Network Design Proposal for Bank

A COURSE PROJECT REPORT

By

Prakhar Sarraf (RA2011003010628)
Aniket Singh (RA2011003010629)
Ananya Ravichandran (RA2011003010630)
Shruti Tiwari (RA2011003010631)

Under the guidance of

Ida Seraphim

In partial fulfillment for the Course

of

18CSC302J - COMPUTER NETWORKS

in C.Tech

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

Kattankulathur, Chengalpattu District

NOVEMBER 2022

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this mini project report "**Project Title** " is the bonafide work

of

Prakhar Sarraf (RA2011003010628)
Aniket Singh (RA2011003010629)
Ananya Ravichandran (RA2011003010630)
Shruti Tiwari (RA2011003010631)

who carried out the project work under my supervision.

SIGNATURE

Ms. Ida Seraphim B
Assistant Professor
Department of Computing Technologies

SRM Institute of Science and Technology

ACKNOWLEDGEMENT

We express our heartfelt thanks to our honorable **Vice Chancellor Dr. C. MUTHAMIZHCHELVAN**, for being the beacon in all our endeavors.

We would like to express my warmth of gratitude to our **Registrar Dr. S. Ponnusamy,** for his encouragement

We express our profound gratitude to our **Dean (College of Engineering and Technology) Dr. T. V.Gopal,** for bringing out novelty in all executions.

We would like to express my heartfelt thanks to Chairperson, School of Computing **Dr. Revathi Venkataraman,** for imparting confidence to complete my course project

We wish to express my sincere thanks to **Course Audit Professor Dr.Annapurani Panaiyappan, Professor and Head, Department of Networking and Communications** and **Course Coordinators** for their constant encouragement and support.

We are highly thankful to our Course project Faculty **Ms Ida Seraphim B , Assistant Professor , Department of Computing Technologies,** for her assistance, timely suggestion and guidance throughout the duration of this course project.

We extend my gratitude to our **HoD Dr. M Pushpalatha, Professor & Head, Department of Computing Technologies** and my Departmental colleagues for their Support.

Finally, we thank our parents and friends near and dear ones who directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my Course project.

TABLE OF CONTENTS

ABSTRACT

In this project we will primarily focus on design and implementation of Bank Network using Cisco Packet Tracer (CPT). Security breach in the sector of banks is one of the most important concerns that needs to be addressed in the first place since loss of information can lead to huge losses to the bank overall. This project will help us curb such concerns by understanding the regulated flow of information/data. We will consider a national bank which has its head offices located in big cities like Chennai. The other small branches will be present in cities like Coimbatore, Madurai, Trichy. Salem, and Tirunelveli. These small branches in each state will be connected through LANs. Apart from this, VLANs and WANS will automatically be a part of the project networking since we are working on a Bank Network. Additionally, bank machines will be made available all around each city in specific to ensure better reach and reliable services to the people. Employees use a special software to access user accounts. The level of access to advanced resources within the bank varies from employee to employee based upon several criteria which include the designation of the employee, criticality of the information etc. The typical servers, mail, web, files and directories will be made available to all the employees to understand the flow of work within the bank.

INTRODUCTION

An ideal Bank Networking system will be fully network base and easy with friendly user interface staff task management system where any banking system manage their networking system somehow Head office, Branch Office, and other office are maintain LAN, MAN, WAN, VLAN, VLSM,VPN and some branch are maintain by manageable switch. LAN is used by Local Area Networking systems for example one office and a building. And MAN are used by the Metropolitan area Network for Example small towns, and WAN are used by the WIDE AREA NETWORK. This networking system is used by all banking users to share their data very easily. So that every user can use Network Structure & Security of Banking System instantly this way anywhere.

Objectives

1. To design and simulate a banking network system which is secure.
2. To simulate a banking network system that will easily manage any banking task.
3. To manage the banking network by a central system

Justification of study

The trend of growth of Online Banking brings many security issues and increasing cost of implementing higher security systems for both Online Banking users and the banks. Classers said security is all about risks and associated cost in his paper .The most critical issue of Online Banking security is to protect valuable information that is susceptible to unauthorized access by attackers. Hence, the banks must constantly increase security. At the same time, the banks must manage costs to make a profit. In contrast, increasing security is increasing the cost for attackers to break into the system, and increasing the punishment that the attackers may suffer. Hence the Internet criminals/attackers/crackers may lose motivation for hacking a high security online banking system.

Scopes of study

The scope of the Network Structure & Security of Banking System includes.

1. Online based day to day transmission.

2. Save time and cost because of day to day transmission.

3. Established relation between one branch to another

4. Connect all branches to the head branch in the same network.

5. Online based update and maintain everyday work.

LITERATURE SURVEY

Review of relevant literature

Networks can also be characterized in terms of spatial distance as local area networks (LANs), metropolitan area networks (MANs), and wide networks (WANs). A given network can also be characterized by the type of data transmission technology in use on it (for example, a TCP/IP or Systems Networks Architecture network); by whether it carries voice, data, or both kinds of signals; by who can use the network (public or private); by the usual nature of its connections (dial-up or swathed, dedicated or no switched, or virtual connections); and by the types of physical links (for example, optical fiber, coaxial cable, and Unshielded twisted Pair). The flowing methods to be traditional (old) way of recurrent.

- Data transfer / transition sends the branch office to the head office by manually.
- Need extra cost for transmission because of manual transmission.
- Time based transmission.
- Low security system .Data is carried or transferred by humans.
- User unfriendly because of the slow process.
- Very complex to maintain.

Computer Networking

A computer network is a system for combination among two or more computers. These networks are fixed (cabled, permanent) or temporary (as via modems). A computer network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange intranet a restricted computer network;
a private network created using World Wide Web software.

IP address

An IP address consists of 32 bits of information. The 32 bit IP address is a structured or hierarchical address. 32 bits are divided into 4 sections. And every section is an 8 bit address. The 32 bits addresses are divided into two parts one is Host section, and another is m section. 32 bits addresses have also 5 classes, which is,

	bits	8bits	8bits	8bits
Class A:	Network	Host	Host	Host
Class B:	Network	Network	Host	Host
Class C:	Network	Network	Network	Host
Class D:	Multicast			
Class E:	Research			

Network address of Class A: 1 to 126

Network address of Class B: 128 to 191

Network address of Class C: 192 to 223

Network address of Class D and E: The addresses between 224 and 255 are reserved for class D and E networks.

Class D is used for multicast addresses, Class E is used for scientific purposes.

VLSM

Network administrators must anticipate and manage the physical growth of networks. This may require them to buy or lease another floor of a building for new network equipment such as racks, patch panels, switches, and routers. Network designers must choose address schemes that allow for growth. Variable-length subnet mask (VLSM) is used to create efficient and scalable address schemes. IPv4 offered an address strategy that was scalable for a time before it resulted in an inefficient allocation of addresses. IPv4 may soon be replaced with IP version 6 (IPv6) as the dominant protocol of the internet. IPv6 has virtually unlimited address space and implementation has begun in some networks. Over the past two decades, engineers have successfully modified IPv4 so that it can survive the exponential growth of the Internet. VLSM is one of the modifications that has helped to bridge the gap between IPv4 and IPv6.

Why is it used?

As IP subnets have grown, administrators have ways to use their address space more efficiently. This page introduces a technique called VLSM. With VLSM, a network administration can use a long mask on networks with few hosts, and a short mask on subnets with many hosts.

VLSM is used for following reasons

- The ultimate solution is IPv6 with 128-bit address space.
- It allows for 340, 283, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456 addresses.

Importance of VLSM

Efficient use of organizations assigned IP address space. Route aggregation VLSM.
Efficient use of the organization"s assigned IP address space Assume that a network
administrator has decided to configure the 130.5.0.0/16 network with a /22
extended-network prefix. This design allows for 64 subnets with 1,022 hosts
each. Fine if the organization plans to deploy a number of large subnets. What about the
occasional small subnet containing only 20 or 30 hosts? About 1,000 IP host addresses
are wasted for every small occasional subnet.

Networking devices

A computer network consists of different devices to share, transmit, and boost the signal,
voice and data. Network devices or components are the physical parts connected to a
network. The basic network devices, Individual computers, Hubs, switches, Bridges, and
Routers. The following are the Devices.
Switch, Router

Ethernet

Ethernet was originally developed by Digital, Intel and Xerox (DIX) in the early 1970"s
and has been designed as a 'broadcast' system, i.e. stations on the network can send
messages whenever and wherever it wants. All stations may receive the messages,
however only the specific station to which the message is directed will
respond. The original format for Ethernet was developed in Xerox Palo Alto Research
Center (PARC) California in 1972 Using Carrier Sense Multiple Access with
Collusion Detection (CSMA/CD) it had a transmission rate of 2.94MBps and could
support 256 devices over cable stretching for 1km. The two inventors were Robert
Metcalf and David Boggs. The' Ether' part of Ethernet denotes that the system is not
meant to be restricted for use on only one medium type, copper cables, fibre cables and
even radio waves can be used.

Physical Connections

IEEE 802.3 specifies several different physical layers, where Ethernet defines only one.

Each IEEE 802.3 physical layer protocol has a named that summarizes its characteristics.

LAN Speed in	"Base"=baseband	LAN segment in 100- meter
	10Base5	
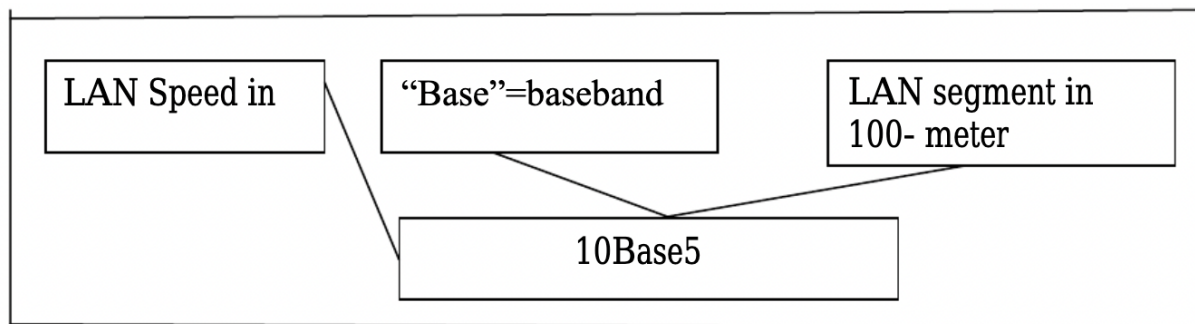
2.6.2 ETHERNET FRAME FORMATS

Field length,
In bytes

Ethernet

7	1	6	6	2	46-1500	4
Preamble	S O	Destination address	Source address	Type	Data	FCS

Field length:-
In bytes:

7	1	6	6	2	46-1500	4
Preamble	S O F	Destination address	Source address	Type	Data	FCS

SOF = Start of frame delimiter   **Figure: Ethernet and IEEE 802.3 Frame Formats**

REQUIREMENTS

NETWORK REQUIREMENTS

From the given scenario, we draw the following requirements:

1. Identifying the appropriate hardware which would be used (Cisco Packet Tracer)

2. Users on the internet should be able to access only https on the bank server.

3. Users on the internet should have access only to the public IP address of the server and not the private IP address.

4. The users in the organization should have full access to the server.

5. TCP/IP Network design with IP addressing

6. Features and configuration required on the hardware with explanation

We need to configure a network design keeping the following requirements in mind.

Functional Requirements

Banking system in India, all banks have an IT department. The IT department solves all types of IT problems and serves the core network. IT creates a core network diagram. This diagram involves all types of usable network mechanisms (Switch, Router, Firewall, Server) etc. Simulation is the most important of any system. An accurate system design, accurate performance and accurate Simulation give the best performance of a system.

NETWORK REQUIREMENT ANALYSIS

As the locations of the banks are spanned across different geographical locations, a VPN solution is recommended as it would be more economical as compared with a leased line solution. VPN appliances are required for the same. The application server is recommended as Windows 2008 / Windows 2012, with appropriate failover clustering to provide high availability to the application. The application server should be set up on a DMZ, where only access to https protocol (TCP port 443), should be made available to users accessing from the outside. Antivirus with desktop firewall should be installed on the server, which would provide host level protection. An appliance, which would perform deep packet inspection, should be set up on the network, to filter incoming traffic to the application server. This would scan the traffic for security threats and attacks.

HARDWARE AND SOFTWARE REQUIREMENT ANALYSIS

1.   At the main office, a VPN appliance would be required, which would have integrated firewall and deep packet inspection. The recommended VPN appliance is Sonic wall NSA 220/W, which has the capacity to support site to site VPN tunnels and also has deep packet inspection and firewall capabilities.

2.   There are 200 users in the main office. A total of 5 no of 48 port switches are recommended considering ports for servers, VPN appliance and expansion plan. The Cisco Catalyst 2960S- 48FPD-L is recommended for the same.

3.   At the branch offices, the Sonicwall TZ105 series is recommended to establish site to site VPN connectivity with the main office.

4.   There are a total of 100 users each at the branch office. A total of 3 nos of 48 port switches is recommended, which are Cisco Catalyst 2960S-48FPD-L, considering future expansion plans.

5.   Windows 11 is recommended for the application server with server hardware.

ADDITIONAL REQUIREMENTS

All the locations have high speed internet connection. At the main office, an additional public IP address would be required to host the application server. The IP address would be registered with a domain name, which would enable users on the outside world (internet), to access the application.

Implementation – Cisco Packet Tracer:

For implementing this bank prototype, we have used Router-PT which have serial ports, So that it will be easy for us to connect to 6 branches and we have also used 2960-24TT switches all over the network to connect to various campuses among the cities which are then interconnected to the servers and users. All the serial ports are assigned with IP addresses so they can be recognized between the cities without confusion.

Cisco Packet Tracer

i.   Cisco Packet Tracer is a visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks.

ii. Using packet tracer we have implemented network topology, assigned routers and switches.

iii.   We can also configure each and every router and network with the IP address and test whether the data transfer is successful or not.

FEATURES AND SERVICES

a. VLAN

Two networks are required at the main office. One network would be for the LAN, where the office's users would be connected. The second network would be the DMZ network, where the application server is hosted. This is required since the application server would require access from outside. Two VLANS would be created which would be mapped with the LAN and DMZ network. VLANS would be configured on the Switches.

b. Access control lists

Access control lists are configured on the VPN appliance at the main office. The ACLs are used to restrict communication from the internet to only the allowed port, which is TCP port 443 on the application server in the DMZ. ACL is also configured to allow all traffic from the branch office networks to the DMZ and LAN network in the main office.

c. Static NAT

Static NAT is configured on the VPN Appliance to allow traffic from the public IP address of the application server, to the LAN IP address.

d. Failover cluster

Failover cluster is configured on Windows 11, on which the application server is hosted. This would ensure that high availability is provided to the application.

e. RIP (Routing Information Protocol)

This protocol is the intradomain (interior) routing protocol which is based on distance vector routing and it is used inside an autonomous system. Routers and network links are called nodes. The first column of the routing table is the destination address. The cost metric in this protocol is hop count which is the number of networks which need to be passed to reach a destination. Here

infinity is defined by a fixed number which is 16; it means that using a Rip network cannot have more than 15 hops.

f. RIP Version-2:

Due to some deficiencies in the original RIP specification, RIP version 2 was developed in 1993. It supports classless Inter-Domain Routing (CIDR) and has the ability to carry subnet information, its metric is also hop count, and max hop count 15 is the same as rip version 1. It supports authentication and does subnetting and multicasting. Auto summary can be done on every router. In RIPv2 Subnet masks are included in the routing update. RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast (255.255.255.255).

Advantages of RIP version-2

1. It's a standardized protocol.
2. It's VLSM compliant.
3. Provides fast convergence.
4. It sends triggered updates when the network changes.
5. Works with snapshot routing – making it ideal for dial networks.

NETWORK TOPOLOGY DIAGRAM
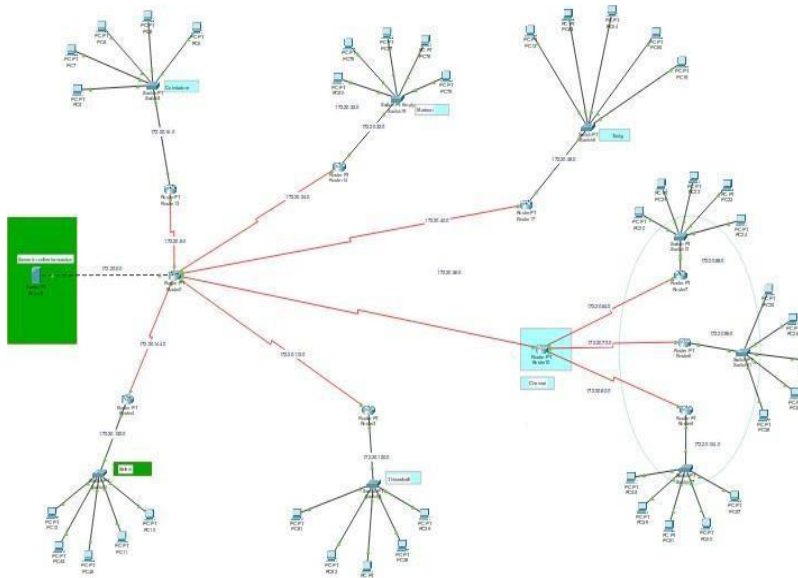
Fig 1: Network Topology

NETWORK TOPOLOGY DIAGRAM EXPLANATION

• **Access Layer**

In this layer, all th**e** end devices are connected to each other to the network and we will be having the layer 1 switch for the further connections.

• **Distribution Layer**

Distribution layer, mostly the layer 3 switches are used to connect the end devices and make the network correspond and this connects to the access and core layers of the network design.

• **Core Layer**

The core layer is the main source of all the layers, where this layer is used to transfer the large amount of traffic very quickly.
There will be 1 main branch and 5 sub-branches for this network topology:

- • Chennai
- • Coimbatore
- • Madurai
- • Trichy
- • Salem
- • Tirunelveli

Each branch is explained separately for better understanding of the network. We'll get started with Chennai network topology then followed by Coimbatore, Madurai,Trichy, Salem, Tirunelveli network topologies.

IP NETWORK DESIGN

- **Chennai – Network Topology:**
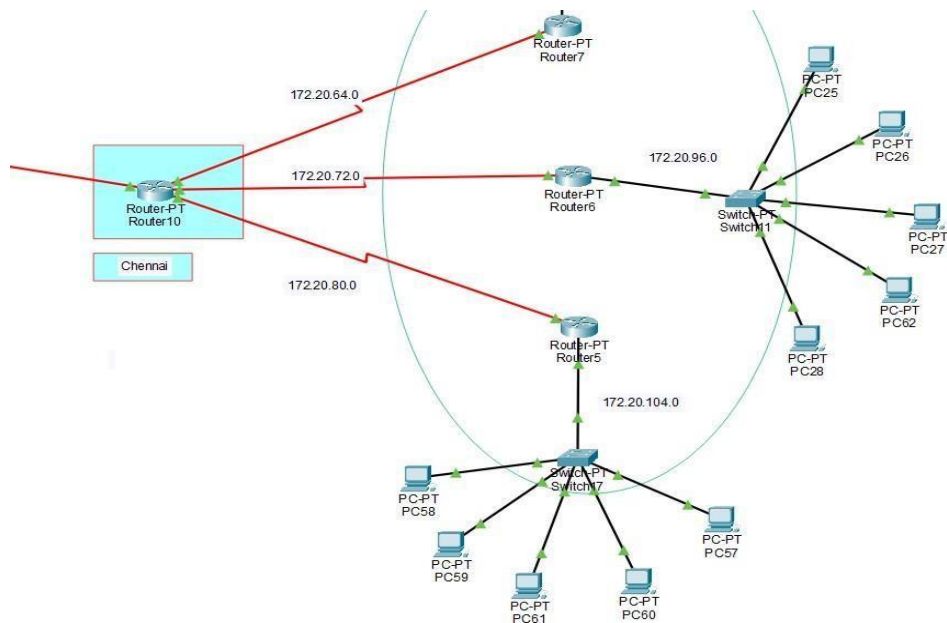
Fig 2: Network Topology of Chennai
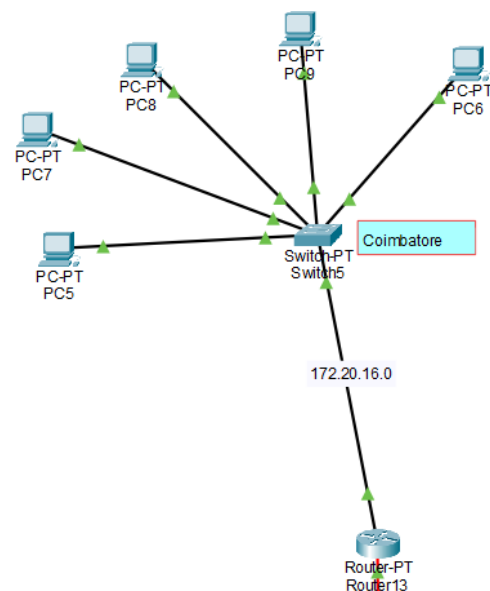
- **Coimbatore – Network Topology:**

Fig 3: Network Topology of Coimbatore
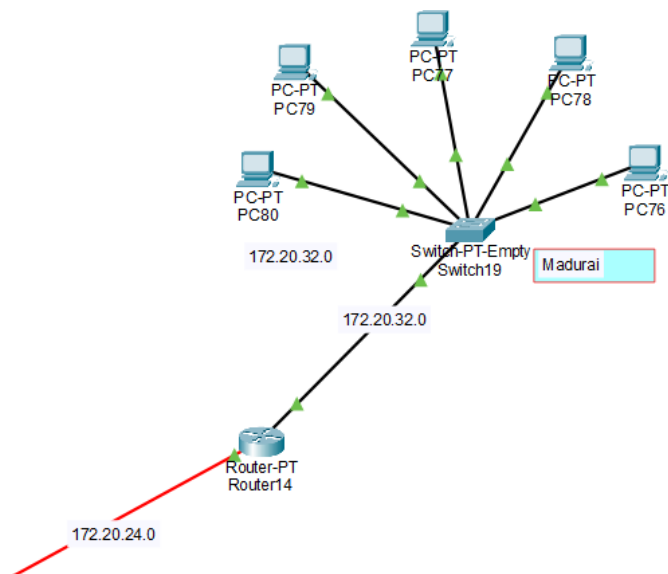
- **Madurai – Network Topology:**
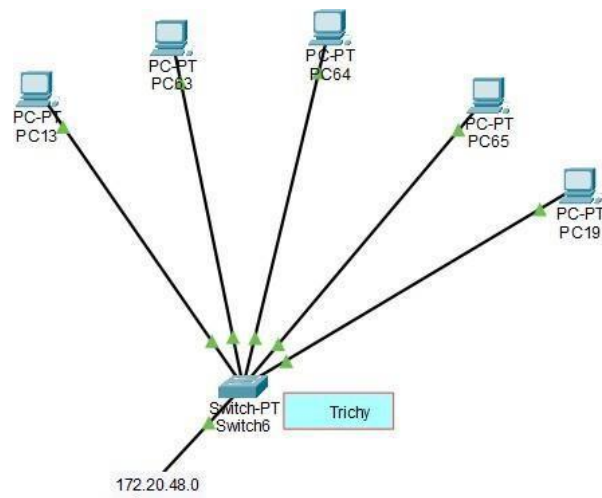

Fig 4: Network Topology of Madurai

- **Trichy – Network Topology:**

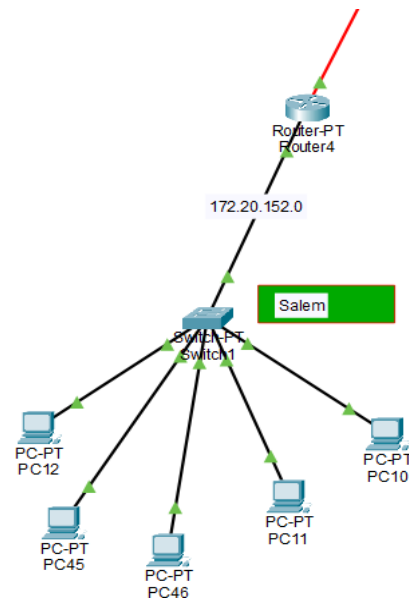Fig 5: Network Topology of Trichy

- **Salem – Network Topology:**

Fig 6: Network Topology of Salem
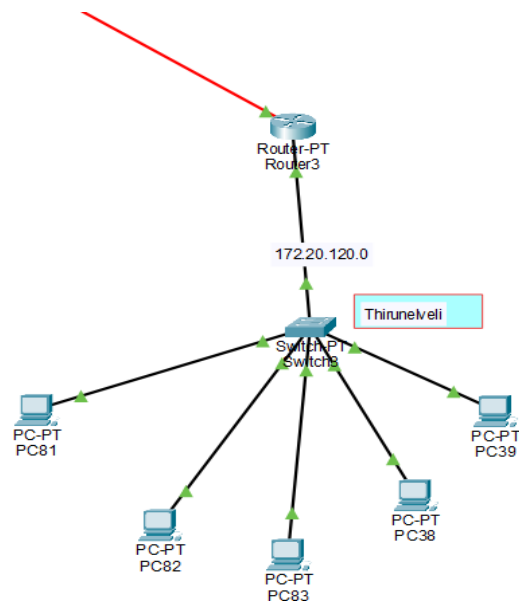
- **Tirunelveli – Network Topology:**

Fig 7: Network Topology of Tirunelveli

IP ADDRESS DESIGN

| Branch	IP Address	Subnet Mask
Chennai	Router – 170.20.56.2/21 Router – 170.20.64.1/21 Router – 170.20.72.1/21 Router – 170.20.80.1/21	255.255.248.0 255.255.248.0 255.255.248.0 255.255.248.0
Coimbatore	Router – 172.20.8.2/21	255.255.248.0
Madurai	Router – 172.20.24.2/21	255.255.248.0
Trichy	Router – 172.20.40.2/21	255.255.248.0
Salem	Router – 172.20.144.2/21	255.255.248.0
Thirunelveli	Router – 172.20.112.2/21	255.255.248.0

NETWORK DESIGN CONFIGURATION AND STRATEGY
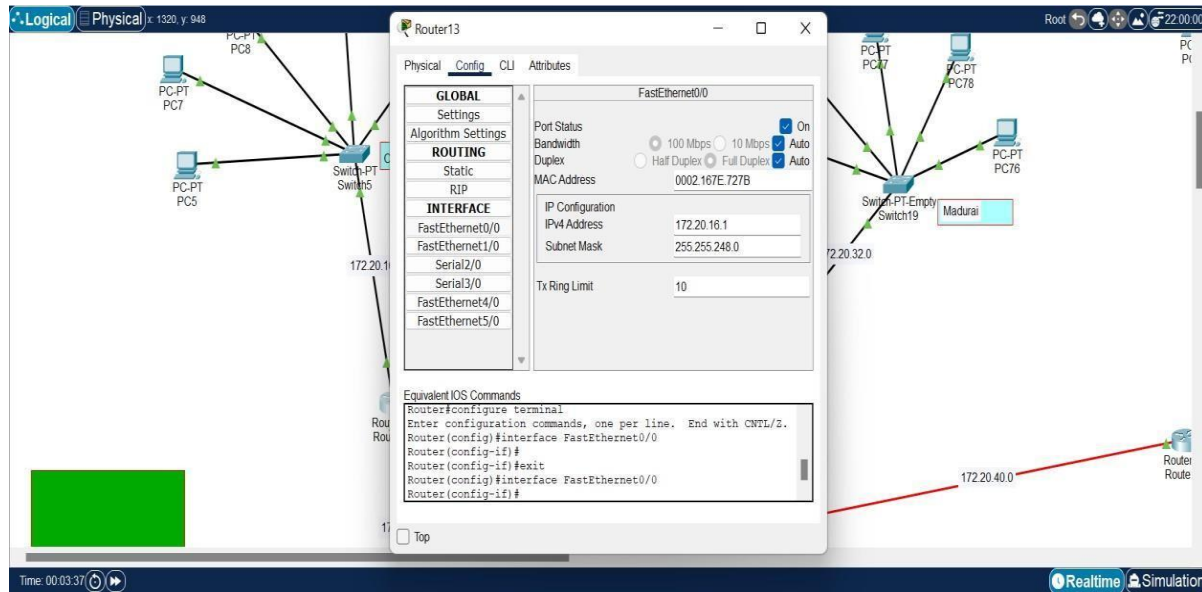
Fig 8: We have manually checked if the network between each user in the branch is connected to one other.

This is done individually with testing from one branch device to other branch devices instead of a buffer manager interface. After testing this manually buffer testing is implemented and checked.

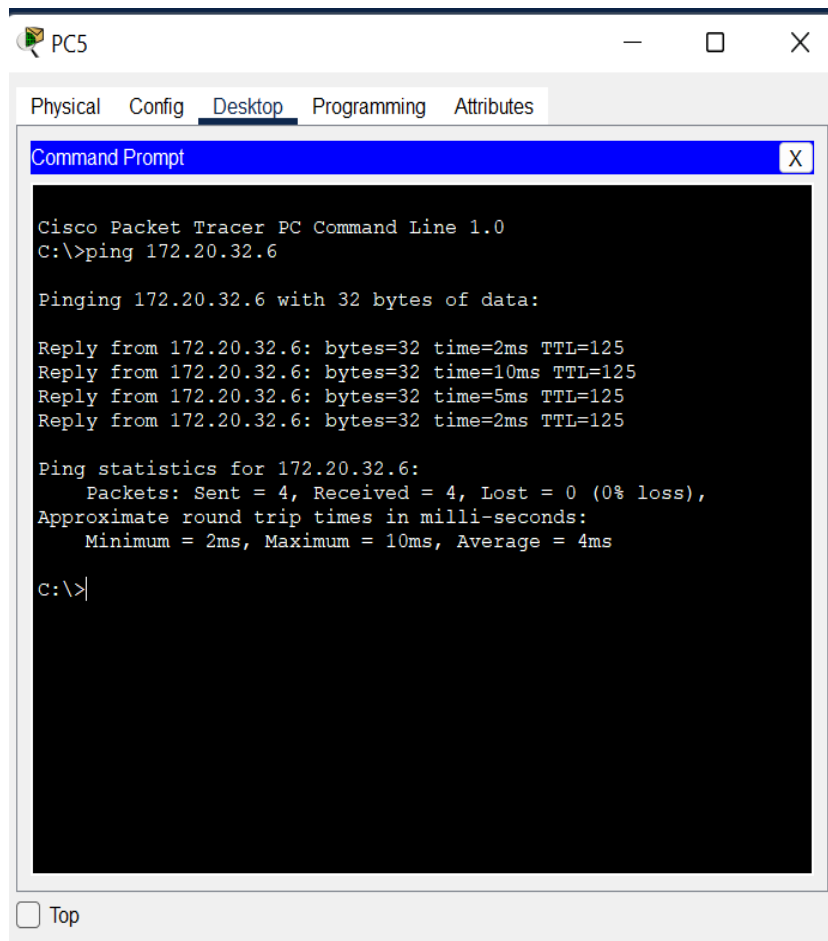**Ping from a PC to Another PC:**

Fig 9: Pinging from one PC to another

- The above screenshot shows the successful implementation of the connection across two different systems, where it executes perfectly.
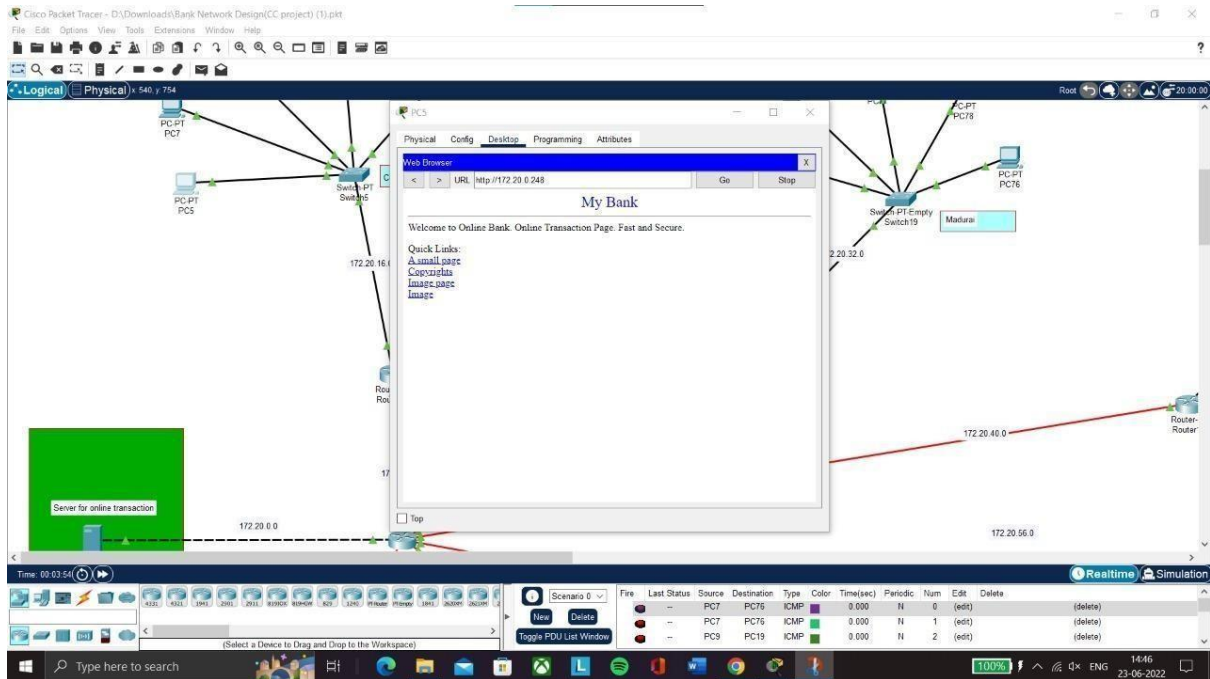- All the data packets are received without any loss of data.

b.

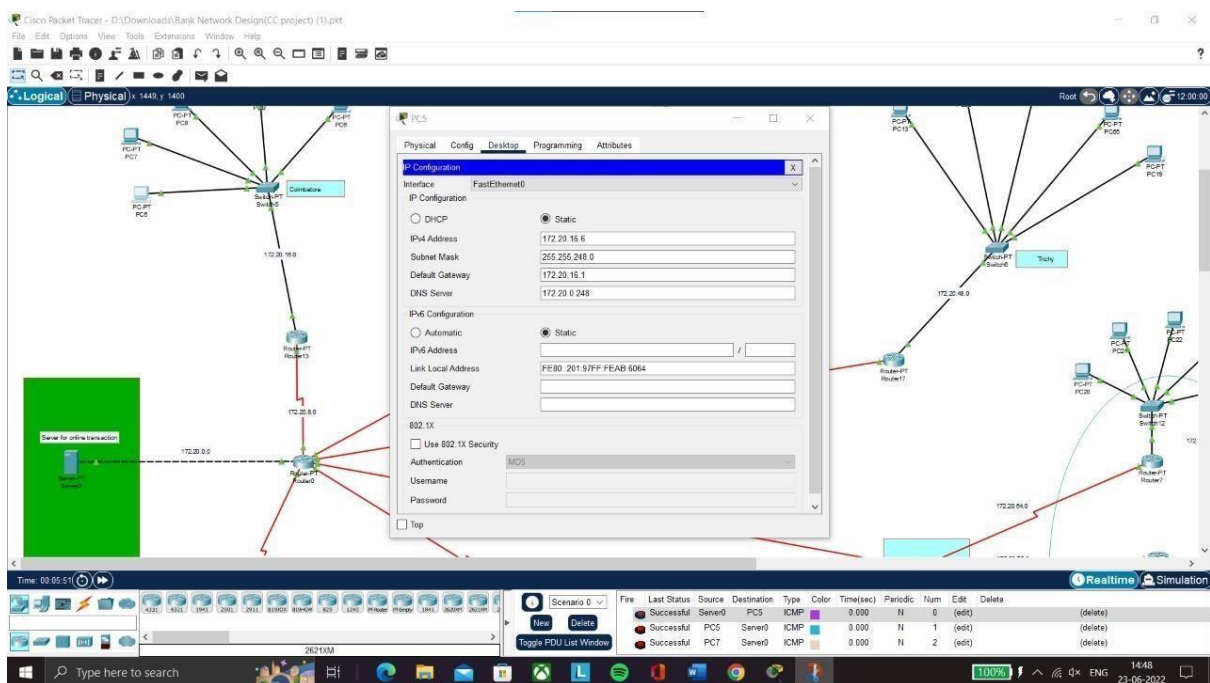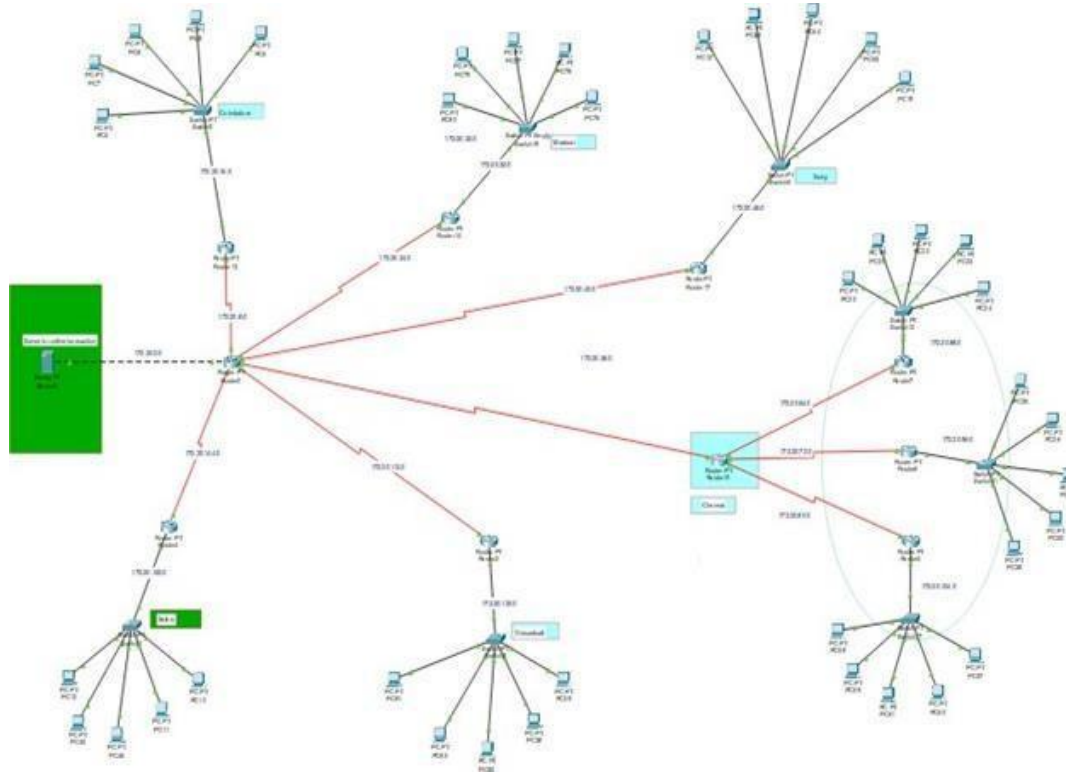Fig 10: Application server for online transaction using HTTPS Protocol

c.

Fig 11: Use of DNS (Domain Name System)

Screenshot of the Project

HARDWARE INVENTORY LIST

Hardware inventory provides a simple way of finding basic information about your installed hardware. Hardware includes processors, memory, serial ports, parallel ports, power supplies, fans, graphics adapters, network adapters, and SCSI and IDE devices such as disks.

Key for Lists = Product
- Cost
- Availability
- Performance
- Maintainability

HP File/Print Server LH 3000
- $4,089.00
- Available/In Stock
- P3 866MHz, 128 MB/4GB RAM, 256KB L2, 32X CD
- 3 Year Warranty and Maintained by Computer Services as needed

HP NetServer Hard Drive
- $379.95
- Available/In Stock

- 9.1 GB SCSI3 7200 RPM LVD, LC2000/LH3 Compatibility
- Maintained by Computer Services as needed

IntelliFax-4750 Commercial Laser Fax
- $499.95
- Available/In Stock
- 250-sheet Universal Paper Cassette, 4 MB, Dual Access Memory (upgradeable to 12 MB or 20 MB), Up to 50 page Auto Document Feeder, Stores up to 270 pages, 14.4 Kbps fax modem
- Maintained by Computer Services as needed

HP Laser Jet 8150N Series
- $2,469.95
- Available/In Stock
- 1200 dpi, 32 MB memory expandable to 192 MB, Network ready 10/100 Base-TX, 2 open EIO Slots, 3/100 (Number of trays/capacity)
- Maintained by Computer Services as needed

Windows 2000 Server
- $819.95
- Available/In Stock
- 5 Licenses included, Full Version
- Maintained by Computer Services as needed

Compaq DeskPro EN P3/600
- $999.00
- Available/In Stock
- 10 GB, 128 MB, 40X CD ROM, NIC DT Win 00; with Windows 2000 OS
- 3 Year Parts and Labor Warranty and Maintained by Computer Services as needed

CAT 5 Cable
- $145.99
- Available/In Stock
- 4 pair solid PVC; 1000 feet
- Maintained by Computer Services as needed

SmartPro 1400
- $454.99
- Available/In Stock
- 6 outlets +LAN
- Maintained by Computer Services as needed

EtherFast 8-Port 10/100 Desktop Hub
- $79.99
- Available/In Stock
- True 10/100 auto-sensing ports, Internal store-and-forward switching segment, built-in data collision and frame re-timing
- Manufacturer's 5 year limited warranty and Maintained by Computer Services as needed

EtherFast 12-Port 10/100 Desktop Hub
- $129.99
- Available/In Stock
- True 10/100 auto-sensing ports, Internal store-and-forward switching segment, built-in data collision and frame re-timing
- Manufacturer's 5 year limited warranty and Maintained by Computer Services as needed

EtherFast 20-Port 10/100 Desktop Hub
- $199.99
- Available/In Stock
- True 10/100 auto-sensing ports, Internal store-and-forward switching segment, built-in data collision and frame re-timing
- Manufacturer's 5 year limited warranty and Maintained by Computer Services as needed

EtherFast II 24-Port 10/100 Switch
- $449.99
- Available/In Stock
- True 10/100 auto-sensing ports, Internal store-and-forward intelligent switching segment, built-in data collision and frame re-timing
- Manufacturer's 5 year limited warranty and Maintained by Computer Services as needed

CISCO 2621 Ethernet Router 2 10/100
- $2,319.00
- Available/In Stock
- Provides remote access and WAN integrations, supports extranet VPN access and multiple modules, two 10/100 RJ45 ports, two WAN slots, one network module slot, one AIM slot
- Maintained by Computer Services as needed
-

Firewall I Internet Gateway V4.1 100 Nodes ONL
- $6,000.00
- Available/In Stock
- Full Version
- Maintained by Computer Services as needed

DS-2 Connection
- $650.00
- Available
- 1 month, exclusive rights
- Maintained by Quest Communications

INFERENCE

Had a deep understanding of how switches, routers and PCs are interconnected to form an in-house network. And also learned how the data is transmitted among different networks using the IP address.

REFERENCES

1. https://brainbell.com/tutors/A+/Hardware/Basic_Requirements_of_a_Network.htm

2. https://www.ccexpert.us/network-design-2/characterizing-types-of-traffic- flow-for-newnetwork-applications.html

3. https://www.netacad.com/courses/packet-tracer

4. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe- 16/iro- xe-16-book/iro-cfg.html

5. https://networklessons.com/ospf/basic-ospf-configuration