LAN Network With Redundancy

A COURSE PROJECT REPORT

By

NEELA SRIKANTH (RA2011003010650)
PRAHARSH TREHAN (RA2011003010652)
AYUSH SAXENA (RA2011003010653)
K.SAI HEMANTH (RA2011003010654)

Under the guidance of

Mrs.B.Ida Seraphim

In partial fulfilment for the Course

of

18CSC302J - COMPUTER NETWORKS

In Department of Computing Technologies

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND

TECHNOLOGY

Kattankulathur, Chenpalpattu District

NOVEMBER 2022

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this mini project report "LAN with REDUNDANCY " is the bonafide work of-

NEELA SRIKANTH(RA2011003010650)

PRAHARSH TREHAN(RA2011003010652)

AYUSH SAXENA(RA2011003010653)

K.SAI HEMANTH(RA2011003010654)

who carried out the project work under my supervision.

SIGNATURE

Mrs.B.Ida Seraphim
Assistant Professor
Department of
Computing
Technologies
SRM Institute of Science and Technology

ABSTRACT

Now more than ever, today's businesses require reliable network connectivity and access to corporate resources. Connections to and from business units, vendors and SOHO's are all equally important to keep the continuity when needed. Business runs all day, every day and even in off hours. Most companies run operations around the clock, seven days a week so it's important to realize that to keep a solid business continuity strategy, redundancy technologies should be considered and/or implemented.

So, we need to keep things up and available all the time. This is sometimes referred to five nines (99.999) uptime. The small percentage of downtime is accounted for unforeseen incidents, or 'scheduled maintenance' and usually set to take place during times of least impact, like in the middle of the night, or on holiday weekends if planned. If this is not a part of your systems and network architecture it should be considered if you want to keep a high level of availability. Because things break and unforeseen events do take place, we need to evaluate the need for creating an architecture that is 'highly available', or up as much as possible, with failures foreseen ahead of time and the only downtime, is to do planned maintenance.

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 my Course project Faculty **Mrs.B.Ida Seraphim, Assistant Professor , C.Tech** for his/her assistance, timely suggestion and guidance throughout the duration of this course project.

We extend my gratitude to our **HoD, Dr.M.Pushpalatha Head of Department, 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

CHAPTERS **CONTENTS**

CHAPTER-1

INTRODUCTION

1.1 Scenario Description

- We will be making a topology on GNS3 which will be a hub and spoke topology in which all the routing protocols will be implemented and a LAN network will be created.
- We will be creating SSL VPN i.e. the virtual private network on a system which will provide us network and we will be able to access our office computers just by sitting at our home.
- To make it secure communication we will be implementing Cisco ASA i.e. Cisco Adaptive Security Appliances and will be assigning a public IP to it.
- Further we will be implementing Network Address Translation so that server can be NAT on ASA and on routers. Through adaptive security appliances we will apply ACL i.e. Access Control List.
- A Graphical User Interface of ASA firewall will be made to make the connection secure and handle the network more reliably and an easy manner. The topology of network will be Hub and Spoke topology.
- For eg: Hub can be the main headquarter situated in Delhi. Spoke can be different offices in Chennai, Jammu & Kashmir etc.

CHAPTER-2

LITERATURE SURVEY

Sr.no:	Title of Paper	Authors Name	Publication Years And Detail	Advantage
1.	Comparative study of Routing protocols using Cisco Packet Tracer.	C. Dumitrache, G. Predusca, L. Circiumarescu, N. Angelescu.	2017, 5th International Symposium on Electrical and Electronics Engineering (ISEEE)	A New Model of Information Access
2.	Free Internet in the LAN of the Pharaohs	Kamel S and Abdel Ghaffar H	Management Association International Conference, Philadelphia, Pennsylvania, USA, 19-21 May 2003	A Study of a developing nation on a mission to narrow its digital divide
3.	Advanced cs integrated	A. I. Kabir, R. Karim, S.	2009, National Defense	To choose the best

	technology		Industry Press.	integration solution.

CHAPTER-3

REQUIREMENTS

1.2 Requirement Analysis

From the given scenario, we draw the following requirements:

- CISCO Packet Tracer for applying basic commands.
- CISCO Routers.
- CISCO switches.
- GNS 3 for making the final network topologies.
- 2 or 3 Laptops.
- LAN Cable for connectivity.
- Network cables.

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

1.3 Hardware Requirement

From the given scenario, we draw the following requirements:

For Company XYZ (Private Network):

Hardware Required:

Cloud – Primary Cloud

1x Router (For address 10.0.0.1)

4x Switches:

2x Department Specific Switches

1x Master Company Dept. Switch

1x Primary Company Switch

6x End Devices:

3x PCs for Software Department Representation

3x PCs for IT Department Representation

For Public Network:

Hardware Required:

1x Switch(Broadband Switch)

3x End Devices(Public Network PCs)

For Network Integration(Private with Public):

Hardware Required:

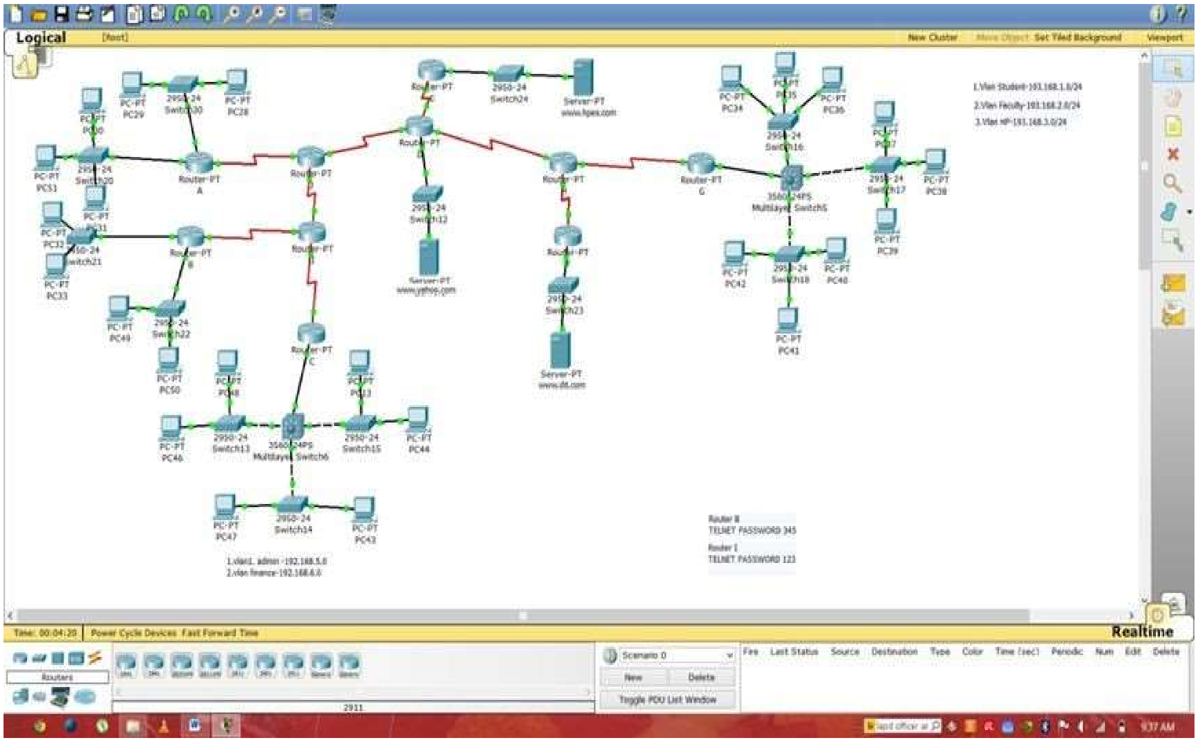
1x Router (Internet Service router say ‘Airtel’)

CHAPTER-4

ARCHITECTURE AND DESIGN

1.4 Network Architecture

The network architecture is as follows:



1.Vlan Student-193.168.1.0/24
2.Vlan Faculty-193.168.2.0/24
3.Vlan HP-193.168.3.0/24

1.vlan1. admin -192.168.5.0
2.vlan finance-192.168.6.0

Router B
TELNET PASSWORD 345

Router I
TELNET PASSWORD 123

The architecture consists of three major networks:

- Company Network(s)
- Public Internet
- Network maintained by the Internet Service Provider

These networks are interconnected with each other with varying degrees (discussed in the implementation chapter).

CHAPTER-5

IMPLEMENTATION

1.5 Address Table

The address table is as follows:

Device	Interface	Address
Switch	FA 0/1	192.168.1.10/24
	FA 0/1	192.168.1.11/24
	FA 0/1	192.168.1.12/24
PC	VLAN 10	192.168.10.50/24
	VLAN 20	192.168.20.20/24
	FA 0/0	192.168.20.1/24
Routers	SE 1/0	192.168.1.1/24
	FA 0/0	192.168.1.2/24
	FA 0/1	192.168.10.1/24
	GIG 0/0	192.168.10.2/24
Modem	FA 0/1	192.168.20.2/24
Cloud	ETH 6	192.168.20.3/24

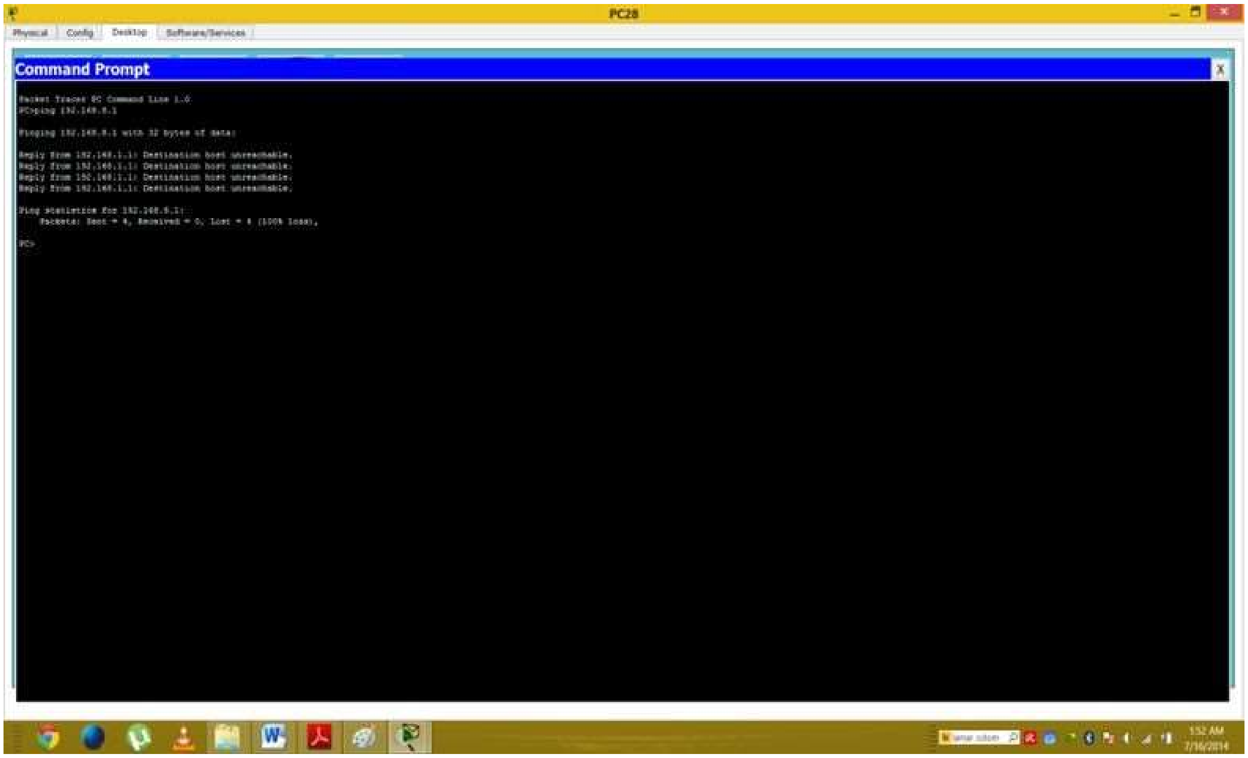
- Study different types of routing protocols.
- Study in detail about firewalls.
- Start making the topology on GNS3.
- Study about virtual private network (VPN).
- Start setting up VPN on the system.
- Study Adaptive Security Appliance.
- Study NAT and Implement it on ASA and on router.
- Apply Access control list through ASA.
- Study MPLs routing and different types of protocols that comes under it.

CHAPTER-6

RESULTS AND DISCUSSION

1.6 Connection Check

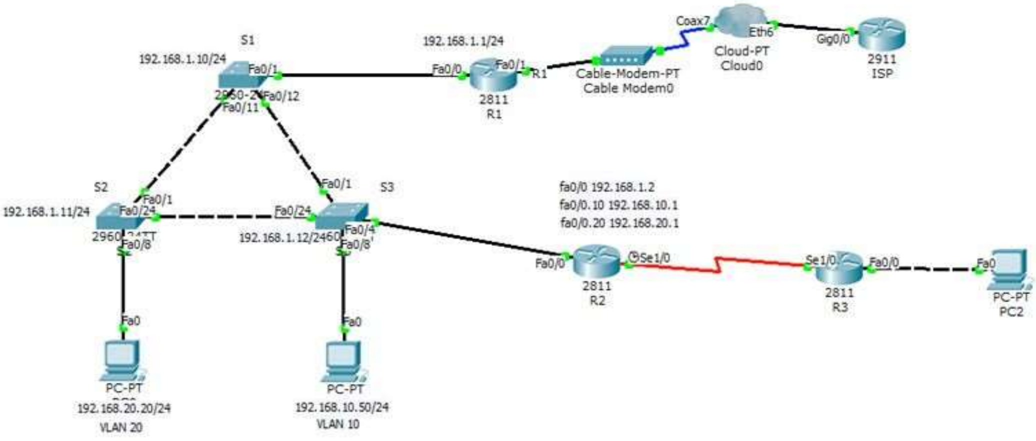
The network connections were checked by ping requests:



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.8.1

Pinging 192.168.8.1 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

VPN (Virtual Private Network):

- A VPN is a type of a secured network that allows the provisioning of private network services for an organization over the unsecured network using tunneling protocols.
- VPN is provisioned using technologies such as Frame Relay and Asynchronous Transfer Mode virtual circuits for long time
- However over the past few years IP and MPLS based VPN's have been a part of innovations.



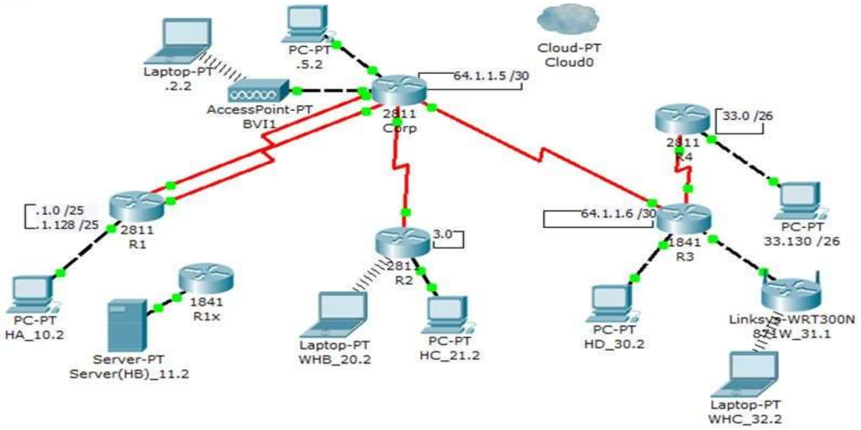
NAT(Network Address Translation):

- NAT is an Internet standard that enables a local-area network (LAN) to use two set of IP address.
- NAT serves three main purposes:

1. Provides a type of firewall by hiding internal IP addresses in the network.

2. To use more internal IP addresses.

3. Allows to combine multiple ISDN (Internet Switched Digital Network) connections into a single Internet connection



Configuring Static NAT

```
[“Router (config )# int e 0/0 Router (config-if)# ipnat inside Router (config)# int s0/0
Router(config-if)# ipnat outside
Router(Config)# ipnat inside source static 172.16.1.51 158.80.1.45
```

Configuring Dynamic NAT

```
[“Router (config )# int e 0/0 Router (config-if)# ipnat inside
Router (config)# int s0/0
Router(config-if)# ipnat outside
Router(Config)# ipnat pool SRM ip address ip address netmask”]
```

Port Address Translation:

```
Router(config)# interface fastethernet 0/0 Router(config-if)# ip nat inside
Router(config)#interface serial 0/0/0 Router(config-if)# ip nat outside
Router(config)# ip nat inside source list 10 interface serial 0/0/0 overload Router(config)#
access-list 10 permit ip add. Subnet mask
```

Routing Commands:

```
[“Router> Enable
Router# Configure terminal Router(config) # int fa (0/0, 1/0)
Route (config-if)# ip address (ip address) (subnet mask) Router(config-if)# no shutdown
Router(config-if)#exit Router(config)#int serial 2/0
Router(config-if)# ip address (ip address) (subnet mask)
Router(config-if)# no shutdown Router(config-if)# exit Router(config)#int serial 3/0
Router(config-if)# ip address (ip address) (subnet mask) Router(config-if)# no shutdown
Router(config-if)# exit”]
```

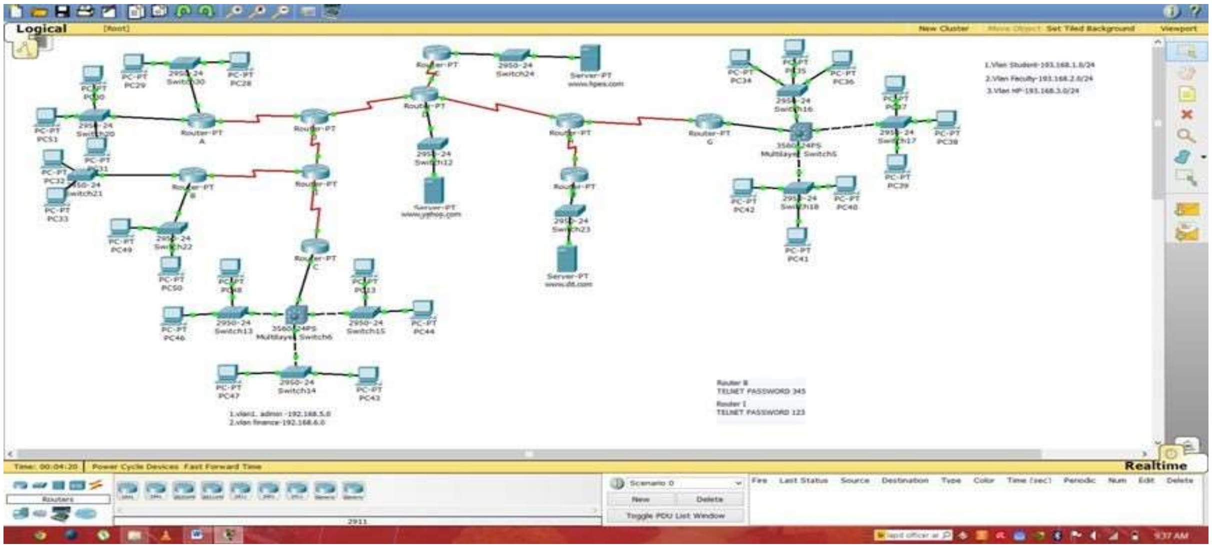
RIP V2 Routing:

```
[“Router(config)# router rip Router(config)# version 2
Router(config-router)# (Connected Network1 address)
Router(config-router)# (connected Network2 address)”]
```

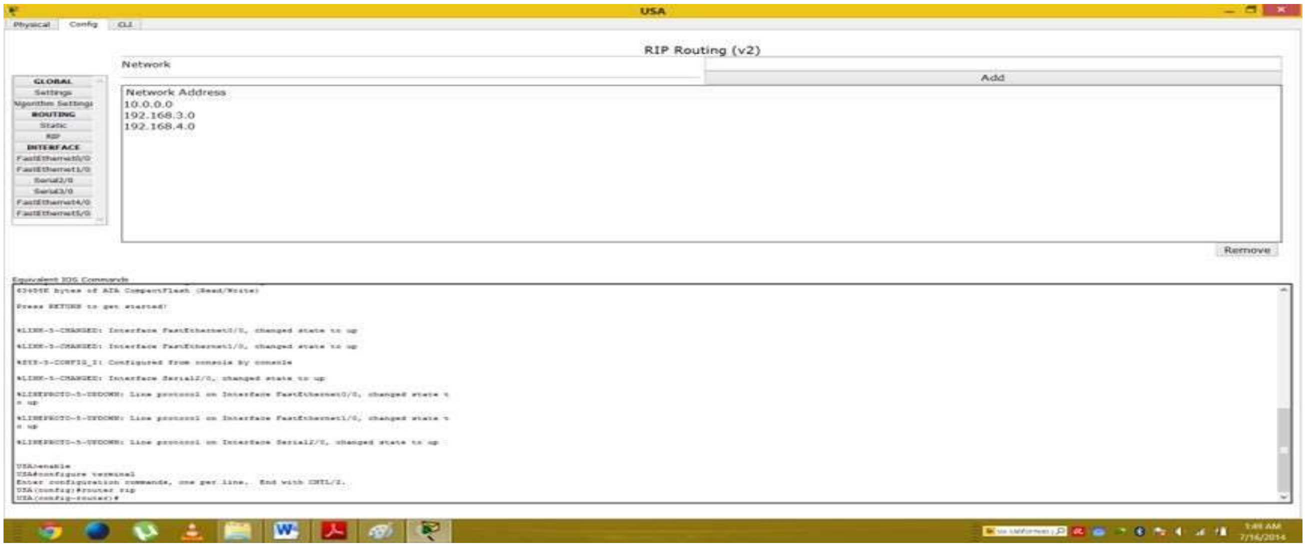
EXPERIMENT RESULT AND ANALYSIS

As we have completed a minor part during these months of our project, the following results has been reflected:

1. **Basic Routing Successful**



2. **RIP Routing Successful**



RIP Routing (v2)

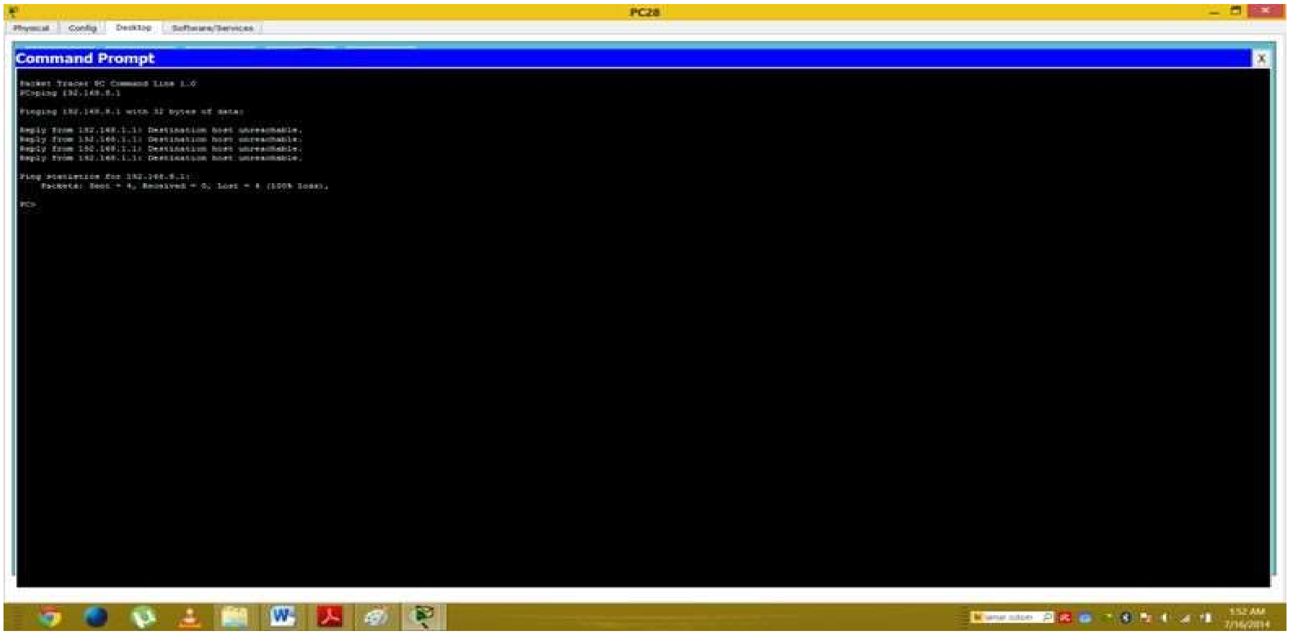
Network

Network Address
10.0.0.0
192.168.3.0
192.168.4.0

Equivalent IOS Commands

```
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%SYS-5-CONFIG_I: Configured from console by console

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state t
o up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up


USA>enable
USA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
USA(config)#router rip
USA(config-router)#
```

3. Configuring Access List Successful



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.8.1

Pinging 192.168.8.1 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

CHAPTER-7

CONCLUSION AND FUTURE ENHANCEMENT

- To conclude we would like to say that we have successfully completed the basic and soul purpose of our project which is to create a Redundant LAN Network which Offers fault tolerance and efficient load balancing across its internal network.
- The Basic Fundamentals and aims we think we have successfully achieved and implemented but as nothing can be perfect so as my project, it needs better implications in future.
- According to us we have completed our project still we are left with lots of improvements and enhancements of this projected structure. We will try my level best to complete it in our near future.

- We will apply all our described networking topologies and protocols in GNS 3 software to make an efficient redundant LAN Network.Going through all the steps it is very easy to configure the whole network in our near future.
- Two or more laptops will be required to show to network connection and to verify it as it is working or not in a proper way.
- To increase the redundancy quotent Cisco Adaptive Appliance Security we will apply which will work as a security measurement interface in the network. By using firewalls we will be implementing security in the network.
- Before setting up the network planning is done in which redundancy is made so we will be providing redundancy in the network so if there is any failure the traffic is routed through different path.

- We will be implementing how a user or client can access the resources of office sitting at home which is great advantage according to user point of view.

CHAPTER-8
REFERENCES

- CISCO Packet Tracer Module (v 6.0.1)
- https://www.ge.com/digital/documentation/ifix/version60/Subsystems/redund/content/enf_whatis_lan_redundancy.html
- Packet guide for Routing and switching
- https://www.auvik.com/franklyit/blog/simple-network-redundancy/
- https://www.oreilly.com/library/view/switched-networks-companion/9780133476446/ch04.html