**Certificate**

I hereby certify that the work which is being presented in the Seminar Report entitled **“CAMPUS NETWORK”** in partial fulfillment of the requirements for the award of the **Bachelor of Technology** in **Information technology** and submitted to the Department of Computer Science and Information Technology **Ideal Institute of Technology, Ghaziabad** (UP), is an authentic record of my seminar carried out during sixth semester under the supervision of **Mr. *Atul Kumar Singh* (Assistant Professor),** Department of Information Technology, Ideal Institute of Technology Ghaziabad and **Mr.Amit Kumar Jaiswal** (Associate Prof. & Head), Department of Computer Science & Engineering and Information Technology, Ideal Institute of Technology Ghaziabad for his guidance of my seminar. With his knowledge and experience, he has guided me to successfully achieve my seminar objective

**Date:**

Signature of Candidate

**Student Name: Ankit Srivastav**

Roll No :1402813002

4th Year (B.Tech)

This is to certify the above statement made by the candidate is correct and true to the best of my knowledge*.*

***Date:***

***Signature of Supervisor Signature of Supervisor & HOD Signature of External Examiner***

**Mr. Atul Kumar Singh Mr. Amit Kumar Jaiswal**

(Assistant Professor) (Associate Professor)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ABSTRACT** | | | | | **iii** |
| **List of Figures** | | | | | **iv-v** |
| **List of Tables** | | | | | **vi** |
| **ACKNOWLEDGMENT** | | | | | **vii** |
|  | | |  | |  |
| 1. | | | **INTRODUCTION** | | 7-16 |
|  | | | 1.1. WHAT IS A NETWORK? | | 7 |
|  | | | 1.2. NEED FOR COMPUTER NETWORKS | | 8 |
|  | | | 1.3. TYPES OF NETWORKS | | 9 |
|  | | | 1.4. APPLICATIONS | | 15 |
| 2. | | | **PROBLEM FORMULATION** | | **17-19** |
|  | | | 2.1. PROBLEM STATEMENT | | 17 |
|  | | | 2.2. IMPORTANT TERMS | | 18 |
|  | | | 2.3. THE SOLUTION | | 19 |
| **3.** | | | **SOFTWARE PACKAGE USED** | | **20-23** |
| **4.** | | **CH-1 : IP ADDRESSING** | | **24-26** | | |
|  | | | 4.1. WHAT IS IP ADDRESS | | 24 | | |
|  | | | 4.2. CLASSES OF IP ADDRESSES | | 24 | | |
|  | | | 4.3. TYPES OF IP ADDRESS | | 25 | | |
|  | | | 4.4. SUBNET MASK | | 25 | | |
|  | | | 4.5. SUBNETTING | | 26 | | |
|  | | | 4.6. VARIABLE LENGTH SUBNET MASK (VLSM) | | 26 | | |
| **5. CH-2: ROUTERS & THEIR CONFIGURATION** | | | **27-32** | | |
| 5.1. WHAT ARE ROUTERS | | | 27 | | |
| 4.2. FEATURES OF ROUTERS | | | 27 | | |
| 5.3. ROUTER INTERFACES | | | 28 | | |
| 5.4. ROUTER MEMORY ELEMENTS | | | 29 | | |
| 5.5. WORKING MODES OF ROUTER | | | 29 | | |
| 5.6. ROUTER CONFIGURATION | | | 30 | | |

|  |  |  |
| --- | --- | --- |
| **6.** | **CH-3 : ROUTING** | **33-45** |
|  | 6.1. WHAT IS ROUTING? | 33 |

|  |  |
| --- | --- |
| 6.2. STATIC ROUTING | 34 |
| 6.3. DEFAULT ROUTING | 35 |
| 6.4. DYNAMIC ROUTING | 36 |
| 6.5. ROUTING PROTOCOLS BASICS | 37 |
| 6.6. RIP (ROUTING INFORMATION PROTOCOL) | 39 |
| 6.7. IGRP (INTERIOR GATEWAY ROUTING PROTOCOL) | 42 |
| 6..8. EIGRP (ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL) | 44 |
| 6.9. OSPF (OPEN SHORTEST PATH FIRST) | 45 |

|  |  |  |
| --- | --- | --- |
| **7. CH -4 : VLAN & SECURITY 45-48** | |  |
| **8. NETWORK DESIGN & IMPLEMENTATION 49-56** | | **51-57** |
| **9.** | **FUTURE SCOPE 57** |  |
| 10. | **REFERENCES 58** |  |

ABSTRACT

Campus network in all the Deptt. of the university/campus is quite important this days as used by student for their study purposes and for teacher for teaching purposes etc.As such a computer network for campus ideally requires a reliable and scalable network comprising of vendor neutral infrastructure both in terms of hardware and software. The network should be able to balance load at times of peak demand and failsafe should be built in the network to withstand minor faults that may affect some sections of the network. Therefore it should have redundant paths built into it so that the network can withstand most of the fluctuations and faults that are encountered by businesses every day.

Moreover the network in itself should be automatically configurable to a greater extend by having provision for dynamic allocation of IP configurations using DHCP.

Since the campus network is quite important now days as needed for education purposes so it should have a high speed connection that allows for faster data rates at relatively inexpensive rates to save taxpayers money.

|  |  |
| --- | --- |
| **List of Figures** | **Page** |
| Fig 1.1 – Computer network | 8 |
| Fig 1.2 – Client-Server Model | 9 |
| Fig 1.3 – Peer-to-Peer Model | 10 |
| Fig 1.4 – MAN composed of various LANs | 11 |
| Fig 1.5 – WAN composed of various LANs and MANs | 12 |
| Fig 1.6 – Mesh Topology | 13 |
| Fig 1.7 – Bus Topology | 13 |
| Fig 1.8 – Star Topology | 14 |
| Fig 1.9 – Ring Topology | 15 |
| Fig 3.1 – Cisco Packet Tracer | 20 |
| Fig 3.2 – Cisco Packet Tracer – Initial Screen | 21 |
| Fig 3.3 – Router Configuration Options in Cisco Packet Tracer | 22 |
| Fig 3.4 – End Device Configuration Options in Cisco Packet Tracer | 23 |
| Fig 4.1 – IP Address Example | 24 |
| Fig 4.2 – Network and Host Bits | 24 |
| Fig 5..1 – Router Symbol | 27 |
| Fig 5.2 – Router Ports | 28 |
| Fig 5.3 – Router Ports & Modules | 30 |
| Fig 5.4 – Router Configuration on Cisco Packet Tracer | 31 |
| Fig 6.1 – Static Routing on Cisco Packet Tracer | 34 |
| Fig 6.2 – Default Routing on Cisco Packet Tracer | 36 |
| Fig 6.3 – Network for RIP Configuration in Cisco Packet Tracer | 38 |
| Fig 6.4 – Checking RIP Configuration in Cisco Packet Tracer | 40 |
| Fig 6.5 – Network for EIGRP in Cisco Packet Tracer | 41 |
| Fig 6.6 – Checking RIP Configuration in Cisco Packet Tracer | 42 |
| Fig 6.7 – Network for OSPF in Cisco Packet Tracer | 44 |
| Fig 6.8 – Checking OSPF Configuration in Cisco Packet Tracer | 45 |
| Fig 8.1 – Initial Network Layout | 49 |
| Fig 8.2 – Connecting Devices with Suitable Cables | 49 |
| Fig 8.3 – Interfacing Router Ports | 50 |

|  |  |  |  |
| --- | --- | --- | --- |
| Fig 8.4 – Displaying Router Interfaces and Link States | | | 50 |
| Fig 8.5 – Configuring DHCP in CLI mode of the server | | | 51 |
| Fig 8.6 | – Requesting DHCP configurations on an End Device | | 51 |
| Fig 8.7 | – Applying Routing on the Routers | | 52 |
| Fig 8.8 | – Checking applied Routing on the Routers | | 52 |
| Fig 8.9 | – Configuring Frame Relay on the Sub-interfaces created on the Routers | | 53 |
| Fig 8.10 – Checking Configured Sub-interfaces on the Routers | | | 53 |
| Fig 8.11 | | – Configuring DLCI on the Routers | 53 |
| Fig 8.12 | | – Verifying DHCP on the Devices | 55 |
| Fig 8.13 (a) & (b) – Verifying routing on Deptt. routers | | | 56 |
| Fig 8.14 | | – Verifying Packet Delivery among different Deptt.s | 56 |

|  |  |  |
| --- | --- | --- |
|  | **List of Tables** | **Page** |
|  |  |  |
| Table 1 | – Classes of IP Address | 24-25 |
| Table 2 | – AD values for various Routing Protocols | 38 |

**Acknowledgement**

Successfully completing any task gives us satisfaction as well as internal strength for future problems but the person alone has never existed. He is truly accompanied by few people. They use to give the person support as well as suggestion to successfully complete his work. So I am pleasured in thanking all such people who motivates me and provides there kind support at all stages of my research work.

Firstly, I would like to honor my institute *“****Ideal Institute of Technology, Ghaziabad****”.* Here I have been provided with a workplace to learn recent techniques and conceptual background to strengthen my programming and professional skills.

I am very much grateful to ***Dr. Prabal Chakrabarti, (Director) and Mr. Amit Kumar Jaiswal (Associate Professor & Head of*** ***Department of Computer Science & Engineering & Information Technology) Ideal* Institute of Technology, Ghaziabad,** for his helpful attitude and encouragement in time to time to excel in our studies.

I would like to express my sincere heartfelt gratitude to my honourable, esteemed supervisor ***Mr. Amit Kumar Singh*** (Assistant professor), Department of Computer Science and Engineering for his kind and valuable guidance for the successful completion of the presentation work. I am glad to work under his supervision.

Furthermore, I am thankful to, all faculty members for motivating me and to the ***Staffs of computer labs***in the department for providing excellent valuable facility as well as issuing me a computer system of good configuration and providing regular maintenance.

I would like to extend special thanks to all my batch mates for their love, encouragement and constant support.

Last but not least I would like to thank my parents for supporting me to complete my presentation report in all ways.

Ankit Srivastav

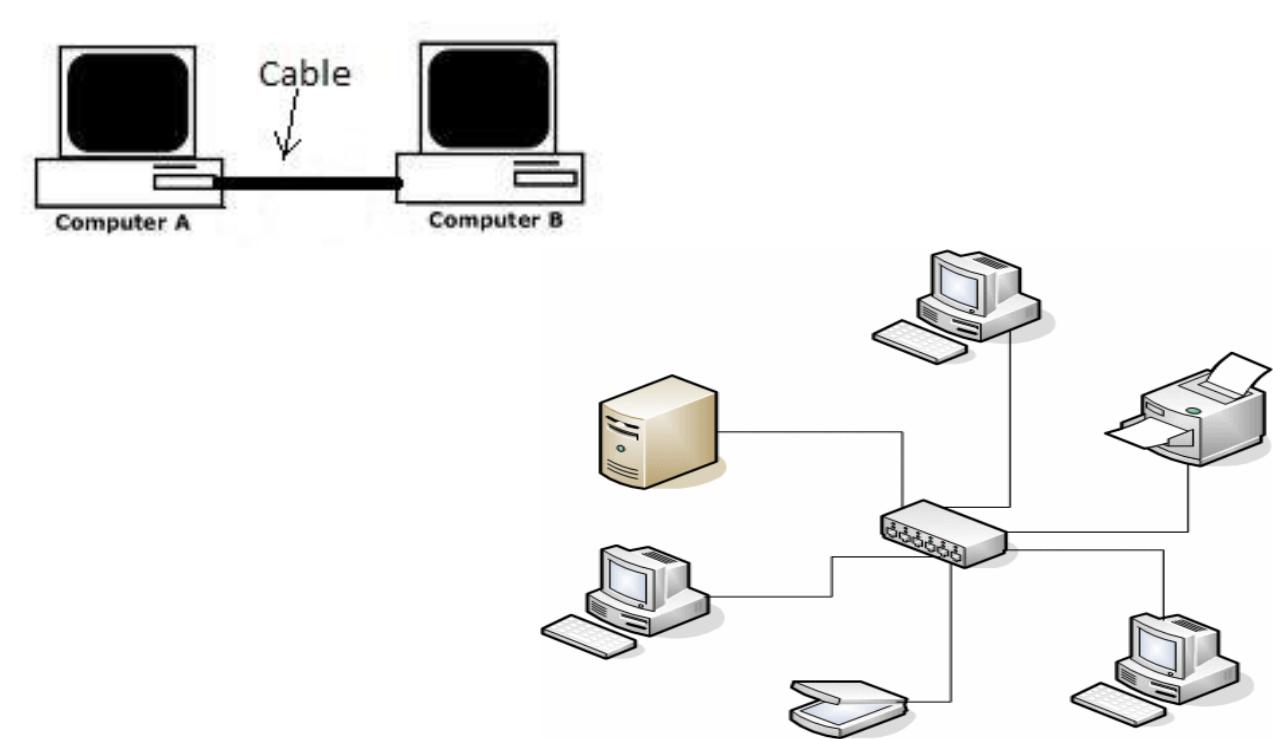
1402813002

**INTRODUCTION**

The concept of networking can simply be described as a network in action. A network in turn is, simply put an interconnected set of some objects. Most of us are familiar with the Radio, Television, Railway, Highway, Bank and other types of networks. However the network that impacts our life is the most on a day-to-day basis is the **Computer network**. By computer network we mean an interconnected set of autonomous (or functionally independent) computers. These computers exchange information with each other through the communication network system. Computer networks have emerged as a result of the convergence of two technologies of this century- Computer and Communication. The consequence of this revolutionary merger is the emergence of an integrated system that transmit all types of data and information.

**1.1 What is a network?**

A network is a connection between terminals, computers, servers, and components which allows for the easy flow of data and use of resources between one another. Different network examples include telephone network, cable TV. network, transport network of a city etc.

Consequently a computer network consists of a group of computers and devices which are connected with each other. It allows the computers to communicate with each other and share resources which include information, software and peripheral devices such as printers, scanners. A simple computer network is shown in the figure 1.1

**Fig 1.1 – Computer network**

Thus a computer network may consists of various computer and devices connected using a host of media such as radio waves, wires (Ethernet Cable), routers, leased lines, infrared, Bluetooth, optical fiber etc.

**1.2 Need for Computer Networks**

When computers are joined in a network it helps the users to share resources and communicate with each other. Computer networks can be used for many purposes:

* Sharing hardware resources such as network printers, devices etc.

In a relatively large workplace investment into hardware can be minimized by using the benefits of networking. In such an environment rather than buying hardware such as printers, optical drives, etc. we can buy a very limited number of such peripheral devices and set them up as network devices for everyone to use. This also makes more sense considering the fact that these devices are not used continuously and are seldom in use. A network printer can be used by 30- 40 workstations. This is also more energy efficient along with being more economical. This also reduces the setup and troubleshoot time (which will be discussed in subsequently). An example can be of a computer lab in a school or a college. Rather than buying complete computer systems consists of CPUs etc., a central server can be set up and all the individual systems can consists of just a customary I/O devices (monitor, Keyboard, Mouse) and a simple network interface. All the softwares can be installed on a central server that contains the master copy of all the softwares which can then be maintained at one single place.

* Sharing files, folders, data and information.

Growing connection speeds and reliability has resulted in better collaboration with advent of cloud technology. Now it is possible for people present at multiple locations around the globe to collaborate and work on a single project or a file on a real time basis. This also helps backup multiple copies of a file and contribute greatly to information security.

Simply put, a sales person in New York might sometimes need access to a product inventory database in Singapore. In other words, the mere fact that a user happens to be 15,000 km away from his data should not prevent him from using the data as though they were local. This goal may be summarized by saying that it is an attempt to end the ‘’tyranny of geography.’’

Apart from providing security, better networking also results in real time flow of information that makes a number of modern day marvels (such as ATMs, etc.) possible. This aspect of networking has left such an impression on present day civilization that it has led to present times being called as information age.

* + Sharing software applications.

Another aspect of networking is the ability to share software applications. This has the added the advantage of saving installation time as well as cost. Often software developers supply network as well as standalone licenses. Network licenses allow network administrators to install softwares on the network servers rather than installing a separate copy on individual systems. This also ensures compatibility regarding the softwares used by a team or a group of people.

From the perspective of security this helps as important updates can be delivered to all and vulnerabilities can be patched before it may be exploited by a malicious attacker.

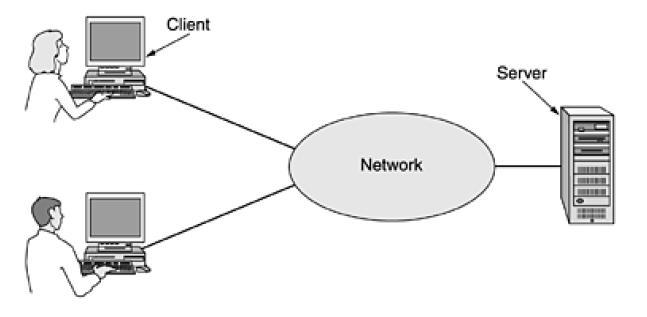
**1.2 Types of Networks**

Networks can be divided into various categories based on certain metrics such as network configuration, network topology, area covered etc.

On the basic of network configuration, networks are grouped as belonging to either of two models:

 Client-Server Model

This model can be illustrated by imagining a company’s information system as consisting of one or more databases and some number of employees who need to access them remotely. In this model, the data are stored on powerful computers called servers. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simpler machines, called clients, on their desks, with which they access remote data, for example, to include in spreadsheets they are constructing.



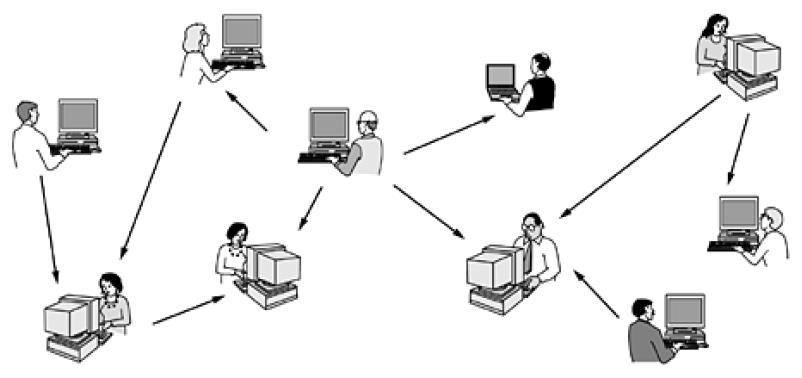
**Fig 1.2 – Client-Server Model**

It is widely used and forms the basis of much network usage. It is applicable when the client and server are both in the same building (e.g., belong to the same company), but also when they are far apart.

If we look at the client-server model in detail, we see that two processes are involved, one on the client machine and one on the server machine. Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back

* 1. reply.
* Peer to Peer Model

Another type of networking model is the peer to peer model. In this model, individuals who form a loose group can communicate with others in the group, as shown in Fig. 1.3. Every person can, in principle, communicate with one or more other people; there is no fixed division into clients and servers.



**Fig 1.3 – Peer-to-Peer Model**

In a network based on point-to-point communication the end devices that wish to communicate are called *stations*. The switching devices are called *nodes*. Some Nodes connect to other nodes and some to attached stations. It uses FDM or TDM for node-to-node communication. There may exist multiple paths between a source-destination pair for better network reliability. The switching nodes are not concerned with the contents of data. Their purpose is to provide a switching facility that will move data from node to node until they reach the destination.

As a general rule (although there are many exceptions), smaller, geographically localized networks tend to use broadcasting, whereas larger networks normally use are point-to-point communication.

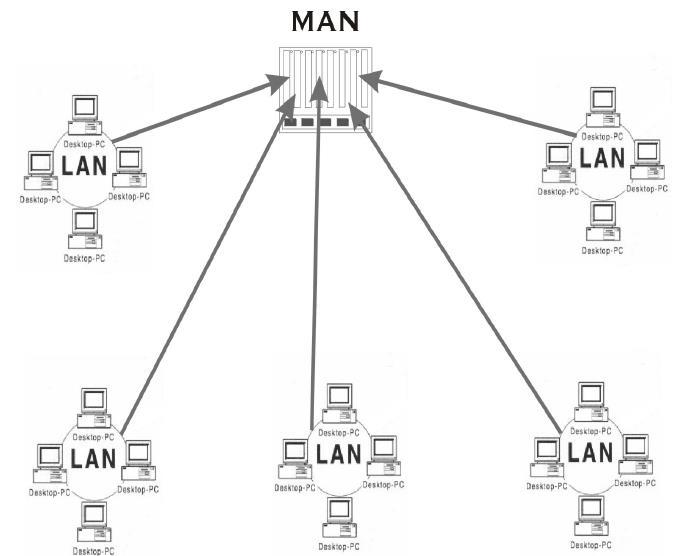
Similarly on the basis of scale of the network (area encompassed by it), networks can be

classified as

* LAN

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building. Rarely are LAN computers more than a mile apart. In a typical LAN configuration, one computer is designated as the file server. It stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The workstations can be less powerful than the file server, and they may have additional software on their hard drives. On most LANs, cables are used to connect the network interface cards in each computer.

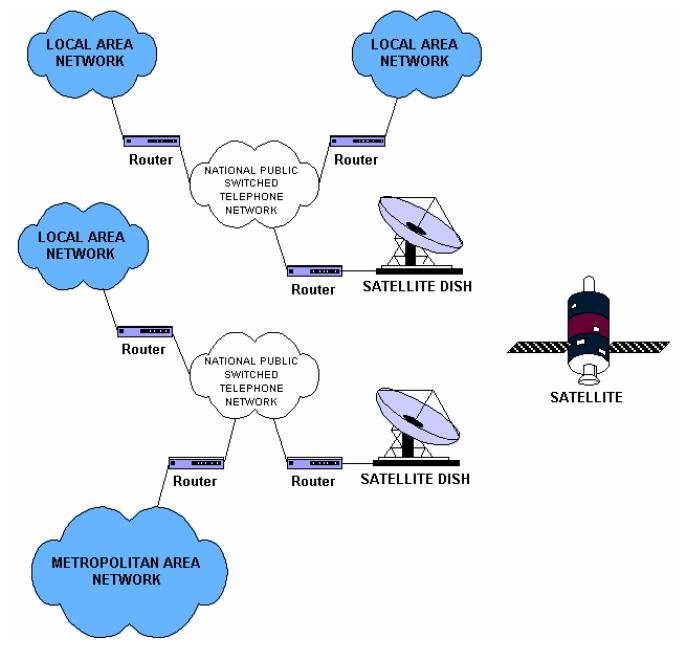
* MAN

A Metropolitan Area Network (MAN) covers larger geographic areas, such as cities or school districts. By interconnecting smaller networks within a large geographic area, information is easily disseminated throughout the network. Local libraries and government agencies often use a MAN to connect to citizens and private industries.

**Fig 1.4 – MAN composed of various LANs**

WAN

Wide Area Networks (WANs) connect larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of network. Using a WAN, schools in Florida can communicate with places like Tokyo in a matter of minutes, without paying enormous phone bills. A WAN is complicated. It uses multiplexers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN or a MAN.



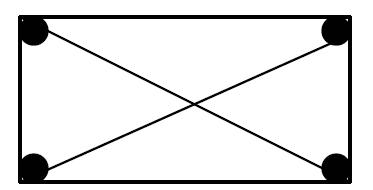
**Fig 1.5 – WAN composed of various LANs and MANs**

Various network topologies that are in use are:

* Mesh

In this topology each node or station is connected to every other station as shown in figure. The key characteristics of this topology are as follows:

* + Fully connected
  + Robust – Highly reliable
  + Not flexible

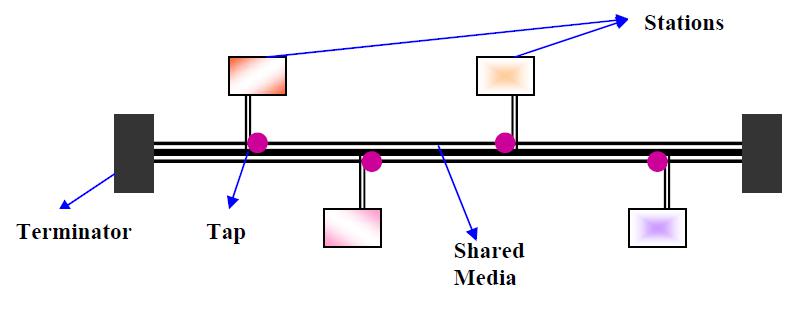


 Poor expandability **Fig 1.6 – Mesh Topology**

Two nodes are connected by dedicated point-point links between them. So the total number of links to connect n nodes = n(n-1)/2; which is proportional to n2 . Media used for the connection (links) can be twisted pair, co-axial cable or optical fiber. With this topology there is no need to provide any additional information that is from where the packet is coming, along with the packet because two nodes have a point-point dedicated link between them. And each node knows which link is connected to which node on the other end. Mesh Topology is not flexible and has a poor expandability as to add a new node n links have to be laid because that new node has to be connected to each of the existing nodes via dedicated link.

* Bus

In Bus Topology, all stations attach through appropriate hardware interfacing known as a *tap*, directly to a linear transmission medium, or bus as shown in Fig. 5.7 Full-duplexoperation between the station and the tap allows data to be transmitted onto the bus and received from the bus. A transmission from any station propagates the length of the medium in both directions and can be received by all other stations. At each end of the bus there is a *terminator*, which absorbs any signal, preventing reflection of signal from the endpoints. If the terminator is not present, the endpoint acts like a mirror and reflects the signal back causing interference and other problems.



**Fig 1.7 – Bus Topology**

Key Characteristics of this topology are:

* Flexible
* Expandable
* Moderate Reliability
* Moderate performance

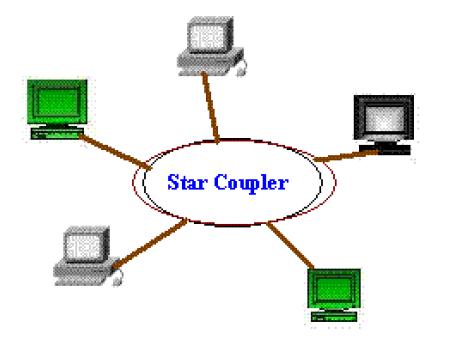
A shared link is used between different stations. Hence it is very cost effective. One can easily add any new node or delete any node without affecting other nodes; this makes this topology easily expandable.

* Star

In the star topology, each station is directly connected to a common central node as shown in Fig. 5.8 Typically, each station attaches to a central node, referred to as the *star coupler*, via two point-to-point links,

one for transmission and one for reception. Key features:

* + High Speed
  + Very Flexible
  + High Reliability
  + High Maintainability



**Fig 1.8 – Star Topology**

In general, there are two alternatives for the operation of the central node.

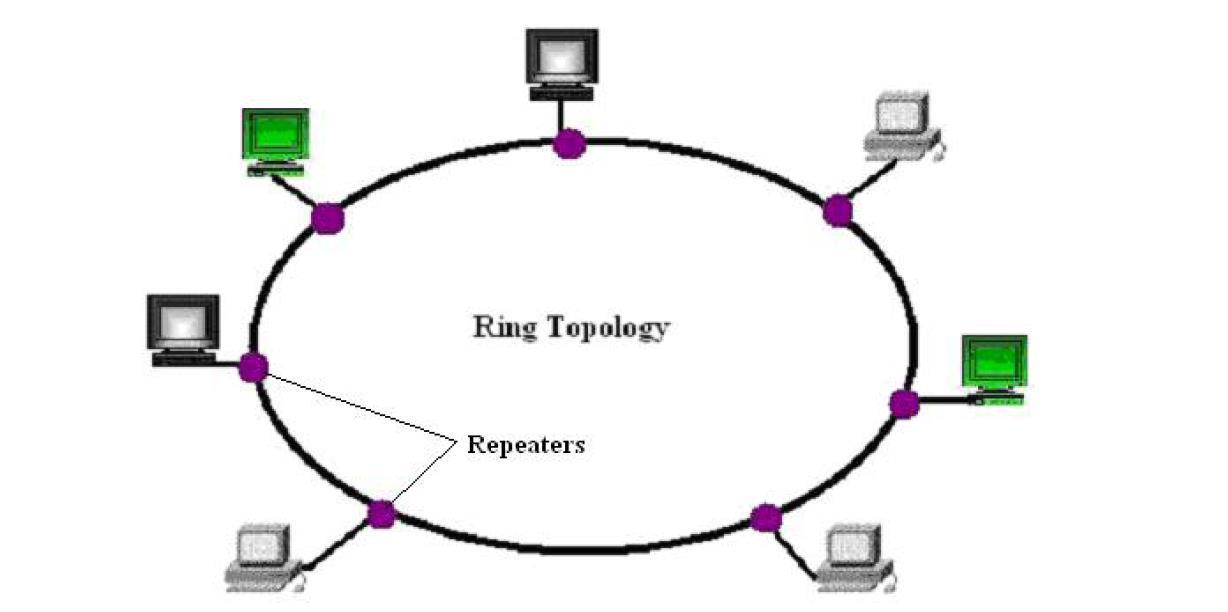
* One approach is for the central node to operate in a broadcast fashion. A transmission of a frame from one station to the node is retransmitted on all of the outgoing links. In this case, although the arrangement is physically a star, it is logically a bus; a transmission from any station is received by all other stations, and only one station at a time may successfully transmit. In this case the central node acts as a *repeater*.
* Another approach is for the central node to act as a frame-switching device. An incoming frame is buffered in the node and then retransmitted on an outgoing link to the destination station. In this approach, the central node acts as a *switch* and performs the switching or routing function. This mode of operation can be compared with the working of a telephone exchange, where

the caller party is connected to a single called party and each pair of subscriber

who needs to talk have a different connection.

* Ring

In the ring topology, the network consists of a set of repeaters joined by point-to-point links in a closed loop as shown in Fig. 5.1.5. The repeater is a comparatively simple device, capable of receiving data on one link and transmitting them, bit by bit, on the other link as fast as they are received, with no buffering at the repeater. The links are unidirectional; that is data are transmitted in one direction only and all are oriented in the same way. Thus, data circulate around the ring in one direction (clockwise or counterclockwise).



**Fig 1.9 – Ring Topology**

Each station attaches to the network at a repeater and can transmit data onto the network through that repeater. As with the bus and tree, data are transmitted in frames.

As a frame circulates past all the other stations, the destination station recognizes its address and copies the frame into a local buffer as it goes by. The frame continues to circulate until it returns to the source station, where it is removed. Because multiple stations share the ring, medium access control is needed to determine at what time each station may insert frames.

**1.4 Applications**

In a short period of time computer networks have become an indispensable part of business, industry, entertainment as well as a common-man’s life. These applications have changed tremendously from time and the motivation for building these networks are all essentially economic and technological.

Initially, computer network was developed for defense purpose, to have a secure communication network that can even withstand a nuclear attack. After a decade or so, companies, in various fields, started using computer networks for keeping track of inventories, monitor productivity, communication between their different branch offices located at different locations. And now after almost two decades, computer networks have entered a new dimension; they are now an integral part of the society and people.

The main area of applications can be broadly summarized into following categories:

**Scientific and Technical Computing**

Client Server Model, Distributed Processing Parallel Processing, Communication Media

**Commercial**

Advertisement, Telemarketing, Teleconferencing, Worldwide Financial Services

**Network for the People**

Telemedicine, Distance Education, Access to Remote Information, Person-to-Person Communication, Interactive Entertainment

**PROBLEM FORMULATION**

We classify the task into easy steps based on priorities that we wish to assign to different variables. First of all we define the various terms that we will use while discussing the problem and working out a solution.

**2.1 Problem Statement**

The main problem that we are tackling is about providing users with a well-established and running ipv4 network topology containing routers and switches connecting various departments of campus to other departments as well as other offices. Each department needs be equipped with servers of its own which can be accessed by other departments as well so as to form an extended memory repository as well as form a failsafe in case network load increases at any specific department. These servers are also to be used for website hosting and their management. Also high bandwidth connectivity is to be provided for communication among the deptt.. Apart from this we wish to provide an auto mated IP management system using DHCP (Dynamic Host Configuration Protocol).if hosts are at diff. network then grouping hosts according to their resorce need necessitates the laber of relocating nodes or rewiring data links.

.

**2.2 Terms**

* + **User**

User refers to the officials as well as other contractors, consultants etc. associated with the Northern Deptt. of Indian Railways. The aim of the project is to provide them with a highly reliable and fast network so that they can dispense their duties efficiently and with ease.

* + **Bandwidth**

Bandwidth is also defined as the amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second.

* + **Latency**

Network latency is an expression of how much time it takes for a packet of data to get from one designated point to another. In some environments, latency is measured by sending a packet that is returned to the sender; the round-trip time is considered the latency.

* **Router**

Also referred to as layer 3 switches, routers are used to connect networks together and route packets of data from one network to another. Basically, router functions can be summarized as Packet switching, Packet Filtering, Internetwork communication and Path selection.

* **Routing**

Routing is the process of selecting best paths in a network. In the past, it also meant forwarding network traffic among networks. However, that latter function is better described as forwarding.

* **Switch**

The main purpose of a switch is to optimize the performance of a network, providing more bandwidth for the LAN’s users. And switches don’t forward packets to other networks as routers do. Instead they only switch frames from one port to another within the switched network.

* **DHCP**

DHCP stands for Dynamic Host Configuration Protocol. It succeeded BOOTP (Bootstrap Protocol) and is used to assign IP Addresses, Subnet Mask, DNS server etc. DCHP helps in automating IP address management.

* **Server**

A server is an instance of a computer program that accepts and responds to requests made by another program; known as a client. Less formally, any device that runs server software could be considered a server as well. Servers are used to manage network resources.

* **Frame-Relay**

A packet-switched technology that emerged in the early 1990s, Frame Relay is a successor to X.25 and is a Data Link and Physical layer specification that provides high performance. It is more cost effective than point-to-point links, and can typically run at speeds of 64Kbps up to 45Mbps. It provides dynamic bandwidth allocation and congestion control.

**2.3 The Solution**

The Solution lies in the proper selection among the already prevalent routing protocols and hardware. We have based our model in Cisco Packet Tracer software which is a simulation software provided by Cisco and thus have used on Cisco hardware, however this is far from reality as a network of this importance cannot be held hostage to the monopoly of a single vendor. As such the goal is to design such a network which is vendor neutral and can be scaled up according the needs of the client (here, Campus Network).

Effort has therefore been made to design a robust network which is open in a general sense. For routing information, we have chosen OSPF (Open Shortest Path First) among other protocols such as RIP, EIGRP, etc. The main advantage being its open nature i.e. compatible with all vendors as well as other advantages such as ease of scalability and no hop limitations. For providing connectivity between different department of the network, we have used distribution point connectivity providing a meshed network of point-to-point connections between all the departments. ipv4 to ipv6 conversion is used to make network more flexible . virtual lan is used so host can switch from one network to other if need.

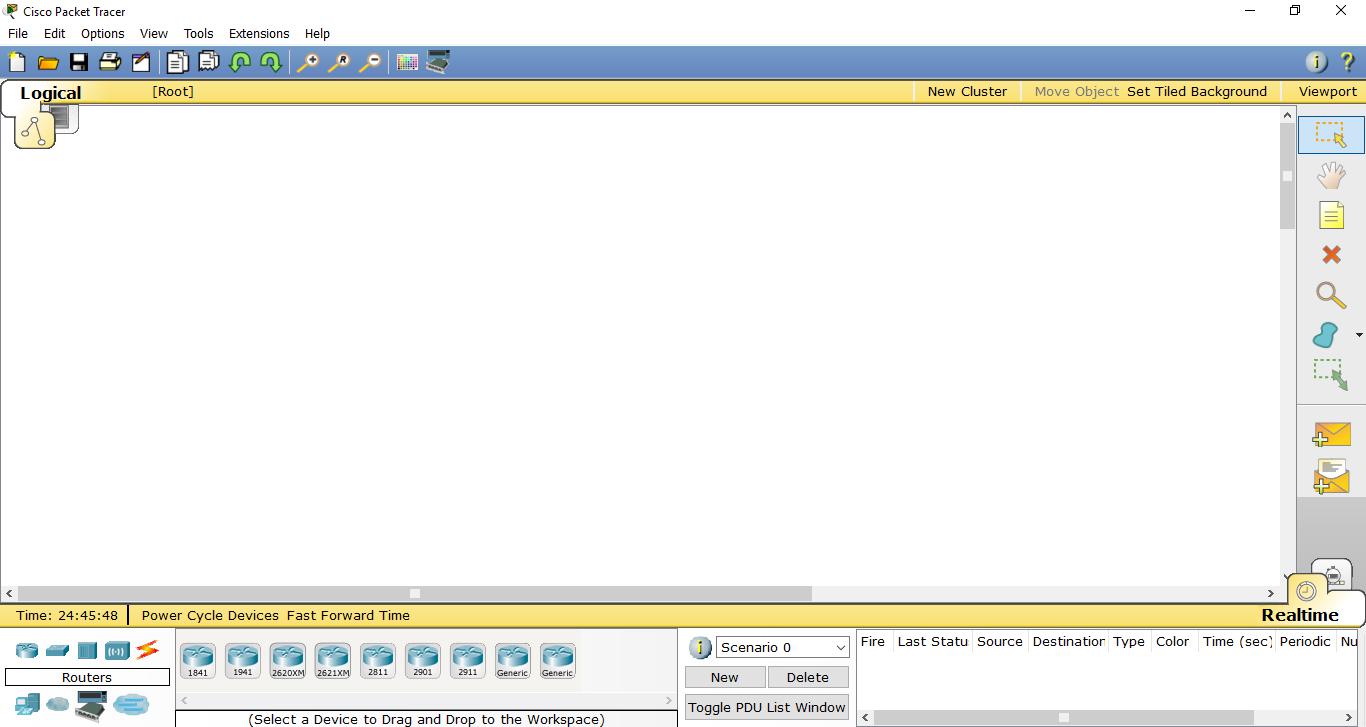
**SOFTWARE PACKAGE USED**

For the purpose of simulation and of designing the network infrastructure for our project we have used the Cisco Packet Tracer. Packet Tracer is a cross-platform network simulator designed by Cisco Systems to run on Mac OS, Linux and Microsoft Windows. A similar Android app is also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a “cable” item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BDP.

Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs.

**Fig 3.1 – Cisco Packet Tracer**

**THE WORKSPACE**



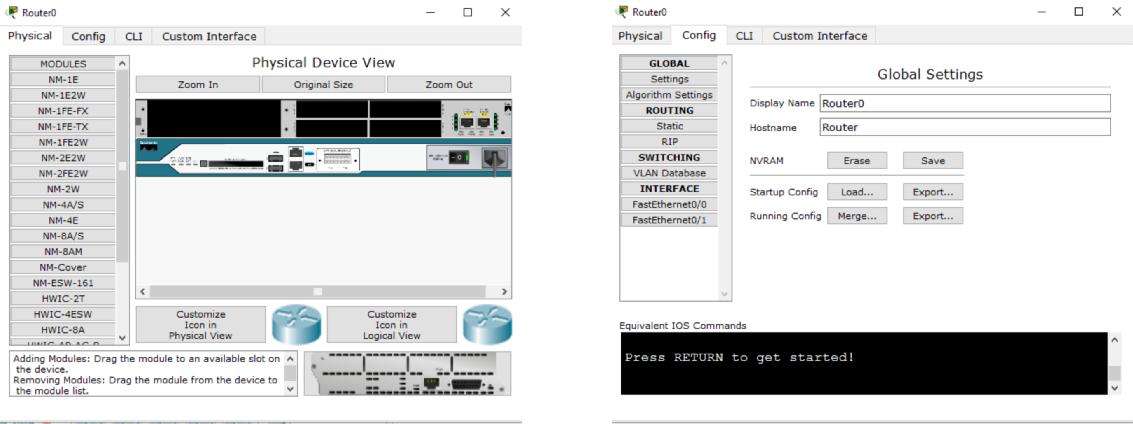
**Fig 3.2 – Cisco Packet Tracer – Initial Screen**

On startup, Cisco Packet Tracer looks like Fig 4.2. On the top are menu tabs as well as some GUI options such as New, Open, Save, Print, Undo, Redo, Zoom in, Zoom Reset, Zoom Out etc.

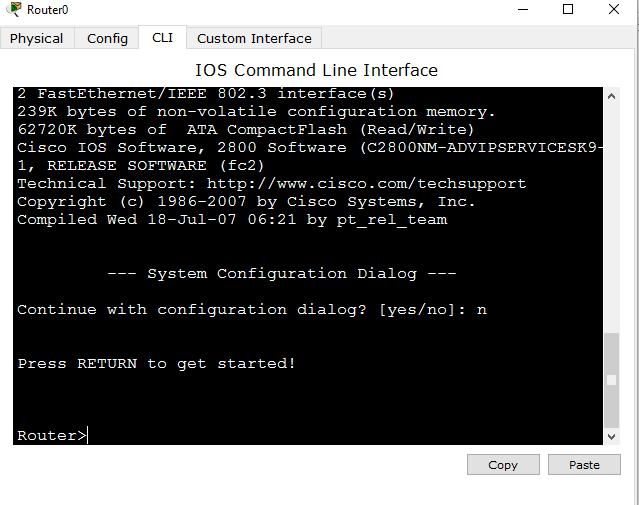
On the left side of the screen, are Select, Move Layout, Place Note, Delete, Add Simple PDU, Add Complex PDU etc.

Below the screen, on the leftmost side we can select various hardware devices such as Routers, Switches, Hubs, WAN, End Devices etc. On clicking on these hardware types, the box net to it shows the various devices (both Cisco devices and Generic) that are part of these device categories. On the rightmost side we can see the status of packets that have been successful or unsuccessful along with the Source, Destination, Type etc.

Now when any device is placed in the workspace and clicked on, we have the option to configure its physical configuration as well as Software configurations. For example in the case of a router, on clicking it window in Fig 4.3 is displayed.



(a) Physical (b) Config



(c) Command Line Interface – CLI

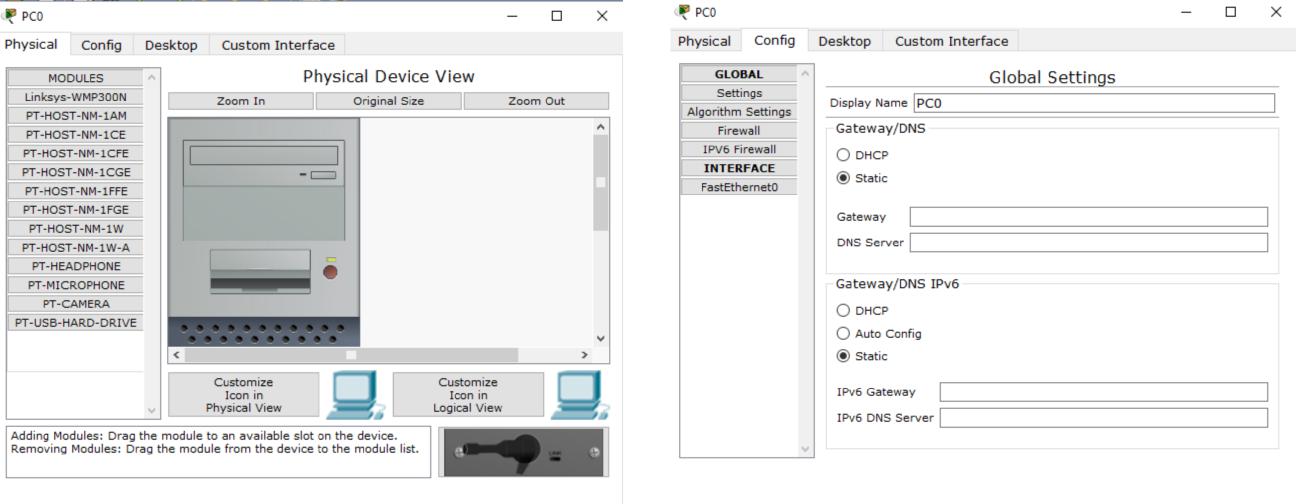
**Fig 3.3 – Router Configuration Options in Cisco Packet Tracer**

Here we have the following tabs –

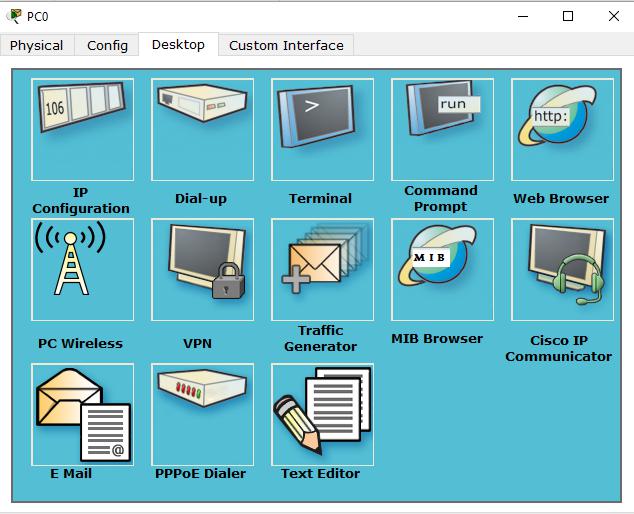
Physical (for adding/removing modules physically) Config (GUI mode for configuring Router)

CLI (Command Line Interface) – Command Line mode for configuring Device.

Similarly in the case of end devices like PCs, Laptops or Servers, windows in Fig 4.4 is displayed



(a) Physical (b) Config



(c) Desktop

**Fig 3.4 – End Device Configuration Options in Cisco Packet Tracer**

Here we have the following tabs –

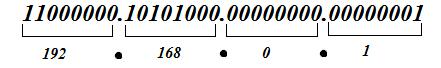
Physical (for adding/removing modules physically) Config (GUI mode for configuring Router)

Desktop – Has Look and Feel of a Desktop on an end node and can be used for options such as IP assigning, Terminal, Command Prompt, Web Browser etc.

**IP ADDRESSING**

**4.1 What is IP Address?**

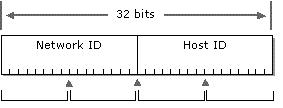
IP (Internet Protocol) is a 32-bit logical address. It has 4 octets and each octet contains maximum 8 bits. Each octet of IP Address varies from 0 to 255. Machines read the IP address as a stream of 32 bits. However, for human consumption, the IP address is written in dotted decimal notation. The decimal numbers are separated by periods, or dots. For example-



**Fig 4.1 – IP Address Example**

It consists of two components, they are-

* **Network bits**- The network bits make up the left portion of the address. They consist ofthe first bit up to some boundary.
* **Host bits**- The second component is the host portion of the address, consisting of the hostbits. The host bits make up the right portion of the address. They consist of the remaining bits not included with the network bits.



**Fig 4.2 – Network and Host Bits**

**5.2 Classes of IP Addresses**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Class** | **Range** |  | **Default** | **Application** |
|  |  |  | **Subnet Mask** |  |
|  |  |  |  |  |
| Class A | 1 – 126 | (1.0.0.0 – 127.255.255.255) | 255.0.0.0 | LAN or WAN |
|  |  | |  |  |
| Class B | 128 – 191 (128.0.0.0 – 191.255.255.255) | | 255.255.0.0 | LAN or WAN |
|  |  | |  |  |
| Class C | 192 – 223 (192.0.0.0 – 223.255.255.255) | | 255.255.255.0 | LAN or WAN |
|  |  | |  |  |
| Class D | 224 – 239 (224.0.0.0 – 239.255.255.255) | | 255.255.255.255 | Multicasting |
|  |  | |  |  |
| Class E | 240 – 255 (240.0.0.0 – 255.255.255.255) | | 255.255.255.255 | Research & |
|  |  |  |  | Development |
|  |  |  |  |  |
|  |  | **Table 1 – Classes of IP Address** | |  |
|  |  |  |  |  |

**4.3 Types of IP Address**

There are basically two types of IP Addresses

* Private Address

Private IP address can be used to configure private network. We can use private IP to build our network without paying a single rupee. But one biggest problem with private IP is that with private we cannot access the internet. This is the point where ISP comes from. ISP purchases a bulk of public IP address and provides them on rent. Whatever we pay to ISP for accessing internet is actually the charge of using public IP address.

Private IP addresses in different classes are-

 Class A: 10.0.0.0-10.255.255.255

 Class B: 172.16.0.0-172.31.255.255

 Class C: 192.168.0.0-192.168.255.255

 Public Address

An IP address is considered public if the IP number is valid and falls outside any of the IP address ranges reserved for private uses by Internet standards groups.

**NOTE**

1. 0 is reserved and represents all IP addresses.
2. 127 is a reserved address and is used for testing, like a loop back on an interface.
3. 255 is a reserved address and is used for broadcasting purposes.

**4.4 Subnet Mask**

A subnet mask is a 32-bit value that allows the receiver of IP packets to distinguish the network ID portion of the IP address from the host ID portion of the IP address. Every IP address is composed of a network component and a host component. The subnet mask has a single purpose: to identify which part of an IP address is the network component and which part is the host component. It is represented with all 1’s in the network portion and with all 0’s in the host portion.

Example

– Class A network 10.0.0.0 with subnet mask 255.0.0.0.

– Class B network 172.168.0.0 with subnet mask 255.255.0.0.

– Class C network 192.168.0.0 with subnet mask 255.255.255.0.

**4.5 Subnetting**

Subnetting is a network design strategy that divides a single network into multiple networks. Subnetting is also called FLSM (Fixed Length Subnet Mask).

**Advantages of Subnetting-**

* Reduced network traffic.
* Optimized network performance.
* Simplified management.

**4.6 Variable Length Subnet Mask (VLSM)**

VLSM, originally defined in RFC 1812, allows you to apply different subnet masks to the same class address space. Classful protocols, such as RIPv1 and IGRP, do not support VLSM. To deploy VLSM requires a routing protocol that is classless—BGP, EIGRP, IS-IS, OSPF, or RIPv2.

**Advantages of VLSM**

* Provides more efficient use of addressing.
* Ability to perform route summarization. Route summarization is the ability to take a bunch of contiguous network numbers in our routing table and advertise these contiguous routes as a single summarized route. Route summarization, or supernetting, is needed to reduce the number of routes that a router advertises to its neighbor. Remember that for every route we advertise, the size of our update grows. Summarization allows us to create a more

efficient routing environment by providing the following advantages:

* It reduces the size of routing tables, requiring less memory and processing.
* It reduces the size of updates, requiring less bandwidth.

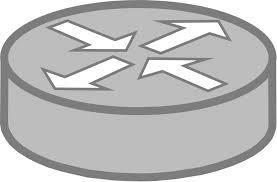
**ROUTERS & THEIR CONFIGURATION**

**5.1 What are Routers?**

Router is a device which makes communication possible between two or more different networks present in different geographical locations.

The routers work in the Network layer thus giving them the ability to understand the protocols being used to carry the data over the network. Since routers can understand protocols they can use the rules to decide what to do with a specific data.

TCP/IP uses the term gateway to refer to routers.



**Fig 5.1 – Router Symbol**

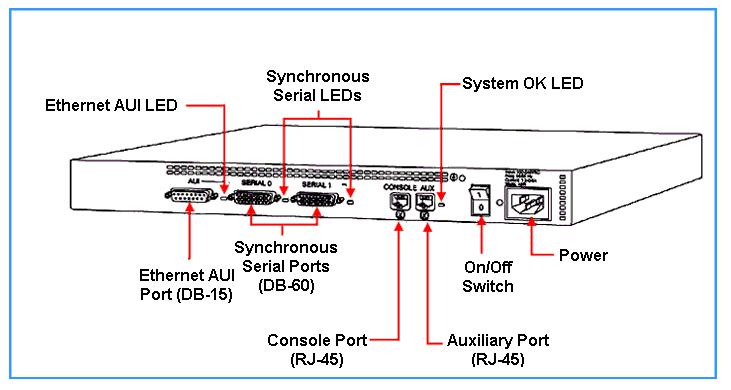
**5.2 Features of Routers**

* Multiple Active paths - Routers are able to keep track of multiple active paths between any given source and destination network.
* Traffic Management - Routers provide excellent traffic management using intelligent path selection, selecting the best route which is based on traffic loads, line speeds, number of hops or administrator preset costs.
* Identify address - Routers work at the network layer and can access more information than a bridge and can identify source and destination network addresses within packets.
* Filtering bad data - Routers do not forward any information that does not have a correct network address. Routers also filter broadcast traffic by not routing broadcast packets.
* Sharing information - Routers can share status and routing information with other routers. By doing this they can listen to the network and identify which connections are busy and which are not.

**5.3 Router Interfaces (External Components of Router)**

Components of a router include the following:

1. Console Port - The console port is used for local management connections. This means that we must be able to physically reach the console port with a cable. The console port looks exactly like an Ethernet port. It uses the same connector, but it has different wiring and is often identified with a light blue label "CONSOLE."



**Fig 5.2 – Router Ports**

1. Aux Port - The AUX port is really just another console port that is intended for use with a modem, so we can remotely connect and administer the device by phoning it. However using aux port for configuration create some security issues, so make sure that we get advice on addressing those before setting this up.
2. Ethernet Port AUI - An Ethernet port (which might be a Fast Ethernet or even a Gigabit Ethernet port, depending on our router model) is intended to connect to the LAN. Some routers have more than one Ethernet or Fast Ethernet port; it really depends on what we need and of course what we purchase. The Ethernet port usually connects to the LAN switch with a straight-through cable.
3. Serial Port - A Cisco serial port is a proprietary design, a 60-pin D-sub. This connector can be configured for almost any kind of serial communication. We need a cable that has the Cisco connector on one end and the appropriate type of connector for the service we want to connect to on the other.

* 1. BRI Port - Basic Rate Interface used to connect ISDN to the router. It is a RJ45 port. It is available on 2503 and 2520 model routers.
  2. 10 Base T Port - It is a RJ45 port and used for connecting LAN to the routers. Its function is same as the AUI port but there is no need for a transceiver. It is available on 2520 model router.

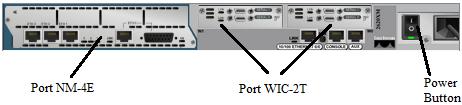
**5.4 Router Memory Elements**

* 1. Boot ROM - It stores the mini IOS (Internet work Operating System) image (RX Boot) with extremely limited capabilities and POST routines and core level OS for maintenance.
  2. FLASH - It is an EPROM chip that holds most of the IOS Image. It maintains everything when router is turned off.
  3. RAM - RAM holds running IOS configurations and provides caching. RAM is a volatile memory and loses its information when router is turned off. The configuration present in RAM is called Running configuration.
  4. NVRAM - It is a re-write able memory area that holds router’s configuration file. NVRAM retains the information whenever router is rebooted. Once configuration is saved, it will be saved in NVRAM and this configuration is called Startup Configuration.

**5.5 Working Modes of Router**

* 1. User Mode (Default mode)
  2. Privilege or Administrative Mode
  3. Global Configuration Mode
  4. Interface Configuration Mode
  5. Line Configuration Mode
  6. Router Mode
  7. Sub-Interface Mode

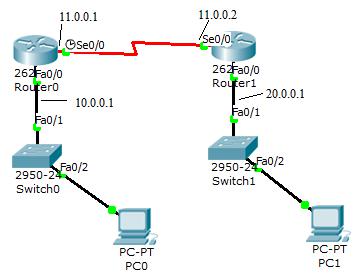
**5.5 Router Configuration**

Configuring routers involves configuring port interfaces on a router. This is necessary for routers to assign ports for communication. However this should not be confused with routing. Configuring a router essentially means making a router aware of its connections on its ports.

**fig 5.3– Router Ports & Modules**

Steps involved in configuring routers are as follows: 1. Applying Ports

2. Configuring Interfaces



**Fig 5.4 – Router Configuration on Cisco Packet Tracer**

* **Configuring serial ports**

For Router0

Router> enable

Router# configure terminal Router (config) # interface se0/0

Router (config-if)# ip address 11.0.0.1 255.0.0.0 Router (config-if)# no shutdown

Router (config-if)# ex Router (config)#ex Router# ex

Similarly for Router 1 with IP address 11.0.0.2 255.0.0.0

* **Configuring Ethernet Ports**

For Router0

Router> enable

Router# configure terminal Router (config)# interface fa0/0

Router (config-if)# ip address 10.0.0.1 255.0.0.0 Router (config-if)# no shutdown

Router (config-if)# ex Router (config)#ex Router# ex

Similarly for Router 1 with IP address 20.0.0.1 255.0.0.0

**ROUTING**

**6.1 What is Routing?**

Routing is the process of providing the best route to forward the data packet from source to destination and maintain the route. There are basically three types of routing:

* Static Routing-

In this type of routing the network administrator manually assigns the route to forward the data packet from source to destination. However, this type of routing is suitable for small area network but it is faster than the other type of routings.

* Dynamic Routing-

In this type of routing the network administrator automatically defines the route for forwarding packets with the help of routing protocols. It is the most widely used way of routing a network.

* Default Routing-

A default route of a computer that is participating in computer networking is the packet forwarding rule (route) taking effect when no other route can be determined for a given Internet Protocol (IP) destination address.

To be able to route packets, a router must know following:

o Destination address

o Neighbor routers from which it can learn about remote networks

o Possible routes to all remote networks

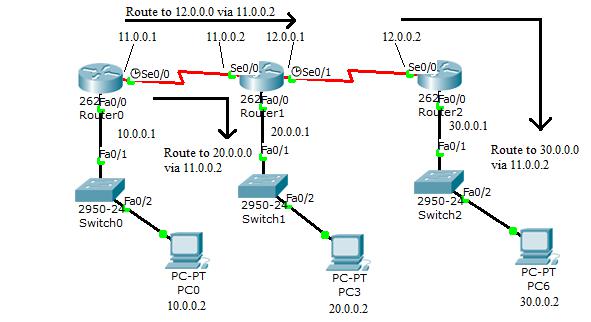
* 1. How to maintain and verify routing information

**6.2 Static Routing**

Static routing is the process of manually adding routes in each router’s routing table. Static routers specify the path packets take, allowing precise control over a network’s routing behavior. Static routes are sometimes used to define a gateway of last resort that is where a packet is routed if no other suitable path can be found. Static routers are also used when routing to a stub network. Static routers are also used for security reasons or when the network is small.

By using static routing, we mean that someone must hand type all network locations into a routing table. If static routing is used, the administrator is responsible for updating all changes by hand into all routers.

* Benefits of Static Routing-
  + There is no overhead on the router CPU, which means we can possibly buy a cheaper router than dynamic routing.
  + There is no bandwidth usage between routers.
  + It adds security, because the administrator can choose to allow routing access to certain networks only.
* Disadvantages of Static Routing-
  + The administrator must really understand the internetwork and how each router is connected in order to configure routers correctly.
  + If a network is added to the internetwork, the administrator has to add a route to it on all routers by hand.
  + It’s not feasible in large network because maintaining it would be a full-time job in itself.
* Static Routing Commands



**Fig 6.1 – Static Routing on Cisco Packet Tracer**

**For Router 0-**

Router> enable Router # config t

Router (config)# ip route 12.0.0.0 255.0.0.0 11.0.0.2 Router (config)# ip route 20.0.0.0 255.0.0.0 11.0.0.2 Router (config)# ip route 30.0.0.0 255.0.0.0 11.0.0.2 Router (config)#ex

Router# ex

Similarly for Router1 (with IP routes 10.0.0.0 255.0.0.0 11.0.0.1 & 30.0.0.0 255.0.0.0 12.0.0.2) and Router2 (with IP routes 11.0.0.0 255.0.0.0 12.0.0.1; 10.0.0.0 255.0.0.0

* + - 1. & 20.0.0.0 255.0.0.0 12.0.0.1)

**6.3 Default Routing**

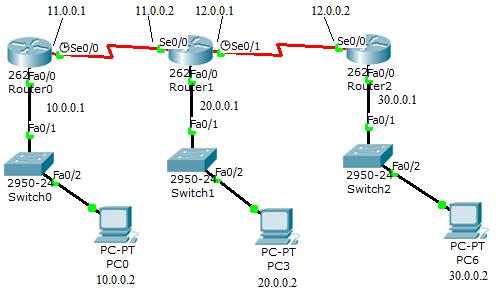
Default Routing is used to send packets with a remote destination networking not in the routing

table to the next- hop router. We can also use default routing on stub networks those with only

one exit path out of network.

* Default Routing Commands

In the same above shown scenario we now apply default routing commands.



**Fig 6.2 – Default Routing on Cisco Packet Tracer**

**For Router 0-**

Router> enable Router # config t

Router (config)# ip route 0.0.0.0 0.0.0.0 11.0.0.2 Router (config)# ip route 0.0.0.0 0.0.0.0 11.0.0.2 Router (config)# ip route 0.0.0.0 0.0.0.0 11.0.0.2 Router (config)# ex

Router# ex

Similarly for Router1 & Router 2

**6.4 Dynamic Routing**

Dynamic routing is when protocols are used to find networks and update routing tables on router. It is easier than using static or default routing, but it will cost in terms of router CPU processes and bandwidth on network links. A routing protocol defines the set of rules used by a router when it communicates routing information between neighbor routers.

The Different Dynamic Routing Protocols are-

* RIP (Routing Information Protocol)
* IGRP (Interior Gateway Routing Protocol)
* EIGRP (Enhanced Interior Gateway Routing Protocol)
* OSPF (Open Shortest Path First)

**6.5 Routing Protocols Basics**

* **Administrative Distances-**

The Administrative Distance or AD is used to rate trustworthiness of routing information on a router received from the neighbor router. The AD value lies between 0 and 255, where) means the most trusted route and 255 means that no traffic can pass through this route. If a router receives updates listing same remote network then the first thing router does id checking the AD value. If one of the advertised routes has the lowest AD value then that path is placed in the routing table.

The table below shows the Default AD values of Different Routing Protocols

|  |  |
| --- | --- |
| **Routing Protocol** | **AD Value** |
|  |  |
| Connected Interface | 0 |
| Static Route | 1 |
| EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| RIP | 120 |
| External EIGRP | 170 |
| Unknown | 255 |

**Table 2 – AD values for various Routing Protocols**

**• Routing Protocols**

There are three types of routing Protocols

* + Distance Vector

The distance vector protocols find the best path to a remote network by judging distance. Each time a packet goes through a router it’scalled a hop. The router with least number of hops to the network is determined to be the best path. The vector indicates the direction to the remote network. Both RIP and IGRP are distance- vector routing protocols. They send the entire routing table to directly connected neighbors. The distance-vector routing algorithm passes complete routing table contents to neighboring routers, which then combine the received routing table with their own routing tables to complete the router’s routing table. This is called routing by rumor, because a router receiving an update from a neighbor router believes the information about remote networks without actually finding out for itself. It’s possible to have a network that has multiple links to the same network, and if that’s the case, the administrative distance is checked first. If AD is same, the protocols will have to use other metrics to determine the best path to use to that network. RIP uses only hop count to determine the best path to a network. If RIP finds more than one link to the same remote network with same hop count, it will automatically perform a load balancing. RIP can perform load balancing for up to six equal cost links (four by default).

* + Link State Protocols

In link state protocols, also called shortest path first protocol, the routers each create three separate tables. One of these tables keeps track of directly attached neighbors, other determines the network topology and the third is the routing table. Link state protocol knows more about the internetwork than any other distance vector routing protocol. OSPF is a routing protocol that is completely link state. Link state protocol send updates containing the state of their own links to all other routers on the network.

* + Hybrid Protocols

Hybrid protocols use aspects of both distance vector and link state for example,

EIGRP.

**6.6 RIP (Routing Information Protocol)**

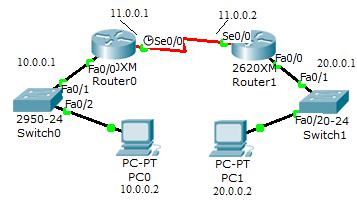
RIP is a distance vector routing protocol. It updates the routing table in every 30 seconds. The maximum hop count of RIP is 15, which means that 16 is deemed unreachable. The AD value of RIP is 120. It is suitable for small area networks and is unsuitable for large area networks, slow WAN links or on networks with large number of routers installed.

RIP has two versions-

* **RIP version1-** This version uses Classfull routing which means that all devices in thenetwork must have same subnet mask. This is because RIP sends updates without the subnet mask information.
* **RIP version2-** This is something called prefix routing. It doesn’t send subnet maskinformation with routing updates. It is also called Classless routing.

**Timer value of RIP**

* Route Update Timer - Sets the interval of 30 seconds between routing updates in which it sends the copy of routing table to all its neighbors.
* Route Hold down Timer - This sets the amount of time during which routing information is suppressed. The default is 180 seconds.
* Route Invalid Timer - Determine the length of time that must elapse before a router determines that a route has become invalid. The default is 180 seconds.
* Router Flush Timer - It sets the time between a router becoming invalid and its removal from the routing table. The default flush timer is 240 seconds.

**Example of RIP configura****tion-**

**Fig 6.3 – Network for RIP in Cisco Packet Tracer**

**Commands-**

**For Router 0-**

Router> enable

Router# config t

Router (config)# route RIP

Router (config-router)# network 10.0.0.0

Router (config-router)# network 11.0.0.0

Router (config-router)# ex

Router (config)# ex

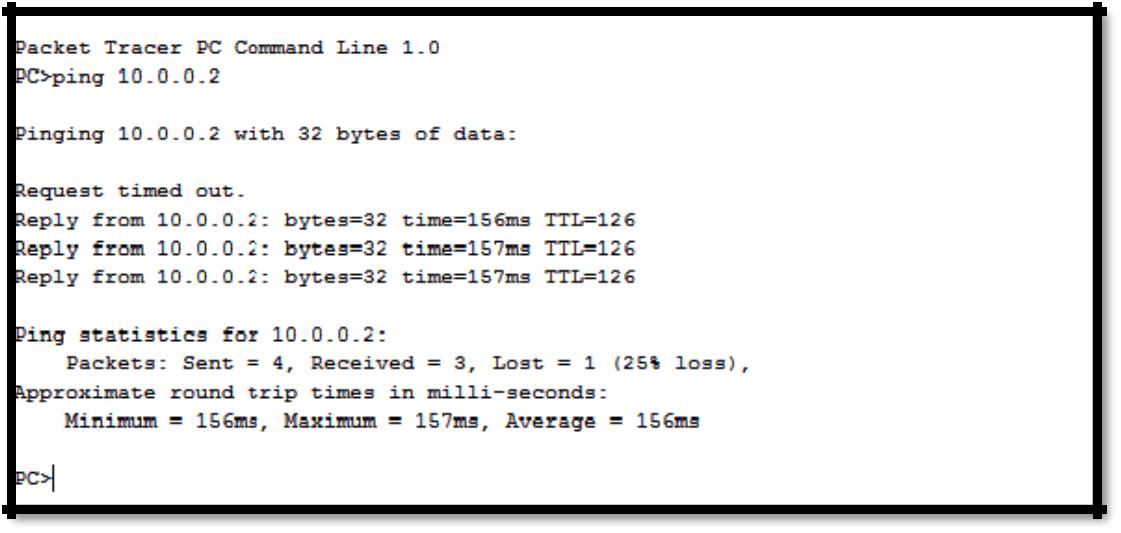
Router# ex

Similarly for Router 1 with network 20.0.0.1 & 11.0.0.0

**Checking for the Routing Result**

To check if communication is taking place between PC0 and PC1, in the command prompt

of the PC1 write ping 10.0.0.2. If reply comes then communication is taking place.



**Fig 6.4 – Checking RIP Configuration in Cisco Packet Tracer**

**6.7 IGRP (Interior Gateway Routing Protocol)**

IGRP is a cisco proprietary distance vector protocol. This means that to configure IGRP the

router has to be of cisco. IGRP was introduced to overcome problems posed by RIP. The

maximum hop count of IGRP is 255 and default of 100. This helps in routing of large area

networks as it increases hop count.

IGRP uses bandwidth and delay as metric for determining the best route. It is also called

composite metric.

IGRP is not used now a days as it was only limited to cisco routers. It was succeeded by EIGRP

which is being used now days.

Value of IGRP

* Update Timer- 90 seconds
* Hold Down Timer- 270seconds
* Invalid Timer- 280 seconds
* Flush Timer- 630 seconds

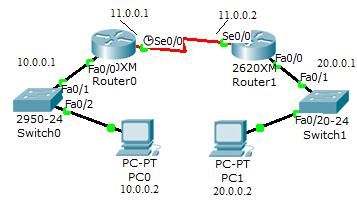
**6.8 EIGRP (Enhanced Interior Gateway Routing Protocol)**

EIGRP is a classless, distance vector protocol which gives a real edge over IGRP. EIGRP uses autonomous system number to describe the contiguous set of router that run the same routing protocol and share routing information. But unlike IGRP, EIGRP uses subnet masks in its routing updates. EIGRP comes under hybrid protocol as it has characteristics of both distance vector and link state protocols. It has maximum hop count of 255. It has AD value of 90.

EIGRP uses following metrics

* Bandwidth
* Delay
* Load
* Reliability

**Example of EIGRP configuration-**



**Fig 6.5 – Network for EIGRP in Cisco Packet Tracer**

**EIGRP Commands-**

**For Router 0-**

Router> enable

Router# config t

Router (config)# route EIGRP 20

Router (config-router)# network 10.0.0.0

Router (config-router)# network 11.0.0.0

Router (config-router)# ex

Router (config)# ex

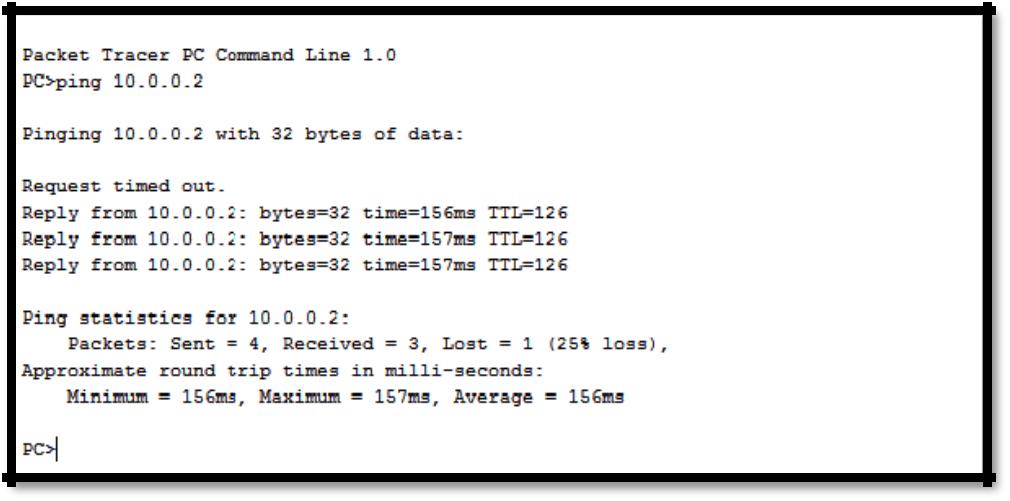
Router# ex

Similarly for Router 1 with network 20.0.0.0 & 11.0.0.0

**Checking for the Routing Result**

To check if communication is taking place between PC0 and PC1, in the command prompt of

the PC1 write ping 10.0.0.2. If reply comes then communication is taking place.



**Fig 6.6 – Checking RIP Configuration in Cisco Packet Tracer**

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

OSPF is link state routing protocol and it works on SPF algorithm. First shortest path first tree

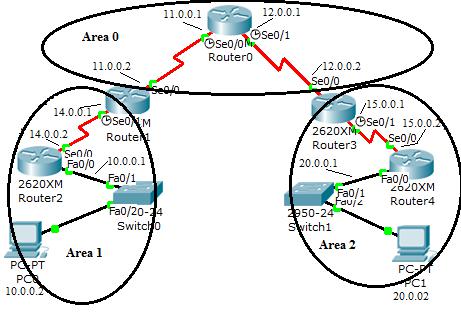
is formed and then the routing table is populated with resulting best routes. If we want to build

large networks then OSPF is the best routing protocol to be used. It has AD value of 110.

OSPF has following features-

* Consists of areas and supports both different and same autonomous system.
* Minimize routing update traffic.
* Allows scalability.
* Supports VLSM/CIDR.
* Has unlimited hop count.
* Allows multi-vendor deployment.
* Supports Wild card mask. Wild card mask is reverse of subnet mask.

**Example of OSPF configuration-**



**Fig 6.7 – Network for OSPF in Cisco Packet Tracer**

In this scenario of OSPF the whole network is divided into areas and each area is connected to

others with a backbone router, which in this case is Router 0. Router 1 and Router 3 are ABR

(Area Border Router) and router 2 and Router 4 are ASBR (Area Stub Border Router).

**OSPF Routing Commands-**

**For Router 0-**

Router> enable

Router# config t

Router (config)# route OSPF 20

Router (config-router)# network 12.0.0.0 0.255.255.255 area 0

Router (config-router)# network 11.0.0.0 0.255.255.255 area 0

Router (config-router)# ex

Router (config)# ex

Router# ex

Similarly

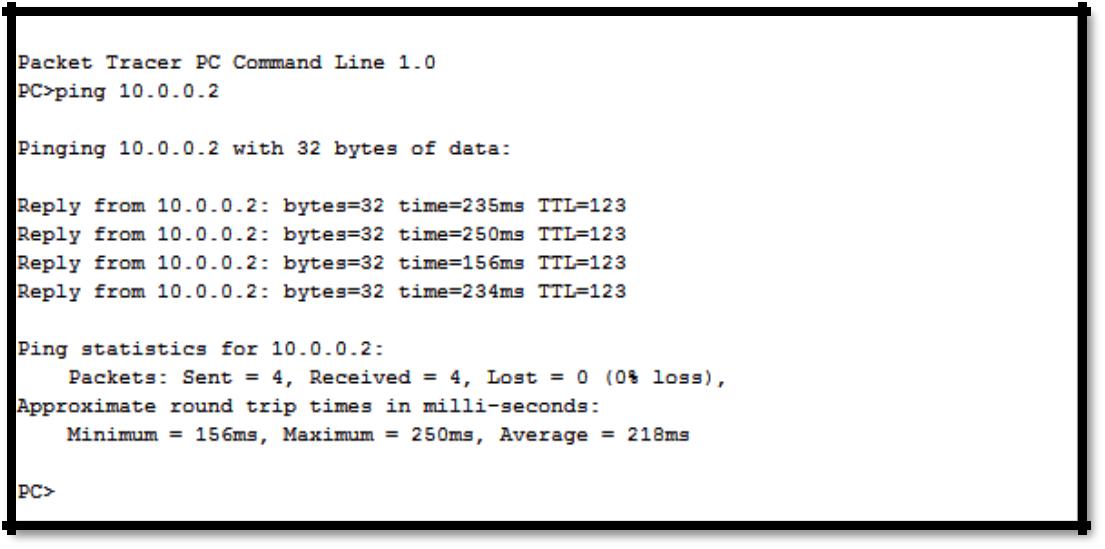
Router1 (with network 11.0.0.0 0.255.255.255 area 0 & 14.0.0.0 0.255.255.255 area 1), Router2 (with network 14.0.0.0 0.255.255.255 area 1 & 15.0.0.0 0.255.255.255 area 1), Router3 (with network 12.0.0.0 0.255.255.255 area 0 & 15.0.0.0 0.255.255.255 area 2), Router4 (with network 15.0.0.0 0.255.255.255 area 2 & 20.0.0.0 0.255.255.255 area 2).

**Checking for the routing result**

Here we check whether the PC0 of area 1 communicates with PC1 of area 2. Thus in command

prompt of PC0 we write ping 20.0.0.2. If reply is received then communication has been

established.

**fig 6.8 – Checking OSPF Configuration in Cisco PacketTracer**

**VLAN AND SECURITY**

**What is VLAN**

VLAN is a logical grouping of networking devices. When we create VLAN, we actually break large broadcast domain in smaller broadcast domains. Consider VLAN as a subnet. Same as two different subnets cannot communicate with each other without router, different VLANs also requires router to communicate.

**Advantage of VLAN**

VLAN provides following advantages:-

* Solve broadcast problem
* Reduce the size of broadcast domains
* Allow us to add additional layer of security
* Make device management easier
* Allow us to implement the logical grouping of devices by function instead of location

**Static VLAN Configuration**

The first step in configuring VLANs is to create the VLAN:

Switch(config)# vlan 100 Switch(config-vlan)# name MY\_VLAN

The first command creates VLAN 100, and enters VLAN configuration mode. The second command assigns the name MY\_VLAN to this VLAN. Naming a VLAN is not required.

The list of VLANs is stored in Flash in a database file named vlan.dat. However, information concerning which local interfaces are assigned to a specific VLAN is not stored in this file; this information is instead stored in the startup-config file of each switch.

Next, an interface (or range of interfaces) must be assigned to this VLAN. The following commands will assign interface fa0/10 into the newly created MY\_VLAN.

Switch(config)# interface fa0/10

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 100

The first command enters interface configuration mode. The second command indicates that this is an access port, as opposed to a trunk port (explained in detail shortly). The third command assigns this access port to VLAN 100. Note that the VLAN number is specified, and not the VLAN name.

**SECURITY:-**

**AAA** (not fully used in project)

Securing access to Cisco routers and switches is a critical concern. Often, access is secured using enable and vty/console passwords, configured locally on the device.

For large networks with many devices, this can become unmanageable, especially when passwords need to be changed. A centralized form of access security is required.

AAA is a security system based on Authentication, Authorization, and Accounting.

Authentication is used to grant or deny access based on a user account and password. Authorization determines what level of access that user has on the Router/router when authenticated. Accounting can keep track of who logged into what device, and for how long.

AAA must be enabled globally on a router/Router. By default, it is disabled

**Switch Port Security**

Port Security adds an additional layer of security to the switching network.

The MAC address of a host generally does not change. If it is certain that a specific host will always remain plugged into a specific switch port, then the switch can filter all MAC addresses except for that host’s address using Port Security. The host’s MAC address can be statically mapped to the switch port, or the switch can dynamically learn it from traffic.

Port security cannot be enabled on trunk ports, dynamic access ports, Etherchannel ports, or a SPAN destination port.

To enable Port Security on an interface:

Switch(config)# interface fa0/5

Switch(config-if)# switchport port-security

By default, Port Security will allow only one MAC on an interface. The maximum number of allowed MACs can be adjusted, up to 1024:

Switch(config-if)# switchport port-security maximum 2

To statically specify the allowed MAC address(es) on a port:

Switch(config-if)# switchport port-security mac-address 0001.1111.2222

Switch(config-if)# switchport port-security mac-address 0001.3333.5555

Only hosts configured with the above two MAC addresses will be able to send traffic through this port. If the maximum number of MAC addresses for this port had instead been set to 10, but only two were statically specified, the switch would dynamically learn the remaining eight MAC addresses.

MAC addresses that are dynamically learned with Port Security are referred to as Sticky Addresses. Dynamically learned addresses can be aged out after a period of inactivity (measured in minutes):

Switch(config-if)# switchport port-security aging time 10

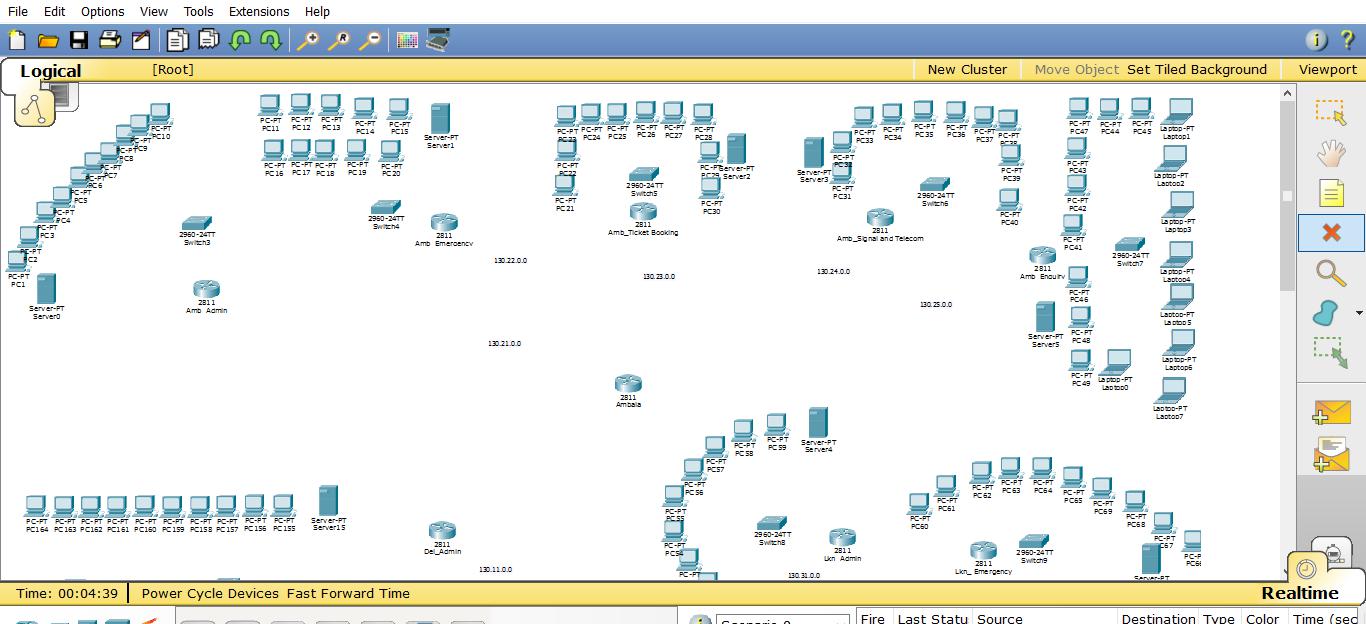
Port Security aging is disabled by default.

**NETWORK DESIGN & IMPLEMENTATION**

The designing and implementation of the network in our project comprised of the following steps

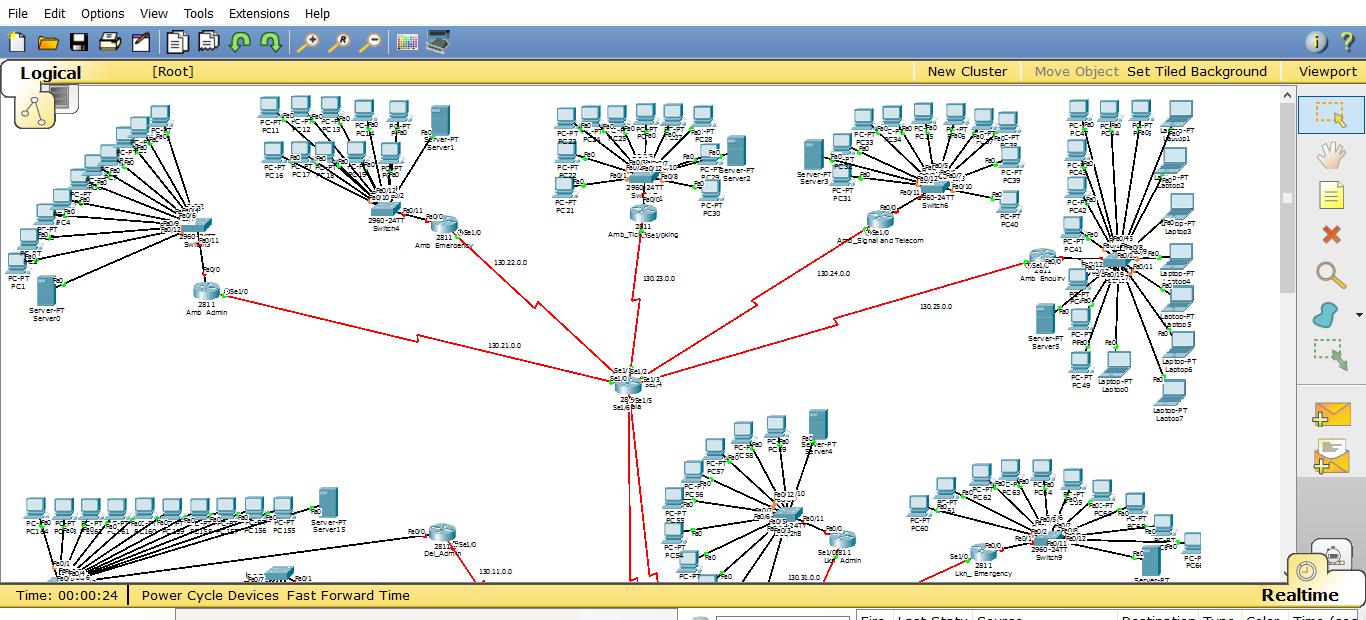
**Step 1**

The first step involves designing and setting up the network schematic in the Logical Topology window of Cisco Packet Tracer.



**Fig 8.1 – Initial Network Layout**

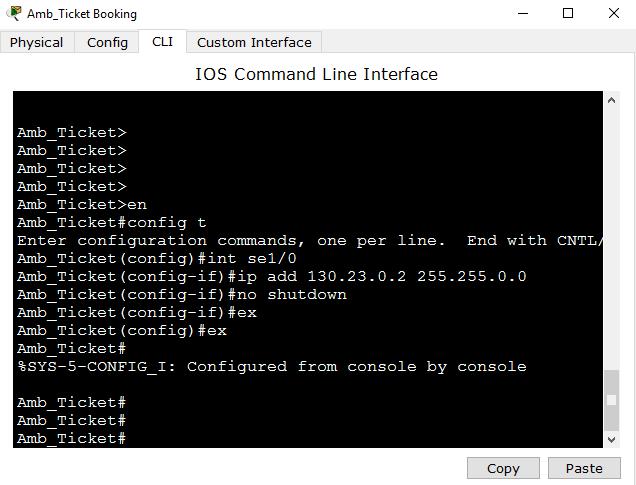
**Step 2**

The after the initial layout for the schematic is developed. We connect the devices in a hierarchical fashion.

**Fig 8.2 – Connecting Devices with Suitable Cables**

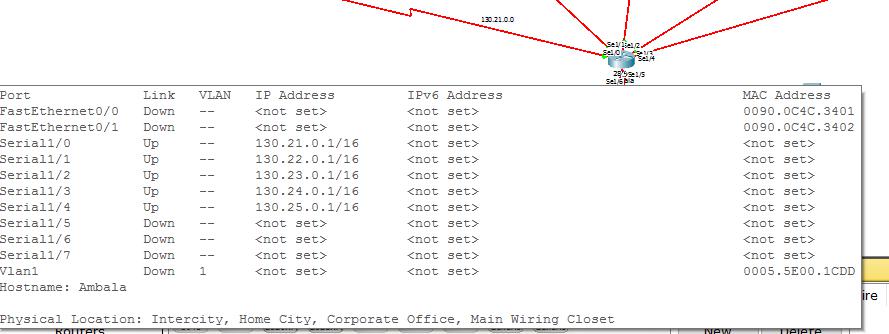
**Step 3**

After the layout is finalized the ports of the routers need to be interfaced to make them aware of their physical connections. [Code for the same is in Appendix I]



**Fig 8.3 – Interfacing Router Ports**

After all the ports are configured, the respective lights will change from red to green and link state will change to up.

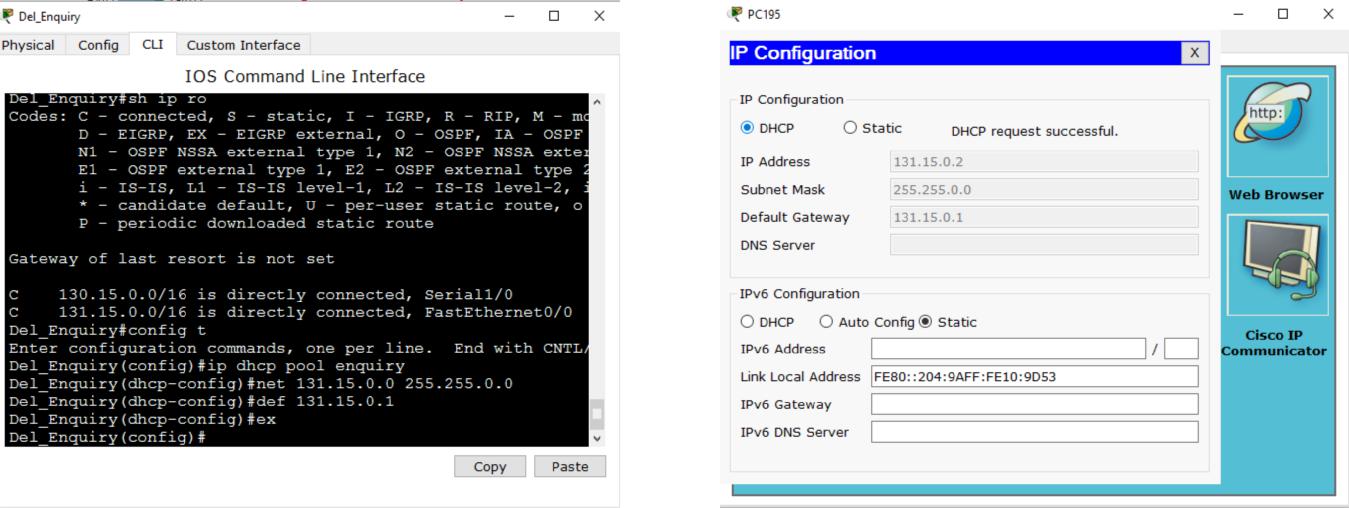


**Fig 8.4 – Displaying Router Interfaces and Link States**

**Step 4**

We now configure DHCP on each of the routers so that the process of assigning IP configuration is automated. This also helps in quickly scaling of the networks as a device joining the network can start working straight away without wasting time waiting for configurations to be configured by the network administrator. This also eliminates the need of stationing the network administrator in every network. Moreover this helps in freeing up

addresses for future use when a device leaves the network. [Code for the same is in Appendix II]

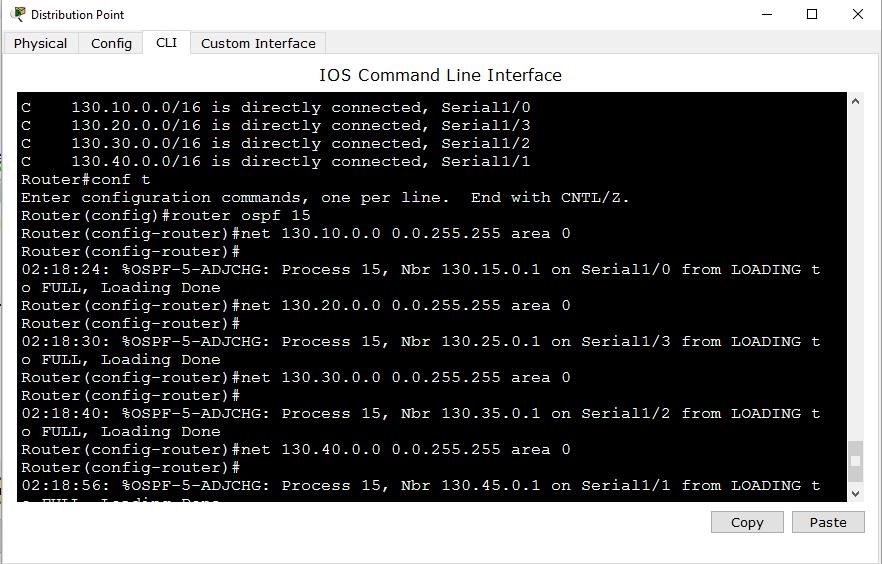


**Fig 8.5 – Configuring DHCP in CLI** **Fig 8.6 – Requesting DHCP**

**mode of the server** **configurations on an End Device**

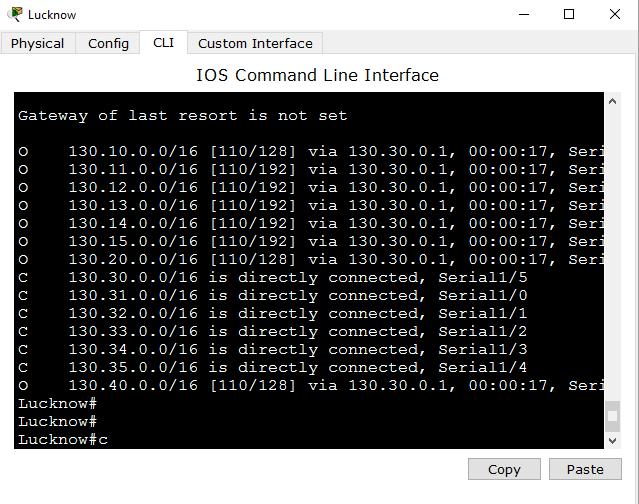
**Step 5**

Now we provide routes by configuring our desired routing protocol on each of the routers. Here our protocol of choice has been OSPF (Open Shortest Path First) owing to its vendor neutrality and superior routing algorithm. [Code for the same is in Appendix III]



**Fig 8.7 – Applying Routing on the Routers**

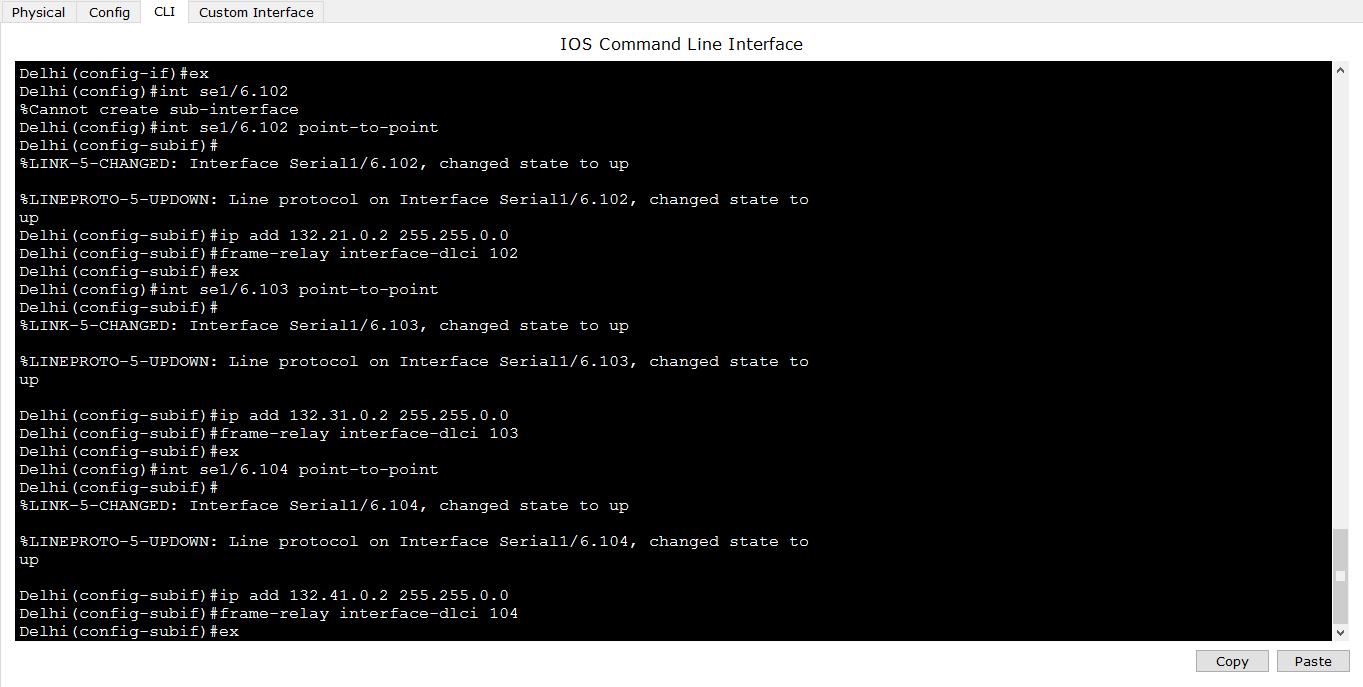
Post routing we can see the connected as well as routed routes with command *Show IP routes* as in Fig 7.4



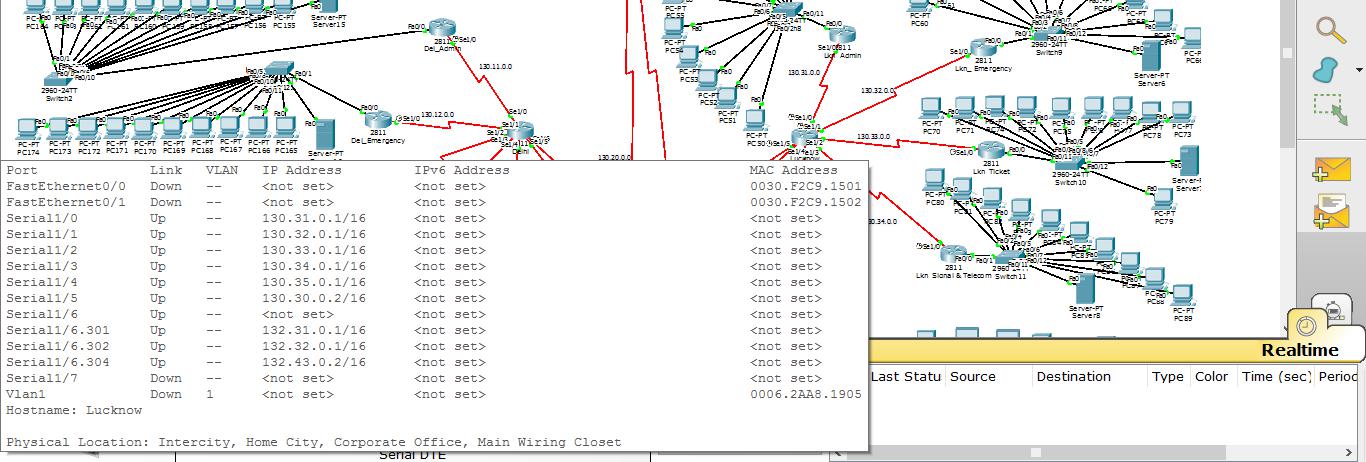
**Fig 8.8 – Checking applied Routing on the Routers**

**Step 6**

After connecting and routing all the networks we need to provide a high speed network for these routers to connect to and transmit their data onto. For this purpose we make use of the point-to-point frame-relay. We create sub interfaces on the ports connected to the WAN and then uses these sub-interfaces to form a meshed network of point-to-point connection between the sub-Deptt.s.



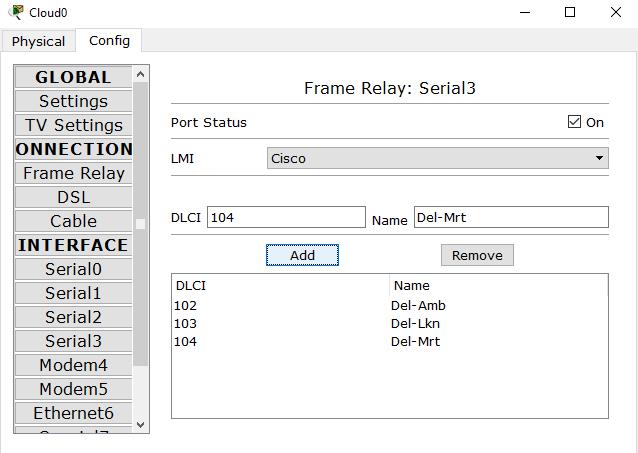
**Fig 8.9– Configuring Frame Relay on the Sub-interfaces created on the Routers**



**Fig 8.10 – Checking Configured Sub-interfaces on the Routers**

**Step 7**

After adding frame-relay on the sub-interfaces, we configure them with DLCI numbers

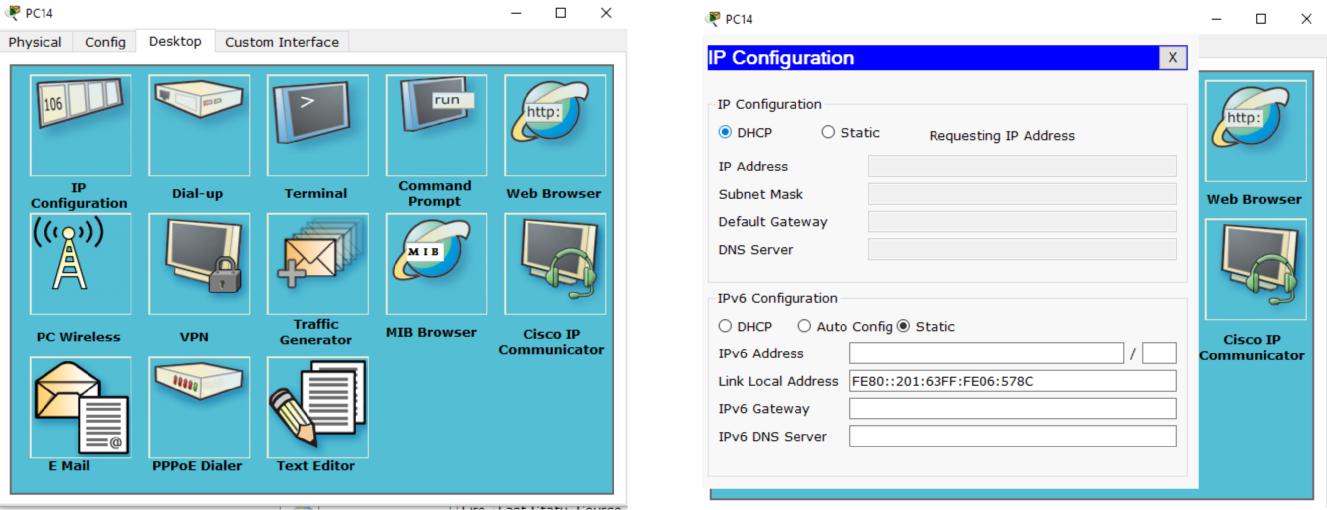


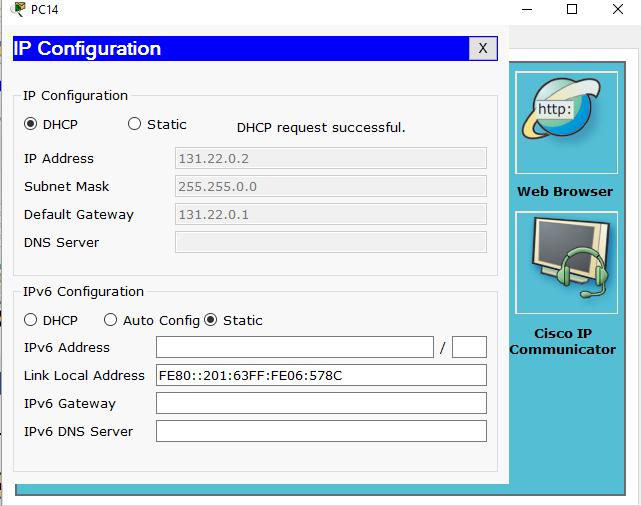
**Fig 8.11 – Configuring DLCI on the Routers**

**Step8**

Verifying Routing, DHCP and other network Configurations.

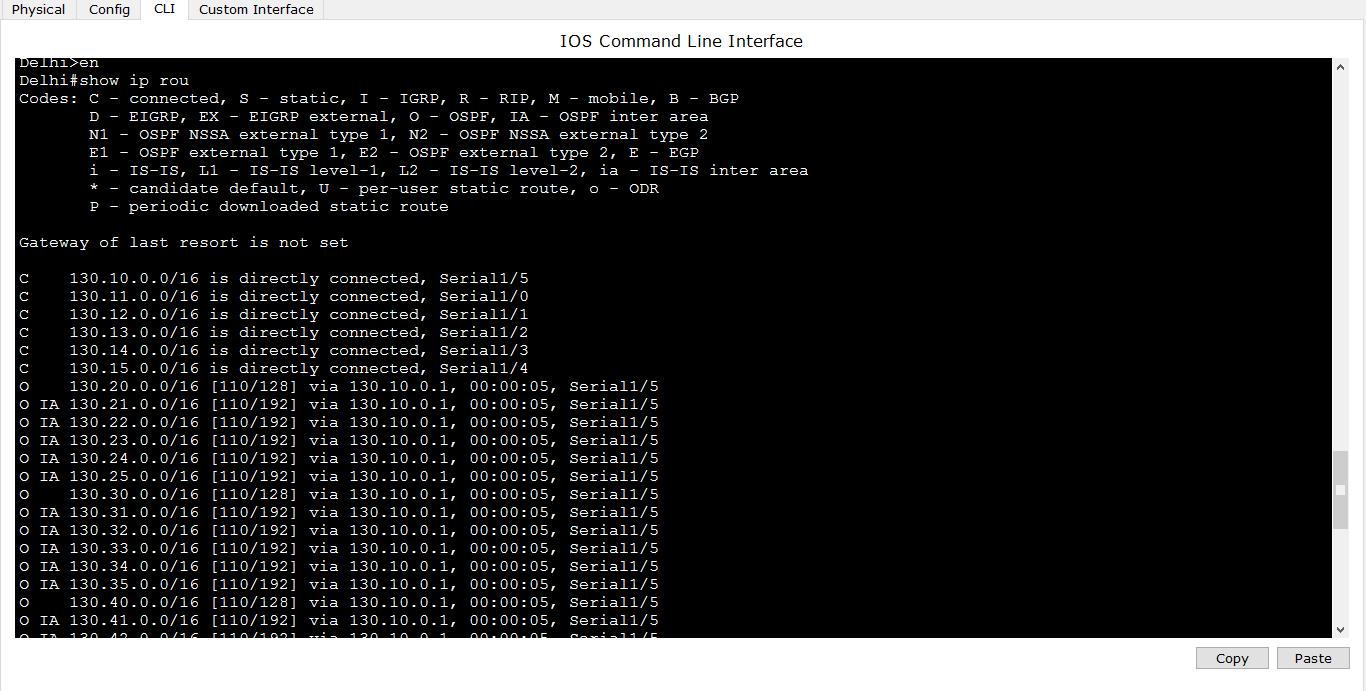
Verifying DHCP



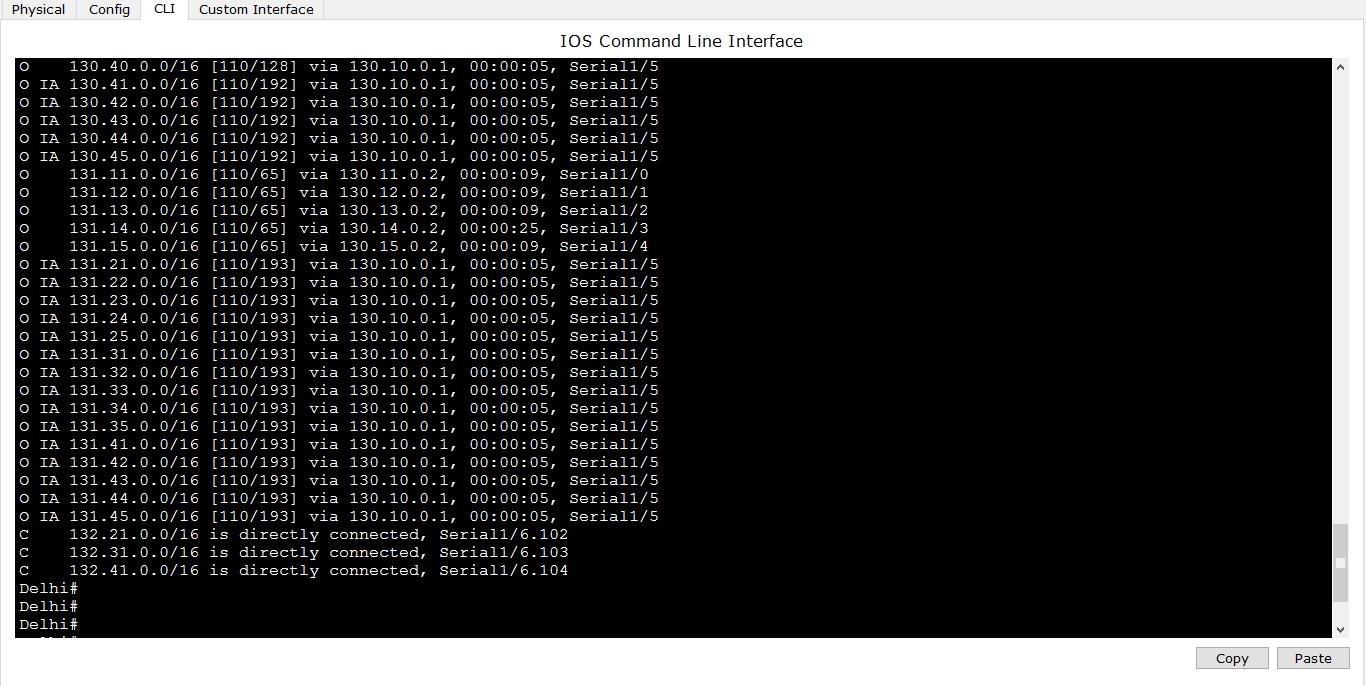
1. b)

(c)**Fig 8.12 – Verifying DHCP on the Devices**

Verifying Routing



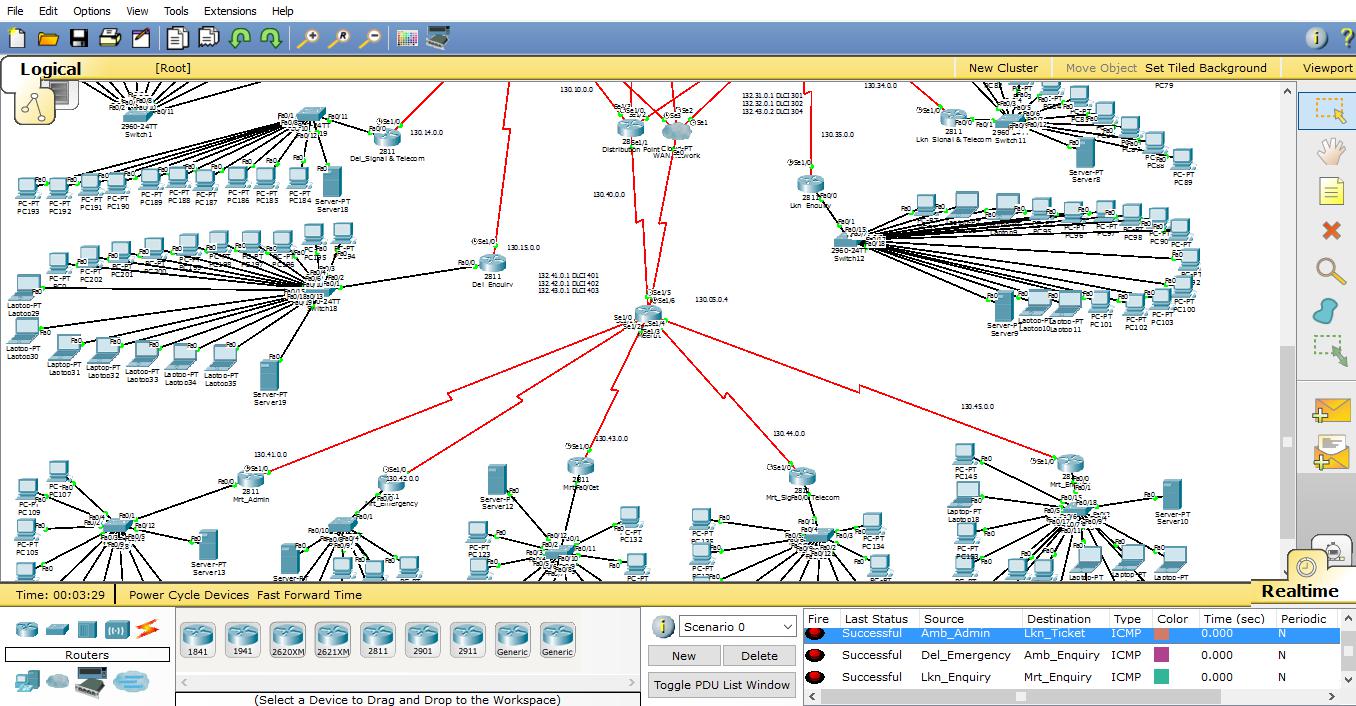
(a)



(b)

**Fig 8.13 (a) & (b) – Verifying routing on Deptt. routers**

Verifying Packet Delivery



**Fig 8.14 – Verifying Packet Delivery among different Deptt.s.**

**FUTURE SCOPE**

The project developed here is just a start and we believe that it has tremendous potential to be developed further with improvement in routing algorithms and newer devices being configured and developed.

Moreover with more and more devices getting on the internet need for providing more mobile solutions as well as better response time has peaked. Solutions need to be provided fast and provided in a format that is readable by a variety of devices that are in use today.

Moreover this project has been based on IPv4 addressing, however growing need of times has resulted in accelerated deployment of IPv6 addressing. We would like future versions of this network to be based on IPv6 addressing scheme. Also for the sake of simplicity we have made use of classful addressing which has a huge drawback of wasting a number of IP addresses. We would like subsequent versions of this network to make use of classless addressing so that we can make more efficient use of IP addresses available to us with using never addressing concepts like VSLM (Variable Length Subnet Mask) etc.

**REFERENCES**

We have made use of various online as well as offline resources for our project. Various books assigned to us as textbooks have been used as reference as well as other books. These include

1. Behrouz A Forouzan – Data Communication and Networking – McGraw Hill Publishers
2. Andrew S. Tanenbaum – Computer Networks – Pearson Education
3. Todd Lammle – CCNA Routing and Switching Study Guide – Wiley Publishers

Various online resources such as [www.wikipedia.org,](http://www.wikipedia.org/) [www.scholar.google.com](http://www.scholar.google.com/) etc. have come handy for clearing occasional doubts or as a quick guide.