

BUILDING RESILIENT CARRIER GRADE WAN NETWORK FOR CORPORATE

Submitted in partial fulfilment of the requirements for the award of
Bachelor of engineering degree in Computer Science and Engineering

By

THOTA CHAITHANYA (17SCS0467)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

www.sathyabama.ac.in

MARCH 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with "A" Grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai - 600 119.

Phone: 044 - 2450 3150 / 51 / 52 / 54 / 55 Fax: 044 - 2450 2344

www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **THOTA CHAITHANYA (17SCS0467)** who carried out the project entitled "**BUILDING RESILIENT CARRIER GRADE WAN NETWORK FOR CORPORATE**" under my supervision from January 2020 to March 2021.

INTERNAL GUIDE

DR. M.SELVI, M.E, Ph.D.,

HEAD OF THE DEPARTMENT

**Dr. VIGNESHWARI.,M.E.,Ph.D.,
Dr. L. Lakshmanan., M.E., Ph.D**

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **THOTA CHAITHANYA (17SCS0467)** hereby declare that the Project Report entitled “**BUILDING RESILIENT CARRIER GRADE WAN NETWORK FOR CORPORATE**” done by me under the guidance of **Dr. M.SELVI, M.E, Ph.D.**, is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering Degree in Computer Science and Engineering.

DATE :

PLACE :

SIGNATURE OF CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge our sincere thanks to Board of management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr.T.Sasikala,M.E.,Ph.D., Dean, School of computing,** **Dr.L.Lakshmanan,M.E.,Ph.D** and **Dr.S.Vighneshwari,M.E.,Ph.D., Heads of the Department, Department of Computer Science and Engineering** for providing us the necessary support and details at the right time during the progressive reviews.

I would like to express our sincere and deep sense of gratitude to our Project Guide **Dr.M.SELVI,M.E.,Ph.D.,** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express our thanks to all Teaching and Non-teaching staff members of the Department of **COMPUTER SCIENCE AND ENGINEERING** who were helpful in many ways for the completion of the project.

ABSTRACT

In this paper a corporate WAN infrastructure constituting of routers and switches has been proposed to make the network reliable. The topology based on the hierarchy of network is designed and each layer of is configured using techniques like layer 2 link aggregation control protocol, layer 3 redundancy and MPLSTE. A carrier grade network refers to a software or hardware system that is dependable and well tested. This is used to meet high availability. A fault-tolerant and fast fail over corporate network which is capable of processing huge amount of traffic has been analysed. The scalable network which will be capable to handle and process high amount of traffic has been built. The link level and the node level failure are averted in the designed network and above 96 percentage of the availability has been achieved.

TABLES OF CONTENTS

Chapter No.	TITLE	Page No.
	ABSTRACT	v
	LIST OF TABLES	viii
	LIST OF FIGURES	viv
1	INTRODUCTION	1
2	LITERATURE SURVEY	3
	2.1 REVIEW OF LITERATURE SURVEY	3
3	AIM AND SCOPE	7
	3.1 EXISTING SYSTEM	7
	3.1.1 Transport or link level resiliency	8
	3.1.2 Protocol level resiliency	9
	3.2 PROPOSED SYSTEM	12
	3.2.1 Advantages of Proposed System	14
4	MATERIALS AND METHODS	15
	4.1 SOFTWARE REQUIREMENTS	15
	4.1.1 GNS3	15
	4.1.2 Wireshark	15
	4.2 MULTI-PROTOCOL LABEL SWITCHING	15
	4.3 LABEL DISTRIBUTION PROTOCOL	16
	4.4 TRAFFIC ENGINEERING	19
	4.5 SPANNING TREE PROTOCOL	19

4.6	ROOT BRIDGE	20
4.7	LINK AGGREGATION CONTROL PROTOCOL	20
4.8	HOT STAND-BY ROUTING PROTOCOL	22
4.9	CALCULATION OF AVAILABILITY	23
5	RESULTS AND DISCUSSIONS	35
5.1	RESULTS	35
5.1.1	Results for LACP	35
5.1.2	Results for HSRP	36
6	SUMMARY AND CONCLUSION	39
6.1	APPLICATION	39
6.2	CONCLUSION	39
6.3	FUTURE WORK	39
	REFERENCES	40

LIST OF TABLES

TABLE NO.	TABLE NAME	PAGE NO.
3.1	STP cost based on bandwidth	8

LIST OF FIGURES

FIGURE No.	FIGURE NAME	PAGE No.
3.1	Basic issues	7
3.2	HSRP design	10
3.3	MPLS topology	11
3.4	Block Schematic	12
3.5	Network Architecture	13
3.6	Multi-Layer Network	14
4.1	MPLS configuration in designed network	16
4.2	When one way of the gateways fails	16
4.3	ping tracer report	18
4.4	Uptime and downtime	18
4.5	When an MPLS link fails	19
4.6	LACP configuration in the network	20
4.7	Ping tracer report	21
4.8	Uptime and downtime	22
4.9	HSRP configuration in the network	22
4.10	Pc1 configuration	23
4.11	Pc2 configuration	24
4.12	Pc3 configuration	24

4.13	Router R1 configuration of tunnels	25
4.14	Router R1 OSPF configuration	26
4.15	Router R1 interfaces	27
4.16	Router R2 interfaces	27
4.17	Router R2 MPLS configuration	28
4.18	Router R3 configuration	29
4.19	Router R3 interfaces	29
4.20	Router R4 configuration	30
4.21	Router R4 interfaces	30
4.22	Router R4 OSPF configuration	31
4.23	Router R5 interfaces	31
4.24	Router R5 configuration	32
4.25	Router R6 interfaces	32
4.26	Router R6 configuration	33
4.27	Switch1 interface	34
4.28	Switch2 interface	34
5.1	Node failure for node R7 to R6	35
5.2	Connectivity Re-established	35
5.3	Data transfer through configured Backup path	36
5.4	Link failure from R5 to R1	36
5.5	Connection Re-established	37

5.6	Data transfer through configured backup link	37
5.7	Primary connection Re-established	37

CHAPTER 1

INTRODUCTION

The society is more dependent on the communication network because most of the infrastructure like banking, telecom services is very much dependent on communication. This dependency has led to concentrate the high availability, reliability and resilient. Whenever the network is unable to transfer the data such situation is referred to a network failure. The failure can be viewed as utterance of an activity or service due to congestion.

These failures include link failures, node failures, software failures, natural disaster, human errors and physical attacks. This dependency of society on communication makes us realize how important to make a network resilient. To avoid failure in network the network has to be designed in such a way that the network is fault-tolerant and fast failover introducing optimum redundancies at appropriate multiple levels on hardware (physical media, networking elements) and software (services and protocols) to claim having 100percent up time. If a network fails, the proposed network is durable enough to with stand reacting to faults. Whenever there is a failure in the links, nodes and other elements the network has to recover.

For the network to improve redundancy and high availability some techniques have been used. This technique is classified into – 1 Network design 2 Basic issues 3 Transport or link level resiliency 4 Protocol level resiliency. These techniques mainly concentrate on the traffic management and the failure that may occur in the link level and protocol level. The traffic management obtain to transfer the load in network such that a failure has less impact when the connection effected by the failure. For the purpose of traffic management in MPLS network we have to use LACP backup path. The goal is to make a

network to be highly available to the end users by providing continues service and to control the congestion. This can be achieved by designing network that has strong enough to failure in function of nodes & links and configuring protocol that

are fault tolerant. When we make a network the most important factor, we must investigate is cost. We must see that the cost is always minimum.

If we consider satellite application the availability of network should be always high because we may face many several difficulties because of temperature, radiation etc. These systems are designed to decrease the down time and increase the availability.

One can think that reaching high availability by using redundancy techniques is easy. In this paper the second section discuss about the network design and the third section discuss about the issues one may face in a network. Finally, the last section sums up the paper.

CHAPTER 2

LITERATURE SURVEY

2.1 REVIEW OF LITERATURE SURVEY

[1] “APPLICATION LAYER ANY CASTING” S. Bhattacharjee et al In this paper it has been fully discussed about the any casting in the application layer. Since every layer has to be concentrated in the network, the focus is mainly on the application layer. To improve the service availability, focusing on the layers is very much important, so one layer is concentrated and that is application layer. Techniques based on the routing may be used to reduce the impact of failures in the network that might decrease the service availability. Installing highly available servers create problems due to link failures. A particular user may not be able to find a particular server focusing only one layer is not enough because we have six other layers.

[2] “Wide Area Network Ecology” Jon T. Meek et al During the past year AHP started to switch its leased line-based WAN to managed Frame Relay networks. Most of the previous WAN usage was for bulk file transfer, database synchronization, light interactive TTY sessions, and some http traffic. The program for performing connectivity checks and routine RTT measurements is part of the mon distribution. The programs to measure RTT as a function of packet size and to read tcp dump output may be made available in the future. Readers are directed to MRTG [Oet98] for a system that produces Web based reports on router traffic and other parameters. We have found that Internet traffic often consumes a very large portion of the available WAN bandwidth. While there is controversy over the use of Internet usage logs due to privacy and related issues, we have found them to be a very useful tool for managing bandwidth.

[3] “Resilient overlay networks” D. Andersen et al This paper makes the case for Resilient Overlay Networks (RONs), an application-level routing and packet forwarding service that gives end-hosts and applications the ability to take advantage of network paths that traditional Internet routing cannot make use of, thereby improving their end-to-end reliability and performance.

Using RON, nodes participating in a distributed Internet application configure themselves into an overlay network and cooperatively forward packets for each other. Each RON node monitors the quality of the links in the underlying Internet and propagates this information to the other nodes; this enables a RON to detect and react to path failures within several seconds rather than several minutes, and allows it to select application-specific paths based on performance. We argue that RON has the potential to substantially improve the resilience of distributed Internet applications to path outages and sustained overload.

[4] “Internet Content Adaptation Protocol (ICAP) DS-2326” Network Appliance, Sunnyvale, CA, In this paper it has been fully discussed that brief introduction to ICAP, explains what ICAP means to the future of Internet content handling, and discusses how NetCache is ideally suited to handle these ICAP enabled value-added services. The following section introduces ICAP, shows why it is needed, and how it can be leveraged to standardize and modularize Internet content manipulation (content vectoring). ICAP in its most basic form is a "lightweight" HTTP based remote procedure call protocol. In other words, ICAP allows its clients to pass HTTP based (HTML) messages (Content) to ICAP servers for adaptation. Adaptation refers to performing the particular value added service (content manipulation) for the associated client request/response.

[5] “Resource management for scalable disconnected access to Web services” B. Chandra et al Disconnected operation, in which a client accesses a service without relying on network connectivity, is crucial for improving availability, supporting mobility, and providing responsive performance. Because many web services are not cachable, disconnected access to web services may require mobile service code to execute in client caches. Unfortunately, (a) this code is untrusted, (b) this code may have nearly limitless resource demands due to prefetching, and (c) a large number of competing code modules must coexist. Thus, resource management is a key problem both for preventing denial of service attacks and for providing good performance across many services. This paper addresses the feasibility of meeting the resource management needs of an environment where service code is shipped to clients, proxies, or content distribution intermediaries.

It first examines the requirements of such a system and then develops a resource-management strategy to meet these requirements by (a) providing isolation across services to prevent denial of service attacks, (b) automatically providing appropriate allocations to different services to provide good global performance, and (c) requiring no hand tuning across a wide range of system configurations and workloads.

[6] “Spare capacity allocation in two-layer networks” D. Vajanapoom et al In this paper we consider the problem of provisioning spare capacity in two-layer backbone networks using shared backup path protection. First, two spare capacity allocation (SCA) optimization problems are formulated as integer linear programming (ILP) models for the cases of protection at the top layer against failures at the bottom layer. The first model captures failure propagation using overlay information between two layers for backup paths to meet diversity requirements. The second model improves bandwidth efficiency by moving spare capacity sharing from the top layer to the bottom layer. This exposes a tradeoff between bandwidth efficiency and extra cross-layer operation. Next, the SCA model for common pool protection is developed to allow spare capacity sharing between two layers. Our previous SCA heuristic technique, successive survivable routing (SSR) is extended for these optimization problems. Numerical results for a variety of networks indicate that the common pool protection is attractive to enhance bandwidth efficiency without loss of survivability and that the SSR heuristic quickly results in near optimal solutions.

[7] “Availability models for underlay aware overlay networks” Madhu Kumar et al In this paper it is discussed that Event broker networks are P2P overlays constructed out of a few select nodes of the underlying physical network (aka underlay). Reliable event delivery on such networks requires the overlay to be highly available. While high availability is usually achieved by redundant paths between the rendezvous node and the subscriber, redundancy at the overlay level alone is insufficient to guarantee availability - redundant paths in the overlay have to correspond to node disjoint paths in the underlay network for true availability. In this paper, we propose two models of availability. In the Manifest Availability model, distinct paths at the overlay level are node disjoint at the underlay as well - this is a strong availability condition.

We can weaken this to the Latent Availability model where it is only guaranteed that any two overlay nodes have a guaranteed number of node disjoint paths between them in the underlay. We analyze both the models for complexity of formation and maintenance, and prove that in the general case, both are NP-complete. We then identify a set of practical constraints applicable to large scale networks. We demonstrate that under these constraints, constructing latent availability overlays reduces to a polynomial time problem. We also introduce the concept of reduced underlays, and further reduce the complexity of the problem of determining latent availability overlays.

[8] “Resilient overlay networks”, Andersen et al In this paper it is discussed that a Resilient Overlay Network (RON) is an architecture that allows distributed Internet applications to detect and recover from path outages and periods of degraded performance within several seconds, improving over today’s wide-area routing protocols that take at least several minutes to recover. A RON is an application-layer overlay on top of the existing Internet routing substrate. The RON nodes monitor the functioning and quality of the Internet paths among themselves, and use this information to decide whether to route packets directly over the Internet or by way of other RON nodes, optimizing application-specific routing metrics. Results from two sets of measurements of a working RON deployed at sites scattered across the Internet demonstrate the benefits of our architecture. For instance, over a 64-hour sampling period in March 2001 across a twelve-node RON, there were 32 significant outages, each lasting over thirty minutes, over the 132 measured paths. RON’s routing mechanism was able to detect, recover, and route around all of them, in less than twenty seconds on average, showing that its methods for fault detection and recovery work well at discovering alternate paths in the Internet. Furthermore, RON was able to improve the loss rate, latency, or throughput perceived by data transfers; for example, about 5% of the transfers doubled their TCP throughput and 5% of our transfers saw their loss probability reduced by 0.05. We found that forwarding packets via at most one intermediate RON node is sufficient to overcome faults and improve performance in most cases. These improvements, particularly in the area of fault detection and recovery, demonstrate the benefits of moving some of the control over routing into the hands of end-systems.

CHAPTER 3

AIM AND SCOPE

3.1 EXISTING SYSTEM

The basic issues in the existing system and the solution has been discussed. The major factor that changes amount of the redundancy fault tolerant mechanism is the cost. Because of the cost networking has become a business. So, the network availability has become intense. The cost limitation makes difference in network resilience to limit the redundancy that one can afford to infrastructure. The cost limits the network connectivity.

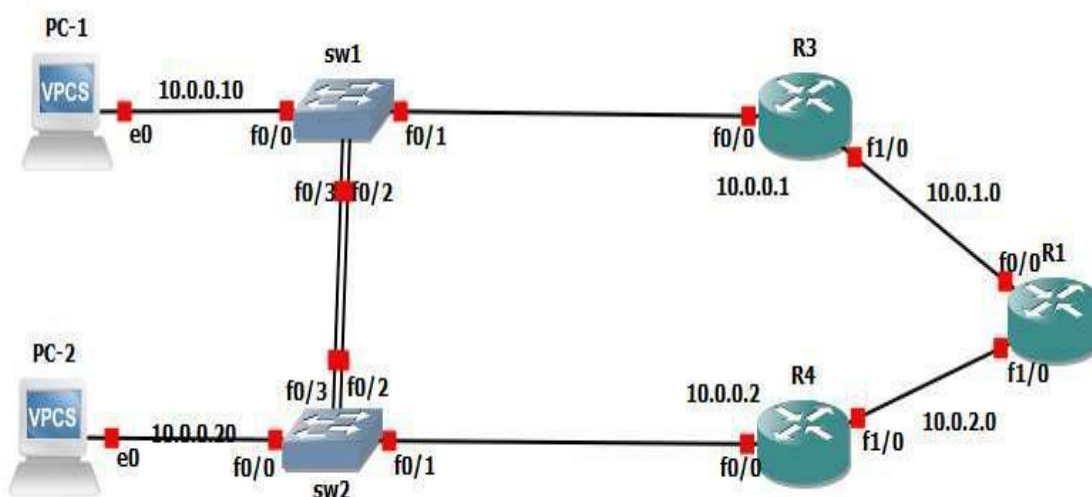


Fig 3.1: Basic issues

When the network topology is designed each layer is to be concentrated such that there should be no chance in network fail. In this paper we mainly concentrate on the first three layers. In the first layer the main thing we must concentrate is the cables and the power supply. In the data link layer, we concentrate more on the link and the node. In the network layer we concentrate more on protocols. We use the concepts of HSRP, LACP, SPANNING TREE PROTOCOL, MPLS TRAFFIC ENGINEERING.

3.1.1 Transport or link level resiliency

For the link level resiliency, the techniques used are LACP (link aggregation control protocol). In the link level to avoid the failure LACP is configured. Two manageable switches when connected using a single link may lead to loss of data packets whenever there is a failure in the link. So, we configure these manageable switches with two links. So that whenever there is a one link fails the second link can be automatically turn on. In this way we can avoid link failure. LACP packets are exchanged in two modes. There is active mode which makes the port to act in active state and passive which makes the port to act in passive state. LACP system priority is to configure on each router. The priority can be configured automatically or through CLI. LACP port priority is configured on each port using CLI or automatically. Each and every port that is added to channel port must be configured identically. This LACP help in dividing traffic between network interfaces.

Table 3.1: STP Cost Based on Band Width

Data rate	STP Cost
4 Mbits/s	250
10 Mbits/s	100
16 Mbits/s	62
100 Mbits/s	19
1 Gbits/s	4
2 Gbits/s	3
10 Gbits/s	2
100 Gbits/s	Nil
1 Tbits/s	Nil

Whenever two links are used between two manageable switches looping may occur which may also lead to loss of data. So, another solution is to use STP. It is a protocol which makes topology logical with a connection that is free of loops. The main function of STP is to stop bridge loops and to include backup links to provide fault tolerant. A STP creates the spanning tree. It allows only a single active path between two nodes. In LAN the networks are inter connected using links that are redundant to improve resilience. This connection creates loop resulting instability. Whenever the redundant links are used then the loops are needed to be avoided. The STP decides one layer-2 switch as specified bridge. In this route bridge the active and inactive links are calculated. This route bridge continuously communicates with another switch using BPDUs. This route bridge calculates the cost of each path based on bandwidth it will select the path with less cost that means the bandwidth is high. The STP turns on the active link as the only the way transfers the frames between tow switches and disable the all other links. The STP elects the route bridge and all non-route bridges assign one of the ports as route port. The route port is either connects the switches to the route bridge or if there are several parts, the port with referred paths calculated by route bridge. Each switch gets cost from neighboring switches and adds the cost of its own path.

3.1.2 Protocol level resiliency

In the layer-3 to provide redundancy layer 3 redundancy protocols are used. They are three types of layer-3 redundancy protocols. In this paper HSRP is configured to improve un interrupted gateway. This HSRP connection between two gateways is established in order to achieve gateway failure. Whenever the primary gateway is un reachable the secondary gateway comes into action. This HSRP provides high availability by providing redundancy for traffic. In a group there are two routers the active and the standby. Then the active router route packets whereas standby is the router that takes the responsibility whenever the active router fails. In case group-1 router R1 acts as an active router based on the priority and router R2 acts as standby router for which the priority maybe low. The default priority for a router in HSRP is 100 and router with high priority acts as active router.

In group-2 router R1 acts as standby router and router R2 acts as active router. Consider two users in which one of the user's gateway is per say 10.0.0.3 which is the virtual IP of group-1. The second user has a gateway per say 10.0.0.4 which is a virtual IP of group-2, whenever the user tries to reach the destination and suppose if the gateway fails, immediately the other router takes responsibility and the packet immediately switch to the standby router. Whenever the first user tries to reach the destination using group-1 virtual IP as gateways and whenever the gateway fails immediately the standby router takes the responsibility and then transfer the data packets with the loss of only 4 packets. This technique helps to increase the uptime and reduce the downtime and the packet loss is limited to four packets. The use of HSRP makes the network to be self-healing and fault tolerant. Therefore, HSRP makes the network to be highly available with more than 90 percentage availability. To calculate the availability percentage, the uptime and the down time is to be calculated. The uptime refers to the time for how much the service is available and the down time refers to the time for which the service is unavailable. The availability is uptime to the total time. The total time is the sum of uptime and downtime.

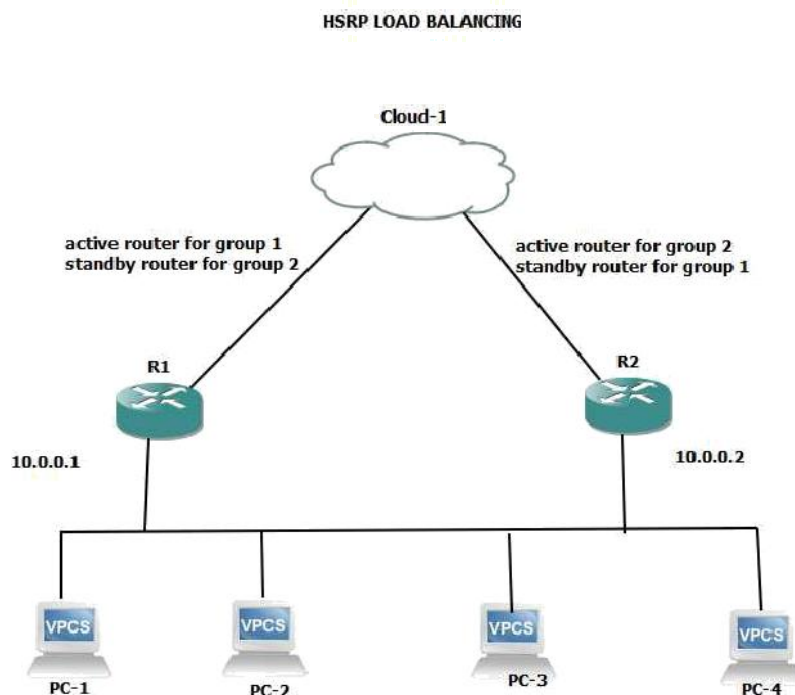


Fig 3.2: HSRP Design

Multiprotocol Label switching (MPLS) is a technique that is designed for speeding up and shapes the traffic flows in the WAN networks and then service provider networks also. It transfers the data from one node to other depending on short path labels. At first, we will add the label whenever the packet goes to the MPLS network. Based on the label the routers will forward the packets with the help of push operation. With the help of pop up action the label is removed whenever the packet goes outside the MPLS network. The very first router sitting at the edge of the MPLS network is called Provider Edge router (PE). Then the router sitting inside MPLS and does not have any contact to other non MPLS is termed as Provider router (P). When the label is added to the router in the MPLS in the starting id the Ingress LER(R2). And when the label is removed in the router is said to be as egress LER(R4). Provider router(R3) does swapping of labels. Forwarding Equivalence Class (FEC) is the group of packets that has to be given equal priority or treated same inside.

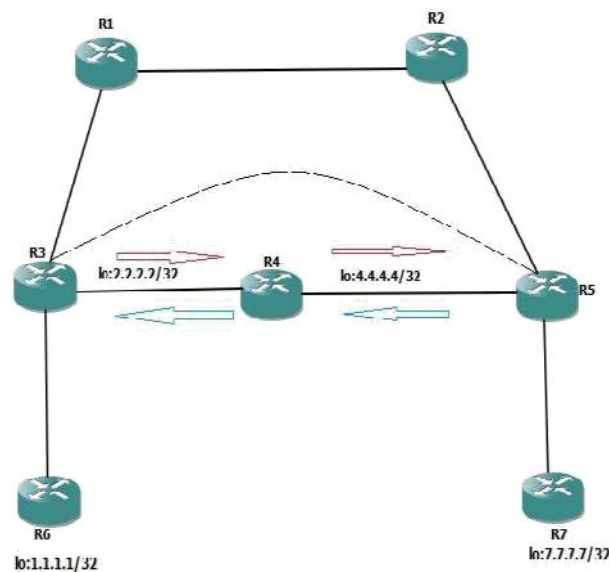


Fig 3.3: MPLS Topology

Cisco Express Forwarding (CEF) plays a key role in such a way that without enabling CEF, MPLS cannot be enabled there are three tables in MPLS, which is RIB (Routing Info Based) is the routing table of MPLS. The three tables are LIB-Label Info Based, FIB-Forwarding Info Based, LFIB-Label Forwarding Info Base. Traffic engineering develops the performance in MPLS networks. Actually, MPLS has been created to improve packet performance in the core of networks. All configurations in MPLS traffic engineering is run on a particular node which is called headend node. All tunnels and constraints have been created here. At the head-end the destination address of tunnel is mentioned. Tail-end is said to be tunnel destination. These tunnels are unidirectional and identical.

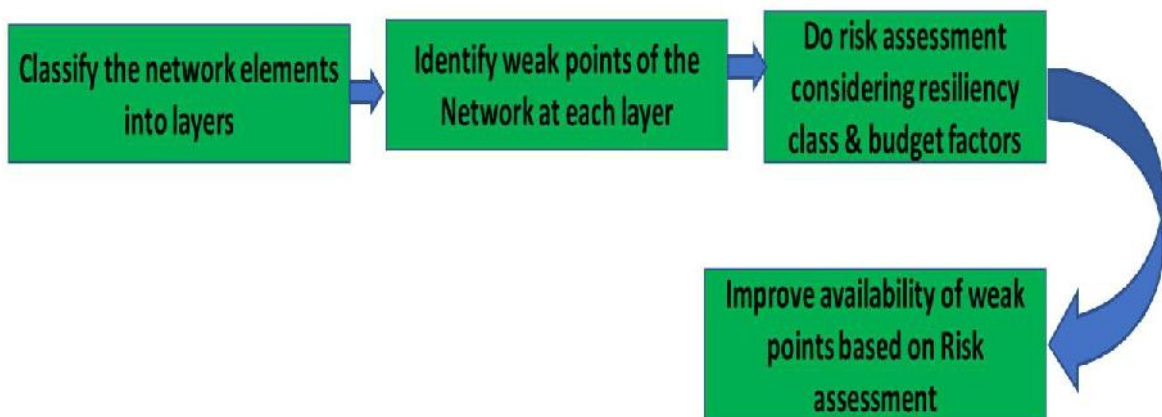


Fig 3.4: BLOCK SCHEMATIC

3.2 PROPOSED SYSTEM

A sample network topology is designed. The aim to show the how to face the challenges in failure in network and provide frame solution.

In current scenarios communication infrastructure consists of sets of inter connected networks. They are classified based on either access network or wide area network. Network access provide us end communication. A redundancy little or more are present in various topologies usually in access network.

Due to the limitation in cost WAN also known as long haul network or core backbone. There is a pre-planned failure network has to be implemented in mesh topology. These component network will be owned and operated by many organizations like service provider. Basically, the process steps are divided into

three levels. They are access network, distributed network and core network. The top layer provides data, voice, network at high level. The layers may contain many sub-layers.

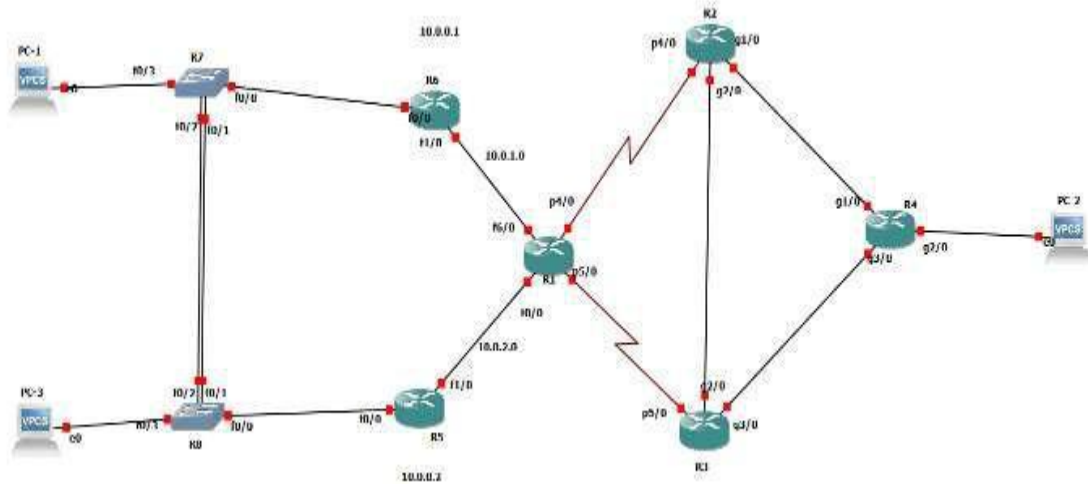


Fig 3.5: Network Architecture

We must concentrate on each layer and assume different ways in which the network failure may occur and apply certain techniques to improve redundancy. The resilient network concept can be classified into link-disjoint and node-disjoint. For suppose a mesh topology the traffic is sent from source to destination, the path in which the traffic is routed is called active path. Whenever the network failure occurs, the network is designed in such a way that the backup path is configured to route packets through the backup path. Whenever we build a network, we must configure support path in order to avoid the down time such that the network will recover soon.

First of all, make sure study about the complete network and examine the weak points then implement the techniques to rectify the weak points by using different methods and implement fault tolerant with high in availability.

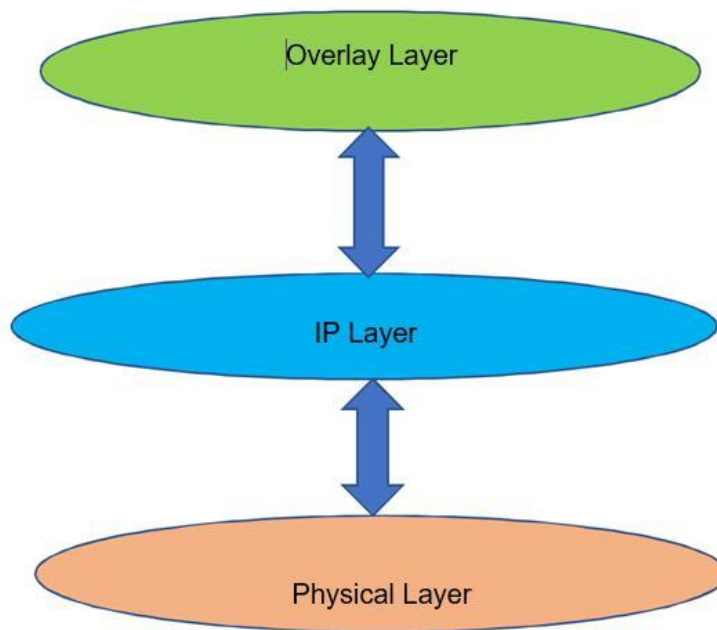


Fig 3.6: Multi-Layer Network

3.2.1 ADVANTAGES OF PREPOSED SYSTEM

-) Time delay can be reduced.
-) Redundancy is improved so that the path will be automatically chosen if there is a failure in the network.
-) A network with more than 95% of availability is built.
-) The service availability is more.
-) The network will be fault tolerant.

CHAPTER 4

MATERIALS AND METHODS

4.1 SOFTWARE REQUIREMENTS

The software that is used to implement a carrier grade WAN network is GNS3 and Wireshark.

4.1.1 GNS3

This GNS3 combines the virtual devices and the real devices for many real time applications. This is used in the simulation of many complex topology networks. One more software is used by GNS3 called Dynamyps for the cisco ios. The process to build topology is so simple and it can be easily adapted by anyone.

-) Click on file
-) Click on new project
-) The left side all the installed ios images and the devices will be displayed. Drag and drop all the devices necessary that has to be used to build a topology.
-) Connect the devices using wires.
-) The routers have to be configured first to connect wires. The slots have to be added.
-) Open the console cable and the commands has to be given.
-) Give command Ping the devices to check the connectivity.

4.1.2 WIRESHARK:

To check the packets or to analyze the packets, this Wireshark is used, this has so many uses like troubleshooting and for protocols development and for many purposes.

4.2 MPLS (Multi-Protocol Label Switching)

Packets are classified in MPLS domain into forwarding equivalence class and each FEC is bound between labels and at the label binding are then distributed to the label switch routers through a separate protocol which is called as label distribution protocol.

The label allocation in the MPLS networks is discussed further. Label can be done either based on downstream based label allocations or upstream based label allocations.

The various techniques are Downstream unsolicited label assignments by downstream peers and distributed to neighbouring LSR. Downstream on demand, upstream LSR specifically requests a label assignment.

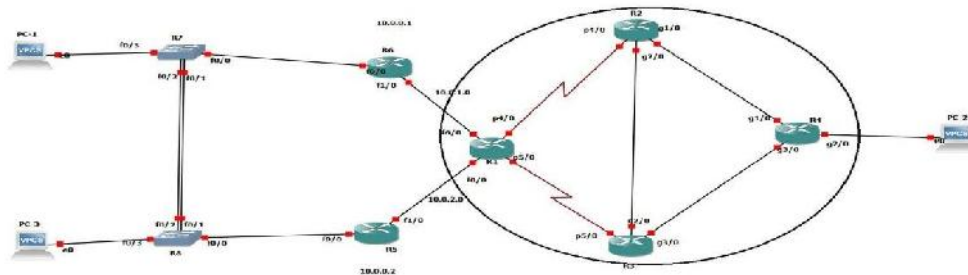


Fig 4.1: MPLS configuration in design network

4.3 LDP (Label Distribution Protocol):

-) LSR Discovery mechanism.
-) Four classes of messages.
-) To provide constant & quality in delivery of messages.
-) Easy in extensive using messages specified as collections of TLV.

Label Distribution Protocol (LDP) is a protocol in which routers capable of Multi-Protocol Label Switching (MPLS) exchange label mapping information. Two routers with an established session are called LDP peers and the exchange of

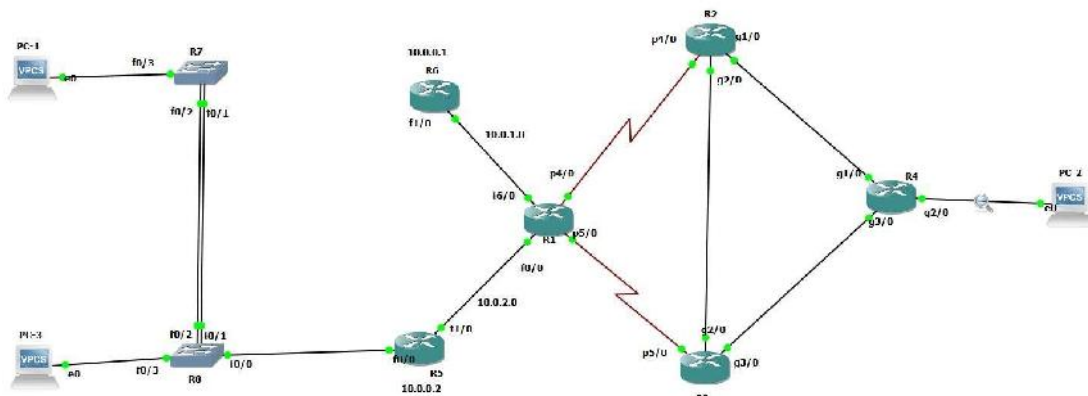


Fig 4.2: When one of the gateways fails

information is bi-directional. LDP is used to build and maintain (LSP) databases that are used to forward traffic through MPLS networks.

LDP can be used to distribute the inner label (VC/VPN/service label) and outer label (path label) in MPLS. The Label Distribution Protocol (LDP) is a protocol defined by the IETF for the purpose of distributing labels in an MPLS environment.

LDP runs over TCP application even though we may not need other features of TCP like heavy control or flow control mechanisms. The LDP is easily extensible.

In QOS based routing, we will choose a path which will be optimal with respect to a certain metric and it will be subject to availability of bandwidth on the link. The difference between QOS based routing and the TE algorithm, QOS ER are typically greedy.

So, once they choose a way which clears the certain constraints and if another request comes and if that request can be accommodated by readjusting the load, that will typically be not done in a QOS B algorithm.

TE algorithm may try to read just the loads in such a manner.

```

PC-1 PC-3 PC-2
84 bytes from 200.200.200.2 icmp_seq=22 ttl=60 time=65.951 ms
84 bytes from 200.200.200.2 icmp_seq=23 ttl=60 time=69.955 ms
84 bytes from 200.200.200.2 icmp_seq=24 ttl=60 time=62.959 ms
84 bytes from 200.200.200.2 icmp_seq=25 ttl=60 time=71.954 ms
84 bytes from 200.200.200.2 icmp_seq=26 ttl=60 time=67.959 ms
84 bytes from 200.200.200.2 icmp_seq=27 ttl=60 time=61.938 ms
84 bytes from 200.200.200.2 icmp_seq=28 ttl=60 time=65.966 ms
84 bytes from 200.200.200.2 icmp_seq=29 ttl=60 time=47.969 ms
84 bytes from 200.200.200.2 icmp_seq=30 ttl=60 time=59.963 ms
84 bytes from 200.200.200.2 icmp_seq=31 ttl=60 time=61.955 ms
84 bytes from 200.200.200.2 icmp_seq=32 ttl=60 time=69.958 ms
84 bytes from 200.200.200.2 icmp_seq=33 ttl=60 time=50.968 ms
84 bytes from 200.200.200.2 icmp_seq=34 ttl=60 time=70.955 ms
84 bytes from 200.200.200.2 icmp_seq=35 ttl=60 time=69.956 ms
84 bytes from 200.200.200.2 icmp_seq=36 ttl=60 time=60.961 ms
84 bytes from 200.200.200.2 icmp_seq=37 ttl=60 time=63.960 ms
84 bytes from 200.200.200.2 icmp_seq=38 ttl=60 time=52.967 ms
84 bytes from 200.200.200.2 icmp_seq=39 ttl=60 time=54.967 ms
200.200.200.2 icmp_seq=40 timeout
200.200.200.2 icmp_seq=41 timeout
200.200.200.2 icmp_seq=42 timeout
200.200.200.2 icmp_seq=43 timeout
84 bytes from 200.200.200.2 icmp_seq=44 ttl=60 time=176.889 ms
84 bytes from 200.200.200.2 icmp_seq=45 ttl=60 time=69.958 ms
84 bytes from 200.200.200.2 icmp_seq=46 ttl=60 time=50.967 ms
84 bytes from 200.200.200.2 icmp_seq=47 ttl=60 time=67.954 ms

```

Fig 4.3: ping tracert report

No.	Time	Source	Destination	Protocol	Length	Info
96	61.046103	200.200.200.2	10.0.0.10	ICMP	98	Echo (ping) reply id=0x4b60, seq=41/10496, ttl=64 (request in 95)
97	61.102910	10.0.1.1	200.200.200.2	ICMP	70	Destination unreachable (Host unreachable)
98	61.854288	ca:04:05:b4:00:38	ca:04:05:b4:00:38	LOOP	60	Reply
99	63.072291	10.0.0.10	200.200.200.2	ICMP	98	Echo (ping) request id=0x4d60, seq=42/10752, ttl=59 (reply in 100)
100	63.073739	200.200.200.2	10.0.0.10	ICMP	98	Echo (ping) reply id=0x4d60, seq=42/10752, ttl=64 (request in 99)
101	63.139851	10.0.1.1	200.200.200.2	ICMP	70	Destination unreachable (Host unreachable)
102	65.067497	10.0.0.10	200.200.200.2	ICMP	98	Echo (ping) request id=0x4f60, seq=43/11008, ttl=59 (reply in 103)
103	65.067784	200.200.200.2	10.0.0.10	ICMP	98	Echo (ping) reply id=0x4f60, seq=43/11008, ttl=64 (request in 102)
104	65.111547	10.0.1.1	200.200.200.2	ICMP	70	Destination unreachable (Host unreachable)
105	65.007074	100.100.100.1	10.0.0.1	ICMP	60	Walla Zerkat

Fig 4.4: uptime and the downtime

4.4 TE (Traffic Engineering):

Routers are most favourable to some scalar metric subject to bandwidth availability on individual links. The congestion trunks are actually collections of individual micro flows. The traffic trunks are actually routed in MPLS domain in the form of labels switch direction are mapped on the routers of avl, BW and delays. So, depends on capacity of links and tunnels the traffic are diverted in different ways. The stability is increased.

4.5 STP (spanning tree protocol):

STP delays the loops when you have multiple links between switches. The STP stops delaying broadcast, multiple frame copies and instability in data base. spanning tree protocol is an open standard (IEEE 802.1D). spanning tree protocol is starts by natural on all cisco catalyst switches. spanning tree protocol work depends on of selecting the both ports in designated and non-designated.

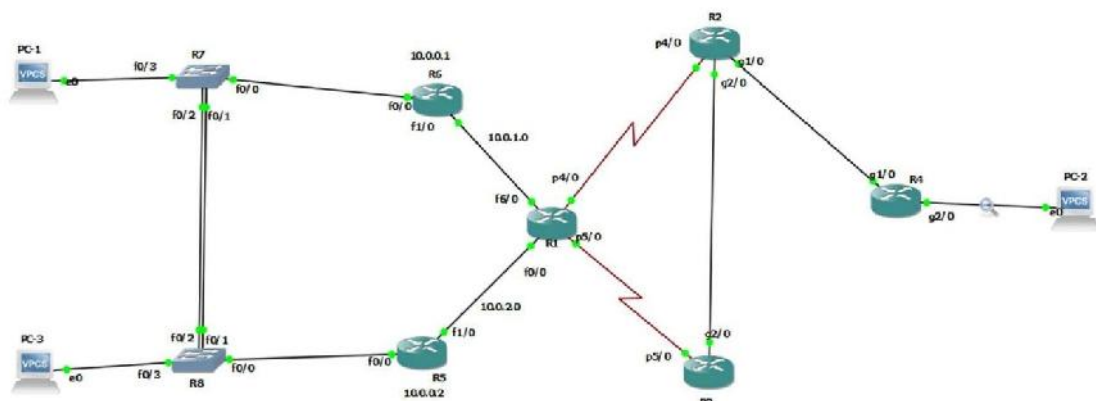


Fig 4.5: when an MPLS link fails

When this MPLS network fails, still the network does not stop working because of the OSPF protocol that is configured in the network that utilizes bandwidth from another side of topology. If this protocol fails, an additional or backup rip protocol which can be used at the time of protocol failure. In the MPLS network three tunnels is configured because, the critical traffic has to be taken in to notice and three tunnels are virtual. One tunnel is from router R1, R2, R4. The other tunnel is from router R1, R3, R2, R4. The third tunnel is from R1, R3, R4. These tunnels come into use only when there is a critical traffic.

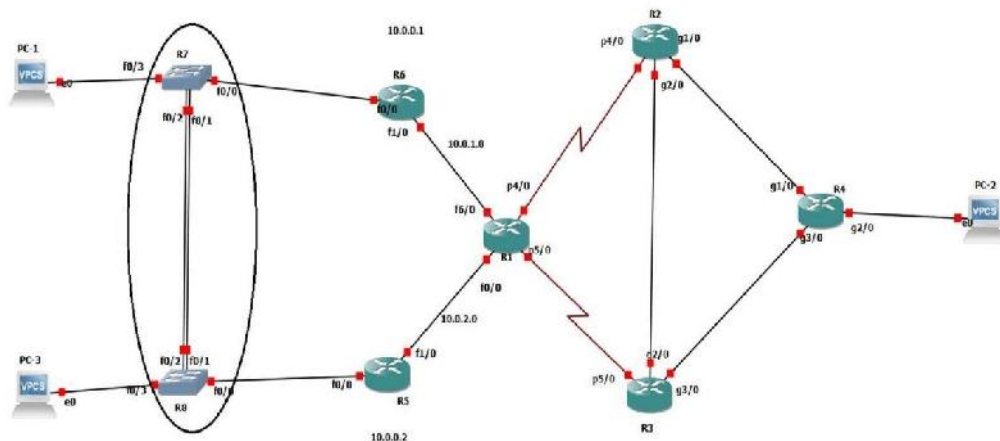


Fig 4.6: LACP configuration in the network

This LACP configuration in the network allows the path change from one link to other, when there are multiple links connected.

4.6 RB (Root Bridge):

In all the switches in the network one of them considered as a root bridge that becomes the local point in the network. In LAN it has two types bridges namely root bridges and non-root bridges.

4.7 LACP (Link Aggregation Control Protocol):

So, we have to be sure in network that having the bandwidth we need and we have the backup for the redundancy and have to make sure that we should not less connectivity. so, in the end we should have more than 1gb of bandwidth.so by only one interface, the loss of connectivity, for this we have to build so many interfaces for more redundant network. It helps to maintain a dynamic environment for that we can do LA in simple manner. Also called as Nic teaming or IP bunding. Actually, it is an idea of making many links but work as 1. By these logical interfaces, we have tripped the BW. If one link goes down, then we still have two gigabyte per second running and nothing has dropped. And so, we are not switching to other and not laying and waiting to work it.

```
PC-1> ping 200.200.200.2 -t
84 bytes from 200.200.200.2 icmp_seq=1 ttl=60 time=142.913 ms
84 bytes from 200.200.200.2 icmp_seq=2 ttl=60 time=86.945 ms
84 bytes from 200.200.200.2 icmp_seq=3 ttl=60 time=84.947 ms
84 bytes from 200.200.200.2 icmp_seq=4 ttl=60 time=62.959 ms
84 bytes from 200.200.200.2 icmp_seq=5 ttl=60 time=66.960 ms
84 bytes from 200.200.200.2 icmp_seq=6 ttl=60 time=76.949 ms
84 bytes from 200.200.200.2 icmp_seq=7 ttl=60 time=62.960 ms
84 bytes from 200.200.200.2 icmp_seq=8 ttl=60 time=64.954 ms
84 bytes from 200.200.200.2 icmp_seq=9 ttl=60 time=53.968 ms
84 bytes from 200.200.200.2 icmp_seq=10 ttl=60 time=53.968 ms
84 bytes from 200.200.200.2 icmp_seq=11 ttl=60 time=59.963 ms
84 bytes from 200.200.200.2 icmp_seq=12 ttl=60 time=61.960 ms
84 bytes from 200.200.200.2 icmp_seq=13 ttl=60 time=61.944 ms
84 bytes from 200.200.200.2 icmp_seq=14 ttl=60 time=48.972 ms
84 bytes from 200.200.200.2 icmp_seq=15 ttl=60 time=37.975 ms
84 bytes from 200.200.200.2 icmp_seq=16 ttl=60 time=61.961 ms
84 bytes from 200.200.200.2 icmp_seq=17 ttl=60 time=57.963 ms
84 bytes from 200.200.200.2 icmp_seq=18 ttl=60 time=134.917 ms
84 bytes from 200.200.200.2 icmp_seq=19 ttl=60 time=62.962 ms
84 bytes from 200.200.200.2 icmp_seq=20 ttl=60 time=75.955 ms
84 bytes from 200.200.200.2 icmp_seq=21 ttl=60 time=127.919 ms
84 bytes from 200.200.200.2 icmp_seq=22 ttl=60 time=66.958 ms
84 bytes from 200.200.200.2 icmp_seq=23 ttl=60 time=69.956 ms
84 bytes from 200.200.200.2 icmp_seq=24 ttl=60 time=100.938 ms
84 bytes from 200.200.200.2 icmp_seq=25 ttl=60 time=69.957 ms
84 bytes from 200.200.200.2 icmp_seq=26 ttl=60 time=92.939 ms
84 bytes from 200.200.200.2 icmp_seq=27 ttl=60 time=95.940 ms
```

Fig 4.7: Ping tracert report

The screenshot shows a terminal window for a Virtual PC Simulator. The title bar at the top includes tabs for R6, PC-1 (active), PC-2, PC-3, R1, R2, R3, and R4. The terminal output is as follows:

```

Welcome to Virtual PC Simulator, version 0.6.1
Dedicated to Daling.
Build time: Jun  1 2015 11:42:32
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 10.0.0.10 255.255.255.0 gateway 10.0.0.3

PC-1> show

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC-1      10.0.0.10/24  10.0.0.3     00:50:79:66:68:01  10080  127.0.0.1:10081
          fe80::250:79ff:fe66:6801/64

PC-1> 

```

Fig 4.10: PC1 Configuration

This HSRP configuration in the network helps in recovering the gateways, when one of the gateways fails during the operation. The neighbour router immediately changes from standby state to the active state, where ever the active router fails. In this way one downtime can, be avoided so to increase the uptime.

4.9 Calculation of Availability:

The availability in the network is,

$$\text{Availability} = 92.019872/94.001977$$

$$\text{Availability} = 98\%$$

The availability depends on how much time the service is active.

```

Welcome to Virtual PC Simulator, version 0.6.1
Dedicated to Daling.
Build time: Jun  1 2015 11:42:32
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD"
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 200.200.200.2 255.255.255.0 gateway 200.200.200.1

PC-2> show

```

Fig 4.11: PC2 Configuration

```

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 10.0.0.20 255.255.255.0 gateway 10.0.0.4

PC-3> show ip interface brief

show [ARG]
  Show information for ARG
  ARG:
    arp          Show arp table
    dump         Show dump flags
    echo         Show the status of the echo flag. See set echo ?
    history      List the command history
    ip [all]     Show IPv4 details
                Shows VPC Name, IP address, mask, gateway, DNS, MAC,
                lport, rhost:rport and MTU
    ipv6 [all]   Show IPv6 details
                Shows VPC Name, IPv6 addresses/mask, gateway, MAC,
                lport, rhost:rport and MTU
    version      Show the version information

Notes:
1. If no parameter is given, the key information of the current VPC will be
   displayed
2. If 'all' parameter is given for ip/ipv6 a reduced view in tabular
   format will be displayed.

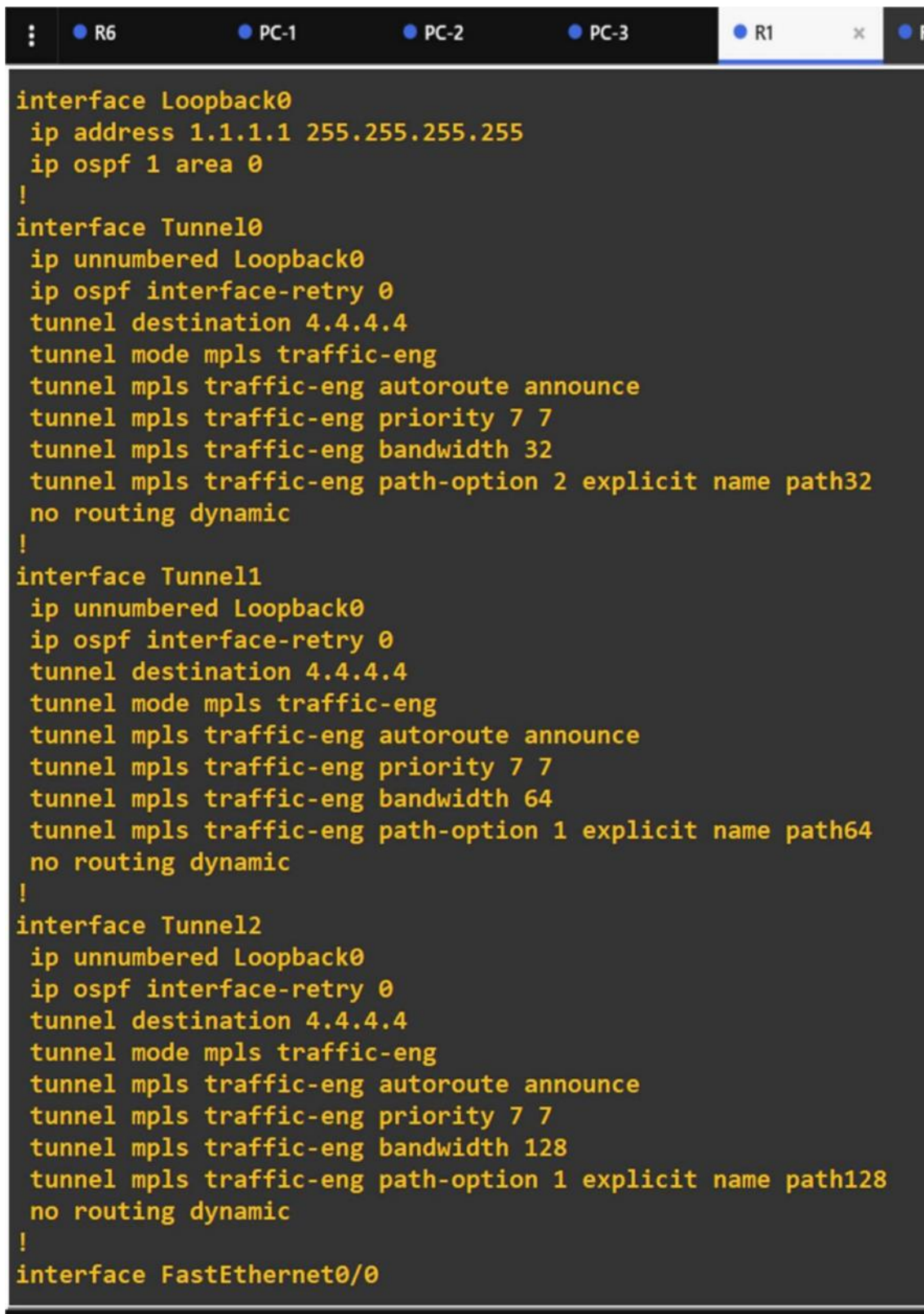
PC-3> show

```

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC-3	10.0.0.20/24	10.0.0.4	00:50:79:66:68:02	10082	127.0.0.1:10083
	fe80::250:79ff:fe66:6802/64				

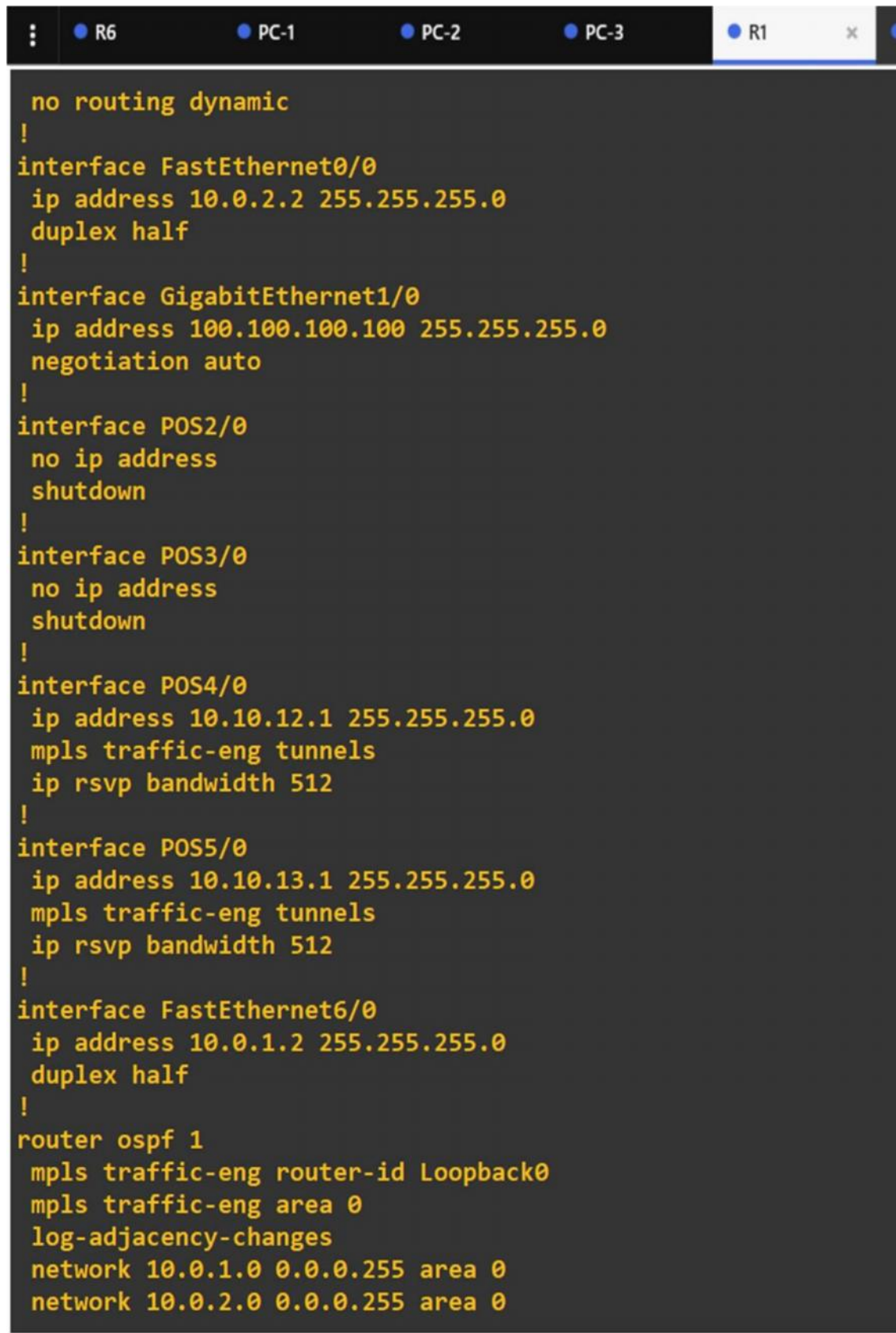
Fig 4.12: PC3 configuration

This is the information regarding the tunnels that are created in router R1, there are three tunnels, tunnel 0, tunnel 1, tunnel 2.



```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
ip ospf 1 area 0
!
interface Tunnel0
ip unnumbered Loopback0
ip ospf interface-retry 0
tunnel destination 4.4.4.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth 32
tunnel mpls traffic-eng path-option 2 explicit name path32
no routing dynamic
!
interface Tunnel1
ip unnumbered Loopback0
ip ospf interface-retry 0
tunnel destination 4.4.4.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth 64
tunnel mpls traffic-eng path-option 1 explicit name path64
no routing dynamic
!
interface Tunnel2
ip unnumbered Loopback0
ip ospf interface-retry 0
tunnel destination 4.4.4.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth 128
tunnel mpls traffic-eng path-option 1 explicit name path128
no routing dynamic
!
interface FastEthernet0/0
```

Fig 4.13: Router R1 configuration of tunnels



```
no routing dynamic
!
interface FastEthernet0/0
 ip address 10.0.2.2 255.255.255.0
 duplex half
!
interface GigabitEthernet1/0
 ip address 100.100.100.100 255.255.255.0
 negotiation auto
!
interface POS2/0
 no ip address
 shutdown
!
interface POS3/0
 no ip address
 shutdown
!
interface POS4/0
 ip address 10.10.12.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 512
!
interface POS5/0
 ip address 10.10.13.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 512
!
interface FastEthernet6/0
 ip address 10.0.1.2 255.255.255.0
 duplex half
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 log-adjacency-changes
 network 10.0.1.0 0.0.0.255 area 0
 network 10.0.2.0 0.0.0.255 area 0
```

Fig 4.14: Router R1 ospf configuration

```

!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end

R1#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.0.2.2	YES	NVRAM	up	up
GigabitEthernet1/0	100.100.100.100	YES	NVRAM	up	up
POS2/0	unassigned	YES	NVRAM	administratively down	down
POS3/0	unassigned	YES	NVRAM	administratively down	down
POS4/0	10.10.12.1	YES	NVRAM	up	up
POS5/0	10.10.13.1	YES	NVRAM	up	up
FastEthernet6/0	10.0.1.2	YES	NVRAM	up	up
SSLVPN-VIF0	unassigned	NO	unset	up	up
Loopback0	1.1.1.1	YES	NVRAM	up	up
Tunnel0	1.1.1.1	YES	TFTP	up	up
Tunnel1	1.1.1.1	YES	TFTP	up	up

Fig 4.15: Router R1 Interfaces

```

end

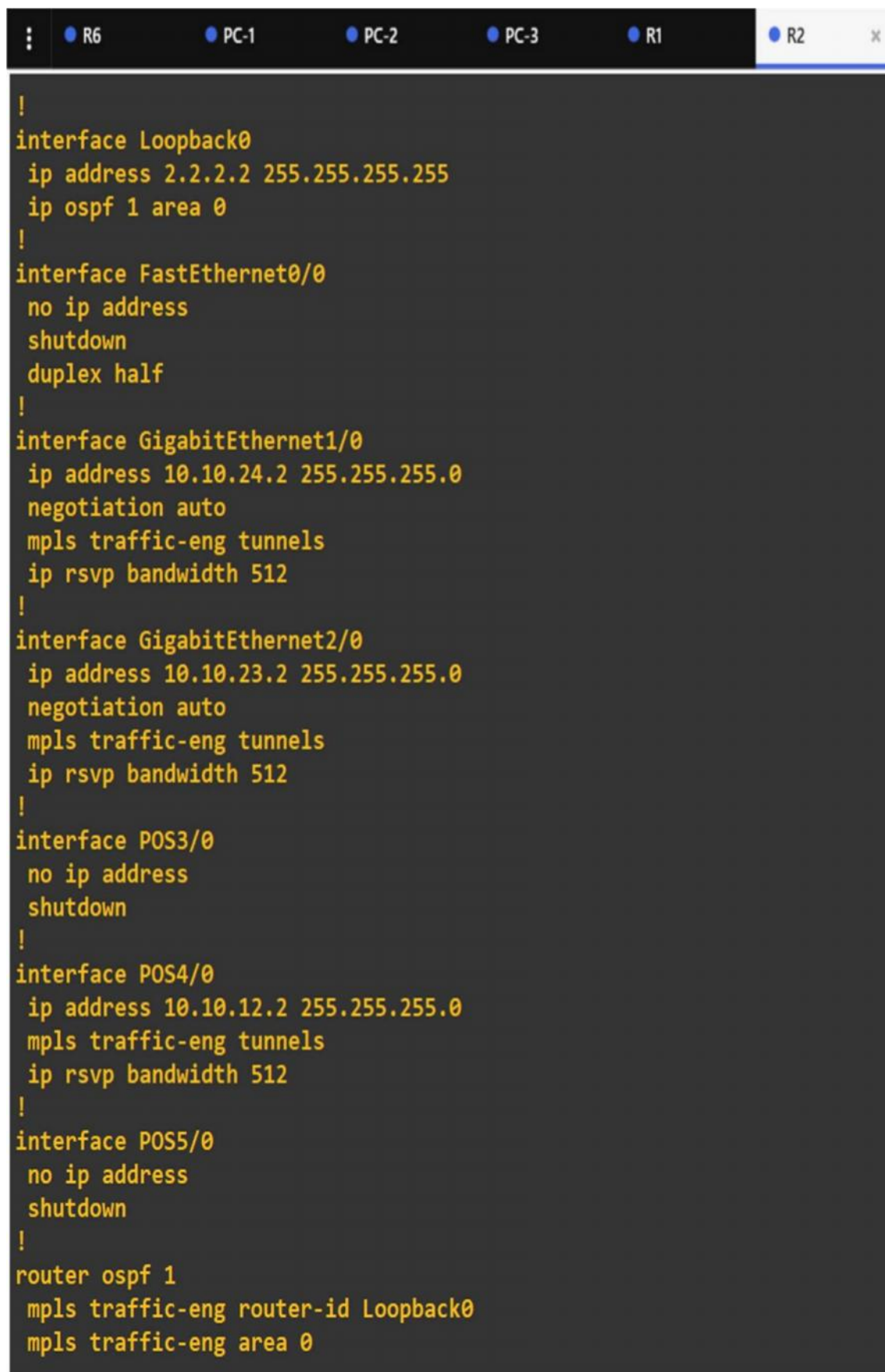
R2#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet1/0	10.10.24.2	YES	NVRAM	up	up
GigabitEthernet2/0	10.10.23.2	YES	NVRAM	up	up
POS3/0	unassigned	YES	NVRAM	administratively down	down
POS4/0	10.10.12.2	YES	NVRAM	up	up
POS5/0	unassigned	YES	NVRAM	administratively down	down
SSLVPN-VIF0	unassigned	NO	unset	up	up
Loopback0	2.2.2.2	YES	NVRAM	up	up

R2#

Fig 4.16: Router R2 Interfaces



```
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 ip ospf 1 area 0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 ip address 10.10.24.2 255.255.255.0
 negotiation auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 512
!
interface GigabitEthernet2/0
 ip address 10.10.23.2 255.255.255.0
 negotiation auto
 mpls traffic-eng tunnels
 ip rsvp bandwidth 512
!
interface POS3/0
 no ip address
 shutdown
!
interface POS4/0
 ip address 10.10.12.2 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 512
!
interface POS5/0
 no ip address
 shutdown
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
```

Fig 4.17: Router R2 MPLS configuration

R6 PC-1 PC-2 PC-3 R1 R2 R3

```

!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex half
!
interface GigabitEthernet1/0
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet2/0
  ip address 10.10.23.3 255.255.255.0
  negotiation auto
  mpls traffic-eng tunnels
  ip rsvp bandwidth 512
!
interface GigabitEthernet3/0
  ip address 10.10.34.3 255.255.255.0
  negotiation auto
  mpls traffic-eng tunnels
  ip rsvp bandwidth 512
!
interface POS4/0
  no ip address
  shutdown
!
interface POS5/0
  ip address 10.10.13.3 255.255.255.0
  mpls traffic-eng tunnels
  ip rsvp bandwidth 512
!
interface POS6/0
  no ip address
  shutdown
!
router ospf 1
  mpls traffic-eng router-id Loopback0
  
```

Fig 4.18: Router R3 configuration

```

R3#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet1/0	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet2/0	10.10.23.3	YES	NVRAM	up	up
GigabitEthernet3/0	10.10.34.3	YES	NVRAM	up	up
POS4/0	unassigned	YES	NVRAM	administratively down	down
POS5/0	10.10.13.3	YES	NVRAM	up	up
POS6/0	unassigned	YES	NVRAM	administratively down	down
SSLVPN-VIF0	unassigned	NO	unset	up	up
Loopback0	3.3.3.3	YES	NVRAM	up	up

```

R3#

```

Fig 4.19: Router R3 interfaces

```

interface Tunnel0
 ip unnumbered Loopback0
 ip ospf interface-retry 0
 tunnel destination 1.1.1.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 32
 tunnel mpls traffic-eng path-option 2 explicit name path32
 no routing dynamic
!
interface Tunnel1
 ip unnumbered Loopback0
 ip ospf interface-retry 0
 tunnel destination 1.1.1.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 64
 tunnel mpls traffic-eng path-option 1 explicit name path64
 no routing dynamic
!
interface Tunnel2
 ip unnumbered Loopback0
 ip ospf interface-retry 0
 tunnel destination 1.1.1.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 128
 tunnel mpls traffic-eng path-option 1 explicit name path128
 no routing dynamic
!

```

Fig 4.20: Router R4 Configuration

```

R4#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet1/0	10.10.24.4	YES	NVRAM	up	up
GigabitEthernet2/0	200.200.200.1	YES	NVRAM	up	up
GigabitEthernet3/0	10.10.34.4	YES	NVRAM	up	up
SSLVPN-VIF0	unassigned	NO	unset	up	up
Loopback0	4.4.4.4	YES	NVRAM	up	up
Tunnel0	4.4.4.4	YES	TFTP	up	up
Tunnel1	4.4.4.4	YES	TFTP	up	up
Tunnel2	4.4.4.4	YES	TFTP	up	up

```

R4#

```

Fig 5.21: Router R4 Interfaces

```

!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex half
!
interface GigabitEthernet1/0
  ip address 10.10.24.4 255.255.255.0
  negotiation auto
  mpls traffic-eng tunnels
  ip rsvp bandwidth 512
!
interface GigabitEthernet2/0
  ip address 200.200.200.1 255.255.255.0
  negotiation auto
  mpls traffic-eng tunnels
  ip rsvp bandwidth 512
!
interface GigabitEthernet3/0
  ip address 10.10.34.4 255.255.255.0
  negotiation auto
  mpls traffic-eng tunnels
  ip rsvp bandwidth 512
!
router ospf 1
  mpls traffic-eng router-id Loopback0
  mpls traffic-eng area 0
  log-adjacency-changes
  network 10.10.0.0 0.0.255.255 area 0
  network 200.200.200.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
ip explicit-path name path32 enable

```

Fig 4.22: Router R4 OSPF configuration

```

R5# show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.0.0.2	YES	NVRAM	up	up
FastEthernet1/0	10.0.2.1	YES	NVRAM	up	up
FastEthernet2/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet3/0	unassigned	YES	NVRAM	administratively down	down
SSLVPN-VIF0	unassigned	NO	unset	up	up

```

R5#

```

Fig 5.23: Router R5 interfaces

```

!
!
interface FastEthernet0/0
 ip address 10.0.0.2 255.255.255.0
 duplex half
 standby 1 ip 10.0.0.3
 standby 1 timers 1 2
 standby 1 preempt delay minimum 2
 standby 2 ip 10.0.0.4
 standby 2 timers 1 2
 standby 2 priority 110
 standby 2 preempt delay minimum 2
!
interface FastEthernet1/0
 ip address 10.0.2.1 255.255.255.0
 duplex half
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 10.0.2.0 0.0.0.255 area 0
!

```

Fig 4.24: Router R5 configuration

```

R6#
R6#
R6#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.0.0.1	YES	NVRAM	up	up
FastEthernet1/0	10.0.1.1	YES	NVRAM	up	up
FastEthernet2/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet3/0	unassigned	YES	NVRAM	administratively down	down
SSLVPN-VIF0	unassigned	NO	unset	up	up

```

R6#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.0.0.1	YES	NVRAM	up	up
FastEthernet1/0	10.0.1.1	YES	NVRAM	up	up
FastEthernet2/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet3/0	unassigned	YES	NVRAM	administratively down	down
SSLVPN-VIF0	unassigned	NO	unset	up	up

```

R6#

```

Fig 4.25: Router R6 interfaces

```
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex half
 standby 1 ip 10.0.0.3
 standby 1 timers 1 2
 standby 1 priority 110
 standby 1 preempt delay minimum 2
 standby 2 ip 10.0.0.4
 standby 2 timers 1 2
 standby 2 preempt delay minimum 2
!
interface FastEthernet1/0
 ip address 10.0.1.1 255.255.255.0
 duplex half
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 10.0.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
```

Fig 4.26: Router R6 Configuration

```

R7#
R7#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up
FastEthernet0/4	unassigned	YES	unset	up	down
FastEthernet0/5	unassigned	YES	unset	up	down
FastEthernet0/6	unassigned	YES	unset	up	down
FastEthernet0/7	unassigned	YES	unset	up	down
FastEthernet0/8	unassigned	YES	unset	up	down
FastEthernet0/9	unassigned	YES	unset	up	down
FastEthernet0/10	unassigned	YES	unset	up	down
FastEthernet0/11	unassigned	YES	unset	up	down
FastEthernet0/12	unassigned	YES	unset	up	down
FastEthernet0/13	unassigned	YES	unset	up	down
FastEthernet0/14	unassigned	YES	unset	up	down
FastEthernet0/15	unassigned	YES	unset	up	down
Port-channel1	unassigned	YES	unset	up	up

Fig 4.27: Switch1 Interfaces

```

R7#
R7#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up
FastEthernet0/4	unassigned	YES	unset	up	down
FastEthernet0/5	unassigned	YES	unset	up	down
FastEthernet0/6	unassigned	YES	unset	up	down
FastEthernet0/7	unassigned	YES	unset	up	down
FastEthernet0/8	unassigned	YES	unset	up	down
FastEthernet0/9	unassigned	YES	unset	up	down
FastEthernet0/10	unassigned	YES	unset	up	down
FastEthernet0/11	unassigned	YES	unset	up	down
FastEthernet0/12	unassigned	YES	unset	up	down
FastEthernet0/13	unassigned	YES	unset	up	down
FastEthernet0/14	unassigned	YES	unset	up	down
FastEthernet0/15	unassigned	YES	unset	up	down
Port-channel1	unassigned	YES	unset	up	up

Fig 4.28: Switch2 Interfaces

CHAPTER 5

RESULTS AND DISCUSSIONS

5.1 RESULTS

-) Thus, as shown in the below figures output has been achieved, the data has been successfully transferred from end to end.

5.1.1 RESULTS FOR LACP

-) Links between Node to Node has been deleted to create a Pre-Planned Network Failure.
-) The Nodes that are failed now go to Hold state and the neighbour Node comes to Active state until the failed path is Recovered.

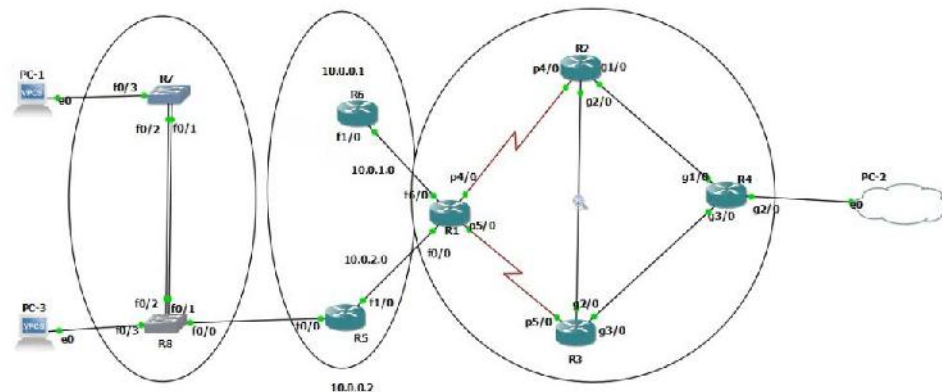


Fig 5.1: NODE FAILURE FOR NODE R7 TO R6

```
84 bytes from 200.200.200.2 icmp_seq=64 ttl=60 time=65.705 ms
84 bytes from 200.200.200.2 icmp_seq=65 ttl=60 time=81.287 ms
84 bytes from 200.200.200.2 icmp_seq=66 ttl=60 time=63.833 ms
84 bytes from 200.200.200.2 icmp_seq=67 ttl=60 time=71.102 ms
200.200.200.2 icmp_seq=68 timeout
200.200.200.2 icmp_seq=69 timeout
200.200.200.2 icmp_seq=70 timeout
200.200.200.2 icmp_seq=71 timeout
84 bytes from 200.200.200.2 icmp_seq=72 ttl=60 time=132.050 ms
84 bytes from 200.200.200.2 icmp_seq=73 ttl=60 time=67.486 ms
```

Fig 5.2: CONNECTIVITY RE-ESTABLISHED

Capturing from Standard input [R1 GigabitEthernet2/0 to R2 GigabitEthernet2/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply and display filter: ...

No.	Time	Source	Destination	Protocol	Length	Info
215	136.604510	10.10.23.2	224.0.0.5	OSPF	78	LS Acknowledge
216	137.577983	10.0.0.10	200.200.200.2	ICMP	102	Echo (ping) request id=0xa889, seq=144/36864, ttl=62 (no response found!)
217	138.663901	10.0.0.10	200.200.200.2	ICMP	102	Echo (ping) request id=0xa889, seq=145/37120, ttl=62 (no response found!)
218	139.752847	10.0.0.10	200.200.200.2	ICMP	102	Echo (ping) request id=0xa889, seq=146/37376, ttl=62 (no response found!)
219	140.104247	10.10.23.3	224.0.0.5	OSPF	110	LS Update
220	140.104247	10.10.23.2	224.0.0.5	OSPF	110	LS Update
221	140.157625	10.10.23.2	224.0.0.5	OSPF	110	LS Update
222	140.161906	10.10.23.3	224.0.0.5	OSPF	110	LS Update
223	140.171882	10.10.23.3	224.0.0.5	OSPF	94	LS Update
224	140.178705	10.10.23.2	224.0.0.5	OSPF	94	LS Update
225	140.853881	10.0.0.10	200.200.200.2	ICMP	102	Echo (ping) request id=0xab89, seq=147/37632, ttl=62 (no response found!)
226	141.453536	10.10.23.2	224.0.0.5	OSPF	94	Hello Packet
227	141.913737	10.0.0.10	200.200.200.2	ICMP	102	Echo (ping) request id=0xac89, seq=148/37888, ttl=62 (no response found!)
228	142.637690	10.10.23.2	224.0.0.5	OSPF	110	LS Acknowledge
229	142.744797	ca:02:34:fc:00:38	ca:02:34:fc:00:38	LOOP	60	Reply
230	142.744799	ca:03:06:e8:00:38	ca:03:06:e8:00:38	LOOP	60	Reply
231	142.988819	10.0.0.10	200.200.200.2	ICMP	102	Echo (ping) request id=0xad89, seq=149/38144, ttl=62 (no response found!)
232	144.873829	10.0.0.10	200.200.200.2	ICMP	102	Echo (ping) request id=0xae89, seq=150/38400, ttl=62 (no response found!)

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
 Ethernet II, Src: ca:03:06:e8:00:38 (ca:03:06:e8:00:38), Dst: ca:02:34:fc:00:38 (ca:02:34:fc:00:38)
 MultiProtocol Label Switching Header, Label: 26, Exp: 0, S: 1, TTL: 62
 Internet Protocol Version 4, Src: 10.0.0.10, Dst: 200.200.200.2
 Internet Control Message Protocol

Fig 5.3: DATA TRANSFER THROUGH CONFIGURED BACKUP PATH

Hence the Network Overcome the failure, there by it transfers the Packets through the configured back up path there by achieving the LACP configuration.

5.1.2 RESULTS FOR HSRP

Links between Router to Router has been deleted to create a Pre-Planned Network Failure.

The Routers Link that are failed now go to Hold state and the neighbour Routers comes to Active state until the failed path is Recovered.

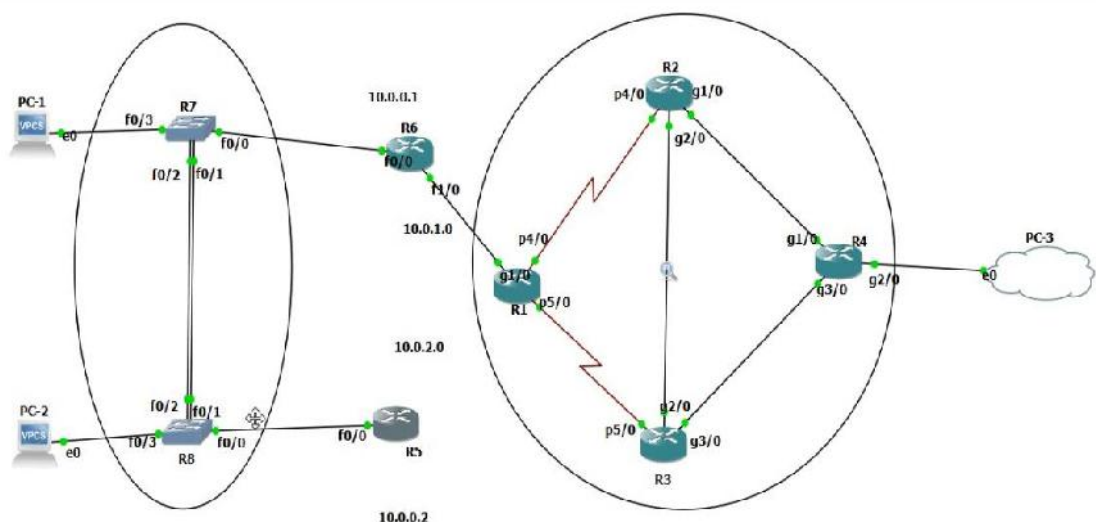


Fig 5.4: LINK FAILURE FROM R5 TO R1

```

84 bytes from 200.200.200.2 icmp_seq=136 ttl=60 time=95.863 ms
84 bytes from 200.200.200.2 icmp_seq=137 ttl=60 time=84.601 ms
84 bytes from 200.200.200.2 icmp_seq=138 ttl=60 time=102.946 ms
84 bytes from 200.200.200.2 icmp_seq=139 ttl=60 time=78.587 ms
200.200.200.2 icmp_seq=140 timeout
84 bytes from 200.200.200.2 icmp_seq=141 ttl=60 time=59.996 ms
84 bytes from 200.200.200.2 icmp_seq=142 ttl=60 time=84.802 ms
84 bytes from 200.200.200.2 icmp_seq=143 ttl=60 time=65.874 ms
84 bytes from 200.200.200.2 icmp_seq=144 ttl=60 time=80.090 ms
84 bytes from 200.200.200.2 icmp_seq=145 ttl=60 time=80.278 ms
84 bytes from 200.200.200.2 icmp_seq=146 ttl=60 time=104.579 ms

```

Fig 5.5: CONNECTION RE-ESTABLISHED

Capturing from - [R3 GigabitEthernet2/0 to R2 GigabitEthernet2/0]

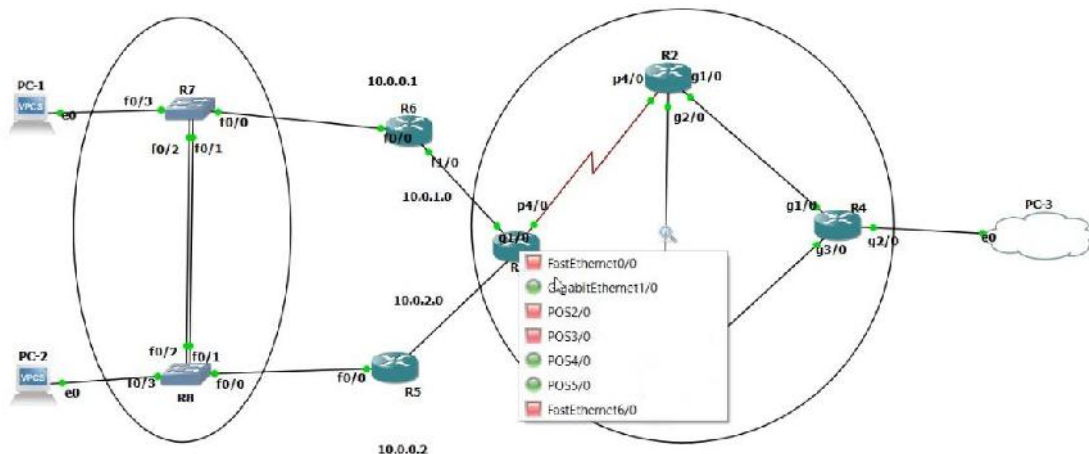
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply as display filter: ... (Ctrl-F)

No.	Time	Source	Destination	Protocol	Length	Info
112	116.793985	10.10.23.2	224.0.0.5	OSPF	94	Hello Packet
113	118.007438	ca:02:34:fc:00:38	CDP/NTP/UDP/PAp2/MDL	CDP	352	Device ID: R2 Port ID: GigabitEthernet2/0
114	118.067912	ca:03:86:e8:00:38	CDP/NTP/UDP/PAp2/MDL	CDP	352	Device ID: R3 Port ID: GigabitEthernet2/0
115	120.241058	10.10.23.3	224.0.0.5	OSPF	94	Hello Packet
116	121.774379	10.10.23.3	224.0.0.5	OSPF	150	LS Update
117	121.774379	10.10.23.2	224.0.0.5	OSPF	150	LS Update
118	124.203709	10.10.23.2	224.0.0.5	OSPF	70	LS Acknowledge
119	124.415802	ca:02:34:fc:00:38	ca:02:34:fc:00:38	LOOP	60	Reply
120	124.462870	ca:03:86:e8:00:38	ca:03:86:e8:00:38	LOOP	60	Reply
121	126.433005	10.10.23.2	224.0.0.5	OSPF	94	Hello Packet
122	126.104323	10.10.23.3	224.0.0.5	OSPF	94	Hello Packet
123	126.915288	10.10.23.3	10.10.23.2	RSPV	142	RSPV Message SESSION: TPu4-LSP, Destination 1.1.1.1, Short Call ID 0, Tunnel ID 2, Ext ID 4040404. FILTERSPEC: TPu4-LSP, Tunnel ...
124	123.166757	1.1.1.1	4.4.4.4	RSPV	238	PATH Message SESSION: TPu4-LSP, Destination 4.4.4.4, Short Call ID 0, Tunnel ID 2, Ext ID 1010101. SENDER TEMPLATE: TPu4-LSP, Tu...
125	124.422774	ca:02:34:fc:00:38	ca:02:34:fc:00:38	LOOP	60	Reply
126	124.461195	ca:03:86:e8:00:38	ca:03:86:e8:00:38	LOOP	60	Reply
127	125.733047	10.10.23.2	224.0.0.5	OSPF	94	Hello Packet
128	127.992089	4.4.4.4	1.1.1.1	RSPV	238	PATH Message SESSION: TPu4-LSP, Destination 1.1.1.1, Short Call ID 0, Tunnel ID 2, Ext ID 4040404. SENDER TEMPLATE: TPu4-LSP, Tu...
129	128.388121	10.10.23.2	10.10.23.3	RSPV	142	RSPV Message SESSION: TPu4-LSP, Destination 4.4.4.4, Short Call ID 0, Tunnel ID 2, Ext ID 1010101. FILTERSPEC: TPu4-LSP, Tunnel ...

Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface -, id 0
 Ethernet II, Src: ca:03:00:a8:00:38 (ca:03:00:a8:00:38), Dst: IPV6mac1_05 (01:00:5e:00:00:05)
 Internet Protocol Version 4, Src: 10.10.23.3, Dst: 224.0.0.5
 Open Shortest Path First

Fig 5.6: DATA TRANSFER THROUGH CONFIGURED BACKUP LINK



-) Hence the Network Overcome the failure, thereby it transfers the Packets through the configured back up Link there by achieving the HSRP configuration.
-) Thus, Carrier Grade WAN Network has been built using GNS3 and WIRESHARK.

CHAPTER 6

SUMMARY AND CONCLUSION

6.1 APPLICATIONS

It is useful in real time WAN network in buildings for corporate.

High availability services can be designed.

Fault tolerant networks can be designed.

6.2 CONCLUSION

In this project a carrier grade WAN network with more availability has been analysed using techniques like HSRP, STP, LACP and MPLSTE. The scalable network which will be capable to handle and process huge amount of traffic has been built. The link level and the node level failure are prevented in the designed network and more availability has been achieved.

6.3 FUTURE WORK

In a network to achieve reliability is by using alternate instances. For every application or a service, the basic and important requirement is timely service and reliability. Difficulties and challenges faced namely cost limitation, traffic and virtual trends, cross layer mapping, super high availability traffic, various networks and operators, issue in regulatory. In further there are many difficulties to be resolved are providing various classes of resilience in multi-layer networks, high availability. Networking is an area which is affluent in problems with more effort to be kept to make the network resilient. In case if there is a risk in network design and the access network reliability must increase.

REFERENCES

- [1] S. Bhattacharjee, M. H. Ammar, E. W. Zegura, N. Shah, and Z. Fei, "Application layer any casting," in Proc. IEEE INFOCOM, 2000
- [2] P. Cao, J. Zhang, and K. Beach, "Active cache: Caching dynamic contents on the Web," in Proc. Middleware, 2001
- [3] D. Andersen, H. Balakrishnan, M. Kai-shek, and R. Morris, "Resilient overlay networks," in Proc. 18th ACM Symp. Operating Systems Principles, 2003
- [4] "Internet Content Adaptation Protocol (ICAP) DS-2326," Network Appliance, Sunnyvale, CA, 2005
- [5] B. Chandra, M. Dahlin, L. Gao, A. Khoja, A. Nayate, A. Razzaq, and A. Sewani, "Resource management for scalable disconnected access to Web services," in Proc. 10th Int. World Wide Web Conf., May 2006
- [6] Liu, Y., Tipper, D., Vajanapoom, K.: Spare capacity allocation in two-layer networks. IEEE Journal on Selected Areas in Communication (2006)
- [7] Madhu Kumar, S.D., Bellur, U.: Availability models for underlay aware overlay networks. In: DEBS'08: Proceedings of the second international conference on Distributed event-based systems, pp. 169, 2008
- [8] Adapt: (2011). URL <http://www.adaptplc.com/>
- [9] Andersen, D., Balakrishnan, H., Kai-shek, F., Morris.: Resilient overlay networks. In: SOSP'01: Proceedings of the eighteenth ACM Operating systems principles (2008)