DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade, ShavigeMalleshwara Hills, Kumaraswamy Layout, Bengaluru-560078.

Minor Project Report

on

"Implementation of Banking VPN Network"

Submitted By

Nikhil Raj(1DS18CS172)
Saurav Suman (1DS18CS186)

Fifth Semester B.E (CSE)
in

Computer Networks Laboratory with Mini-project
18CS5DLCNL

Under the guidance of
Dr. Nagaraj J
Assistant Professor
Dept. of CSE
DSCE, Bangalore

Department of Computer Science and Engineering
Dayananda Sagar College of Engineering
Bangalore-78

CONTENTS

1. Abstract ---------- 1

2. Introduction ---------- 2
   - 2.1 BGP ---------- 2
   - 2.2 VPN ---------- 2
   - 2.3 FTP ---------- 2

3. Design & Configuration ---------- 3
   - 3.1 Subnetting for banking network ---------- 3
   - 3.2 Subnetting for routing network ---------- 4
   - 3.3 VPN Tunnel IP Configuration ---------- 5
   - 3.4 BGP Configuration ---------- 5
   - 3.5 VPN Configuration ---------- 8
   - 3.6 Static Routing Configuration---------- 9 Inside Tunnel

4. Topology ---------- 10

5. Results ---------- 12
   - 5.1 Realtime Mode ---------- 12
   - 5.2 Simulation Mode ---------- 13

6. Conclusion& Future Enhancement ---------- 14
   - 6.1 Future Enhancement ---------- 14

ABSTRACT

We are going to implement a Banking VPN Network with BGP Protocol. To achieve this we are going to use Class C IP with 10 Autonomous systems, with 5 systems each. In our project we are making use of the address 192.168.5.0/29 in the banking network and IP address 10.0.0.0/30 in routing networks. We will be using 10 routers, 10 switches, 3 FTP Server and 50 PCs to get the desired result. The router we will be using 2901 Router and switch 296024TT. So using all these conditions we are going to design and implement our project. We have used hybrid topology which consists of star, mesh and ring topology for the implementation of the Banking VPN Network. Also, VPN Network is used between two banks (i.e. Bank 7 and Bank 8) for secure data transmission between them. FTP is also used in the Implementation of Banking Network for the Banks 5, 6 and 7 for the file transfer services.

INTRODUCTION

2.1 BGP Routing

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous system (AS) on the Internet. BGP is classified as a path-vector routing protocol and it makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator.

BGP used for routing within an autonomous system is called Interior Border Gateway Protocol, Internal BGP (iBGP). In contrast, the Internet application of the protocol is called Exterior Border Gateway Protocol, External BGP (eBGP).

2.2 VPN

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, although not an inherent, part of a VPN connection.

2.3 FTP

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.

FTP is built on a client-server model architecture using separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).

DESIGN & CONFIGURATION

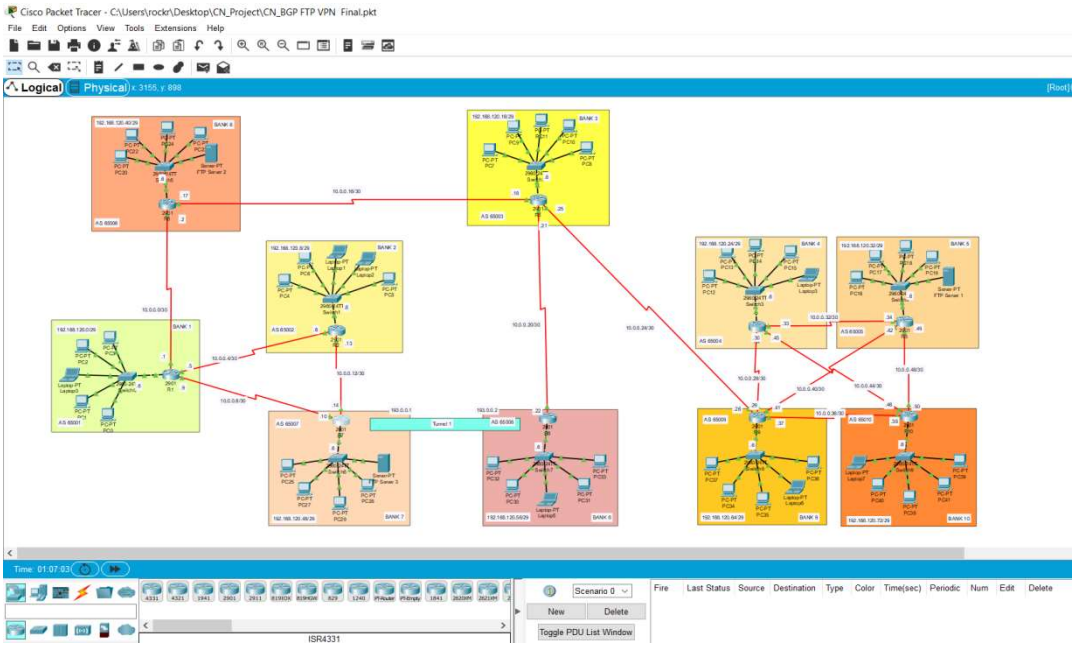

Fig: Topology Design (Hybrid)

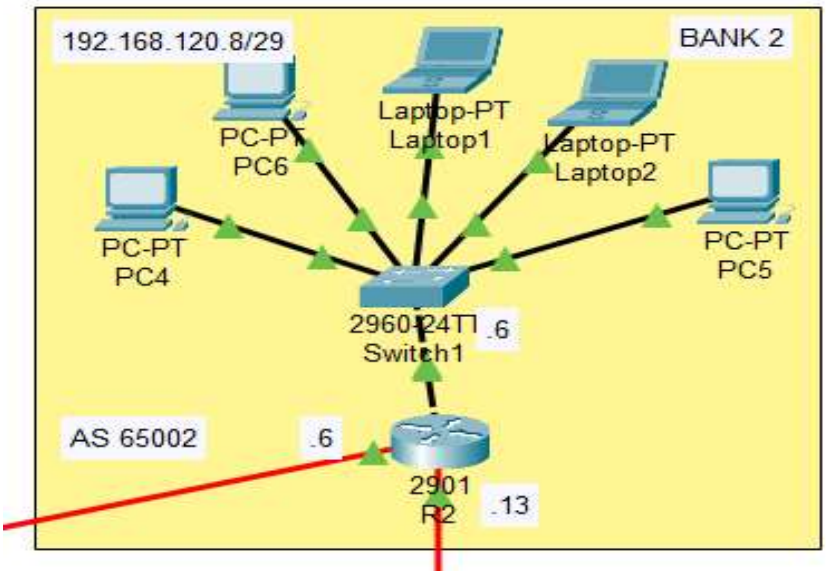

Fig: Single Bank Network

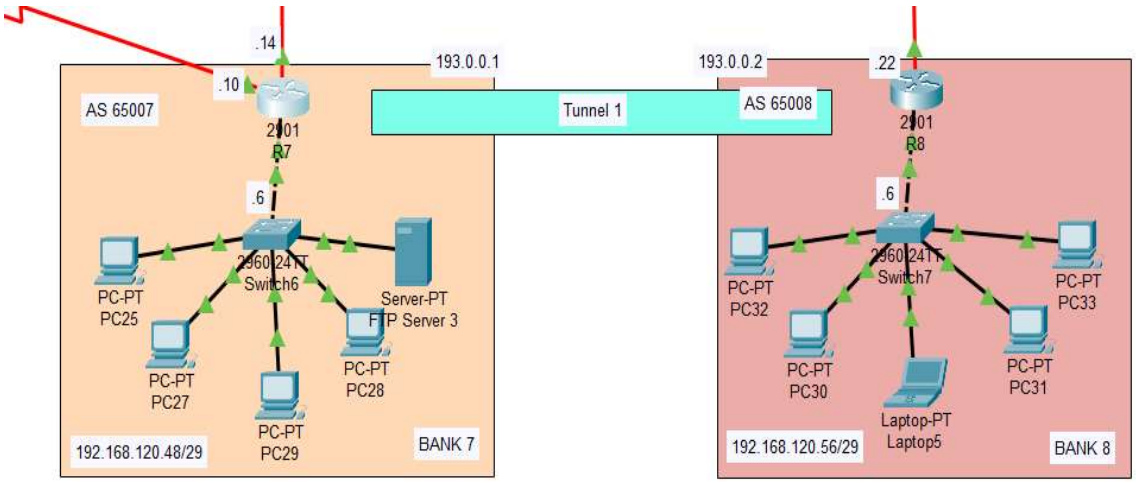

Fig: VPN Tunnel (Between bank 7 and bank 8)

3.1 Subnetting for banking network

IP Address:	192.168.120.0
Total Number of Hosts:	8
Number of Usable Hosts:	6
Subnet Mask:	255.255.255.248
Wildcard Mask:	0.0.0.7
Binary Subnet Mask:	11111111.11111111.11111111.11111000
IP Class:	C
CIDR Notation:	/29
IP Type:	Private
Short:	192.168.120.0 /29

Network Address	Usable Host Range	Broadcast Address
192.168.120.0	192.168.120.1 - 192.168.120.6	192.168.120.7
192.168.120.8	192.168.120.9 - 192.168.120.14	192.168.120.15
192.168.120.16	192.168.120.17 - 192.168.120.22	192.168.120.23
192.168.120.24	192.168.120.25 - 192.168.120.30	192.168.120.31
192.168.120.32	192.168.120.33 - 192.168.120.38	192.168.120.39
192.168.120.40	192.168.120.41 - 192.168.120.46	192.168.120.47
192.168.120.48	192.168.120.49 - 192.168.120.54	192.168.120.55
192.168.120.56	192.168.120.57 - 192.168.120.62	192.168.120.63
192.168.120.64	192.168.120.65 - 192.168.120.70	192.168.120.71
192.168.120.72	192.168.120.73 - 192.168.120.78	192.168.120.79

3.2 Subnetting for routing network

IP Address:	10.0.0.0
Total Number of Hosts:	4
Number of Usable Hosts:	2
Subnet Mask:	255.255.255.252
Wildcard Mask:	0.0.0.3
Binary Subnet Mask:	11111111.11111111.11111111.11111100
IP Class:	C
CIDR Notation:	/30
IP Type:	Private
Short:	10.0.0.0 /30

Network Address	Usable Host Range	Broadcast Address
10.0.0.0	10.0.0.1 - 10.0.0.2	10.0.0.3
10.0.0.4	10.0.0.5 - 10.0.0.6	10.0.0.7
10.0.0.8	10.0.0.9 - 10.0.0.10	10.0.0.11
10.0.0.12	10.0.0.13 - 10.0.0.14	10.0.0.15
10.0.0.16	10.0.0.17 - 10.0.0.18	10.0.0.19
10.0.0.20	10.0.0.21 - 10.0.0.22	10.0.0.23
10.0.0.24	10.0.0.25 - 10.0.0.26	10.0.0.27
10.0.0.28	10.0.0.29 - 10.0.0.30	10.0.0.31
10.0.0.32	10.0.0.33 - 10.0.0.34	10.0.0.35
10.0.0.36	10.0.0.37 - 10.0.0.38	10.0.0.39
10.0.0.40	10.0.0.41 - 10.0.0.42	10.0.0.43

10.0.0.44	10.0.0.45 - 10.0.0.46	10.0.0.47
10.0.0.48	10.0.0.49 - 10.0.0.50	10.0.0.51

3.3 VPN Tunnel IP configuration

Network Address – 193.0.0.0
Subnet mask – 255.0.0.0
Host 1 – 193.0.0.1
Host 2 – 193.0.0.2
IP Class – A

3.4 BGP Configuration

BANK 1 – R1 – AS 65001

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65001
Router(config-router)#network 192.168.120.0 mask
255.255.255.248
Router(config-router)#network 10.0.0.0 mask 255.255.255.252
Router(config-router)#network 10.0.0.4 mask 255.255.255.252
Router(config-router)#network 10.0.0.8 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.2 remote-as 65006
Router(config-router)#neighbor 10.0.0.6 remote-as 65002
Router(config-router)#neighbor 10.0.0.10 remote-as 65007
Router(config-router)#end
```

BANK 2 – R2 – AS 65002

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65002
Router(config-router)#network 192.168.120.8 mask
255.255.255.248
Router(config-router)#network 10.0.0.4 mask 255.255.255.252
Router(config-router)#network 10.0.0.12 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.5 remote-as 65001
Router(config-router)#neighbor 10.0.0.14 remote-as 65007
Router(config-router)#end
```

BANK 3 – R3 – AS 65003

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65003
Router(config-router)#network 192.168.120.16 mask
255.255.255.248
Router(config-router)#network 10.0.0.16 mask 255.255.255.252
Router(config-router)#network 10.0.0.20 mask 255.255.255.252
Router(config-router)#network 10.0.0.24 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.17 remote-as 65006
Router(config-router)#neighbor 10.0.0.22 remote-as 65008
Router(config-router)#neighbor 10.0.0.26 remote-as 65009
Router(config-router)#end
```

BANK 4 – R4 – AS 65004

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65004
Router(config-router)#network 192.168.120.24 mask
255.255.255.248
Router(config-router)#network 10.0.0.28 mask 255.255.255.252
Router(config-router)#network 10.0.0.32 mask 255.255.255.252
Router(config-router)#network 10.0.0.44 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.29 remote-as 65009
Router(config-router)#neighbor 10.0.0.34 remote-as 65005
Router(config-router)#neighbor 10.0.0.46 remote-as 65010
Router(config-router)#end
```

BANK 5 – R5 – AS 65005

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65005
Router(config-router)#network 192.168.120.32 mask
255.255.255.248
Router(config-router)#network 10.0.0.32 mask 255.255.255.252
Router(config-router)#network 10.0.0.40 mask 255.255.255.252
Router(config-router)#network 10.0.0.48 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.33 remote-as 65004
Router(config-router)#neighbor 10.0.0.41 remote-as 65009
Router(config-router)#neighbor 10.0.0.50 remote-as 65010
Router(config-router)#end
```

BANK 6 – R6 – AS 65006

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65006
Router(config-router)#network 192.168.120.40 mask
255.255.255.248
Router(config-router)#network 10.0.0.16 mask 255.255.255.252
Router(config-router)#network 10.0.0.0 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.18 remote-as 65003
Router(config-router)#neighbor 10.0.0.1 remote-as 65001
Router(config-router)#end
```

BANK 7 – R7 – AS 65007

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65007
Router(config-router)#network 192.168.120.48 mask
255.255.255.248
Router(config-router)#network 10.0.0.8 mask 255.255.255.252
Router(config-router)#network 10.0.0.12 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.13 remote-as 65002
Router(config-router)#neighbor 10.0.0.9 remote-as 65001
Router(config-router)#end
```

BANK 8 – R8 – AS 65008

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65008
Router(config-router)#network 192.168.120.56 mask
255.255.255.248
Router(config-router)#network 10.0.0.20 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.21 remote-as 65003
Router(config-router)#end
```

BANK 9 – R9 – AS 65009

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65009
Router(config-router)#network 192.168.120.64 mask
255.255.255.248
```

```
Router(config-router)#network 10.0.0.24 mask 255.255.255.252
Router(config-router)#network 10.0.0.28 mask 255.255.255.252
Router(config-router)#network 10.0.0.36 mask 255.255.255.252
Router(config-router)#network 10.0.0.40 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.25 remote-as 65003
Router(config-router)#neighbor 10.0.0.30 remote-as 65004
Router(config-router)#neighbor 10.0.0.38 remote-as 65010
Router(config-router)#neighbor 10.0.0.42 remote-as 65005
Router(config-router)#end
```

BANK 10 – R10 – AS 65010

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 65010
Router(config-router)#network 192.168.120.72 mask
255.255.255.248
Router(config-router)#network 10.0.0.36 mask 255.255.255.252
Router(config-router)#network 10.0.0.44 mask 255.255.255.252
Router(config-router)#network 10.0.0.48 mask 255.255.255.252
Router(config-router)#neighbor 10.0.0.37 remote-as 65009
Router(config-router)#neighbor 10.0.0.45 remote-as 65004
Router(config-router)#neighbor 10.0.0.49 remote-as 65005
Router(config-router)#end
```

3.5 VPN Configuration

BANK 7 – R7 – AS 65007

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface tunnel 1
Router(config-if)#%LINK-5-CHANGED: Interface Tunnel1, changed
state to up
Router(config-if)#ip address 193.0.0.1 255.0.0.0
Router(config-if)#tunnel source serial 0/1/0
Router(config-if)#tunnel destination 10.0.0.22
Router(config-router)#end
```

BANK 8 – R8 – AS 65008

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface tunnel 1
Router(config-if)#%LINK-5-CHANGED: Interface Tunnel1, changed
state to up
Router(config-if)#ip address 193.0.0.2 255.0.0.0
Router(config-if)#tunnel source serial 0/0/0
Router(config-if)#tunnel destination 10.0.0.14
Router(config-router)#end
```

3.6 Static Routing Configuration Inside Tunnel

BANK 7 – R7 – AS 65007

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.120.56 255.255.255.248
193.0.0.2
Router(config)#end
```

BANK 8 – R8 – AS 65008

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.120.48 255.255.255.248
193.0.0.1
Router(config)#end
```

TOPOLOGY

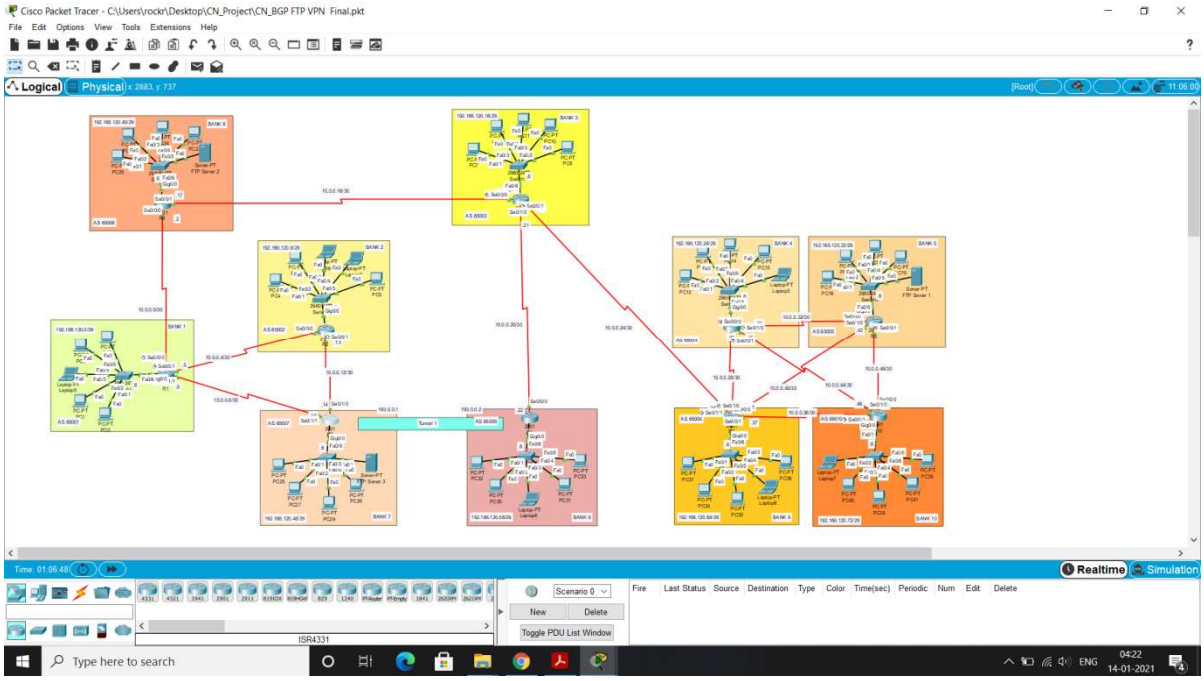

Fig: Topology

In this project, we are using hybrid topology for connection of the different networks. The Hybrid topology consists of star, mesh ring and bus topology. The AS 65001, AS 65002 and AS 65007 are connected in ring topology. AS 65001, AS 65006 and AS 65003 are in bus while AS 65004, AS 65005, AS 65009 and AS 65010 are in mesh topology. The end routers of AS 65008, AS 65009, AS 65006 are connected in star topology with AS 65003. AS 65007 (Bank 7) and AS 65008 (Bank 8) are connected with VPN tunnel.

RESULTS

5.1 Realtime Mode

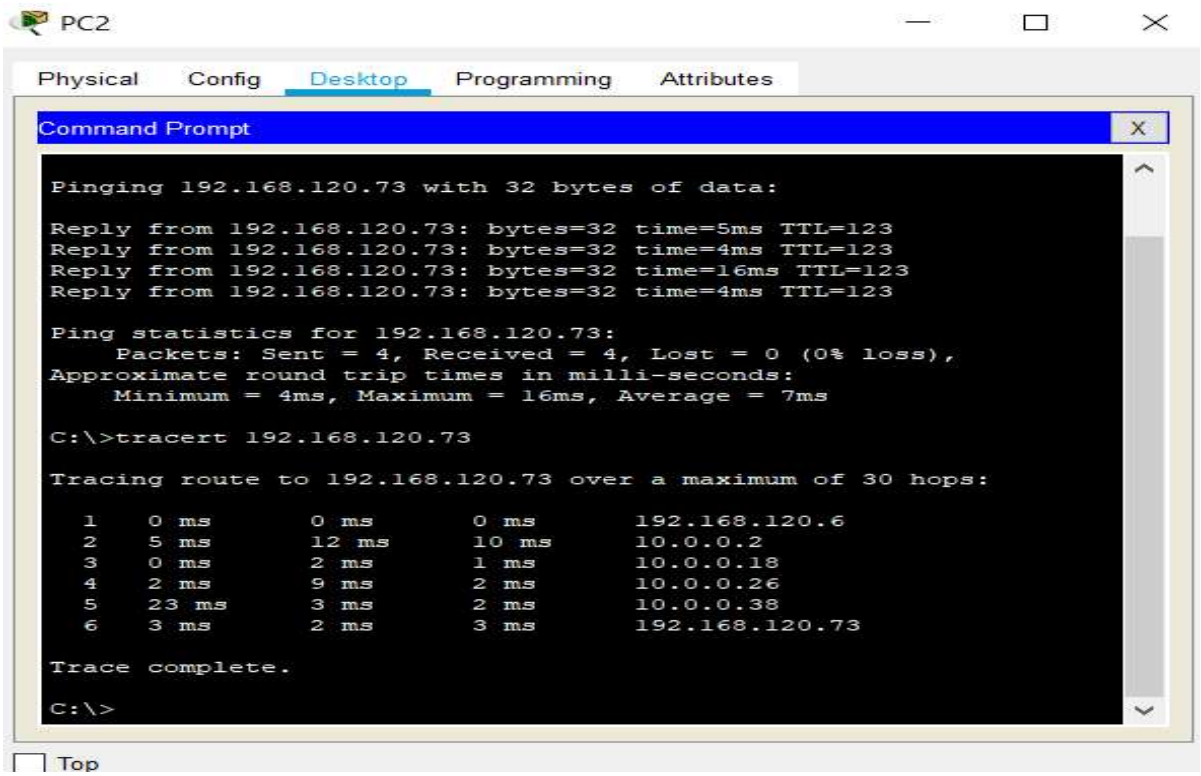

Fig: Ping and Trace from pc of bank 1 to pc of bank 10

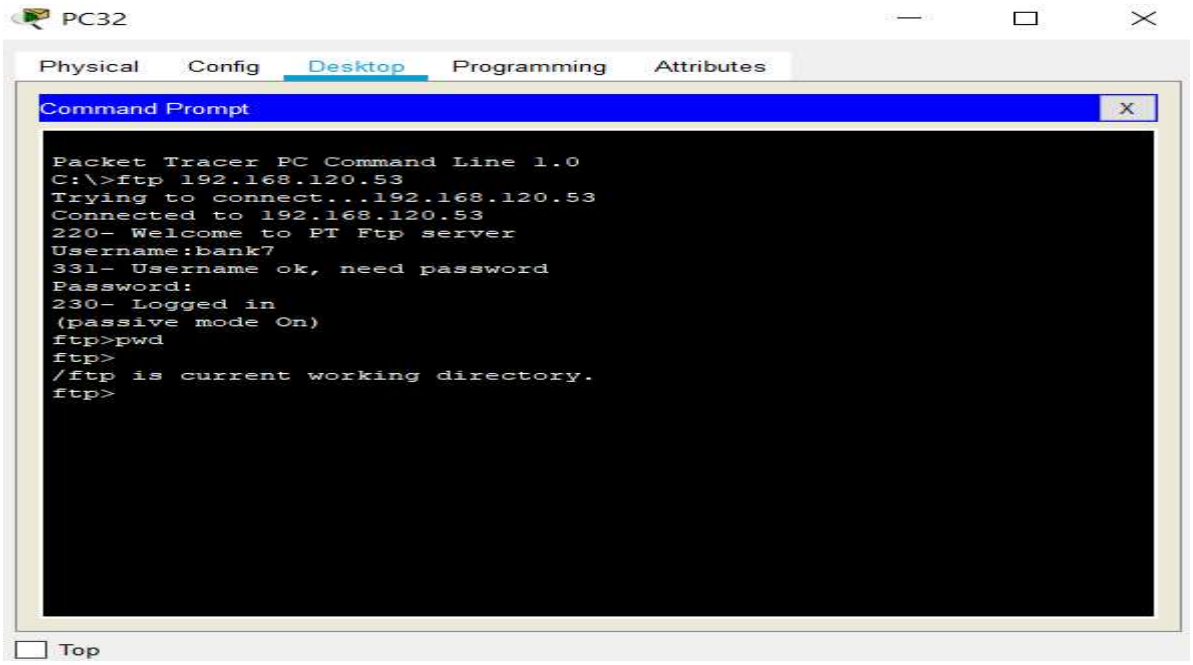

Fig: FTP Server of Bank 7

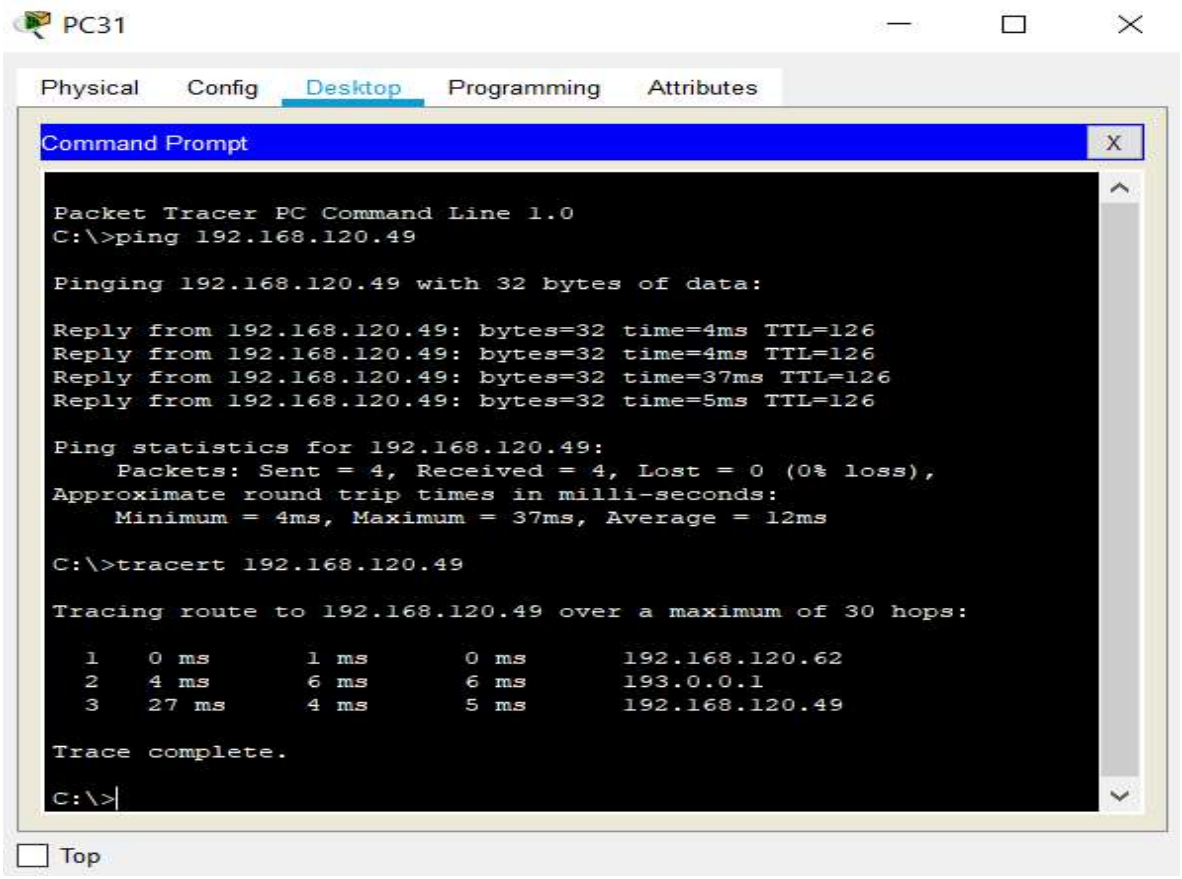

Fig: Ping and trace through VPN Tunnel

5.2 Simulation Mode

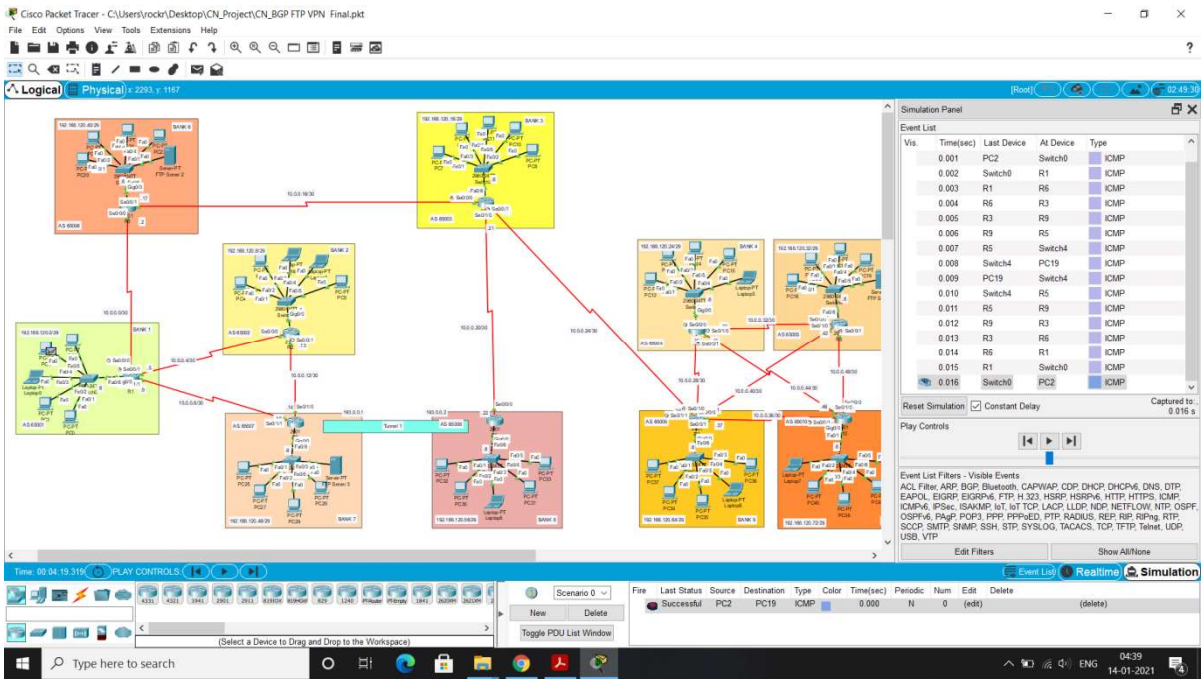

Fig: BGP Simulation Test

CONCLUSION & FUTURE ENHANCMENT

Border Gateway Protocol (**BGP**) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous system (AS) on the Internet. BGP is classified as a path-vector routing protocol and it makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator.

BGP is responsible for looking at all of the available paths that data could travel and picking the best route, which usually means hopping between autonomous systems.

VPNs are frequently used to connect servers and computing clusters to enable better availability and redundancy. It makes the network secures and can be used with many security protocol to maintain confidentiality, integrity and Availablity.

6.1 Future Enhancement

The Project can be further enhanced by using a board VPN network among all banks. For that we can use MPL VPNs. Implementation of servers in all the banks can produce better results. Along with FTP services, DNS, SMTP, NTP etc services can be added to the future versions of this project.