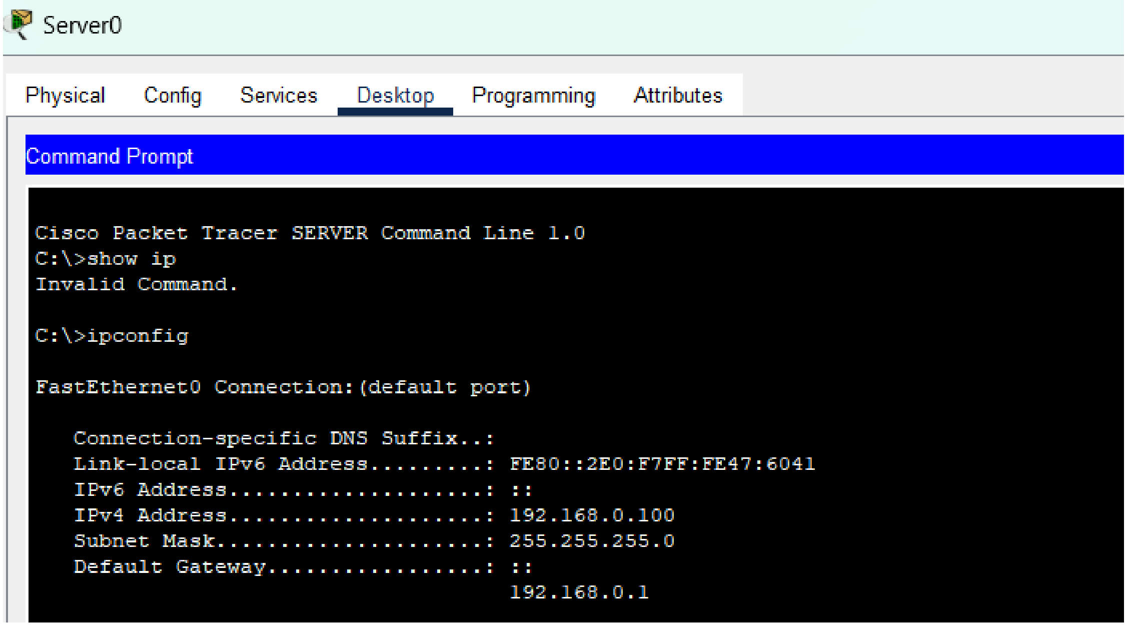
Final IP Addressing Scheme:

Network Segment	Subnet	Device	IP Address
Head Office	192.168.0.0/24	R0 (G0/0)	192.168.0.1
		Server	192.168.0.100
		PC0	192.168.0.101
		PC1	192.168.0.102
Branch 1	192.168.1.0/24	R1 (G0/0)	192.168.1.1
		PC2	192.168.1.3
		PC3	192.168.1.2
Branch 2	192.168.2.0/24	R2 (G0/0)	192.168.2.1
		PC4	192.168.2.3

		PC5	192.168.2.2
Branch 3	192.168.3.0/24	R3 (G0/0)	192.168.3.1
		PC6	192.168.3.2
		PC7	192.168.3.3
Branch 4	192.168.4.0/24	R4 (G0/0)	192.168.4.1
		PC8	192.168.4.3
		PC9	192.168.4.2
WAN Links (/30)		R0-R1 (S0/0/0)	10.0.1.1 / 10.0.1.2
		R0-R2 (S0/0/1)	10.0.2.1 / 10.0.2.2
		R0-R3 (S0/1/0)	10.0.3.1 / 10.0.3.2
		R0-R4 (S0/1/1)	10.0.4.1 / 10.0.4.2

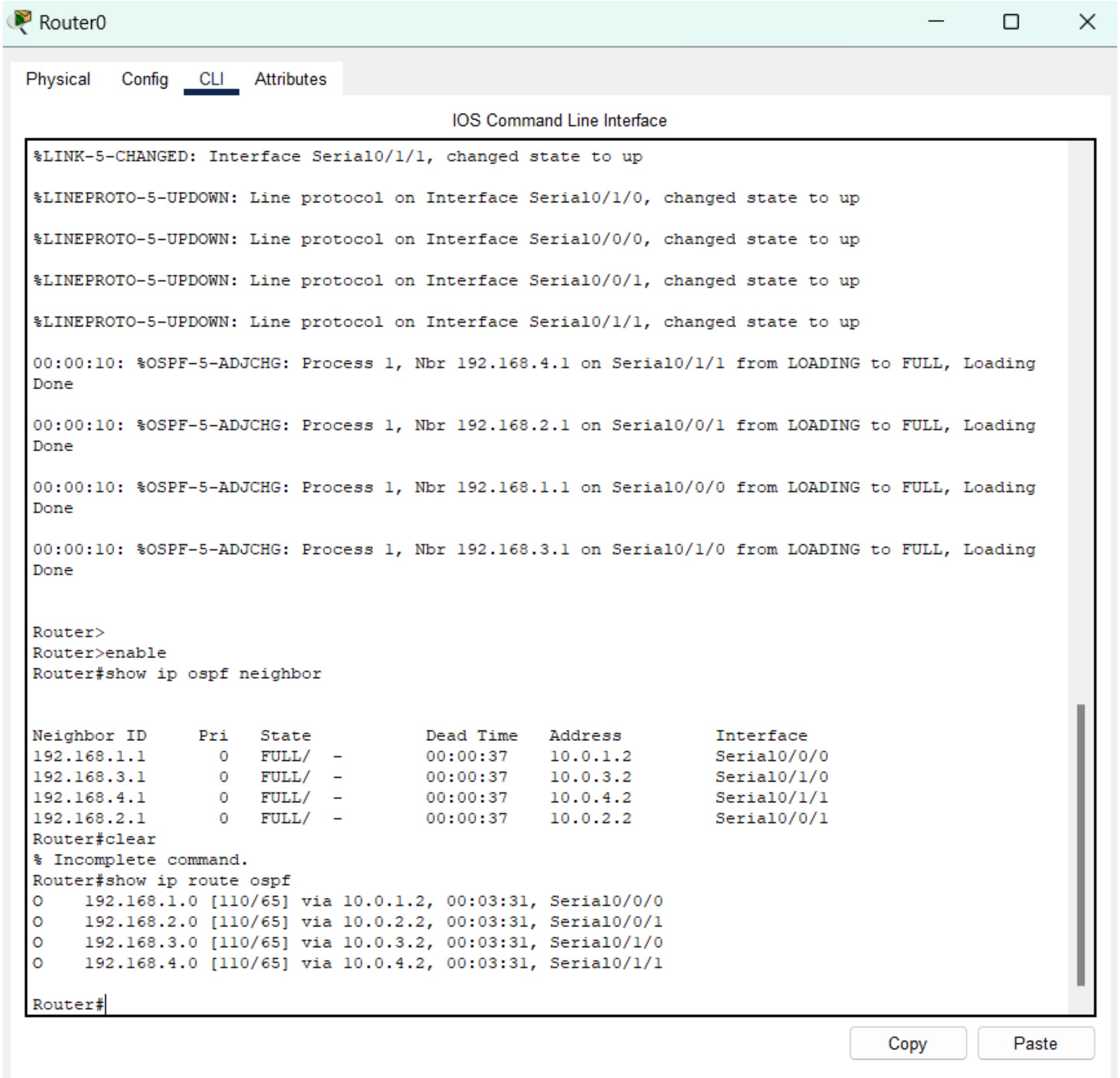
Configuration Files:

BMS Server Configuration details-



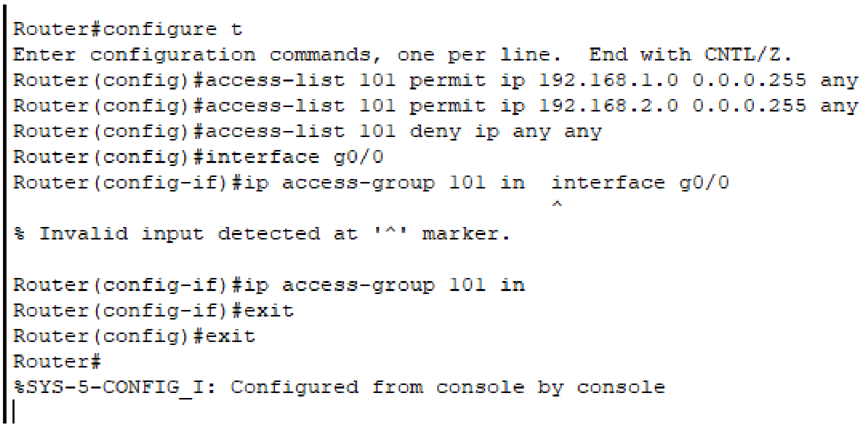
```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>show ip
Invalid Command.

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::2E0:F7FF:FE47:6041
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.0.100
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.0.1
```

Head office router configurations(R0):



```
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.4.1 on Serial0/1/1 from LOADING to FULL, Loading
Done

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/0/1 from LOADING to FULL, Loading
Done

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading
Done

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/1/0 from LOADING to FULL, Loading
Done


Router>
Router>enable
Router#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       0   FULL/  -        00:00:37    10.0.1.2        Serial0/0/0
192.168.3.1       0   FULL/  -        00:00:37    10.0.3.2        Serial0/1/0
192.168.4.1       0   FULL/  -        00:00:37    10.0.4.2        Serial0/1/1
192.168.2.1       0   FULL/  -        00:00:37    10.0.2.2        Serial0/0/1
Router#clear
% Incomplete command.
Router#show ip route ospf
O    192.168.1.0 [110/65] via 10.0.1.2, 00:03:31, Serial0/0/0
O    192.168.2.0 [110/65] via 10.0.2.2, 00:03:31, Serial0/0/1
O    192.168.3.0 [110/65] via 10.0.3.2, 00:03:31, Serial0/1/0
O    192.168.4.0 [110/65] via 10.0.4.2, 00:03:31, Serial0/1/1

Router#
```

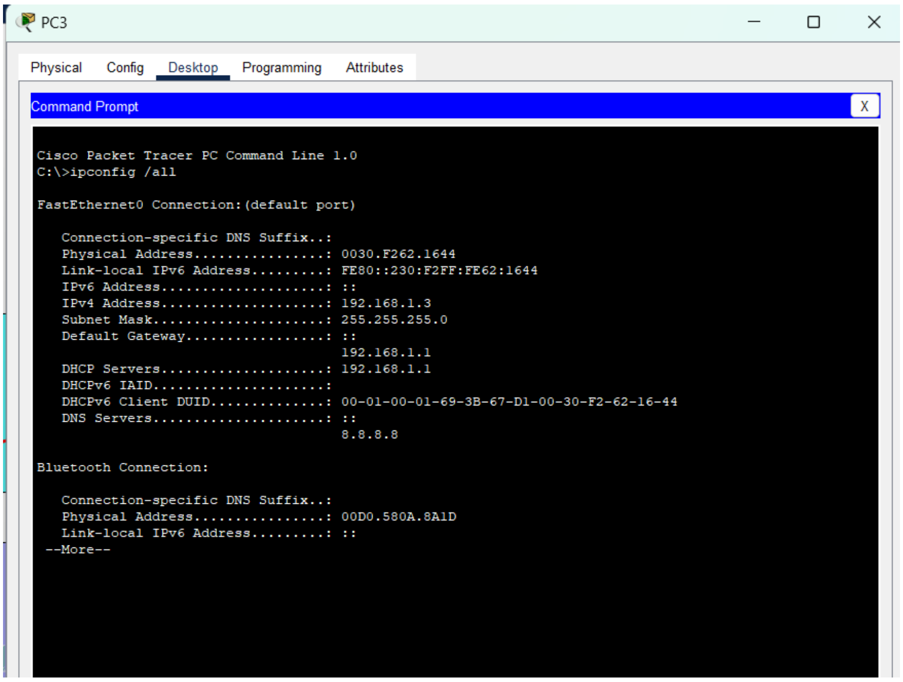
ACL Configuration of R0:



```
Router#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 any
Router(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255 any
Router(config)#access-list 101 deny ip any any
Router(config)#interface g0/0
Router(config-if)#ip access-group 101 in  interface g0/0
                                          ^
% Invalid input detected at '^' marker.

Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

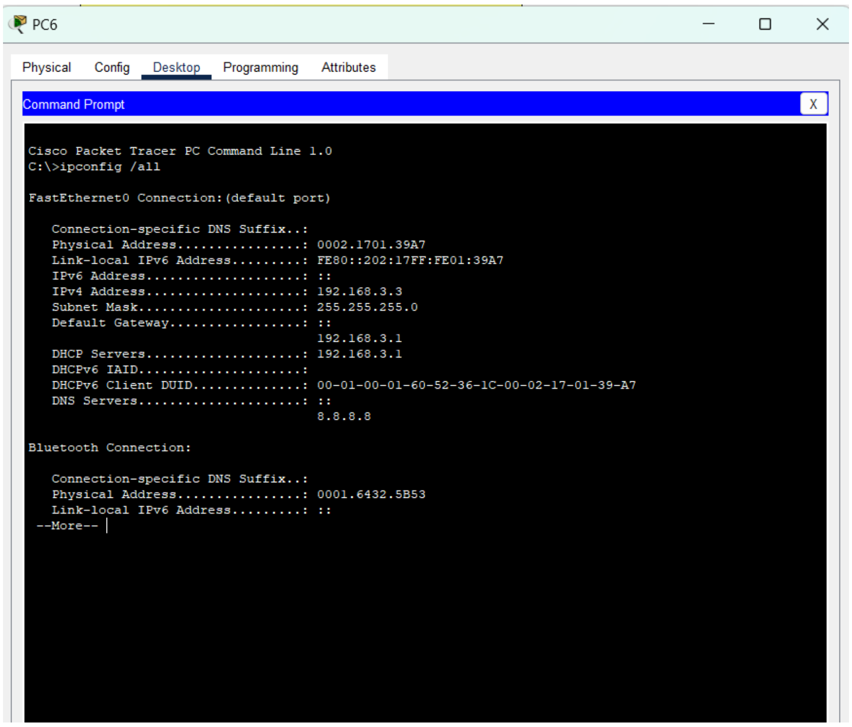
To check the DHCP assignment of PCs by DHCP Server

PC3 IP after assigned by DHCP:



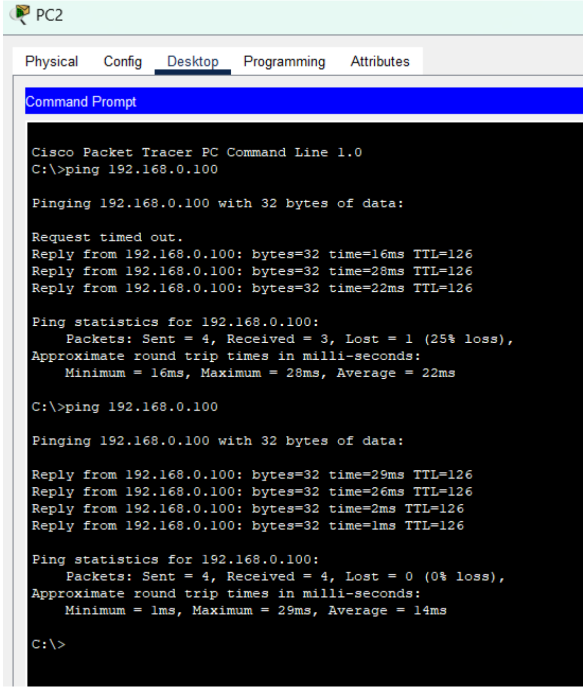
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0030.F262.1644
   Link-local IPv6 Address.........: FE80::230:F2FF:FE62:1644
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.1.1
   DHCP Servers....................: 192.168.1.1
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-69-3B-67-D1-00-30-F2-62-16-44
   DNS Servers.....................: ::
                                     8.8.8.8

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00D0.580A.8A1D
   Link-local IPv6 Address.........: ::
 --More--
```

PC6 IP after assigned by DHCP:



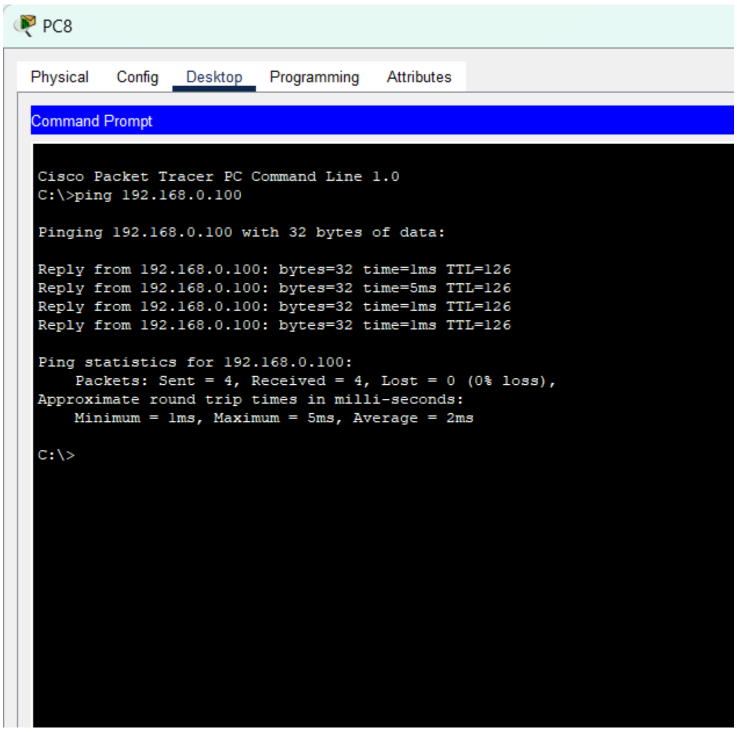
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0002.1701.39A7
   Link-local IPv6 Address.........: FE80::202:17FF:FE01:39A7
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.3.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.3.1
   DHCP Servers....................: 192.168.3.1
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-60-52-36-1C-00-02-17-01-39-A7
   DNS Servers.....................: ::
                                     8.8.8.8

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.6432.5B53
   Link-local IPv6 Address.........: ::
 --More--
```

Message from PC2 to server:



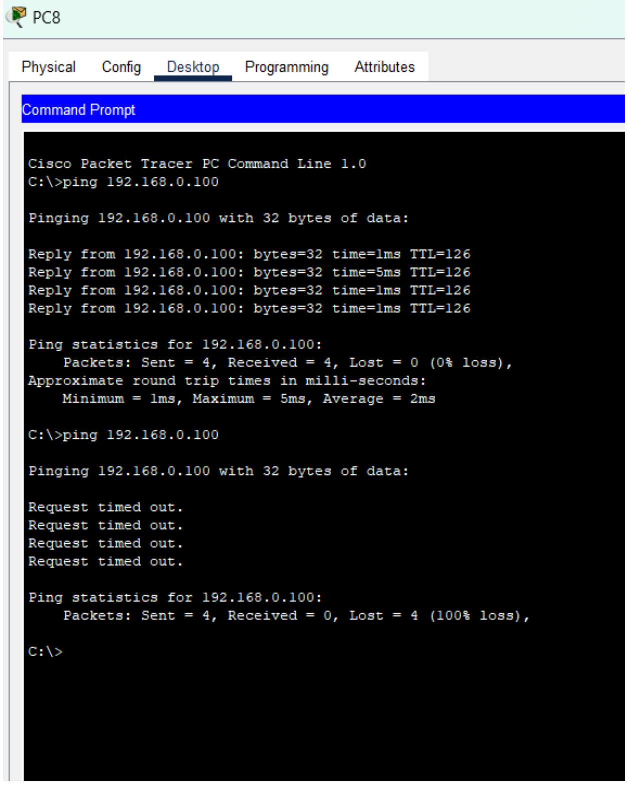
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.100: bytes=32 time=16ms TTL=126
Reply from 192.168.0.100: bytes=32 time=28ms TTL=126
Reply from 192.168.0.100: bytes=32 time=22ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 28ms, Average = 22ms

C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=29ms TTL=126
Reply from 192.168.0.100: bytes=32 time=26ms TTL=126
Reply from 192.168.0.100: bytes=32 time=2ms TTL=126
Reply from 192.168.0.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 29ms, Average = 14ms

C:\>
```

Message from PC8 to server before ACL restriction:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=1ms TTL=126
Reply from 192.168.0.100: bytes=32 time=5ms TTL=126
Reply from 192.168.0.100: bytes=32 time=1ms TTL=126
Reply from 192.168.0.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>
```

Message from PC8 to server after ACL restriction(BRANCH 3 AND 4 RESTRICTED)



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=1ms TTL=126
Reply from 192.168.0.100: bytes=32 time=5ms TTL=126
Reply from 192.168.0.100: bytes=32 time=1ms TTL=126
Reply from 192.168.0.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

:

The network topology for the Secure and Scalable Bank System was designed and implemented. DHCP (Dynamic Host Configuration Protocol) was utilized to automatically assign IP addresses to client PCs, ensuring efficient network management. OSPF (Open Shortest Path First) was deployed to dynamically select the optimal routing paths, thereby facilitating seamless traffic flow across the network.

The **ping** command was employed to verify and confirm the connectivity between the devices and networks, ensuring reliable communication between the branches and the head office.

To enhance security and restrict unauthorized access to the Bank Management System (BMS) server, an Access Control List (ACL) was configured. This effectively blocked Branches 3 and 4 from accessing the BMS server. The restriction was verified by using the **ping** command from a PC in Branch 4 (PC8), confirming that access to the server was indeed blocked.

Conclusion

In conclusion, the design and implementation of a **secure and scalable bank network** using Cisco Packet Tracer effectively addresses the critical requirements of modern banking operations. By establishing a robust infrastructure that connects four branch offices to a centralized head office, the project ensures reliable access to the Bank Management System (BMS) while maintaining high standards of security and efficiency.

The integration of **OSPF** for dynamic routing facilitates seamless communication between branches, allowing the network to adapt to changes and maintain optimal performance. The deployment of **DHCP** services enhances client device management, ensuring that IP addresses are allocated efficiently across all branches. Furthermore, the implementation of **Access Control Lists (ACLs)** provides a vital layer of security, safeguarding sensitive data by restricting unauthorized access to the centralized server.

Through comprehensive testing and validation, the network demonstrates its capability to support uninterrupted communication and enforce security policies effectively. This project not only showcases the practical application of networking concepts but also highlights the importance of designing secure infrastructures in the banking sector. As financial institutions continue to evolve, this scalable network design serves as a foundational model that can accommodate future growth and technological advancements, ultimately contributing to enhanced operational efficiency and improved client services

References

[1] G. D. Singh, *CompTIA Network+ N10-008 Certification Guide*, 2nd ed. Packet Publishing, 2022.

[2] Cisco Networking Academy, *Introduction to Networks v7.0*, Chapter 7: "Routing Dynamically (OSPF Configuration)," pp. 150–180.

[3] Cisco Networking Academy, *Introduction to Networks v7.0*, Chapter 10: "Access Control Lists," pp. 250–280.

[4] Tutorials Point, "Configuring OSPF in Cisco Packet Tracer," Available: https://www.tutorialspoint.com. [Accessed: Jan. 3, 2025].

[5] Techopedia, "Dynamic Host Configuration Protocol (DHCP)," Available: https://www.techopedia.com. [Accessed: Jan. 3, 2025].