VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Electronics Engineering (SENSE)

PROJECT BASED LEARNING (CAMP) - REPORT

COURSE CODE / NAME	BCSE308L – Computer Networks	
PROGRAM / YEAR	B.Tech (Electronics and Computer Engineering)	
LAST DATE FOR REPORT SUBMISSION	21/07/2023	
DATE OF SUBMISSION	21/07/2023	
TEAM MEMBERS DETAILS	**REGISTER NO.**	**NAME**
	21BLC1007	VISHNU KARTHIK R
	21BLC1047	SHRINIVASAN M
	21BLC1079	SUDHARSAN S
J TITLE	**BANK NETWORK DESIGN AND INTRUSION DETECTION SYSTEM**	
COURSE HANDLER'S NAME	Dr. JAYA VIGNESH T	**REMARKS**
COURSE HANDLER'S SIGN		

Table of Contents:

ABSTRACT:

Banks rely heavily on secure and efficient network infrastructure to conduct their operations. Network security is a critical concern for banks due to the sensitive nature of financial transactions and customer data they handle. This project focuses on the above aspects of efficient network design and security. The key objectives of this project are: to analyze the requirements of a banking network system, design a banking network system based on the same, and integrate the Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) with the banking network. A brief overview of the project is as follows: Designing and Implementing a Secure Network for a Bank (based on the given requirements) with Integrated Intrusion Prevention System. The network design ensures the confidentiality, integrity, and availability of sensitive data, protecting against unauthorized access, network attacks, and data breaches. "Cisco Packet Tracer" was used to design and integrate an Intrusion Detection System within the network. The network incorporates within it, a hierarchical model which consists of the core layer, the distribution layer, the access layer, and end devices. The intrusion Detection System was designed using the in-built security features of "Cisco Packet Tracer."

INTRODUCTION:

In modern networking, skilled network designers play a crucial role in ensuring network reliability, security, and scalability as businesses and organizations increasingly rely on seamless connectivity and data exchange. To achieve this, various network components and protocols are utilized, each serving a specific purpose. One fundamental aspect is the dynamic allocation of IP addresses using a DHCP (Dynamic Host Configuration Protocol) server. With DHCP, devices can obtain their unique IP addresses automatically, reducing manual configuration and minimizing potential address conflicts.

Another critical factor for network security and remote accessibility is the configuration of the Secure Shell (SSH) protocol. SSH offers secure encrypted communication, enabling secure command-line access to network devices and minimizing potential vulnerabilities.

To enhance performance, manageability, and security, VLAN (Virtual Local Area Network) setup is employed. This technique logically segments the network, and both VLAN Access and Trunk modes have been explored, which allow devices to communicate efficiently within their respective VLANs or across multiple VLANs. Facilitating inter-VLAN communication is achieved through VLAN routing, enabling seamless data exchange between VLANs and ensuring connectivity between network segments.

The project also includes the implementation of OSPF (Open Shortest Path First), a dynamic routing protocol that optimizes routing paths within the network, providing faster and more efficient data transmission.

In terms of security measures, Access Control Lists (ACLs) are implemented to control traffic flow and filter packets based on specific criteria, thereby mitigating potential security threats. Additionally, Intrusion Detection Systems (IDS) play a pivotal role in modern network security, providing an added layer of defense against potential cyber threats and unauthorized access. These systems continuously monitor network traffic, analyzing data packets and patterns to identify suspicious or malicious activities. IDS operates in two primary modes: signature-based and anomaly-based modes.

ALGORITHM:

1) Identifying Requirements:

   Information regarding the number of LANs and type of routers/switches used has to be collected.

LAN Requirements

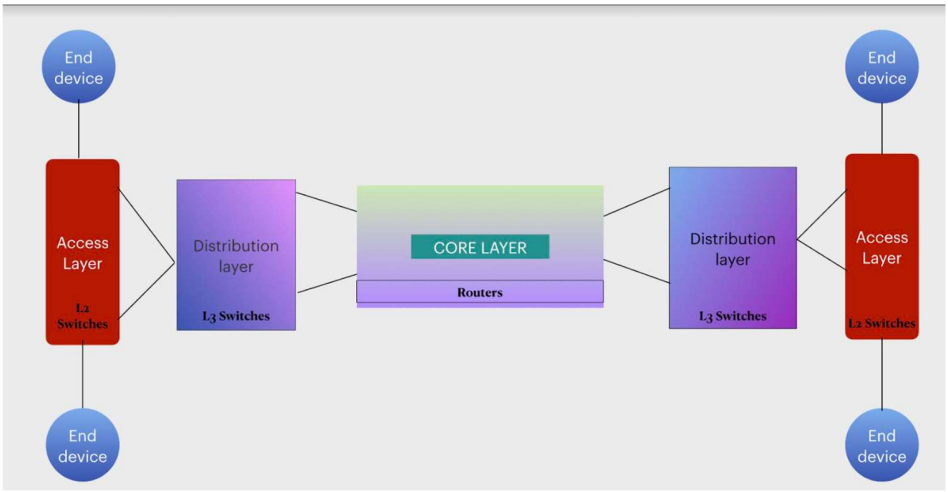
S.No	Name of the Department	Situated on
1	Personal Banking	Floor 1
2	Credit	Floor 1
3	Investment Banking	Floor 1
4	Foreign Exchange	Floor 2
5	Risk Management	Floor 2
6	Legal	Floor 2
7	Budgeting and Accountancy	Floor 3
8	Human Resources	Floor 3
9	IT and Security	Floor 3

Hardware Specification

Router used
2911
Switch used
3650 24PS
2960 24TT

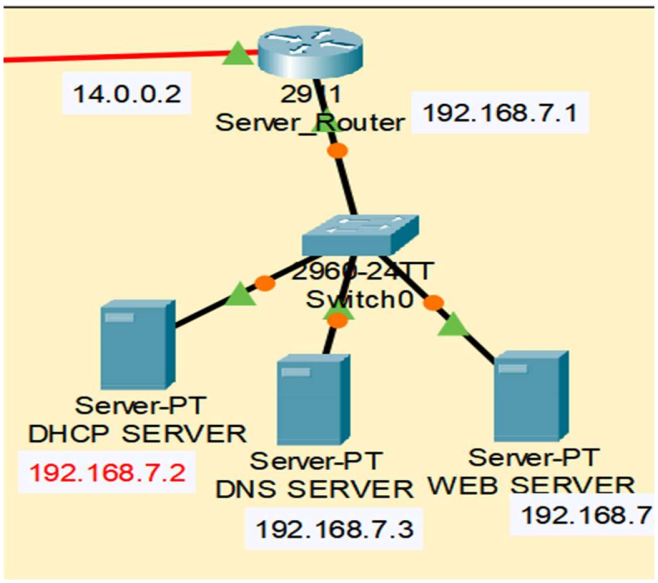
2) Choosing the Network topology

   A hierarchical network model was chosen for this network design. It consists of the core layer, distribution layer and access layer.



3) Determining IP addresses

A DHCP server was used for the dynamic allocation of IP addresses. A DHCP server assigns IP addresses to devices based on their default gateways by creating the appropriate Server Pools.

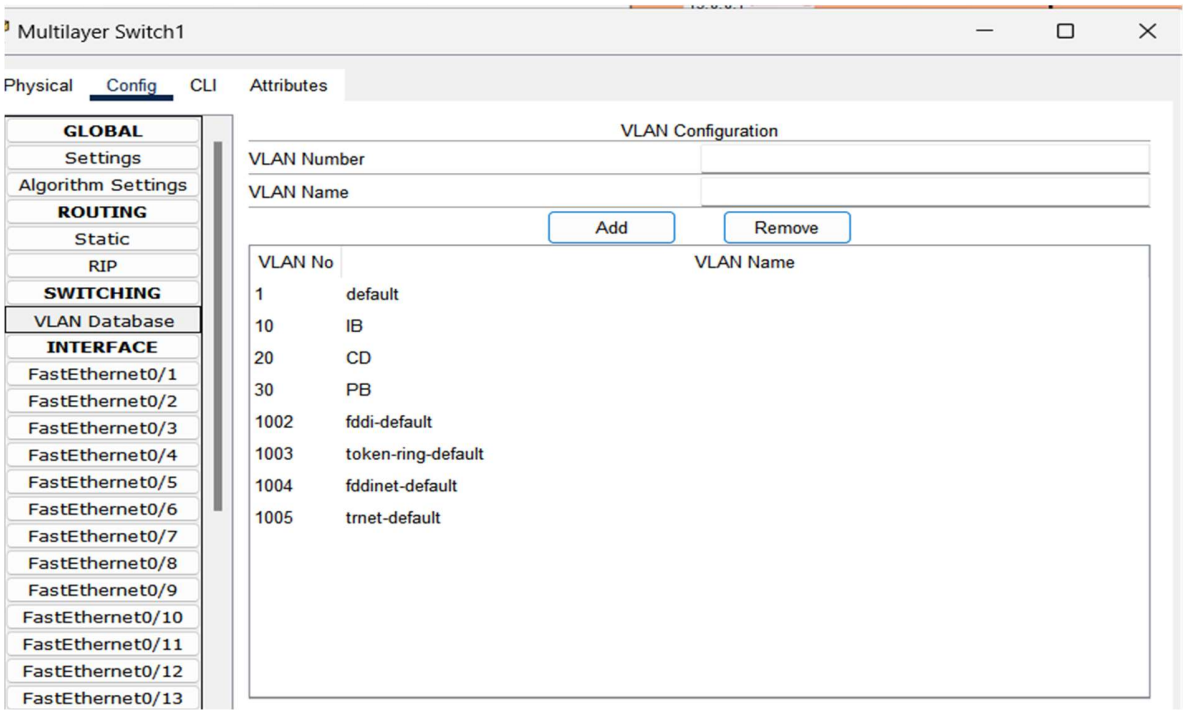


List of IP addresses used for the Network:

Name of the Department	Network ID
Personal Banking	192.168.1.0/26
Credit	192.168.1.64/26
Investment Banking	192.168.1.128/25
Foreign Exchange	192.168.2.0/26
Risk Management	192.168.2.64/26
Legal	192.168.2.128/25
Budgeting and Accountancy	192.168.3.0/26
Human Resources	192.168.3.64/26
IT and Security	192.168.3.128/25
Server Room(Not connected Directly to rest of network)	192.168.7.0/24
	192.168.21.16/30
BETWEEN ROUTERS AND SWITCHES	192.168.21.20/30
	192.168.21.24/30
	10.0.0.0
	11.0.0.0
BETWEEN ROUTERS	12.0.0.0
	13.0.0.0
	14.0.0.0
	15.0.0.0

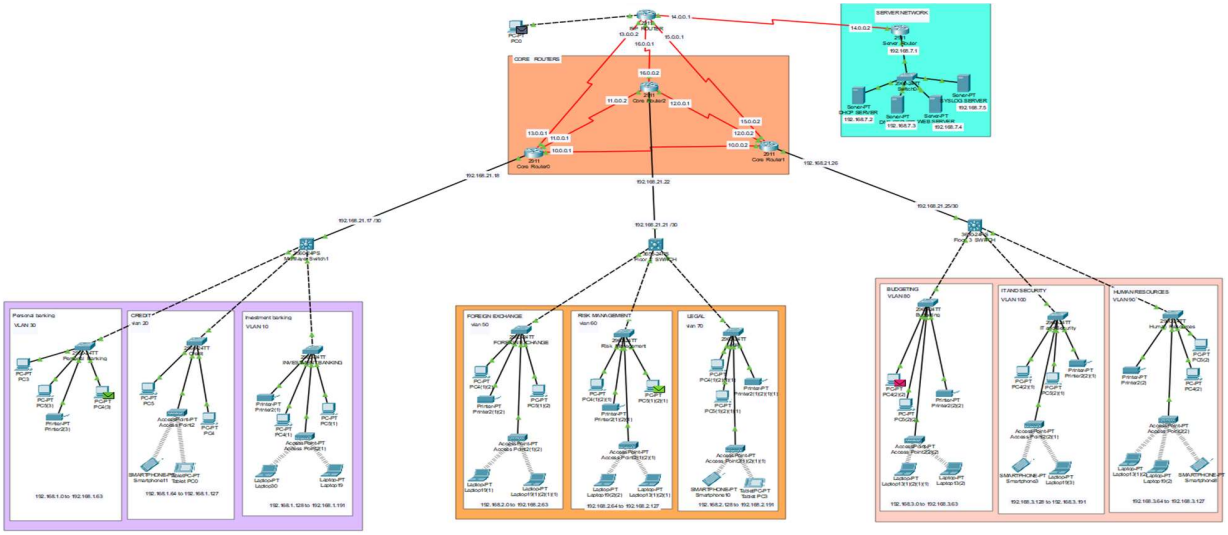
4) Setting up VLANs

Separate VLANs are used for each department in the building. All traffic coming out of these departments is routed through their respective VLANs.



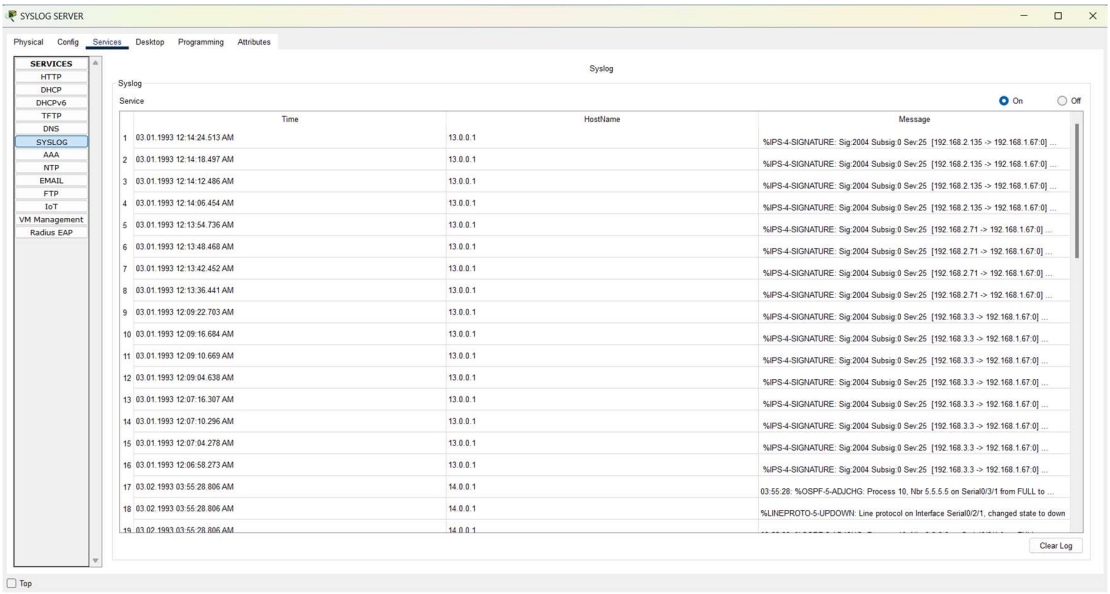
5) Implementation of the design on Cisco Packet tracer

The Network design is implemented on cisco packet tracer by using all the necessary components and connections



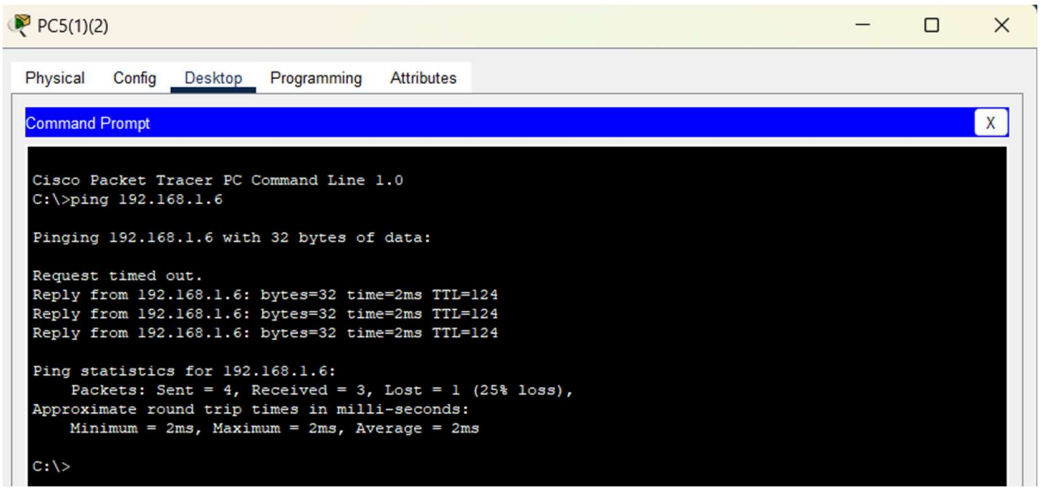
6) Implement Security Features in the Network

Implement SSH, ACL, IDS etc. in the network. A SYSLOG server is used to keep a track of all the incoming messages to the network



7) Testing and Validating

Testing and validating has to be done to ensure proper connectivity between networks. This ensures the integrity of the transmitted message



IMPLEMENTATION (REAL TIME):

The network designing and security project aimed to create a secure banking network infrastructure tailored to meet the specific requirements of the banking domain.

Standards Used:

The project adheres to widely recognized networking standards, such as

- TCP/IP (Transmission Control Protocol/Internet Protocol) for reliable communication
- IPsec (Internet Protocol Security) for secure data transmission
- OSPF (Open Shortest Path First) for efficient routing.
- DHCP Protocol for IP assignment
- UDP protocol as a backbone for other protocols
- ICMP protocol to test connectivity
- DNS protocol as a backbone protocol
- SNMP protocol to facilitate
- HTTP protocol at the end-user level

Test plan used:

To ensure the effectiveness and functionality of the network design, extensive product testing was conducted. The testing process encompassed several stages:

Test Planning: A comprehensive test plan was devised, outlining the objectives, scope, and methodology of testing. The plan identified specific test cases to evaluate the network's performance, security, and compliance with standards.

Functional Testing: The network was tested for its functional aspects, including connectivity, routing, and communication between devices and components.

Security Testing: Testing was carried out by ensuring the functionality of the security features like ACL, SSH and IDS integrate with a syslog server.

CLI COMMANDS:

STATIC IP ASSIGNING:

interface <interface name> ip address <ip address> <subnet mask>

ROUTER NAME CHANGE:

Router (config) # hostname <hostname>

ROUTER DOMAIN NAME AND ENCRYPTION:

<hostname>(config) # ip domain-name <domain name>

<hostname>(config)# crypto key generate rsa general-keys modules 512

ROUTER USER CONFIGURATION:

<hostname> (config) # username <username> privilege 15 password <password>

VLAN SETUP:

Switch#config terminal

Switch(config)#vlan <vlan number>

Switch(config-vlan)#name <vlan name>

VLAN PORT MODE:

Switch(config)#int <interface name>

Switch(config-if)#switchport mode <access or trunk>

Switch(config-if)#switchport access vlan <vlan number>

INTER VLAN ROUTING:

Router(config)#int <interface name>

Router(config-if)#no shutdown

Router(config-if)#int <interface name>.<vlan number>

Router(config-subif)#encapsulation dot1q <vlan number>

Router(config-subif)#ip add <ip address> <subnet mask>

DHCP SERVER:

Router(config)#

Router(config)#ip dhcp pool <pool name>

Router(dhcp-config)#network <network address> <subnet mask>

Router(dhcp-config)#default-router <default gateway>

Router(dhcp-config)#dns-server <dns server ip>

ACL:

clear access-list ipv4

access-list <name> <number> <permit, deny> <inbound, outbound, both> <protocol> <source> <destination> <sport> <dport> <ifid>

OSPF:

router ospf 1

router-id <id>

network <network id> <!subnet mask> area 0

exit

interface <interface name>

ip address <gateway address> <subnet mask>

no shutdown

exit

write memory

SYSLOG SERVER (IDS):

Copy running-config startup-config

Reload

Mkdir <directory name>

Conf t

Ip ips config location flash : <directory name>

Ip pis name iosips

Ip ips notify log

Service timestamps log date time sec

Logging host <host id>

Ip ips signature-category

Category all

Retired true

exit

Category ios_ips basic

Retired false

exit

exit

INTRUSION DETECTION:

//Blocking ICMP packets

Int <interface name>

Ip ips iosips out

exit

Ip ips signature-definition

Signature 2004 0

Status

Retired false

Enabled true

Ex

Engine

Event-action produce-alert

Event-action deny-packet-inline

RESULTS & INFERENCES:

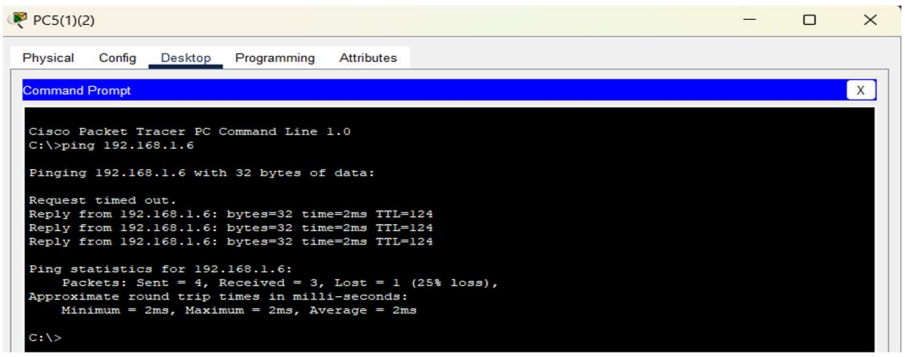
Secure Shell:

An instance of the SSH window is given below

```
User Access Verification

Password:
```

Network Connectivity:

Network Connectivity was established in the designed network. This connectivity ensures that the users would successfully be able to communicate using the network, thus fulfilling its primary use. Network Connectivity is obtained as a result of the working of DHCP and OSPF protocols.



Routing information:

A Standard Routing table was obtained through the OSPF Protocols

```
O    10.0.0.0/8 [110/129] via 192.168.21.22, 02:22:04, GigabitEthernet1/0/2
O    11.0.0.0/8 [110/65] via 192.168.21.22, 02:22:36, GigabitEthernet1/0/2
O    12.0.0.0/8 [110/65] via 192.168.21.22, 02:22:36, GigabitEthernet1/0/2
O    13.0.0.0/8 [110/129] via 192.168.21.22, 02:22:04, GigabitEthernet1/0/2
O    14.0.0.0/8 [110/129] via 192.168.21.22, 02:22:04, GigabitEthernet1/0/2
O    15.0.0.0/8 [110/129] via 192.168.21.22, 02:22:04, GigabitEthernet1/0/2
O    16.0.0.0/8 [110/65] via 192.168.21.22, 02:22:36, GigabitEthernet1/0/2
     192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
O       192.168.1.0/26 [110/67] via 192.168.21.22, 02:22:04, GigabitEthernet1/0/2
O       192.168.1.64/26 [110/67] via 192.168.21.22, 02:22:04, GigabitEthernet1/0/2
O       192.168.1.128/25 [110/67] via 192.168.21.22, 02:22:04, GigabitEthernet1/0/2
     192.168.2.0/24 is variably subnetted, 3 subnets, 2 masks
C       192.168.2.0/26 is directly connected, Vlan50
C       192.168.2.64/26 is directly connected, Vlan60
C       192.168.2.128/25 is directly connected, Vlan70
     192.168.3.0/24 is variably subnetted, 3 subnets, 2 masks
O       192.168.3.0/26 [110/67] via 192.168.21.22, 02:22:26, GigabitEthernet1/0/2
O       192.168.3.64/26 [110/67] via 192.168.21.22, 02:22:26, GigabitEthernet1/0/2
O       192.168.3.128/25 [110/67] via 192.168.21.22, 02:22:26, GigabitEthernet1/0/2
O    192.168.7.0/24 [110/130] via 192.168.21.22, 02:22:04, GigabitEthernet1/0/2
     192.168.21.0/30 is subnetted, 3 subnets
O       192.168.21.16 [110/66] via 192.168.21.22, 02:22:04, GigabitEthernet1/0/2
C       192.168.21.20 is directly connected, GigabitEthernet1/0/2
O       192.168.21.24 [110/66] via 192.168.21.22, 02:22:26, GigabitEthernet1/0/2
```

DHCP SERVER:

As a result of the server, Dynamic host ip allocation was possible.

DHCP

Interface	FastEthernet0	Service	On	Off
Pool Name	serverPool			
Default Gateway	0.0.0.0			
DNS Server	0.0.0.0			
Start IP Address :	192	168	7	0
Subnet Mask:	255	255	255	0
Maximum Number of Users :	0			
TFTP Server:	0.0.0.0			
WLC Address:	0.0.0.0			

Add | Save | Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Credit	192.168.1.65	192.168.7.3	192.168.1.67	255.255.255.192	60	0.0.0.0	0.0.0.0
hr	192.168.3.129	192.168.7.3	192.168.3.131	255.255.255.192	61	0.0.0.0	0.0.0.0
it	192.168.3.65	192.168.7.3	192.168.3.67	255.255.255.192	60	0.0.0.0	0.0.0.0
budget	192.168.3.1	192.168.7.3	192.168.3.3	255.255.255.192	60	0.0.0.0	0.0.0.0
legal	192.168.2.129	192.168.7.3	192.168.2.131	255.255.255.192	61	0.0.0.0	0.0.0.0
risk	192.168.2.65	192.168.7.3	192.168.2.67	255.255.255.192	60	0.0.0.0	0.0.0.0
forex	192.168.2.1	192.168.7.3	192.168.2.3	255.255.255.192	60	0.0.0.0	0.0.0.0
customer	192.168.1.193	192.168.7.3	192.168.1.195	255.255.255.192	60	0.0.0.0	0.0.0.0
investment	192.168.1.129	192.168.7.3	192.168.1.131	255.255.255.192	60	0.0.0.0	0.0.0.0
Banking	192.168.1.1	192.168.7.3	192.168.1.4	255.255.255.192	60	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.7.0	255.255.255.0	0	0.0.0.0	0.0.0.0

ACL:

As a result of the ACL used, the ping becomes unsuccessful

```
SERVER_ROUTER>EN
Password:
SERVER_ROUTER#
SERVER_ROUTER#
SERVER_ROUTER#confi t
Enter configuration commands, one per line.  End with CNTL/Z.
SERVER_ROUTER(config)#
SERVER_ROUTER(config)#access-list 100 deny icmp any any
SERVER_ROUTER(config)#interface GigabitEthernet0/0
SERVER_ROUTER(config-if)#ip access-group 100 in
SERVER_ROUTER(config-if)#interface GigabitEthernet0/0
SERVER_ROUTER(config-if)#ip access-group 100 in
SERVER_ROUTER(config-if)#
SERVER_ROUTER(config-if)#exit
SERVER_ROUTER(config)#exit
SERVER_ROUTER#
*Mar 01, 00:00:39.000: SYS-5-CONFIG_I: Configured from console by console
SERVER_ROUTER#wr
Building configuration...
[OK]
```

PC5(1)(2)(1)(1)

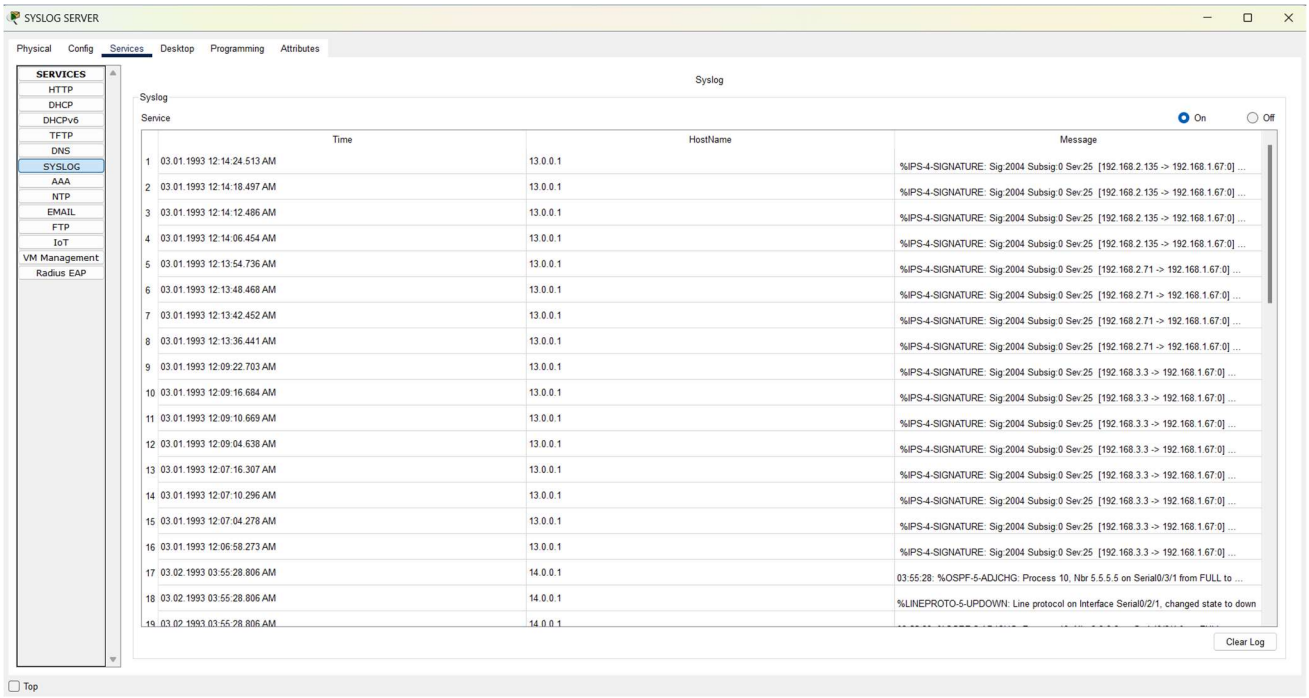
Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

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

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

SYSLOG SERVER:

The packets generating traffic were analysed and each entry was logged with the help of IPS which is displayed using SYSLOG server.



The results showcased a scalable and secure network with low latencies, good performance, and strong protection against cyber threats. The project demonstrated the significance of network security in banking, fostering customer trust and providing seamless and real-time banking services. With a few improvements, this project could very well be implemented in banks in the near future.

APPLICATION ORIENTED LEARNING:

The project's network design and security implementation can be applied in real-time applications in the banking sector. Banks can adopt this design to establish secure and efficient network infrastructures to facilitate real-time transactions, online banking services, and secure data exchange. The integrated Intrusion Detection System ensures proactive monitoring and detection of potential cyber threats, safeguarding sensitive financial data and customer information. By implementing this project, banks can enhance their network security, protect against unauthorized access, and provide seamless and reliable banking services to customers.

Throughout the project, various computer communication concepts were explored and applied, including:

- TCP/IP protocol suite and its role in reliable data transmission over networks.
- Configuration of networking devices such as routers and switches, network security principles, such as encryption, firewalls, and Intrusion Detection/Prevention Systems (IDS/IPS).
- Network architecture design, including hierarchical models and redundancy for fault tolerance. Quality of Service (QoS) for prioritizing critical traffic and minimizing latency.
- Proficiency in using Cisco Packet tracer as the primary tool for network analysis and designing

Potential cost elements include hardware (routers, switches, firewalls), software (security applications, monitoring tools), licensing fees, labor costs for design, implementation, and testing, and ongoing maintenance and monitoring expenses. The actual cost expenditure for the project would be determined by the budget allocated for network infrastructure and security enhancements in the banking organization. The cost incurred would be justified by the increased trust of customers, enhanced service availability, and strengthened resilience against security breaches in the banking network.

CONCLUSION:

In conclusion, the successful design and implementation of a robust banking network require a comprehensive approach that considers various network components and protocols. This report has highlighted the crucial role skilled network designers play in ensuring the reliability, security, and scalability of banking networks. The seamless connectivity and efficient data exchange enabled by dynamic IP address allocation through DHCP and secure encrypted communication with SSH are essential components in safeguarding sensitive financial information. Institutions can fortify their networks against potential vulnerabilities and ensure the protection of sensitive financial data. As technology continues to evolve, ongoing vigilance, continuous monitoring, and adaptation to emerging threats will be essential in maintaining the security and integrity of banking networks in an ever-changing digital landscape.

REFERENCES:

1) https://manuals.gfi.com/en/exinda/help/content/cli/commands
2) https://ipcisco.com/lesson/ssh-configuration-on-packet-tracer/
3) https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r40/addr_serv/command/reference/ir40asrbook_chapter1.html
4) https://computernetworking747640215.wordpress.com/2018/07/05/vlan-configuration-on-a-cisco-switch-in-packet-tracer/
5) https://www.google.com/search?q=dhcp+commands+cisco+packet+tracer&oq=dhcp+comma&aqs=chrome.2.0i512j69i57j0i20i263i512j0i512l4j0i20i263i512j0i512l2.5629j0j7&sourceid=chrome&ie=UTF-8
6) https://www.ciscopress.com/articles/article.asp?p=426638&seqNum=3
7) https://youtu.be/NLMqmaBvD8Q
8) https://medium.com/@soniapaul132002/network-design-proposal-for-bank-b622751a8af1