Network design proposal for Bank

18CSS202J- Computer Communication Project Report

Submitted by

Abhishek S - RA2011033010069
Lagan Mehta - RA2011033010073
Sanskar Sharma - RA2011033010079
Rishu Raj - RA2011033010082

Submitted to

Dr. Vegesna S M Srinivasavarma

Assistant Professor, Department of Computing Technologies

in partial fulfilment for the award of the degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE ENGINEERING WITH SPECIALIZATION IN SOFTWARE ENGINEERING

SCHOOL OF COMPUTING
DEPARTMENT OF COMPUTATIONAL INTELLIGENCE
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR- 603 203

Date - JUNE 2022

Network design proposal for Bank

1. 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 Thirunelveli. 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.

1.1 Objectives

The main objective of this project is to design a network for the bank with the given constrains. In this we have 5 branches and 1 main branch. This network design of bank also has a server for online transaction which is used by the customers of all branches.

2. Network Requirements:

1. Identify the hardware components required to setup the network for the Bank

2. High availability should be available to the application server, which is accessible using https protocol.

3. The application server should be setup in a secure manner with network and host level protection.

4. All traffic into the application server should be scanned for security attacks.

5. IP network design for the branch and main offices.

6. IP addressing range for users and hardware components.

7. The users at different locations should be able to access each other, including the application server.

8. Identify the features and methodology which would be followed to achieve the solution.

9. Network Topology diagram.

2.1 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 setup 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 setup on the network, to filter incoming traffic to the application server. This would scan the traffic for security threats and attacks.

2.2 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 2008/2012 is recommended for the application server with server hardware.

2.3 Additional requirements

1. 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.

3. 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.

3.1 Cisco Packet Tracer:

- Cisco Packet Tracer is a visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks.
- Using packet tracer we have implemented network topology, assigned routers and switches.
- We can also configure each and every router and network with the IP address and tested whether the data transfer is successful or not.

3.2 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

4. Feature and Services

4.1 VLAN

Two networks are required at the main office. One network would be for the LAN, where the offices 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.

4.2 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.

4.3 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.

4.4 Failover cluster

Failover cluster is configured on the Windows 2008/2012, on which the application server is hosted. This would ensure that high availability is provided to the application.

4.5 RIP (Routing Information Protocol)

This protocol are 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 node. The first column of routing table is destination address. The cost of metric in this protocol is hop count which is number of networks which need to be passed to reach 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.

5. 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 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).

5.1 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.

6. Network Topology Diagram

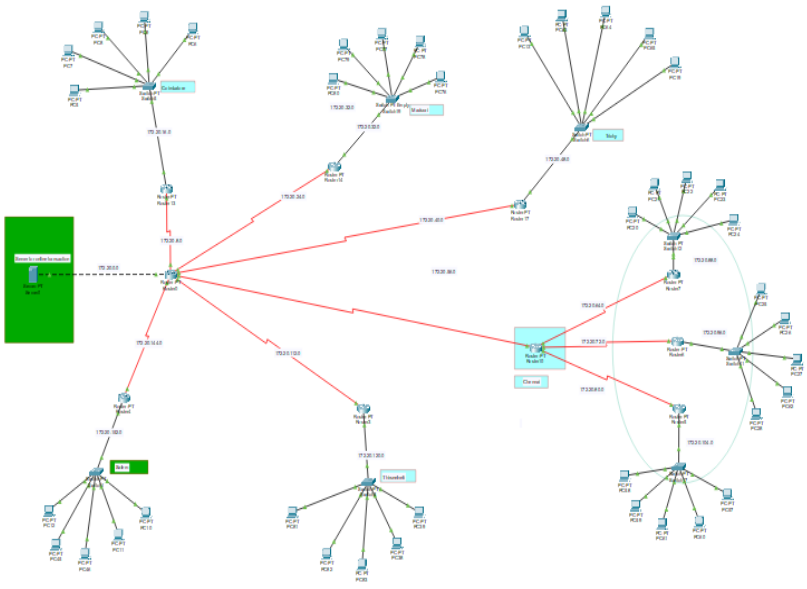

Fig 6a: Network Topology

6.1 Access Layer

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

6.2 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.

6.3 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
- Thirunelveli

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, Thirunelveli network topologies.

6.4 Chennai – Network Topology:

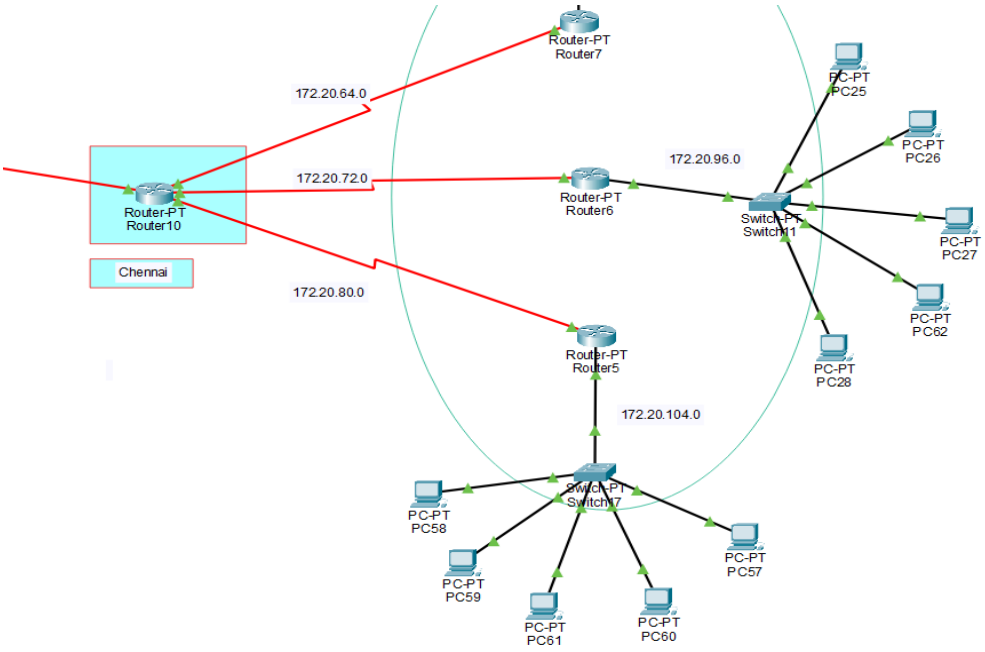

Fig 6b: Network Topology of Chennai

6.5 Coimbatore – Network Topology:

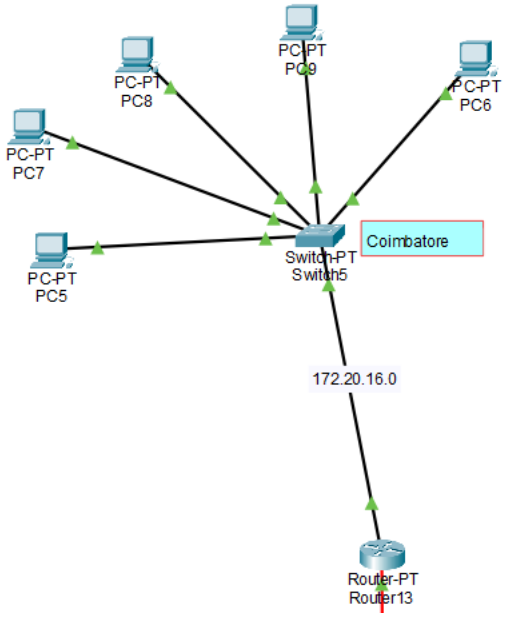

Fig 6c: Network Topology of Coimbatore

6.6 Madurai – Network Topology:

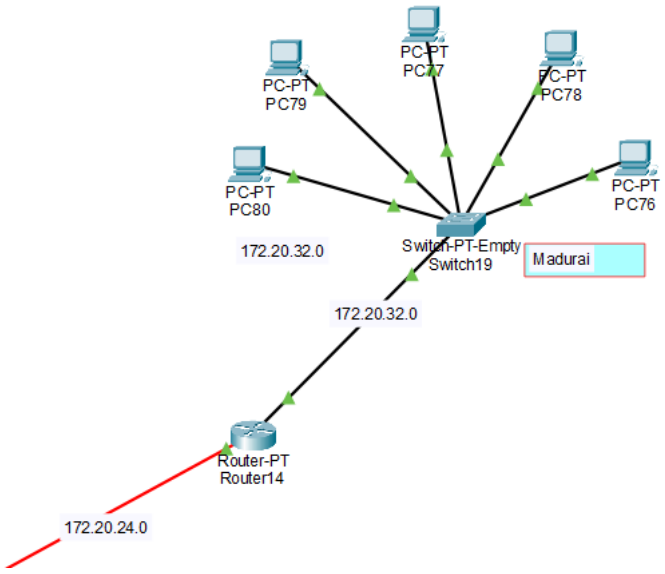

Fig 6d: Network Topology of Madurai

6.7 Trichy – Network Topology:

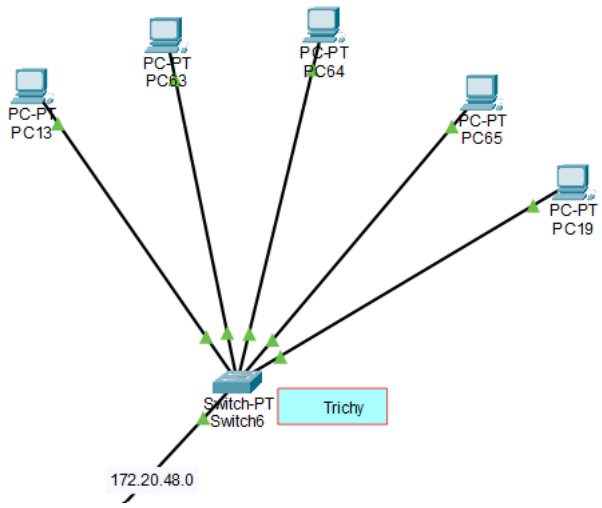

Fig 6e: Network Topology of Trichy

6.8 Salem – Network Topology:

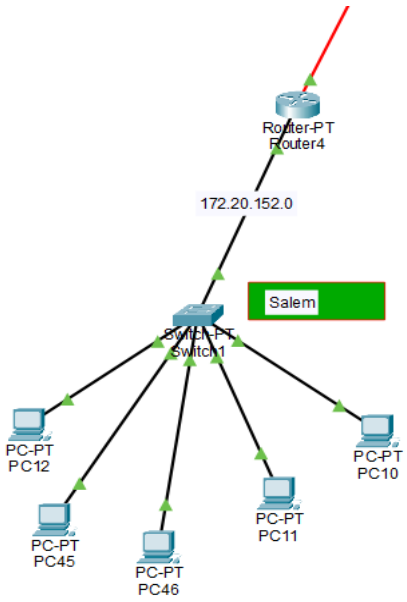

Fig 6f: Network Topology of Salem

6.9 Thirunelveli – Network Topology:

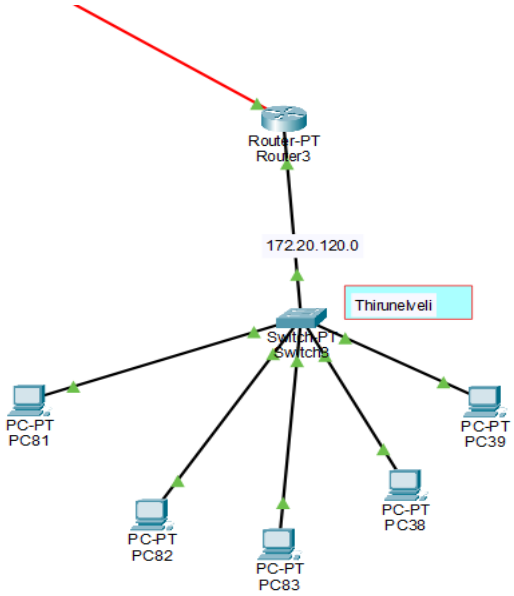

Fig 6g: Network Topology of Thirunelveli

7. Network Design and configuration strategy

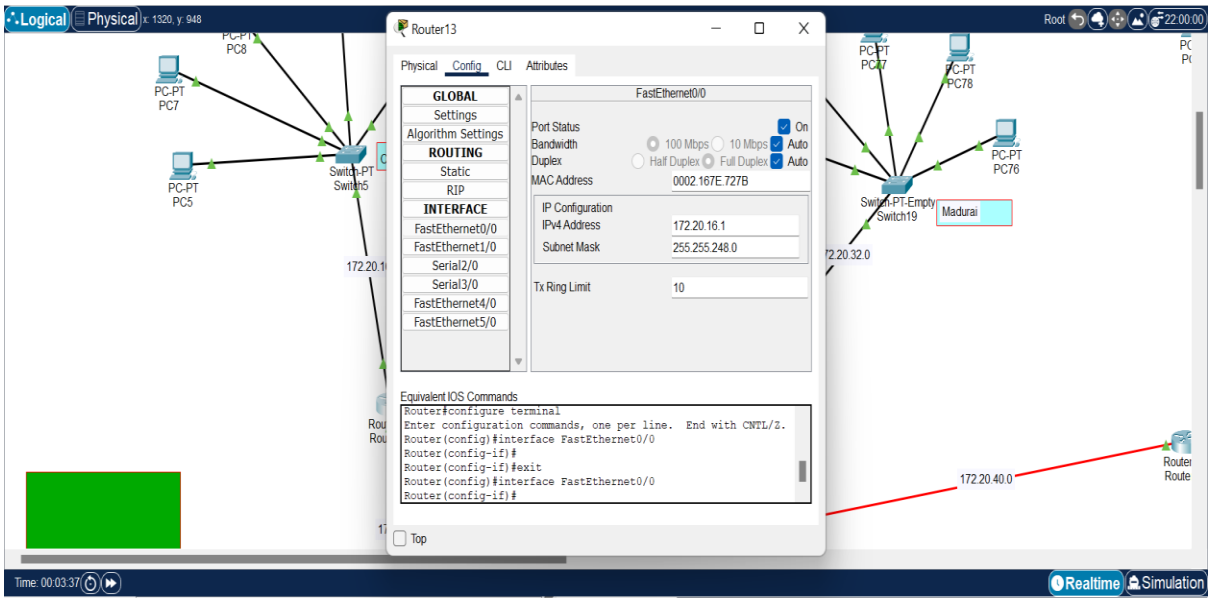

Fig 7a:

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 buffer manager interface. After testing this manually buffer testing is implemented and checked.

7.1 Ping from a PC to Another PC:

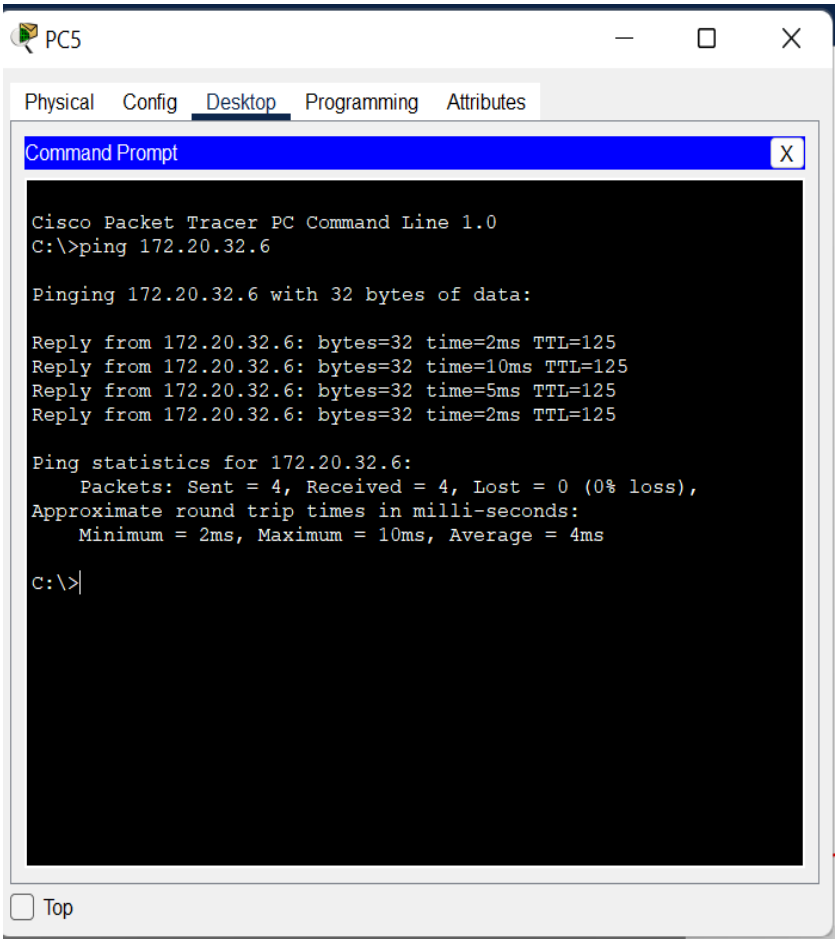

Fig 7b: Pinging from one PC to another

- 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.

7.2

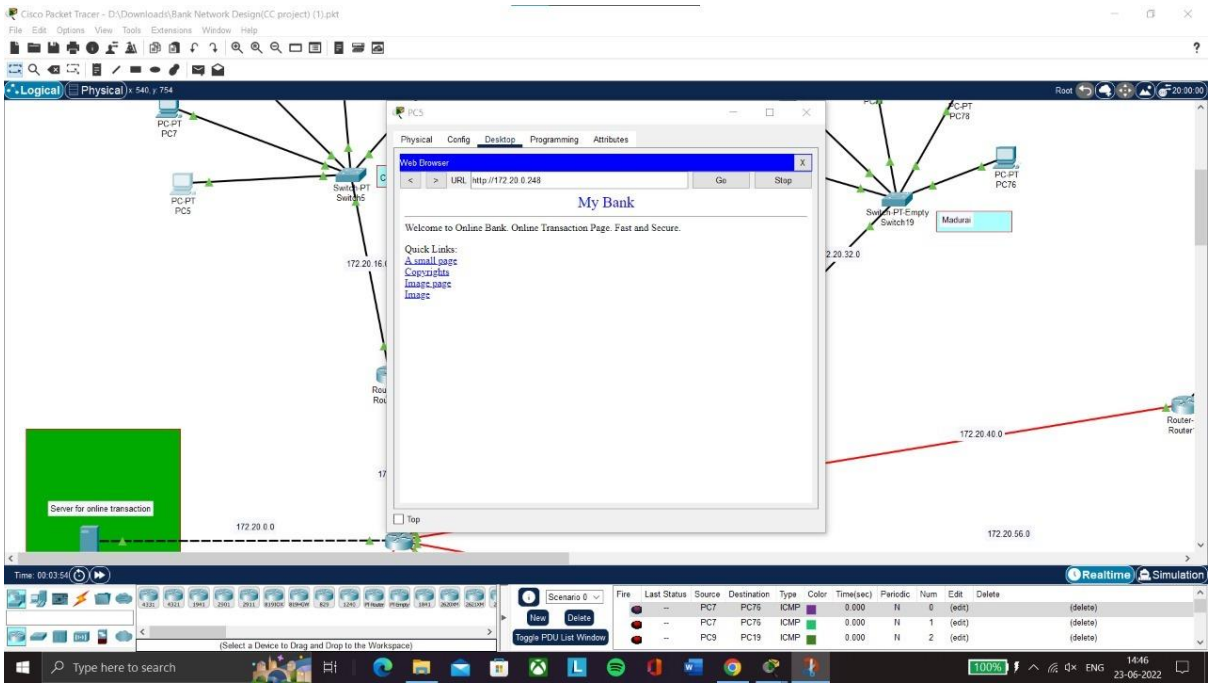

Fig 7c: Application server for online transaction using HTTPS Protocol

7.3

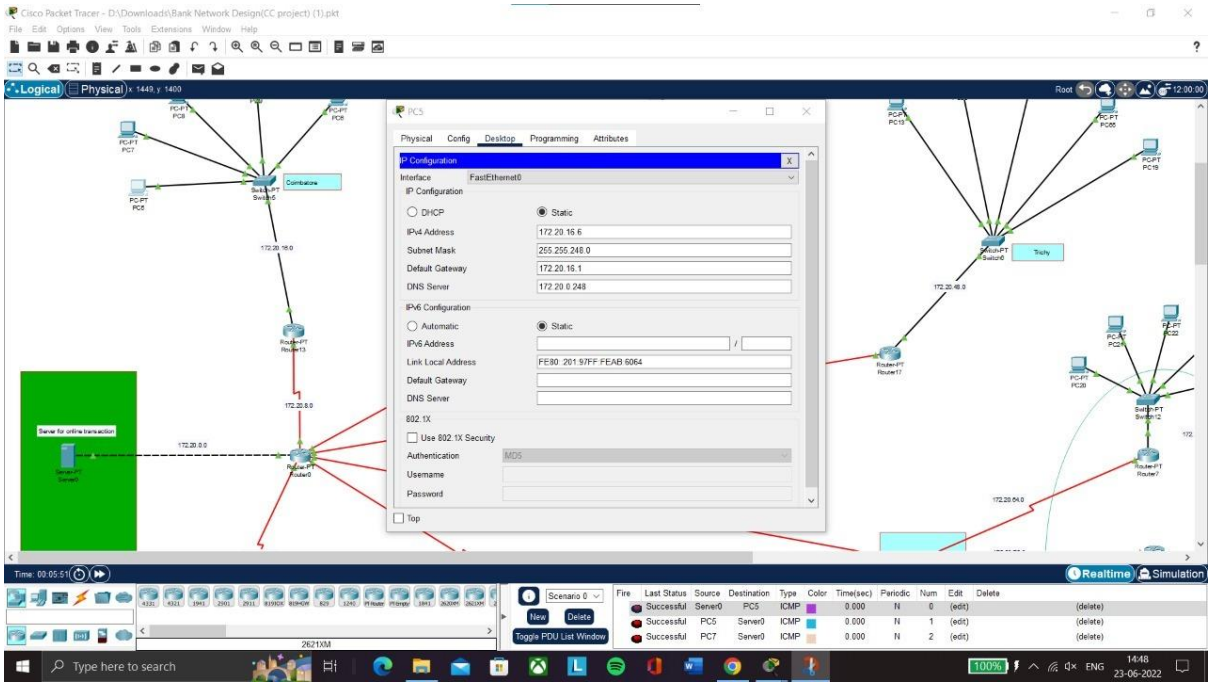

Fig 7d: Use of DNS (Domain Name System)

8. 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