FAULT TOLERANCE ENTERPRISE NETWORK

Submitted in partial fulfillment of the Degree of

Bachelor of Technology

Dec – 2011 to 2015

Enrolment. Nos. -111018, 111021

Name of Students - Sagar Malik, Nishant Ranjan

Name of supervisor - Dr. Rajiv Kumar

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,

WAKNAGHAT

CERTIFICATE

This is to Certify that project report entitled “FAULT TOLERANCE ENTERPRISE NETWORK”, submitted by Nishant Ranjan (111021, Sagar Malik (111018) in partial fulfillment for the award of degree of Bachelor of Technology in Electronics and Communication Engineering to Jaypee University of Information Technology, Waknaghat, Solan is original work and has been carried out under my supervision. This work has not been submitted partially or fully to any other university or Institute for the award of this or any other degree or diploma

Date: **Sagar Malik (111018)**

Nishant Ranjan (111021)

Supervisor’s Name: Dr. Rajiv Kumar

ACKNOWLEDGEMENT

“The successful completion of any task would be incomplete without accomplishing the people who made it all possible and whose constant guidance and encouragement secured us the success.”

We feel pride and privileged in expressing our deep sense of gratitude to all those who have helped us in presenting this project. We express our sincere gratitude to **Dr. Rajiv Kumar** for his inspiration, constructive suggestions, mastermind analysis and affectionate guidance in our work. It was impossible for us to complete this project without his guidance.

Last but not the least we would like to add our deepest gratitude for our entire faculty of **“ECE Department 6th & 7th Sem.”** at **“JAYPEE UNIVERSITY”** from where we have learnt the basics of Computer Networking which helped us a lot in completion of this project.

Date: **Sagar Malik (111018)**

Nishant Ranjan(111021)

TABLE OF CONTENTS

LIST OF FIGURES

Abstract

Enterprise Networks are private computer networks that are owned by a single organization in order to connect their various offices in order to share computer resources. The task of configuring and managing security policies in enterprise networks is becoming harder due to complex policy constraints of the organizations and rapid changes in the network topologies.

The physical systems that compose a network, on the other hand, are subjected to a wide range of problems, ranging from signal distortion to component failures. Redundancy underlies all approaches to fault tolerance. Designing any system to tolerate faults first requires the selection of a fault model, a set of possible failure scenarios along with an understanding of the frequency, duration, and impact of each scenario.

A simple fault model merely lists the set of faults to be considered; inclusion in the set is decided based on a combination of expected frequency, impact on the system, and feasibility or cost of providing protection. Most reliable network designs address the failure of any single component, and some designs tolerate multiple failures.

The temporal characteristics of faults vary widely, but can be roughly categorized as permanent, intermittent, or transient. Failures that prevent a component from functioning until repaired or replaced, such as the destruction of a network fiber by a backhoe, are considered permanent. Failures that allow a component to function properly some of the time are called intermittent. Damaged connectors and electrical components sometimes produce intermittent faults, operating correctly until mechanical vibrations or thermal variations cause a failure, and recovering when conditions change again. Every Network Designer must work towards avoiding these types of faults. Any network that is not fault tolerant is not practical enough to be implemented. Every network should be capable enough to avoid or at least work in case of a node or link failure. Enterprise networks require a lot of configuration expertise and experience from the network designer and the network manager.

CHAPTER 1

Introduction to the basics of Networking

Networking Basics :

When looking at networking basics, understanding the way a network operates is the first step to understanding routing and switching. The network operates by connecting computers and peripherals using two pieces of equipment; switches and routers. Switches and routers, essential networking basics, enable the devices that are connected to your network to communicate with each other, as well as with other networks.

Though they look quite similar, routers and switches perform very different functions in a network.

Basic Networking Devices :

Networking devices are the units that mediate data in a network. Networking Devices are also called network equipment , intermediate systems (IS), Interworking Units. Units which are the last receiver or generate data are called hosts or data terminal equipment.

Routers :

Routers are networking devices that forward data packets along networks by using headers and forwarding/routing tables to determine the best path to forward the packets. Routers work at the Internet layer of the TCP/IP model or layer 3 of the OSI model. Routers also provide interconnectivity between like and unlike media. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Some DSL and cable modems, for home use, have been integrated with routers to allow multiple home computers to access the Internet.

Figure 1.1: Routers

Switches :

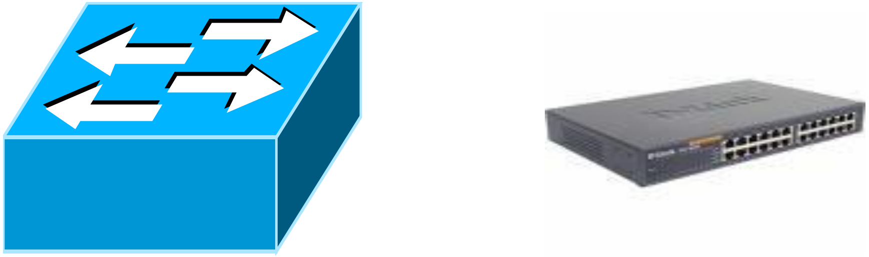


Figure 1.2: Switches

A switch is a device that performs switching. Specifically, it forwards and filters OSI layer 2 datagram (chunk of data communication) between ports (connected cables) based on the Physical-Addresses in the packets. This is distinct from a hub in that it only forwards the datagram to the ports involved in the communications rather than all ports connected.

A switch normally has numerous ports with the intention that most or all of the networks be connected directly to a switch, or another switch that is in turn connected to a switch.

Hubs :

Figure 1.3: Example of Hubs

A hub (concentrator) contains multiple ports, which is used to connect devices in a star topology. When a packet arrives at one port, it is copied to all the ports of the hub. But when the packets are copied, the destination address in the frame does not change to a broadcast address. It does this in a rudimentary way; it simply copies the data to all of the Nodes connected to the hub (broadcast).

Bridges:

Figure 1.4: Example of Bridges

A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which physical addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.

Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Network Interface Cards :

Figure 1.5 : Network Interface Card

A network card, network adapter or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

Designing a network :

Designing a network is the first step of fault diagnosis and probably the trickiest one too. At this stage a network designer has to keep in mind many aspects of this process. In order to give a detailed explanation of how one should start designing a robust and secure network the process is divided into three parts. These parts are enumerated as follows:

- Things to consider while designing the network
- Steps involved in designing the network
- Troubleshooting the network

Things to consider while designing the network :

No. of independent Departments or Offices:

The first step is to consider the number and the type of users that work at different locations and departments in the organisation.

Categorization of nodes for creating VLANs :

A network designer must see all its users or hosts as nodes that have certain requirements and rights. All the users in a network cannot be given equal access rights.

Version of Internet Protocol : IPv4 or IPv6

IPv4

IPv4 is a 32 bit numeric address used for data communication at the internet layer. This has been in use for more than 20 years and served well but growing number of devices in networks has forced us to go for a new addressing scheme and here comes IPv6.

IPv6

IP Version 6 (IPv6) is the newest version of IP, sometimes called “IPng” for “IP, Next Generation”. IPv6 is fairly well defined but is not yet widely deployed. The main differences between IPv6 and the current widely-deployed version of IP (which is IPv4) are:

IPv6 uses larger addresses (128 bits instead of 32 bits in IPv4) and so can support many more devices on the network. IPv6 includes features like authentication and multicasting that had been bolted on to IPv4 in a piecemeal fashion over the years.

Physical Address (Hardware Address/MAC Address)

The MAC (Media Access control) address is a unique value associated with a network adapter. They uniquely identify an adapter on a LAN. MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:

MM:MM:MM:SS:SS:SS
MM-MM-MM-SS

The first half (24 bits) of a MAC address contains the ID number of the adapter manufacturer (Vendor ID). The second half(24 bits) of a MAC address represents the serial number assigned to the adapter by the manufacturer. In the example,

00:A0:C9:14:C8:29

The prefix **00A0C9** indicates the manufacturer is Intel Corporation.

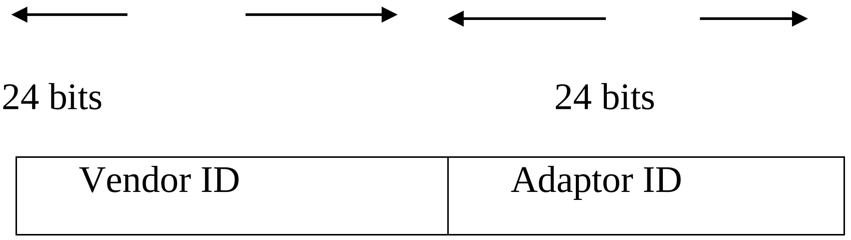


Figure 1.6 : Explanation of MAC address bits

Subnetting :

It is no of users per subnet . Subnetting is one of the most crucial parts of network design . Subnetting, by definition, means dividing a network in parts for assigning IP addresses in an optimal way so as to optimize the utilization of network address space.

Classless Inter domain Routing (CIDR) is used to achieve this.

Deciding the required network topology :

There are many networking topologies available but practically, it is very hard to stick to a single topology such as mesh or start topologies. So, the network designer must try to make the best choice possible by choosing a hybrid network topology. Hybrid network topologies are a combination of different topologies. The network is designed based on the network requirements. Hence, sticking with a single network topology might not be the best way to go about it.

Connecting these devices with proper cables :

The network designer must have enough expertise and experience to know what kind of cable would suit to the needs of the network depending on traffic at a particular interface and compatibility issues. Some of the options are Straight-through cable, cross over cable and serial links.

IP Addressing :

If a device wants to communicate using TCP/IP, it needs an IP address. **I.P.** addressing was designed to allow hosts on one network to communicate with a host on a different network regardless of the type of LANs the hosts are participating in. When the device has an IP address and the appropriate software and hardware, it can send and receive IP packets. Any device that can send and receive IP packets is called an IP host.

IP addressing is the main task in the network designing process. The concepts of Classless Inter Domain Routing and Variable Length Subnet Mask are used for subnetting.

In order to do this dynamically a very widely used protocol is used. It is called Dynamic Host Configuration Protocol (DHCP). The default gateway is made to act like a DHCP server. All the host connected to it get their default configurations from the router acting as default gateway.

Implementation of Variable Length Subnet Mask :

VLSM is implemented during the process of subnetting. VLSM being a conceptual method is very widely used or subnetting.

Assigning other details like hostname, passwords etc. :

Every node in the network must have a hostname, a password etc. These details are for the purpose of convenience of the network manager. Every switch and the routers must be configured with passwords so that no one could make any changes to the configurations of these devices.

Troubleshooting the Network :

This is the phase where packet is send from every host to every other host to check if there is any problem in the desired transmissionscheme. Packet Internet Groper (PING) is mostly used. Every Network design needs to be troubleshoot before it can actually be implemented.

There is a list of steps to be taken to troubleshoot a network :

1. Open DOS and ping 127.0.0.1

2. From the DOS window ping the local host

3. From the DOS window ping the default gateway

4. If steps 1 through 3 were successful, ping the remote server

CHAPTER 2
Properties of Enterprise Network

Properties of Enterprise Network for Large Scale Organization :

Enterprise networks are the networks owned by large scale organizations in which a high performance network is required. They cannot afford to have their network down even for few seconds. Hence, some of the properties that make enterprise networks what they are are as follows:

Redundancy :

Redundancy is the key property of an enterprise network. Enterprise networks are designed in such a way that for every path there must be an alternate one.In case a node or a link goes down, the Enterprise networks are equipped with backup routes.

Router Redundancy :

Router Redundancy is an important property of an Enterprise network. It is a method which is extensively used in enterprises. Basically, Hot Standby Router Protocol removes the need for the old design called "router on a stick".

HSRP (Hot Standby Router Protocol) is a redundancy protocol for setting up a fault-tolerant default gateway in a LAN environment. This is a Cisco proprietary protocol. The standard protocol is VRRP (Virtual Router Redundancy Protocol). HSRP is a new feature of Packet Tracer 6.0 . This protocol can be configured on every Cisco router available in Packet Tracer as well as on Cisco Catalyst 3560 layer 3 switch.
The following IOS commands are available :

- standby <0-4095> ip Enable HSRP and set the virtual IP address
- standby <0-4095> preempt Overthrow lower priority Active routers
- standby <0-4095> priority Priority level
- standby <0-4095> timers Hello and hold timers
- standby <0-4095> track Priority Tracking

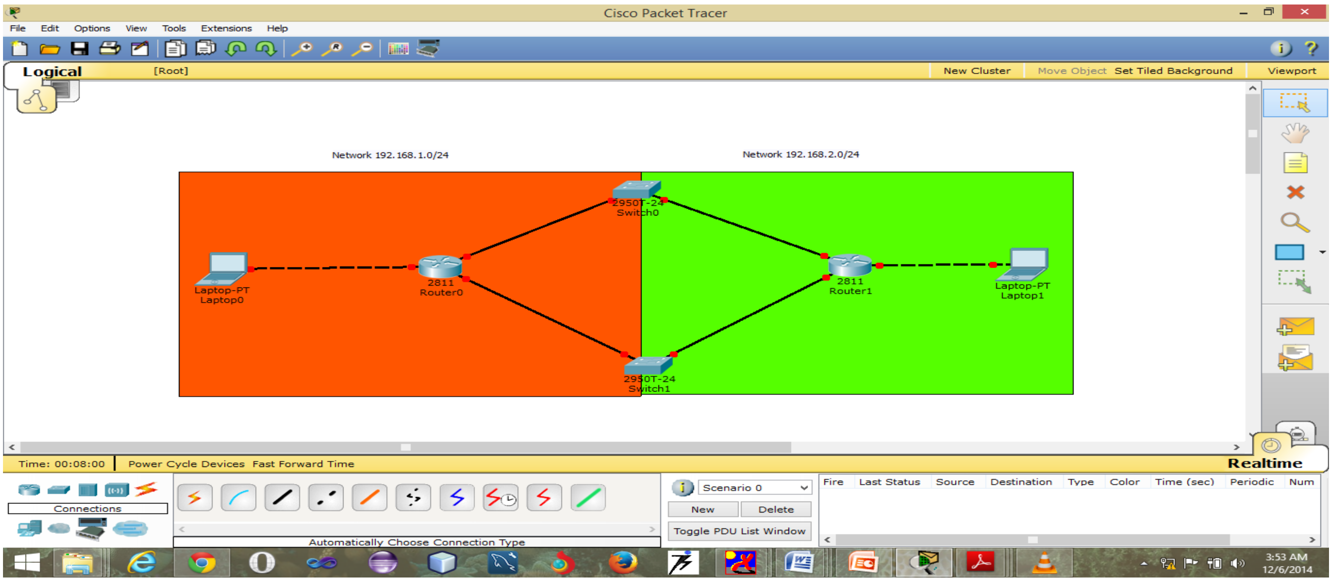


Figure 2.1: Implementation of router redundancy

Routers configuration :

Router0 configuration

```
interface GigabitEthernet0/0
ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 standby version 2
 standby 1 ip 192.168.1.1
 standby 1 priority 120
 standby 1 preempt
```

```
interface GigabitEthernet0/1
 ip address 192.168.2.2 255.255.255.0
 duplex auto
 speed auto
 standby version 2
 standby 2 ip 192.168.2.1
 standby 2 priority 120
 standby 2 preemp
```

Router1 configuration :

```
interface GigabitEthernet0/0
 ip address 192.168.1.3 255.255.255.0
 duplex auto
 speed auto
 standby version 2
 standby 1 ip 192.168.1.1

interface GigabitEthernet0/1
 ip address 192.168.2.3 255.255.255.0
 duplex auto
 speed auto
 standby version 2
 standby 2 ip 192.168.2.1
```

Alternatives:

- Virtual Router Redundancy Protocol (VVRP)
- Common Address Redundancy Protocol (Open Source)

High Availability :

- Providing high availability in the enterprise site can involve deploying highly fault-tolerant devices, incorporating redundant topologies, implementing STP, and configuring HSRP.
- Network designers must incorporate high-availability features throughout the network.
- Adopting a high-availability strategy for an enterprise site is a must.

Use of ACL :

The Cisco Access Control List (ACL) is are used for filtering traffic based on a given filtering criteria on a router or switch interface. Based on the conditions supplied by the ACL, a packet is allowed or blocked from further movement.

Cisco ACLs are available for several types of routed protocols including IP, IPX, AppleTalk, XNS, DECnet, and others. However, we will be discussing ACLs pertaining to TCP/IP protocol only. ACLs for TCP/IP traffic filtering are primarily divided into two types:

- Standard Access Lists, and
- Extended Access Lists

Standard Access Control Lists: Standard IP ACLs range from 1 to 99. A Standard Access List allows you to permit or deny traffic FROM specific IP addresses.

This is the command syntax format of a standard ACL.

access-list *access-list-number* {permit|deny}
{host|sourcesource-wildcard|any}

Standard ACL example:

```
access-list 10 permit 192.168.2.0 0.0.0.255
```

The output looks like:

```
access-list 10 permit 192.168.2.0 0.0.0.255
access-list 10 deny any
```

This list allows traffic from all addresses in the range 192.168.2.0 to 192.168.2.255

Extended Access Control Lists: Extended IP ACLs allow you to permit or deny traffic from specific IP addresses to a specific destination IP address and port. Extended IP ACLs range from 100 to 199.

Extended ACL example:

access-list 110 - Applied to traffic leaving the office (outgoing)

```
access-list 110 permit tcp 92.128.2.0 0.0.0.255 any eq 80
```

ACL 110 permits traffic originating from any address on the 92.128.2.0 network. The 'any' statement means that the traffic is allowed to have any destination address with the limitation of going to port 80. The value of 0.0.0.0/255.255.255.255 can be specified as 'any'.

After the ACL is defined, it must be applied to the interface (inbound or outbound). The syntax for applying an ACL to a router interface is given below:

```
interface<interface>
ip access-group {number|name} {in|out}
```

CHAPTER 3
Fault Tolerance

Fault Tolerance :

Fault tolerance is a term used to describe the ability of a network to continue to function in a manner acceptable to the network users despite the occurrence of one or more faults or failures within the network itself.

Types of faults :

There are four types of basic faults that can occur in a network:

1) Transient

2) Persistent

3) Intermittent

4) Byzantines

Transient Faults:

Transient faults are faults that appear for a very small time. These are temporary in nature. These can be caused by lightening, or voltage fluctuations. These faults are non persistent in nature and remain in the network for a very small time.

Persistent Faults:

Persistent Faults are like permanent faults. These faults have to be corrected as soon as they occur. There can be various reasons for these faults. Once they occur, persistent faults continue to keep the network segment down unless corrected as early as possible.

Intermittent Faults:

Intermittent faults are caused by repetition of transient faults. Unlike transient faults, these faults remain in the network. These faults are crucial as they are hard to pin point. Intermittent faults create noise in the network and can also bring down the network segment in specific network scenarios.

Byzantine Faults:

Byzantine faults are faults that occur due to a combination of transient, intermittent and persistent faults. Byzantine faults are hard to correct and have the capacity to bring down a network segment as it includes persistent as well as intermittent faults.

These four basic faults do not usually occur in their defined forms. The most common type of faults originating in a network are as follows:

- Transient leading to Persistent
- Intermittent leading to Persistent
- Transient, Intermittent, Persistent

CHAPTER 4
Implementation

As a part of the implementation process we have created various simulations and explained the use of each of the techniques used in our project. A combination of these methods and protocols gives us a very robust and fault tolerant network

Technical Details :

The softwares used in our project is CISCO PACKET TRACKER.

Cisco Packet Tracer is a powerful network simulation program that allows the implementers to experiment with network behaviour. As an integral part of the Networking Academy comprehensive learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities of complex technology concepts.

The simulation-based environment helps users develop modern networking models. Packet Tracer allows users to easily learn and demonstrate complex technical concepts and networking systems design.

Supported Protocols :

LAN: Ethernet (including CSMA/CD*), 802.11 a/b/g/n wireless*, PPPOE

Switching: VLANs, 802.1q, trunking, VTP, DTP, STP*, RSTP*, multilayer switching*, Etherchannel, LACP, PAgP

TCP/IP: HTTP, HTTPS, DHCP, DHCPv6, Telnet, SSH, TFTP, DNS, TCP*, UDP, IPv4*, IPv6*, ICMP, ICMPv6, ARP, IPv6 ND, FTP, SMTP, POP3, VOIP(H.323)

Routing: static, default, RIPv1, RIPv2, EIGRP, single-area OSPF, multi-area OSPF, BGP, inter-VLAN routing, redistribution

Other: ACLs (standard, extended, and named), CDP, NAT (static, dynamic, inside/outside, and overload), NATv6

WAN: HDLC, SLARP, PPP*, and Frame Relay*

Security: IPsec, GRE, ISAKMP, NTP, AAA, RADIUS, TACACS, SNMP, SSH, SYSLOG, CBAC, Zone-based policy firewall, IPS

QoS: Layer 2 QoS, Layer 3 Diffserv QoS, FIFO Hardware queues, Priority Queuing, Custom Queuing, Weighted Fair Queuing, MQC, NBAR*

Simulation Parmeters :

Simulation is done using Packet Tracer, employing ICMP protocol (ping). The simulation has been carried out for 8, 16, 32, 64, 128, and 256 nodes.

TTL (Time to Live): Lifetime of a packet before being discarded – 16.

Waiting time for each node is defined as maximum latency for previous transmission.
The packet tracer carries out the ICMP PING request to determine whether the network is faulty or fault-free. To achieve this it carries out PING request through the shortest path possible between the end nodes of the network.

When you switch to the Simulation mode, simulation panel will appear. You can graphically create PDU to send between devices using the Add Simple PDU button and then pressing the Auto capture/Play button to start the simulation scenario. You can control the speed of the simulation by using the play speed slider.

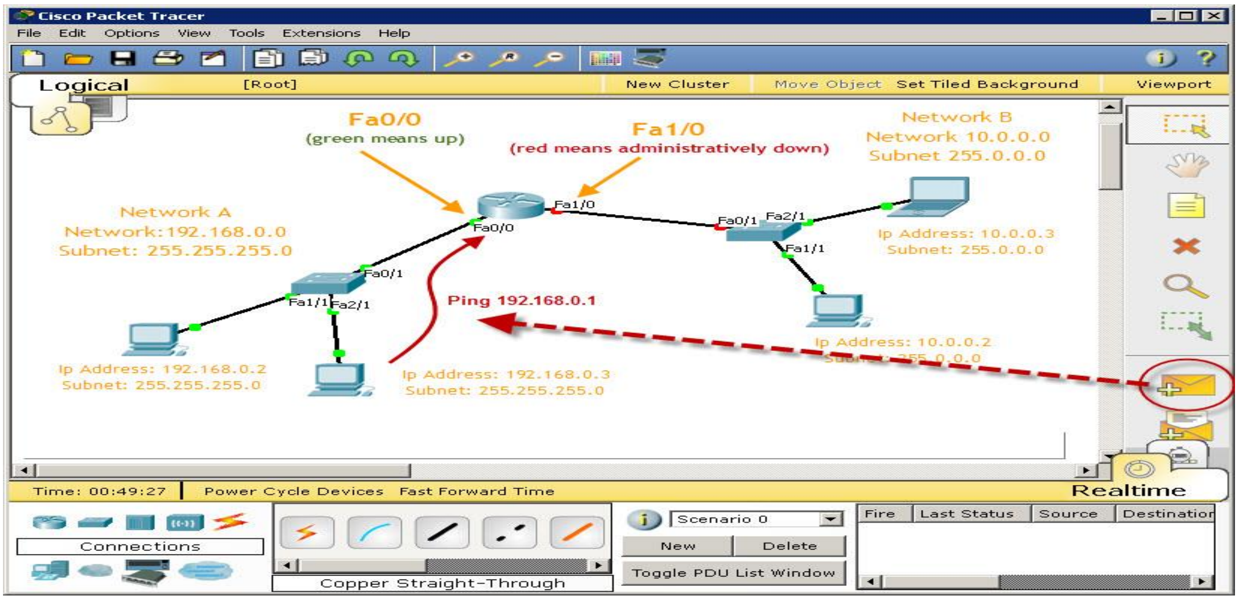


Figure 4.1 : Showing some of the simulation parameter

Fast Convergence :

In an Enterprise network it is very important to keep running without a breakdown even for a second. Hence routing protocols with fast convergence become an unavoidable necessity.

The routing protocols used in Enterprise networks are
RiPv2, OSPF, EIGRP, BGP, IS-IS, etc. These protocols have faster convergence and lower administrative distances. Hence these routing protocols are preferred.

RIP Version 2 (RIPv2) :

RIP version 2 is mostly the same as RIP version 1. Both RIPv1 and RIPv2 are distance-vector protocols, which means that each router running RIP sends its complete routing tables out all active interfaces at periodic time intervals. Also, the timers and loop-avoidance schemes are the same in both RIP versions (i.e., holddown timers and split horizon rule), and both have the same administrative distance (120).

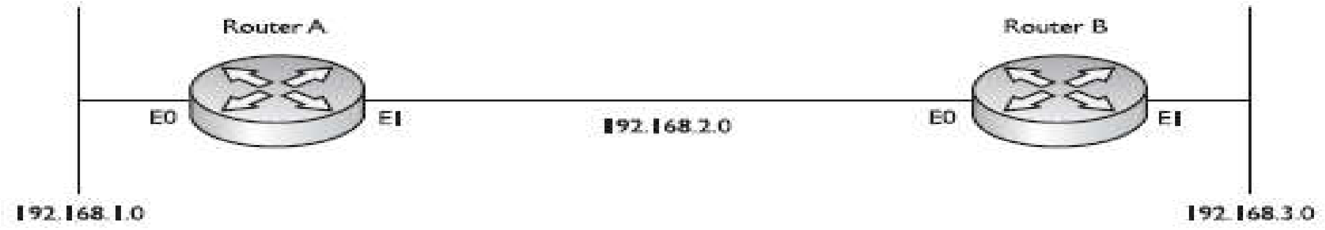


Figure 4.2 : Implementation of RIP protocol

Configuring RIPv2 is straightforward. Here’s an example:

```
RouterC (config)#router rip
RouterC (config-router)#network 192.168.40.0
RouterC (config-router)#network 192.168.50.0
RouterC (config-router)#version 2
```

EIGRP Features and Operation

Enhanced IGRP (EIGRP) is a classless, enhanced distance-vector protocol that gives us a real edge over another Cisco proprietary protocol, Interior Gateway Routing Protocol (IGRP). EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state protocols. EIGRP has link-state characteristics as well—it synchronizes routing tables between neighbors at startup and then sends specific updates only when topology changes occur. There are a number of powerful features that make EIGRP a real standout from IGRP and other protocols. The main ones are listed here:

- Support for IP and IPv6 (and some other useless routed protocols) via protocol dependent modules.
- Considered classless (same as RIPv2 and OSPF).
- Support for VLSM/CIDR.
- Support for summaries and discontiguous networks.
- Efficient neighbor discovery.
- Communication via Reliable Transport Protocol (RTP).
- Best path selection via Diffusing Update Algorithm (DUAL).

Reliable Transport Protocol (RTP)

EIGRP uses a proprietary protocol called Reliable Transport Protocol (RTP) to manage the communication of messages between EIGRP-speaking routers. And as the name suggests, reliability is a key concern of this protocol.

Diffusing Update Algorithm (DUAL)

EIGRP uses Diffusing Update Algorithm (DUAL) for selecting and maintaining the best path to each remote network. This algorithm allows for the following:

- Backup route determination if one is available
- Support of VLSMs
- Dynamic route recoveries
- Queries for an alternate route if no route can be found

EIGRP Metrics

Another thing about EIGRP is that unlike many other protocols that use a single factor to compare routes and select the best possible path, EIGRP can use a combination of four:

- Bandwidth

- Delay
- Load
- Reliability

Like IGRP, EIGRP uses only bandwidth and delay of the line to determine the best path to a remote network by default.

Configuring EIGRP

Here’s the EIGRP routing configuration of the router:

```
Router(config)# router eigrp 200
Router(config-router)# network 172.16.0.0
Router(config-router)# network 10.0.0.0
```

Open Shortest Path First (**OSPF**) :

It is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).

OSPF adheres to the following Link State characteristics:

• OSPF employs a hierarchical network design using Areas.

• OSPF will form neighbor relationships with adjacent routers in the same Area.

• Instead of advertising the distance to connected networks, OSPF advertises the status of directly connected links using Link-State Advertisements (LSAs).

• OSPF sends updates (LSAs) when there is a change to one of its links, and will only send the change in the update. LSAs are additionally refreshed every 30 minutes.

• OSPF traffic is multicast either to address 224.0.0.5 (all OSPF routers) or 224.0.0.6 (all Designated Routers).

• OSPF uses the Dijkstra Shortest Path First algorithm to determine the shortest path. • OSPF is a classless protocol, and thus supports VLSMs.

Other characteristics of OSPF include:

• OSPF supports only IP routing.

• OSPF routes have an administrative distance is 110.

• OSPF uses cost as its metric, which is computed based on the bandwidth of the link. OSPF has no hop-count limit.

Router configuration :

```
Router(config)# router ospf process_ID
Router(config-router)# network IP_address wildcard_mask area area_#
```

Wildcard mask = Full broadcard mask-Subnet mask

Ether Channel :

Ether channeling is a way of logically bundling the transmission link in order to load balance. The bundled links behave as one interface with large transmission capacity. This process is called Link Aggregation.

Three ways to config it :

1. Static(ON).
2. Cisco’s version of Ether Channel is called Port Aggregation Protocol(PAgP) .
   Port state(Desirable,auto).
3. IEEE calls it Link Aggregation Control Protocol (LACP orIEEE802.3ad).
   Port state(Active,Passive).

sw1	sw2	result
on	on	on
active	active	on
active	passive	on
actve	desirable	on
auto	desirable	on
desirable	desirable	on

Configuration :

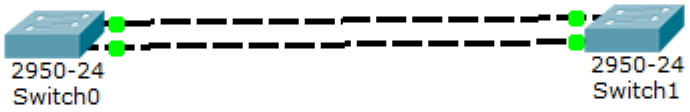


Figure 4.3 : Ether channel configuration

For Switch0 (Layer2 switches)

```
Switch>en
Switch# config terminal
```

```
Switch(config-if-range)channel-group 1 mode active
Switch(config-if-range)do show etherchannel summary
```

For Switch1 (Layer2 switches)

```
Switch>en
Switch# config terminal
Switch(config-if-range)channel-group 1 mode active
Switch(config-if-range)do show etherchannel summary
```

The Host Standby Router Protocol (HSRP)

The Host Standby Router Protocol (HSRP) is a Cisco proprietary protocol, as detailed in RFC 2281. HSRP provides gateway redundancy by sharing IP and MAC addresses between redundant gateways. The protocol consists of virtual MAC and IP addresses that are shared between two or more routers that belong to the same HSRP group.

Working Of HSRP Explained:

HSRP can be configured on a cisco router as a “virtual” router to be used in the routing of packets when the active router interface fails. Basically, what HSRP does is to stand in as a backup router, standing by for when the active router gateway interface fails.

This "virtual" router is configured with a single IP address (layer 3) and MAC address (layer 2) which is shared among two or more router on a LAN segment.

The IP address of the virtual router is configured as the default gateway for the clients on a specific IP segment. When frames are sent from the clients to the default gateway, the clients will use ARP to resolve the MAC address that is associated with the IP address of the default gateway. The ARP then replies with the MAC address of the virtual router. Frames that are sent to the MAC address of the virtual router can then be physically processed by any active or standby router that is part of that virtual router group.

HSRP can be classified as a redundancy protocol that provide a mechanism for determining which router should take the active role in forwarding traffic and determining when that role must be taken over by a standby router.

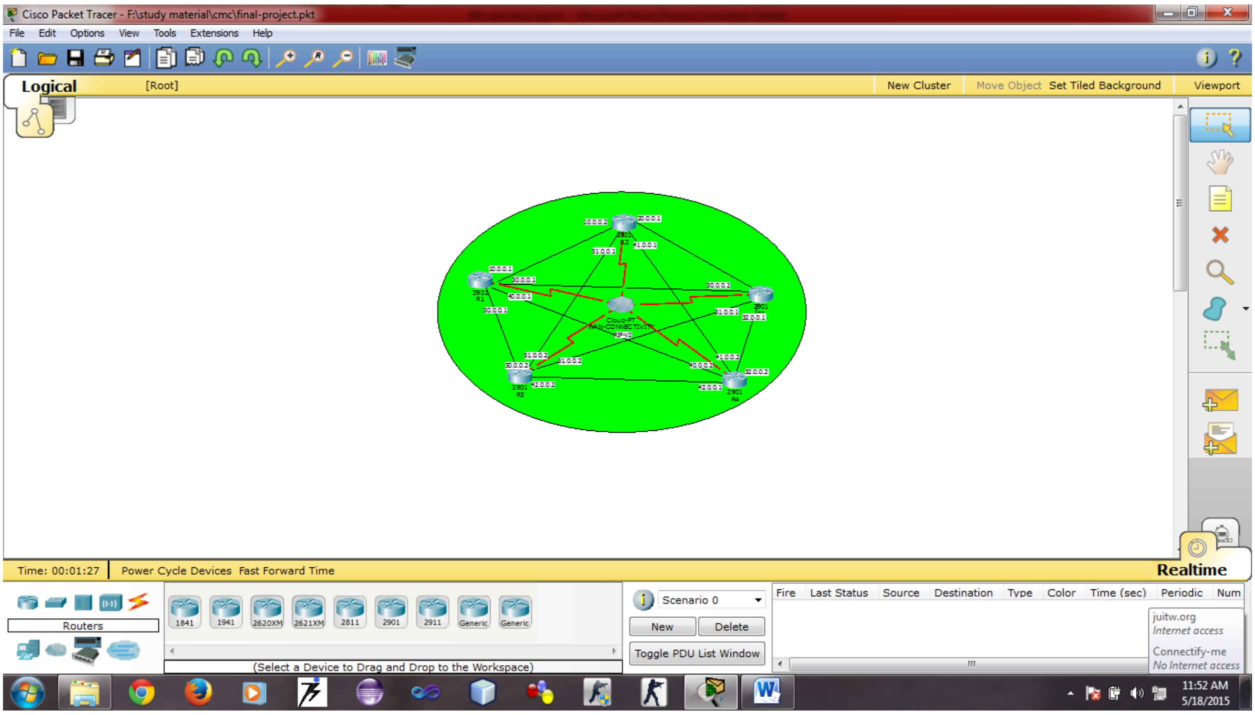


Figure 4.4 : Working of HSRP Diagrammatically

Configuring router:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch# show standby
```

Frame Relay:

Frame Relay is a scalable WAN solution that is often used as an alternative to leased lines when leased lines prove to be cost unaffordable. With Frame Relay, you can have a single serial interface on a router connecting into multiple remote sites through virtual circuits.

Virtual Circuits:

A VC is a logical connection between two devices; therefore, many of these VCs can exist on the same physical connection. The advantage that VCs have over leased lines is that they can provide full connectivity at a much lower price. VCs are also full-duplex: you can simultaneously send and receive on the same VC.

There are two types of VCs: permanent VCs (PVCs) and switched or semipermanent VCs (SVCs).

PVC is similar to a leased line: it is configured up front by the carrier and remains up as long as there is a physical circuit path from the source to the destination.

SVC are similar to telephone circuit-switched connections: whenever you need to send data to a connection, an SVC is dynamically built and then torn down once your data has been sent.

Disadvantage of PVCs is that they require a lot of manual configuration up front to establish the VC. Another disadvantage is that they aren't very flexible: if the PVC fails, there is no dynamic rebuilding of the PVC around the failure.

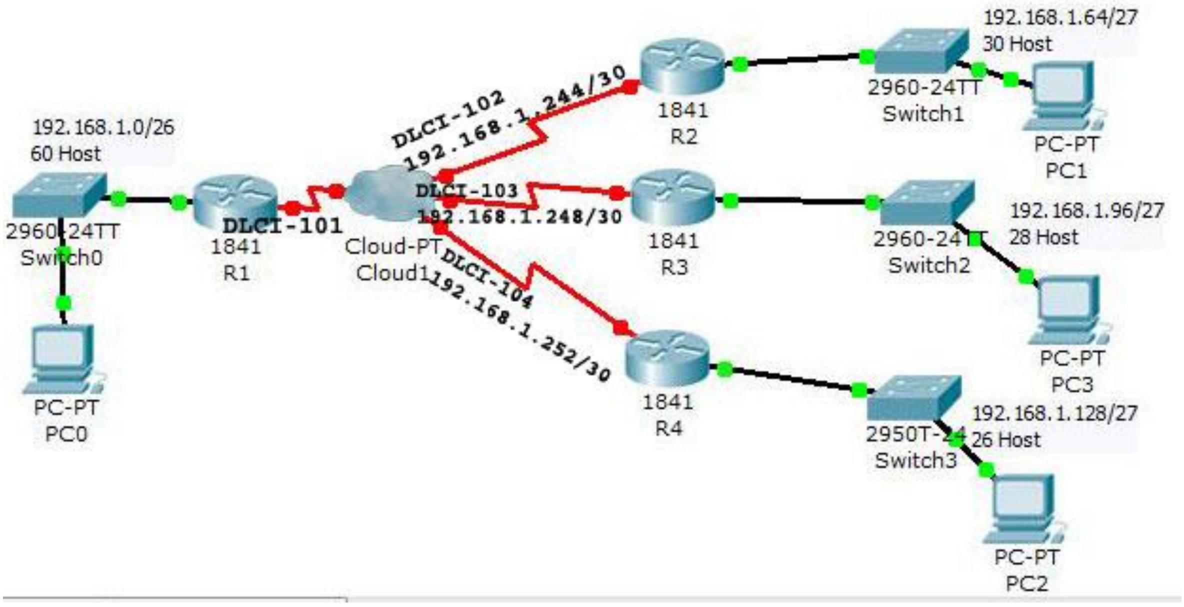


Figure 4.5 : Configuration of Frame Relay

Configure R1:

```
R1>enable
R1#configure terminal
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config-subif)#interface serial 0/0/0.102 point-to-point
R1(config-subif)#ip address 192.168.1.245 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 102
R1(config-subif)#exit
R1(config)#interface serial 0/0/0.103 point-to-point
```

```
R1(config-subif)#ip address 192.168.1.249 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 103
R1(config-subif)#exit
R1(config)#interface serial 0/0/0.104 point-to-point
R1(config-subif)#ip address 192.168.1.253 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 104
R1(config-subif)#exit
R1(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.246
R1(config)#ip route 192.168.1.96 255.255.255.224 192.168.1.250
R1(config)#ip route 192.168.1.128 255.255.255.224 192.168.1.254
R1(config)#exit
```

Configure R2:

```
R2>enable
R2#configure terminal
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation frame-relay
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/0/0.101 point-to-point
R2(config-subif)#ip address 192.168.1.246 255.255.255.252
R2(config-subif)#frame-relay interface-dlci 101
R2(config-subif)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.245
```

Configure R3:

```
R3>enable
R3#configure terminal
R3(config)#interface serial 0/0/0
R3(config-if)#encapsulation frame-relay
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 0/0/0.101 point-to-point
```

```
R3(config-subif)#ip address 192.168.1.250 255.255.255.252
R3(config-subif)#frame-relay interface-dlci 101
R3(config-subif)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.249
```

Configure R4:

```
R4>enable
R4#configure terminal
R4(config)#interface serial 0/0/0
R4(config-if)#encapsulation frame-relay
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface serial 0/0/0.101 point-to-point
R4(config-subif)#ip address 192.168.1.254 255.255.255.252
R4(config-subif)#frame-relay interface-dlci 101
R4(config-subif)#exit
R4(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.253
```

Tunneling:

We can configure IPv6 tunnel across a IPv4 link. To accomplish this, we create a virtual Tunnel interface on both the routers. Tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure (a core network or the figure below). By using overlay tunnels, you can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. Overlay tunnels can be configured between border devices or between a border device and a host.

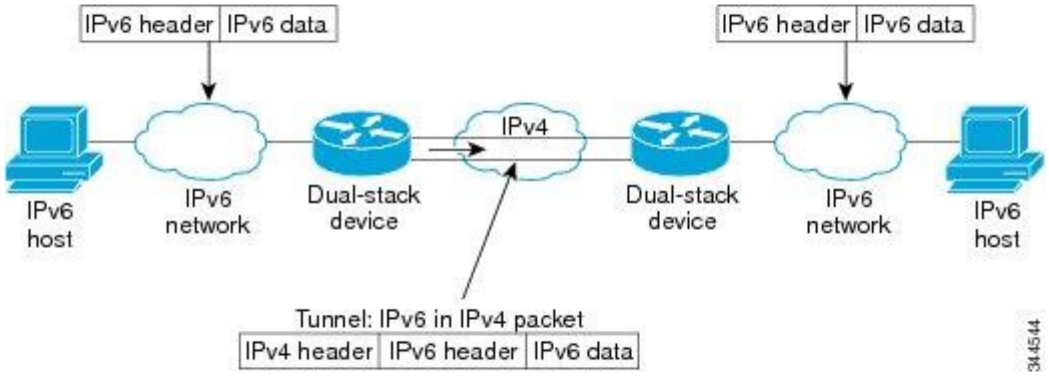


Figure 4.6: Tunneling explained Digrammatically

Configuration of IPv6 tunneling:

The following example configures a manual IPv6 tunnel between router A and router B. In the example, tunnel interface 0 for both router A and router B is manually configured with a global IPv6 address. The tunnel source and destination addresses are also manually configured.

Router A Configuration

```
interface ethernet 0
 ip address 192.168.99.1 255.255.255.0
interface tunnel 0
 ipv6 address 3ffe:b00:c18:1::3/127
 tunnel source ethernet 0
 tunnel destination 192.168.30.1
 tunnel mode ipv6ip
```

Router B Configuration

```
interface ethernet 0
 ip address 192.168.30.1 255.255.255.0
interface tunnel 0
 ipv6 address 3ffe:b00:c18:1::2/127
 tunnel source ethernet 0
 tunnel destination 192.168.99.1
 tunnel mode ipv6ip
```

Inter Virtual Lan:

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast_domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a **virtual local area network**, **virtual LAN** or **VLAN**.

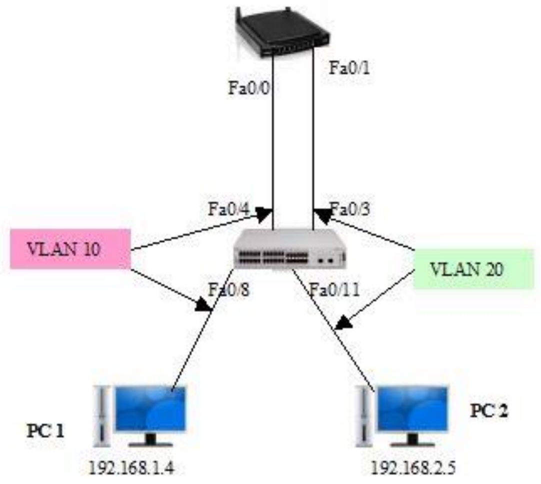


Figure 4.7: Configuration of intervlan

Example of switch SW1 interface configuration command:

```
 SW1#config t
SW1(config)#vlan 10
SW1(config-vlan)#vlan 20
SW1(config-vlan)#exit
SW1(config)#interface fa0/8
SW1(config-if)#switchport access vlan 10
SW1(config-if)#interface fa0/4
SW1(config-if)#switchport access vlan 10
SW1(config-if)#interface fa0/11
SW1(config-if)#switchport access vlan 20
SW1(config-if)#interface fa0/3
SW1(config-if)#switchport access vlan 20
SW1(config-if)#end
#SYS-5-CONFIG_I: configured from console by console
```

In the above example, interfaces F0/4 and F0/8 has been configured on VLAN 10 using the switchport access vlan 10 command. The same process is used to assign VLAN 20 to interface F0/3 and F0/11 on switch SW1.

Network Address Translation :

NAT allows private networks all over the world to use the same internal network numbers, while still allowing their users (or perhaps just some users) access to the Internet. The addresses that private networks around the world use are the RFC 1918 private addresses, sometimes referred to as “1918 addresses”.

The RFC 1918 Private Addresses

Class A	10.0.0.0 / 8
Class B	172.16.0.0 / 12
Class C	192.168.0.0 /16

Configuring the interfaces for Network Address Translation. The Ethernet network is the “inside” network; the Serial interface leading to the Internet is the “outside” network.

```
R3(config)#interface ethernet0
R3(config-if)#ip address 10.5.5.8 255.0.0.0
R3(config-if)#ipnat inside
R3(config-if)#interface serial0
R3(config-if)#ip address 210.1.1.1 255.255.255.0
```

Static NAT Configuration

Let’s take a look at a simple basic static NAT configuration:

```
pnat inside source static 10.1.1.1 170.46.2.2
interface Ethernet0
ip address 10.1.1.10 255.255.255.0
ipnat inside
interface Serial0
ip address 170.46.2.1 255.255.255.0
ipnat outside
```

Dynamic NAT Configuration

Dynamic NAT means that we have a pool of addresses that we will use to provide real IP addresses to a group of users on the inside. We do not use port numbers, so we have to have real IP addresses for every user trying to get outside the local network

Fault Tolerant Enterprise Network implemented in our project

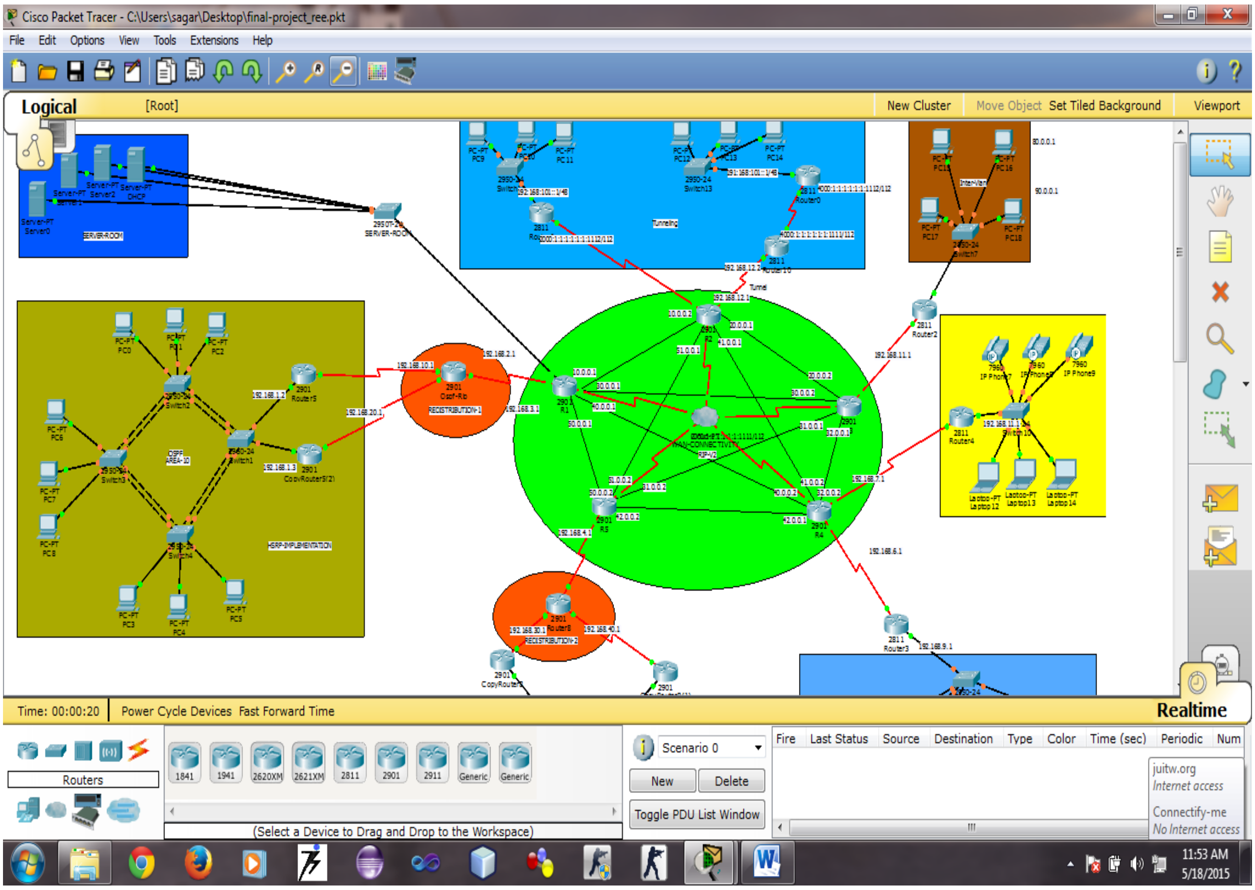
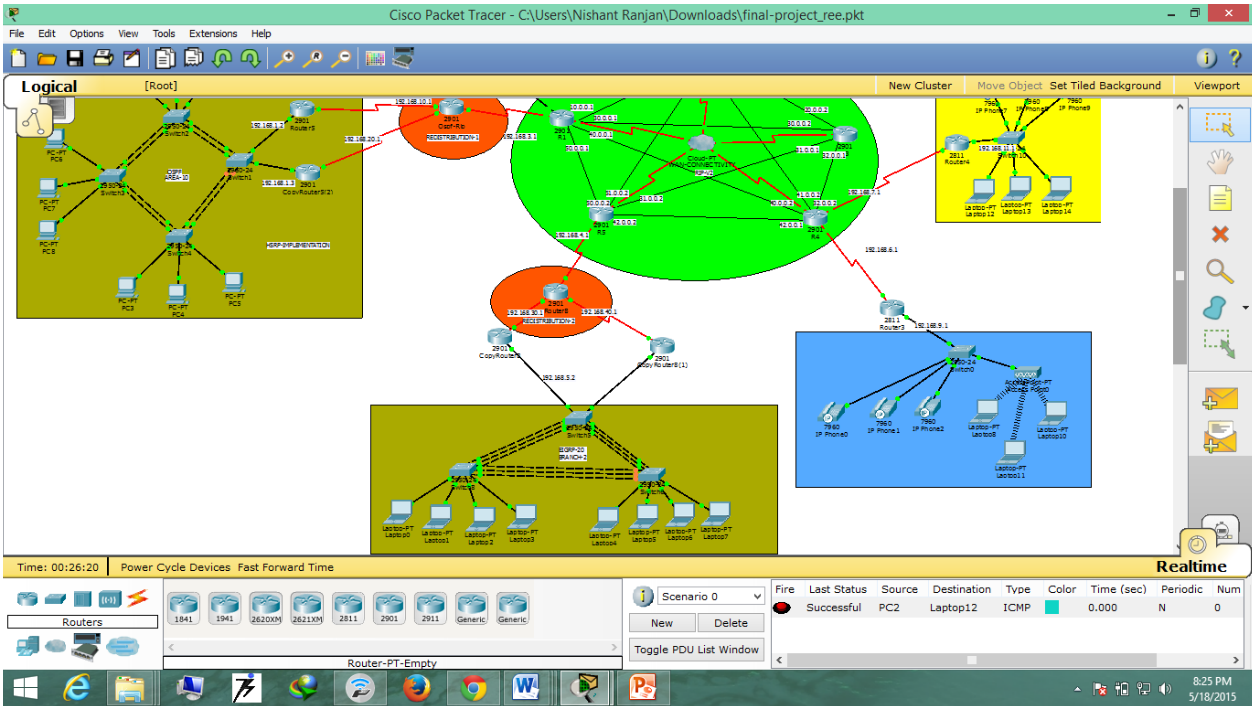


Figure 4.8 : Fault Tolerant Enterprise Network



Cisco Packet Tracer - C:\Users\Nishant Ranjan\Downloads\final-project_ree.pkt

Time: 00:26:20

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num
●	Successful	PC2	Laptop12	ICMP	🟦	0.000	N	0

Figure 4.9: Fault Tolerant Enterprise Network

CHAPTER 5
Conclusions And Results

Results:

- We have implemented various fault tolerant protocols such as Ether channeling, HSRP. Ether Channeling is a way of logically bundling the transmission link in order to load balance and HSRP (Hot Standby Routing Protocol) Once you have this protocol running the fear of a single point of failure is completely eliminated. A back up default gateway becomes available.
- We have configured an IPv6 "tunnel" across an IPv4 link. To accomplish this, we create a virtual tunnel interface on routers.
- We have also implemented redistribution between various fast convergence routing protocols.
- We have established DHCP on routers and DHCP server to distribute static and dynamic IP addresses
- Frame relay increases the performance of data switching, the network achieves connectivity of endpoints. In other words, it can communicate with any other endpoint so long as there is a pre-established connection identifier with the use of virtual circuits.

Detailed Conclusion and Further Study:

- Redundancy can prove to be very helpful in order to reduce link related faults. Anytime a link goes down, a backup link must be available in order for communication to take place. Redundancy is done at

- Looping is extremely helpful in order to avoid node related faults. When looping is done in a smart way, loops can be very helpful in avoiding node related faults. Once a node goes down, only the devices directly connected to the faulty node loose connection.

- Ether channel can be used to handle large amount of data traffic. At network segments where traffic is relatively high we can use Link Aggregation. A method of logically bundling the Ethernet cables. This process is most commonly known as Ether Channel.

- Hot Standby Routing Protocol removes single point of failures. HSRP is a way of achieving router redundancy. This protocol removes the most common problem of single point of failure. When HSRP is running on the routers directly connected to the network segment, the default gateway is actually a virtual interface.

- High availability can be achieved by using Fast convergence techniques. Fast convergence at switch level can be achieved by using Rapid Spanning Tree Protocol. At router level, fast convergence is achieved by using dynamic routing protocols. A Network Designer must choose the best of the best routing protocols when it comes to designing an Enterprise Network.

Refrences :

1. **http://www.networkcomputing.com/netdesign/faultintrob.html**
2. **http://www.packettracernetwork.com/tutorials/hsrp-configuration-new.html**
3. **https://www.youtube.com/watch?v=s4xYzYLvh60**
4. **https://www.youtube.com/watch?v=XhdC39OqpFg**
5. **file:///C:/Program%20Files%20(x86)/Cisco%20Packet%20Tracer%206.0.1/help/default/inde**
6. **http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=628355**
7. **https://www.netacad.com/about-networking-academy/packet-tracer**
8. **http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4768747**