Computer Communication Networks

BS-CE 2020 (5th Semester)

Banking Network System

Project Report

Submitted By:

Muhammad Owais Iqbal Malik	20-CE-012
Zaki Muttayab	20-CE-030
Osama Amjad	19-CE-032

Submitted To:
Sir. Ali Raza

Dated:
20/01/2023

HITEC University, Taxila
Department of Computer Engineering

DECLARATION

We hereby declare that the project entitled **“Banking Network System** submitted for the B.S. Degree is our original work and the project has not formed the basis for the award of any degree, association ship, fellowship or any other similar titles.

Signature of the Students:
Mr. Owais Iqbal Malik
Mr. Zaki Muttayab
Mr. Osama Amjad

ABSTRACT

The general aim of this project is to simulate a banking system which is secure and easy to use. Previously the system was manual, not secure, also working slowly. This proposed system overcomes the lacking of the existing manual system. But now through this system whenever any transaction will be taking place it will store in the central database and authorized person can get necessary information or report when they get into the system from any branches through Wide Area Network (WAN).To implement our project we have used OSI model. This system is using Packet Tracer 7.0 for network simulation. After implementation of all functions, the system is tested in different stages and it was successful for its purpose

TABLE OF CONTENTS

Section I

2.1. INTRODUCTION

2.1.1. Overview of VoIP Technology

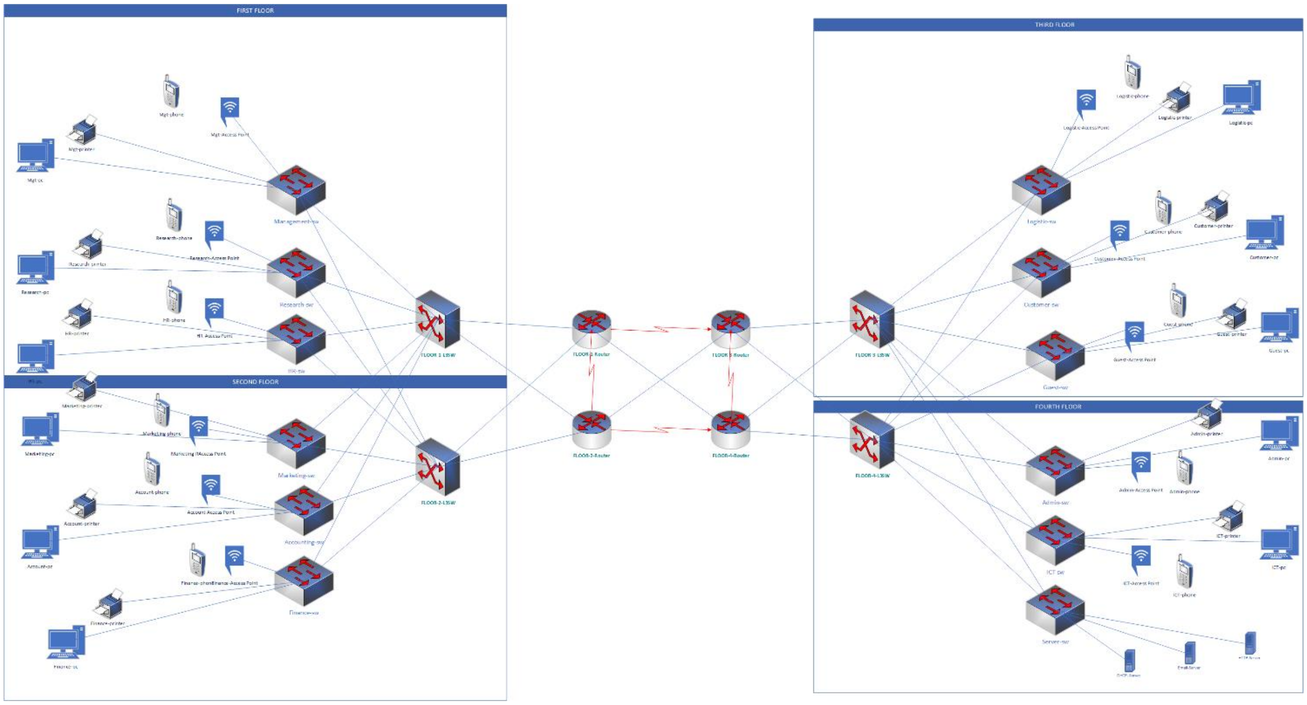

Figure 2.1 Typical Banking Network

The Network design starts from the point of topology. This will include defining the layers and defining the functionality of each layer. The main aspect of dividing the network into layers is to incorporate the functions based on the layered structure and design the connectivity methods and high availability techniques at each layer. It also helps in distribution and control of network functionality.

The aim of the network is to provide highly available and scalable environment for collocation of Internet, Intranet and Extranet services, and applications. It providing high-speed access to data, voice and internet-based applications. The network is planned such that it will provide the necessary backbone connectivity between the different offices to ensure that the network becomes an enabler for business plans.

The design should be in such a way that there will be no single points of failure and should be capable of achieving fast and predictable convergence times. The design should also address the ease of scalability by increasing the port density in the switches. This Low-Level Design has been made in accordance with Cisco’s existing best-practice recommendations. The foundation of the design stems from Cisco’s standard ‘Multilayer Network Design’ model.

2.1.2. Important Concepts

A. OSPF

The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.

The main advantage of a link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements. The main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. Increasing the number of routers increases the size and frequency of the topology updates, and also the length of time it takes to calculate end-to-end routes. This lack of scalability means that a link state routing protocol is unsuitable for routing across the Internet at large, which is the reason why IGPs only route traffic within a single AS.

B. Vlan

VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.

Without VLANs, a broadcast sent from a host can easily reach all network devices. Each and every device will process broadcast received frames. It can increase the CPU overhead on each device and reduce the overall network security.

In case if you place interfaces on both switches into separate VLAN, a broadcast from host A can reach only devices available inside the same VLAN. Hosts of VLANs will not even be aware that the communication took place.

C. SSH

SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.

SSH also refers to the suite of utilities that implement the SSH protocol. Secure Shell provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network, such as the internet.

In addition to providing strong encryption, SSH is widely used by network administrators to manage systems and applications remotely, enabling them to log in to another computer over a network, execute commands and move files from one computer to another.

2.2. OBJECTIVE OF STUDY

- It provides support to various applications of banking
- This Network will let various users of the bank and their employees connect to the main Server.
- The objective only authorized user to access Network including all servers and network devices.
- Provide greater speed & reduce time consumption.
- It provides 99.99% of uptime of Network.
- Allocate bandwidth to servers accordingly by using QoS.
- The proposed Network will be user-friendly so that even a beginner can troubleshoot any issue easily.

2.3. Future Scope

There is a vast future scope of this Network. This Design can be improved and can be used by various banks. If the limitations present in this Design are removed then, this Network will become very reliable and provide 100% uptime.

We can easily implement any changes to the Network Design as we are using the latest protocol like Border Gateway Protocol (BGP) in our network which is having attributes to easily divert or control the flow of data and QOS which can be used to allocate bandwidth to servers accordingly.

2.4. LIMITATIONS

- We will not be able to resolve issues from any of the following by using this Network:
  - Any unreported/ undetected Bugs in standard software's, or tools
  - Any changes in Application Software features
  - Older versions are incompatible with current features

- Lease line uptime depends on a particular Service Provider.

- This Network is limited by the state of technology and functionality of software tools or products deployed.

- Third-party IOS integration will be carried out on the best-effort basis.

- All hardware devices upgrades, hardware re-deployments, and policy changes shall be done after the mutual consent of the customer, based on the impact it would have on the overall security situation and performance of the network.
- Security can be implemented in a better way.

Section II

3.1: Architecture

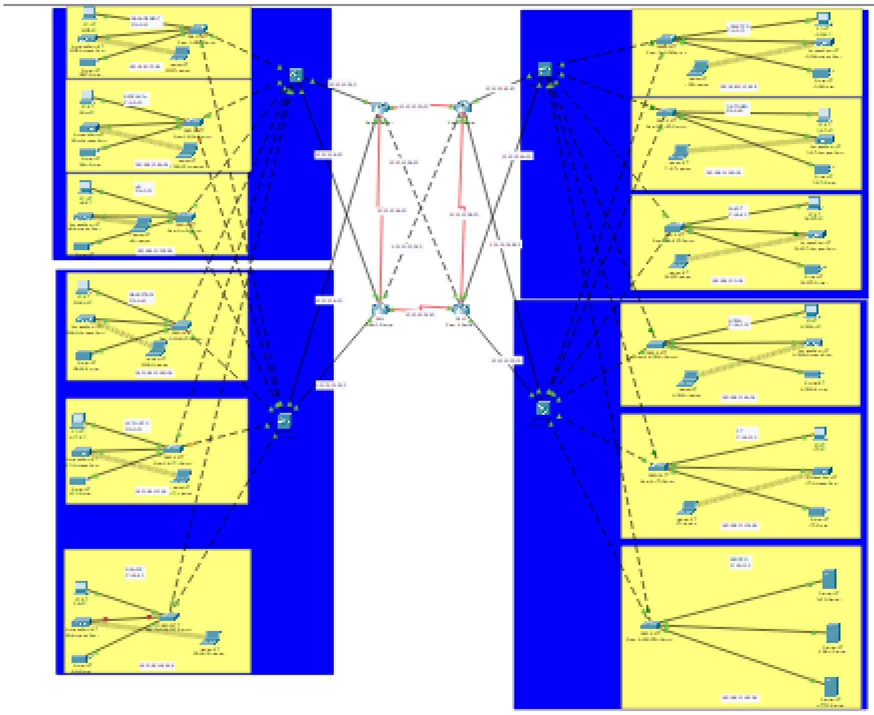

Figure 3.1: Network Diagram of Banking Network

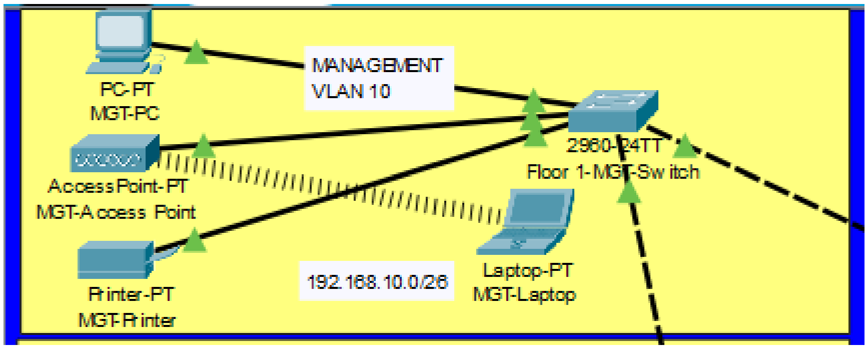

Figure 3.2: Management Department of Banking Network

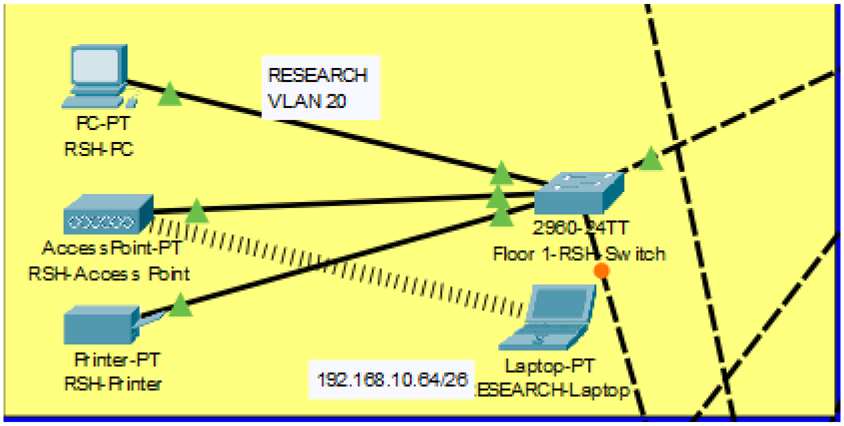

Figure 3.3: Research Department of Banking Network

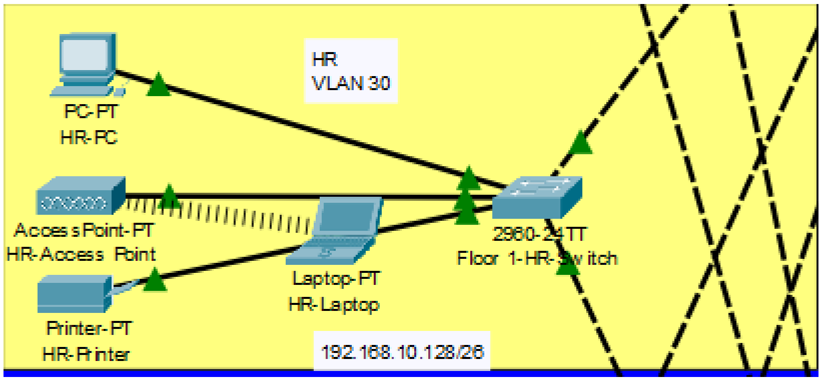

Figure 3.3: HR Department of Banking Network

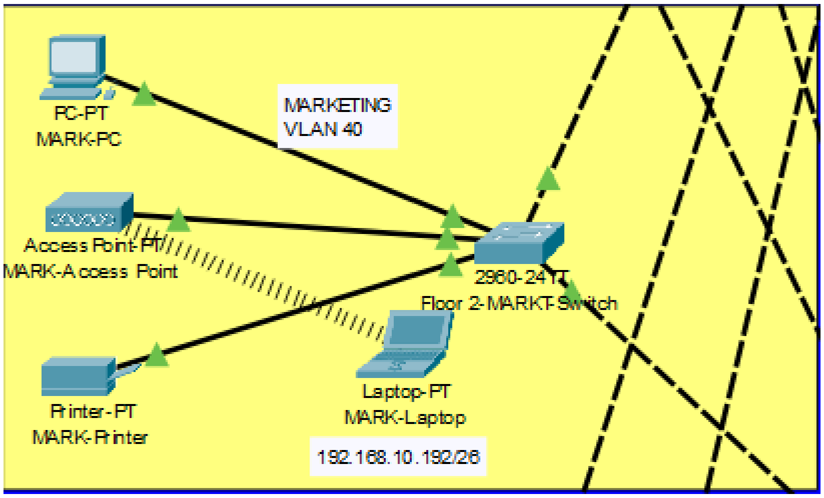

Figure 3.4: Marketing Department of Banking Network

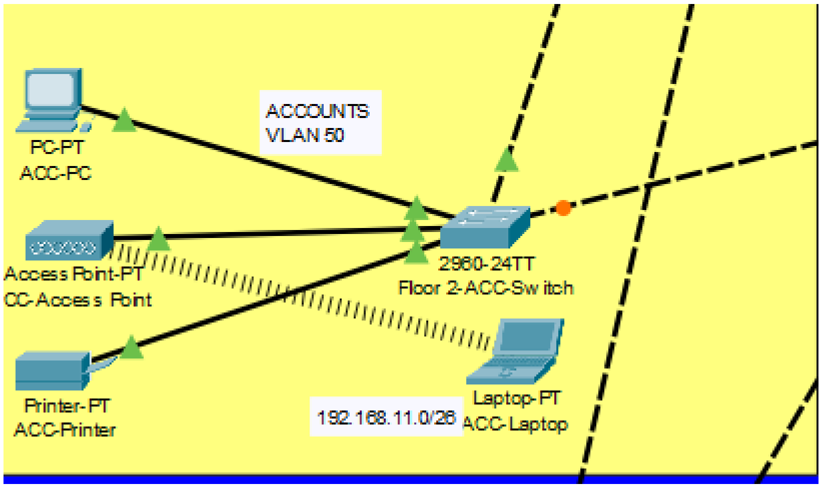

Figure 3.5: Accounts Department of Banking Network

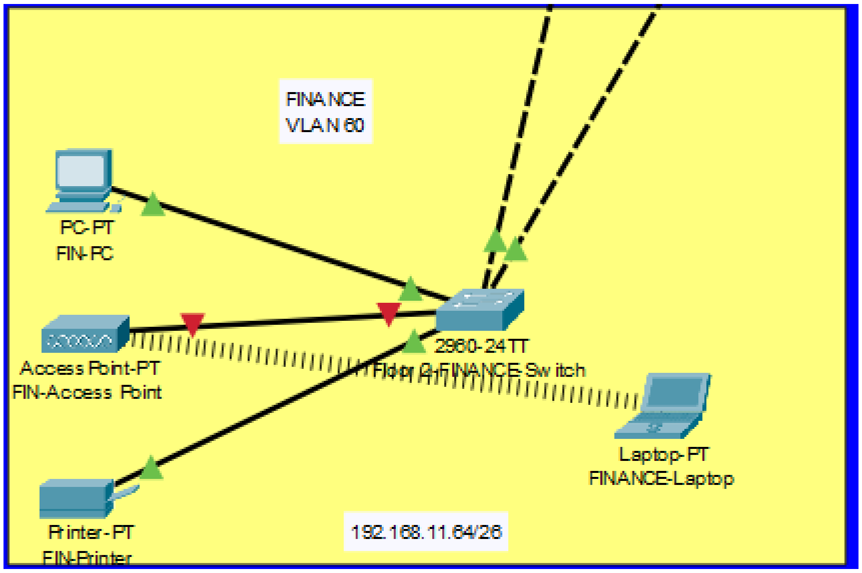

Figure 3.6: Finance Department of Banking Network

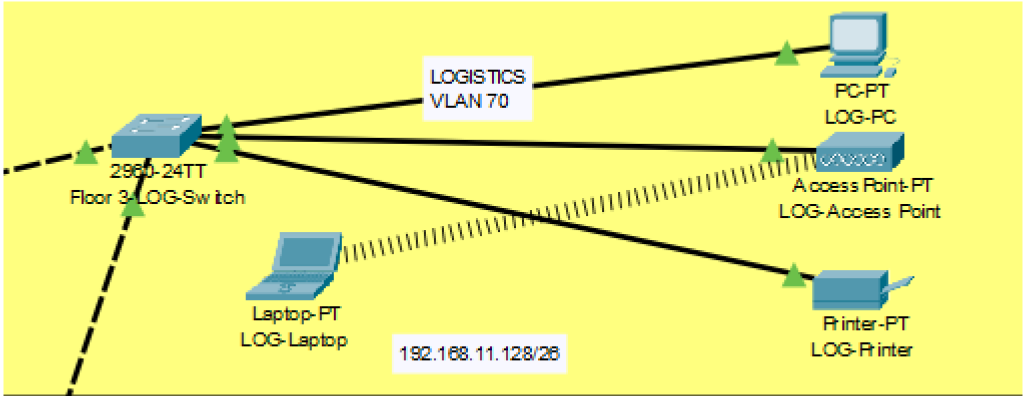

Figure 3.6: Logistics Department of Banking Network

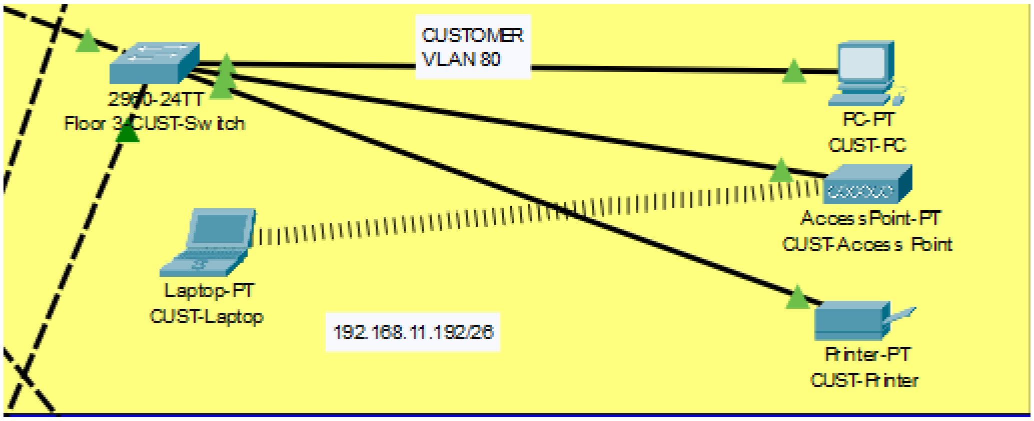

Figure 3.7: Customer Department of Banking Network

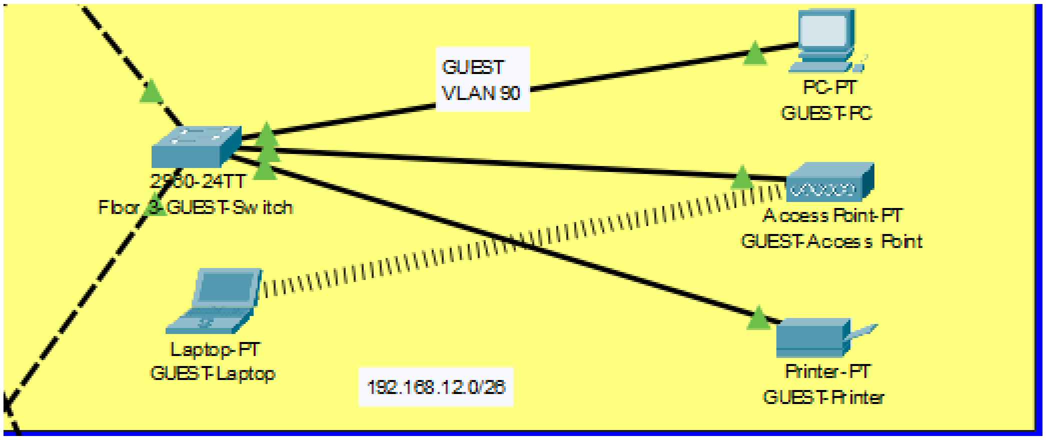

Figure 3.8: Guest Department of Banking Network

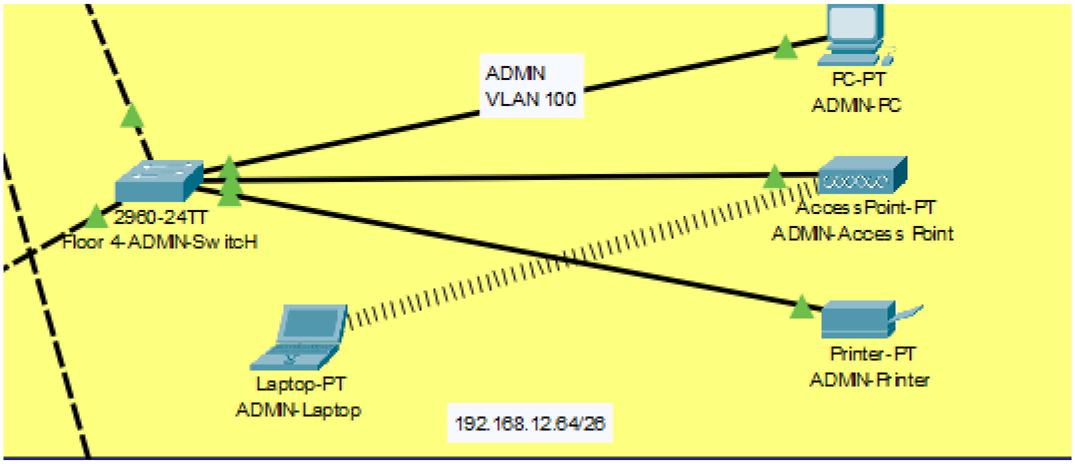

Figure 3.9: Admin Department of Banking Network

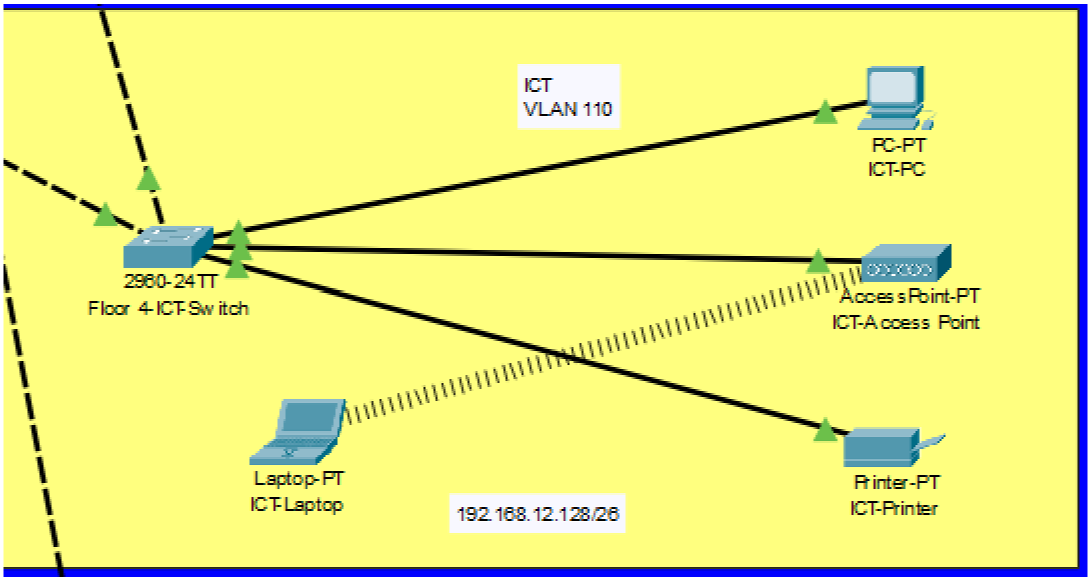

Figure 3.10: ICT Department of Banking Network

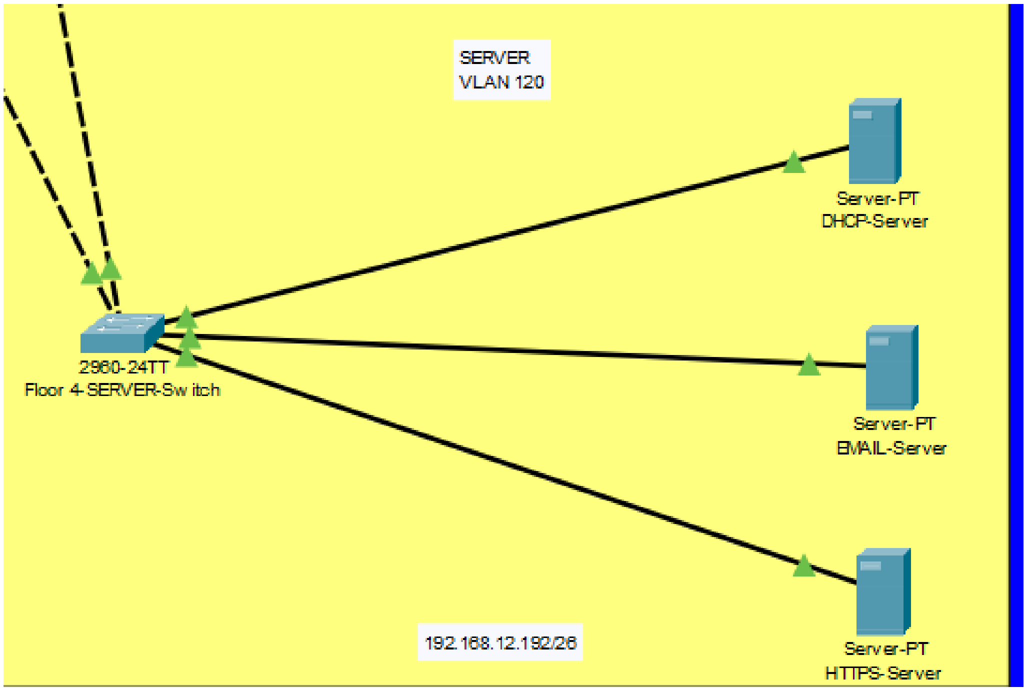

Figure 3.11: Server Department of Banking Network

3.2: Components

1. Routers
2. Switches
3. PCs
4. Laptops
5. Access Points
6. Servers
7. Printers

3.3: Operation

Banking Network provides safety and security to the network. It helps a secure networking between the systems in a building i.e. they can share information with each other with security. The project is providing different Vlans different range of IP addresses through the DHCP server. This helps to share the information in a secure way.

.

Section III

4.1. Network Configurations

1. SSH
2. VLANs
3. DHCP server Configuration
4. OSPF Configuration
5. Trunk mode Configuration
6. IP Routing

4.2. SSH Configuration Steps

```
en
config t

hostname Layer-3-Sw
banner motd #This is Layer3-switch#

line console 0
password cisco
login
exit

ip domain-name cisco.net
username cisco password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit

no ip domain-lookup
enable password cisco
service password-encryption

do wr
```

4.3. VLANs Configuration Steps

```
vlan 10

vlan 20

vlan 30

vlan 40
vlan 50
vlan 60


int vlan 10
no shutdown
ip add 192.168.10.1 255.255.255.192
ip helper-address 192.168.12.196
exit

int vlan 20
no shutdown
ip add 192.168.10.65 255.255.255.192
ip helper-address 192.168.12.196
exit

int vlan 30
no shutdown
ip add 192.168.10.129 255.255.255.192
ip helper-address 192.168.12.196
exit

int vlan 40
no shutdown
ip add 192.168.10.193 255.255.255.192
ip helper-address 192.168.12.196
exit

int vlan 50
no shutdown
```

```
ip add 192.168.11.1 255.255.255.192
ip helper-address 192.168.12.196
exit

int vlan 60
no shutdown
ip add 192.168.11.65 255.255.255.192
ip helper-address 192.168.12.196
exit

do wr
```

4.4. OSPF Configuration Steps

```
en
Config t
router ospf 10
Device(config-router)# network 192.168.129.16 0.0.0.3 area 20
End
```

4.5. Trunk Mode Commands

```
int range gig1/0/3-8
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

4.6. IP Routing

```
ip routing
router ospf 10
network 10.10.10.42 0.0.0.63 area 0
network 10.10.10.40 0.0.0.63 area 0
network 192.168.11.128 0.0.0.63 area 0
network 192.168.11.192 0.0.0.63 area 0
network 192.168.12.0 0.0.0.63 area 0
network 192.168.12.64 0.0.0.63 area 0
network 192.168.12.128 0.0.0.63 area 0
network 192.168.12.192 0.0.0.63 area 0
network 192.168.11.0 0.0.0.63 area 0
network 192.168.11.64 0.0.0.63 area 0
network 192.168.11.128 0.0.0.63 area 0
network 192.168.11.192 0.0.0.63 area 0
do wr
```

4.7. Subnetting

Base Network: 192.168.10.0

First Floor

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
Management	192.168.10.0	255.255.255.192/26	192.168.10.1 to 192.168.10.62	192.168.10.63
Research	192.168.10.64	255.255.255.192/26	192.168.10.65 to 192.168.10.126	192.168.10.127
HR	192.168.10.128	255.255.255.192/26	192.168.10.129 to 192.168.10.190	192.168.10.191

Second Floor

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
Marketing	192.168.10.192	255.255.255.192/26	192.168.10.193 to 192.168.10.254	192.168.10.255
Accounts	192.168.11.0	255.255.255.192/26	192.168.11.1 to 192.168.11.62	192.168.11.63
Finance	192.168.11.64	255.255.255.192/26	192.168.11.65 to 192.168.11.126	192.168.11.127

Third Floor

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
Logistics	192.168.11.128	255.255.255.192/26	192.168.11.129 to 192.168.11.190	192.168.11.191

Customer	192.168.11.192	255.255.255.192/26	192.168.11.193 to 192.168.11.254	192.168.11.255
Guest	192.168.12.0	255.255.255.192/26	192.168.12.1 to 192.168.12.62	192.168.12.63

Fourth Floor

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
Admin	192.168.12.64	255.255.255.192/26	192.168.12.65 to 192.168.12.126	192.168.12.127
ICT	192.168.12.128	255.255.255.192/26	192.168.12.129 to 192.168.12.190	192.168.12.191
Server Room	192.168.12.192	255.255.255.192/26	192.168.12.193 to 192.168.12.254	192.168.12.255

Between Routers and L3-Switches

Base Network Address: 10.10.10.0

No	Network Address	Subnet Mask	Host Address Range	Broadcast Address
1	10.10.10.0	255.255.255.252	10.10.10.33 to 10.10.10.34	10.10.10.35
2	10.10.10.4	255.255.255.252	10.10.10.37 to 10.10.10.38	10.10.10.39
3	10.10.10.8	255.255.255.252	10.10.10.41 to 10.10.10.42	10.10.10.43
4	10.10.10.12	255.255.255.252	10.10.10.45 to 10.10.10.46	10.10.10.47
5	10.10.10.16	255.255.255.252	10.10.10.49 to 10.10.10.50	10.10.10.51
6	10.10.10.20	255.255.255.252	10.10.10.53 to 10.10.10.54	10.10.10.55
7	10.10.10.24	255.255.255.252	10.10.10.33 to 10.10.10.34	10.10.10.35
8	10.10.10.28	255.255.255.252	10.10.10.37 to 10.10.10.38	10.10.10.39
9	10.10.10.32	255.255.255.252	10.10.10.41 to 10.10.10.42	10.10.10.43
10	10.10.10.36	255.255.255.252	10.10.10.45 to 10.10.10.46	10.10.10.47
11	10.10.10.40	255.255.255.252	10.10.10.49 to 10.10.10.50	10.10.10.51

12	10.10.10.44	255.255.255.252	10.10.10.53 to 10.10.10.54	10.10.10.55
13	10.10.10.48	255.255.255.252	10.10.10.33 to 10.10.10.34	10.10.10.35
14	10.10.10.52	255.255.255.252	10.10.10.37 to 10.10.10.38	10.10.10.39

4.8. CONCLUSION

In this project, we implemented a banking network for multi floor bank. The project is all working all the subnets and servers are working. All the devices which are connected are wirelessly are also working fine. It can be used by any bank for working.

4.9. REFERENCE

https://gurutechnetworks.otombenard.com/assetsProject/project5