



**Jaypee University of Information Technology**  
**Solan (H.P.)**  
**LEARNING RESOURCE CENTER**

Acc. Num. *SP07045* Call Num:

**General Guidelines:**

- ◆ Library books should be used with great care.
- ◆ Tearing, folding, cutting of library books or making any marks on them is not permitted and shall lead to disciplinary action.
- ◆ Any defect noticed at the time of borrowing books must be brought to the library staff immediately. Otherwise the borrower may be required to replace the book by a new copy.
- ◆ The loss of LRC book(s) must be immediately brought to the notice of the Librarian in writing.

Learning Resource Centre-JUIT



SP07045

# NETWORK AND SECURITY(CONFIGURATION AND IMPLEMENTATION)

Enrollment no : 071428, 071433

Name Of the Student(s) : Piyush Tandon, Goda Pranav Murty

Name of the Supervisor : Mr. Ravindara Bhatt



Submitted in partial fulfillment of the Degree of  
Bachelor of Technology

DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION  
TECHNOLOGY

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,

WAKNAGHAT

## Table of Contents

Chapter no.	Topics	Page no.
	Certificate from the supervisor	4
	Acknowledgement	5
	Summary	6
<b>Chapter 1</b>	Introduction	8
	OSI model	10
	Data exchange in OSI	11
	Drawbacks of OSI	12
	Comparison of OSI with TCP/IP	13
	Basic TCP/IP	14
	Address Resolution Protocol	15
	RARP	16
<b>Chapter 2</b>	LAN	18
	Ethernet	19
	CSMA/CD	20
	Hubs, Switches and Bridges	20
	MAC Addressing	21
<b>Chapter 3</b>	Network Topologies	24
	Point to Point	25
	Bus	26

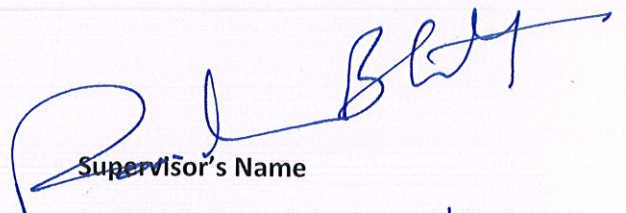
	Star	27
	Ring	28
	Mesh	29
	Tree	30
	Daisy Chains	31
	Decentralization	31
	Centralization	32
<b>Chapter 4</b>	Routing Information Protocol	34
	Versions of RIP	35
	OSPF v/s IS-IS	36
	IGRP	37
<b>Chapter 5</b>	CISCO IOS	38
	Configuration of Network Devices	39
	Working with CISCO Switches	41
	Commands	42
<b>Chapter 6</b>	Configuration and Implementation	43
	Packet Tracer	44
<b>Chapter 7</b>	<b>Observation and Results</b>	<b>48</b>
<b>Chapter 8</b>	<b>Conclusion</b>	<b>50</b>
	<b>References</b>	<b>51</b>

## Certificate

This is to certify that project report entitled "...NETWORK AND SECURITY...", submitted by ...071428... 071433... in partial fulfillment for the award of degree of Bachelor of Technology in Information Technology Engineering to Jaypee University of Information Technology, Wagnaghat, Solan 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: 24.05.2011



Supervisor's Name

Designation Sr. Lecturer

## Acknowledgement

We owe a great many thanks to a great many people who helped and supported us during the completion of this project. My deepest thanks to our guide, **Mr. Ravindara Bhatt**, for guiding and correcting various documents of our and supporting us at every step. He has taken the pain to go through the project and make necessary changes and corrections as and when needed.

I extend my thanks to **Mr. S.P Gherera (HOD, CS/IT Department)** for extending his support.

I would also like to thank my institution and my faculty members without whose support this project would have been a distant reality. I also extend my heartfelt thanks to my well wishers.

Signature of the students :

*Piyush*

*Pranav*

Name of the students : Piyush Tandon

Pranav Murty

Date : 24.05.2011

## Summary

This particular project on Network implementation was carried out in two parts and the work done divided during the academic year 2010-11. In this segment we developed virtual network on a simulating software and tally the results from there itself. Work done primarily consisted of building different topologies on the simulating software, Packet Tracer. Configuration of network devices like Routers, Switches was also done in virtual mode. The network implementation using packet tracer helps in analysis and visualization of the actual network prior to implementation.

## 1.1 Introduction to Computer Network

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

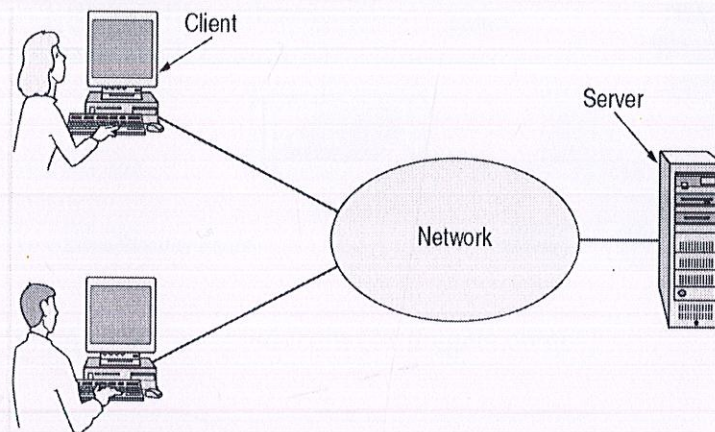


Figure 1.1 : Adapted from Forouzen[7]

- Collection of devices that can communicate together.
- The fabric that ties business applications together.

Computer networks can be classified according to the hardware and software technology that is used to inter connect the individual devices in the network such as wireless LAN, Ethernet, HomePNA.

Ethernet as it is defined by IEEE 802 utilizes various standards and mediums that enable communication between devices. Frequently deployed devices include hubs, switches, bridges or routers. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infra red signals as a transmission medium. ITU-T G.hn technology uses existing home wiring to create high speed local area network.



The network components are summarized as under:

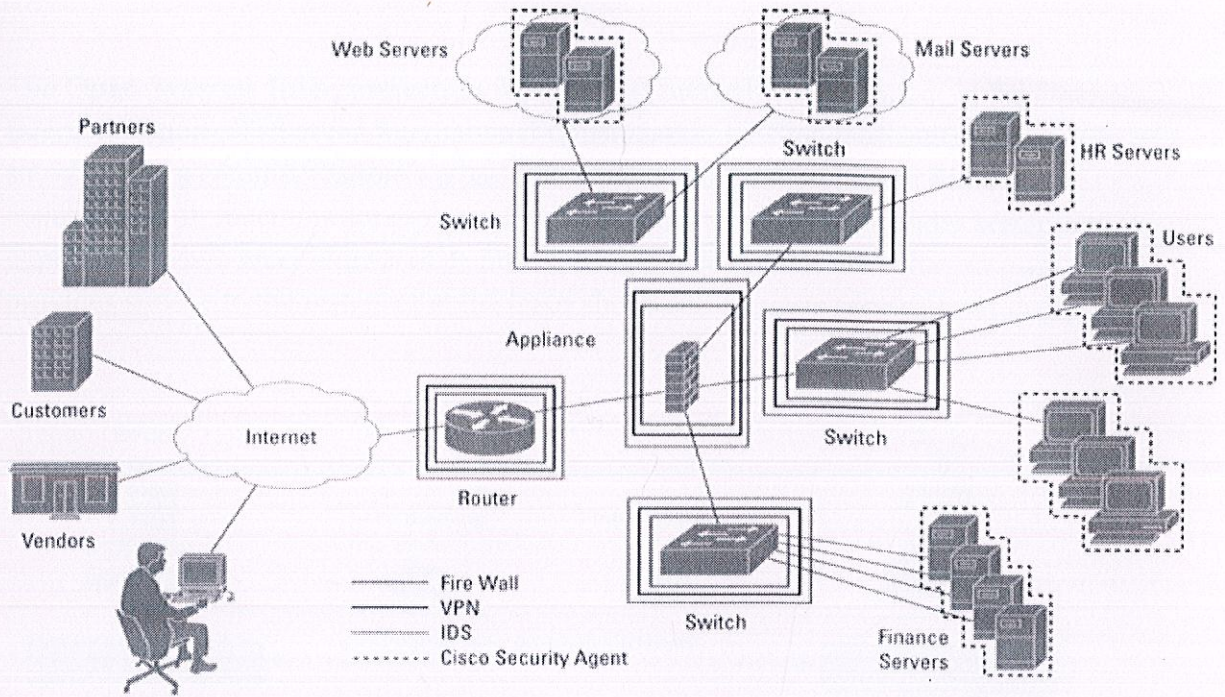


Figure 1.2 : Adapted from cbt nuggets.com[4]

## 1.2 OSI MODEL

The **Open Systems Interconnection model (OSI model)** was a product of the Open Systems Interconnection effort at the International Organization for Standardization. It is a way of sub-dividing a communications system into smaller parts called layers. Similar communication functions are grouped into logical layers. A layer provides services to its upper layer while receiving services from the layer below. On each layer, an *instance* provides service to the instances at the layer above and requests service from the layer below.

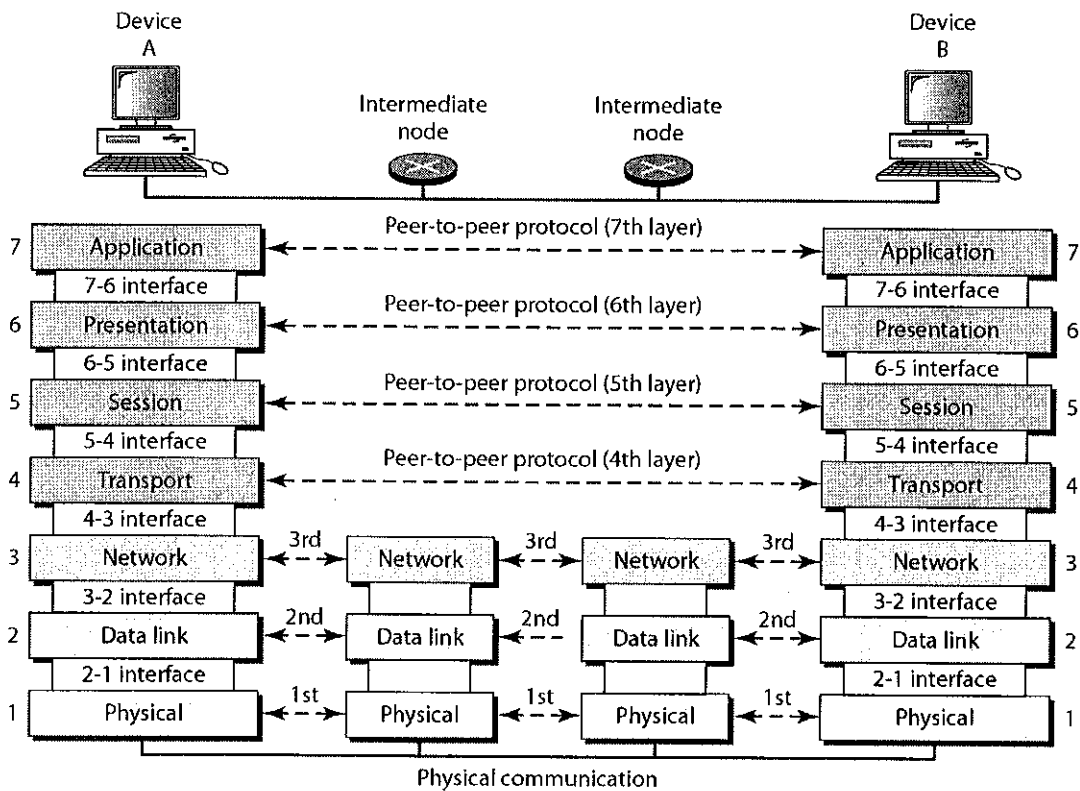


Figure 1.3 : Adapted from Forouzen[7]

## 1.3 Data exchange in OSI

The seven OSI layers use various forms of control information to communicate with their peer layers in other computer systems. This *control information* consists of specific requests and instructions that are exchanged between peer OSI layers.

Control information typically takes one of two forms: headers and trailers. Headers are prepended to data *that has been* passed down from upper layers. Trailers are appended to data *that has been* passed down from upper layers. An OSI layer is not required to attach a header or trailer to data *from upper layers*.

Headers, trailers, and data are relative concepts, depending on the layer that analyzes the information unit. At the network layer, an information unit, for example, consists of a Layer 3 header and data. At the data link layer, however, all the information passed down by the network layer (the Layer 3 header and the data) is treated as data.

In other words, the data portion of an information unit at a given OSI layer potentially *can* contain headers, trailers, and data from all the higher layers. This is known as *encapsulation*..

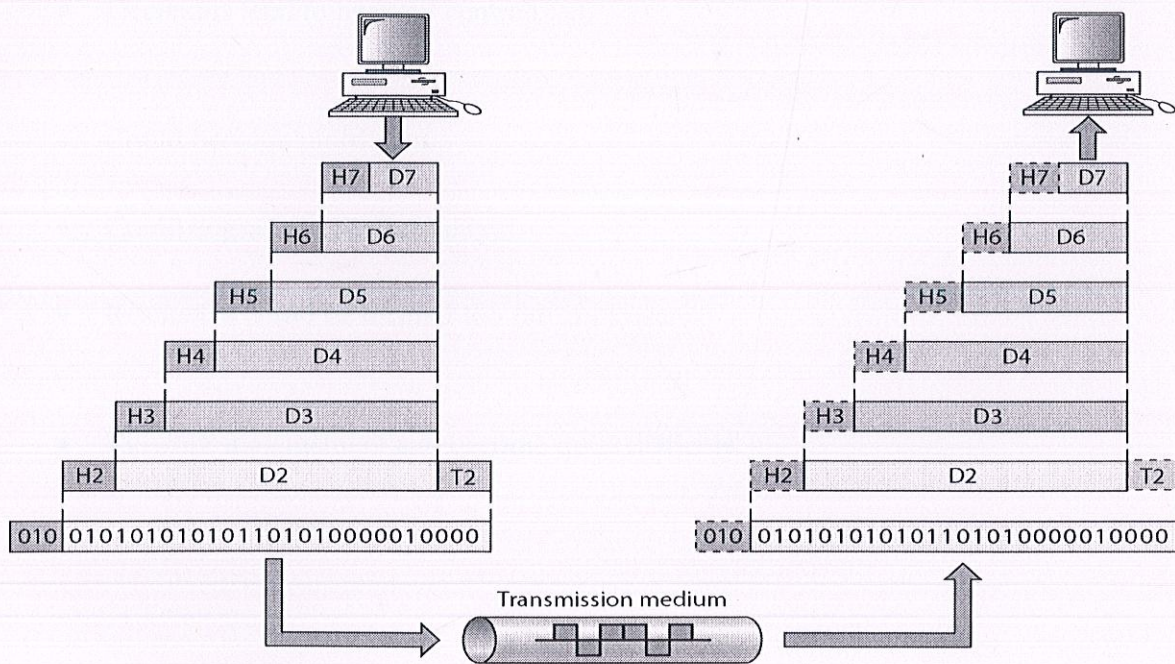


Figure 1.4 : Adapted from Forouzen[7]

## 1.4 Drawbacks of OSI Reference models

- Server faults stops applications being available
- Network faults can cause loss of data.
- Network fault could lead to loss of resources.
- User work dependent upon network.
- System open to hackers.
- Decisions tend to become centralized.
- Could become inefficient
- Could degrade in performance.
- Resources could be located too far from users.
- Network management can become quite difficult.

## 1.5 Comparison of OSI with TCP/ IP suite

The three top layers in the OSI model – the Application Layer, the Presentation Layer and the Session Layer – are not distinguished separately in the TCP/IP model where it is just the Application Layer. While some pure OSI protocol applications, such as X.400, also combined them, there is no requirement that a TCP/IP protocol stack needs to impose monolithic architecture above the Transport Layer. For example, the Network File System (NFS) application protocol runs over the external Data Representation (XDR) presentation protocol, which, in turn, runs over a protocol with the Session Layer functionality, Remote Procedure Call (RPC). RPC provides reliable record transmission, so it can run safely over the best-effort User Datagram protocol (UDP) transport.

The session Layer roughly corresponds to the Telnet virtual terminal functionality, which is part of text based protocols such as the HTTP and SMTP TCP/IP model Application Layer protocols. It also corresponds to TCP and UDP port numbering, which is considered as part of the transport layer in the TCP/IP model. Some functions that would have been performed by an OSI presentation layer are realized at the Internet application layer using the MIME standard, which is used in application layer protocols such as HTTP and SMTP.

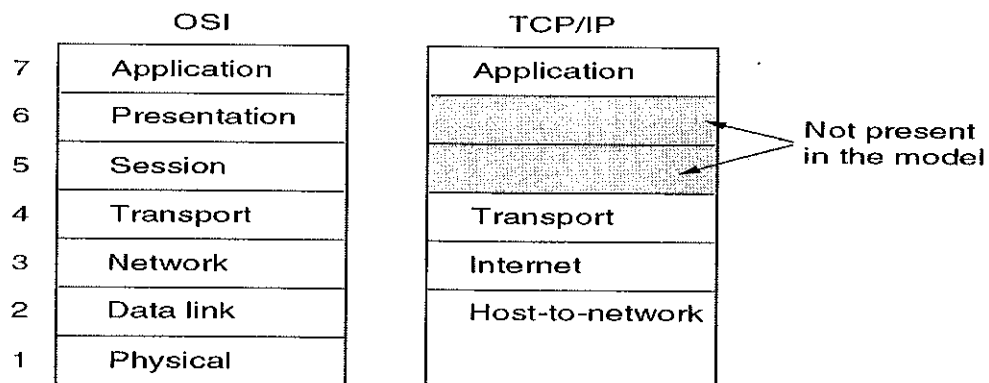


Figure 1.5 : Adapted from Tennanbaum[6]

## 1.6 BASIC TCP/IP

The TCP/IP Model is a description framework for computer network protocols created in the 1970's by DARPA, an agency of the United States Department of Defense. It evolved from ARPANET, which was the world's first wide area network and a predecessor of the Internet. The TCP/IP Model is sometimes called the Internet model or the DoD model.

It has four abstraction layers as defined in RFC 1122. This layer architecture is often compared with the seven-layer OSI Reference Model; using terms such as Internet reference model, incorrectly, however, because it is descriptive while the OSI Reference Model was intended to be prescriptive, hence being a reference model.

The TCP/IP Model, or Internet Protocol Suite, describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network. TCP/IP provides end to end connectivity specifying how data should be formatted, addressed, transmitted, routed, and received at the destination.

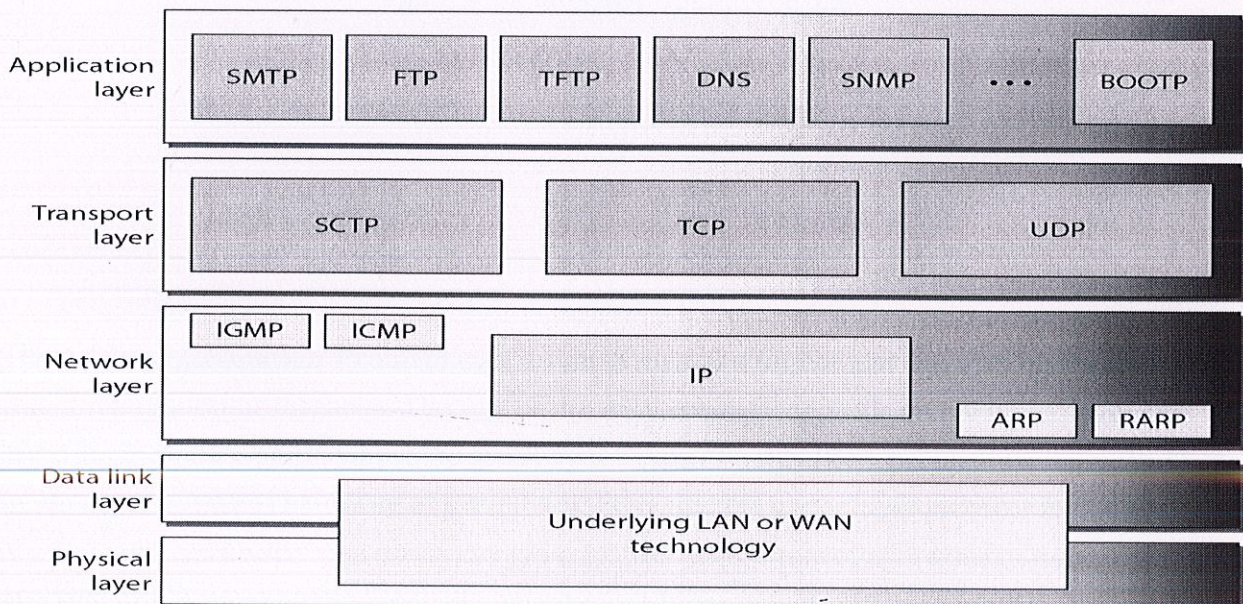
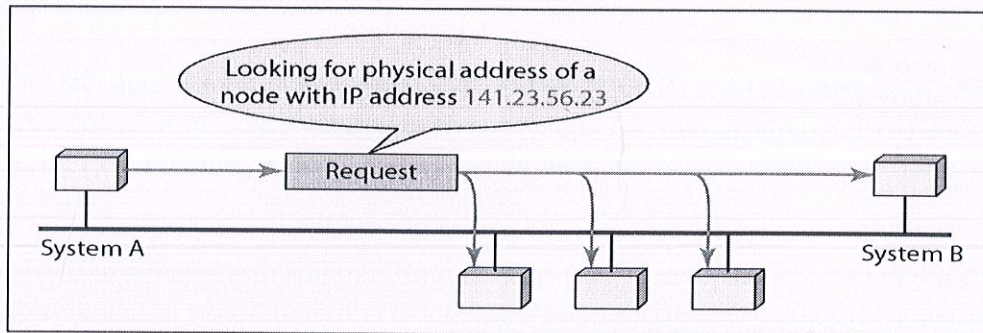
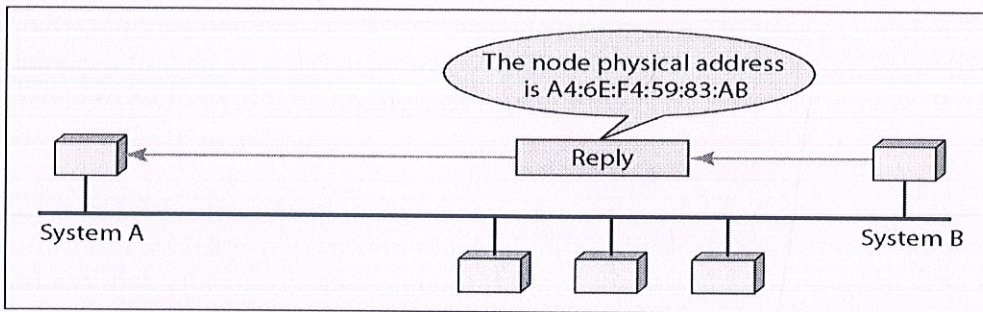


Figure 1.6 : Adapted from Forouzen

## 1.7 Address Resolution Protocol



a. ARP request is broadcast



b. ARP reply is unicast

Figure 1.7 : Adapted from Forouzen

The **Address Resolution Protocol** uses a simple message format that contains one address resolution request or response. The size of the ARP message depends on the upper layer and lower layer address sizes, which are given by the type of networking protocol (usually IPv4) in use and the type of hardware or virtual link layer that the upper layer protocol is running on. The message header specifies these types, as well as the size of addresses of each. The message header is completed with the operation code for request (1) and reply (2).

## 1.8 RARP

The **Reverse Address Resolution Protocol (RARP)** is an obsolete computer networking protocol used by a host computer to request its Internet Protocol (IPv4) address from an administrative host, when it has available its Link Layer or hardware address, such as a MAC address.

RARP is described in Internet Engineering Task Force (IETF) publication RFC 903. It has been rendered obsolete by the Bootstrap Protocol (BOOTP) and the modern Dynamic Host Configuration Protocol (DHCP), which both support a much greater feature set than RARP.

RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses. Media Access Control (MAC) addresses needed to be individually configured on the servers by an administrator. RARP was limited to serving only IP addresses.

Reverse ARP differs from the Inverse Address Resolution Protocol (InARP) described in RFC 2390, which is designed to obtain the IP address associated with another host's MAC address. InARP is the complement of the Address Resolution Protocol used for the reverse lookup.

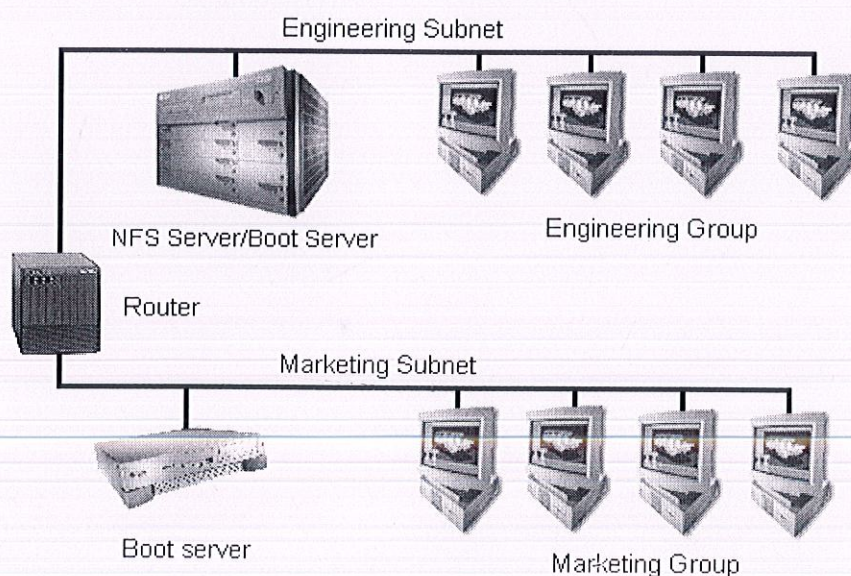


Figure 1.8 : Adapted from Forouzen



The project aims at :

This particular Project aims at implementing a virtual network and a platform like Packet Tracer by using virtual routers and switches.

Chapter 2 deals with the MAC and the physical addressing, followed by chapter 3 which deals with the different network topologies. Chapter 4 deals with the routing protocols while the last two chapters deal with the implementation and commands.

## Chapter 2

(LAN's)

A **local area network (LAN)** is a computer network that connects computers and devices in a limited geographical area such as home, school, computer laboratory or office building. The defining characteristics of LANs, in contrast to wide area networks (WAN's), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

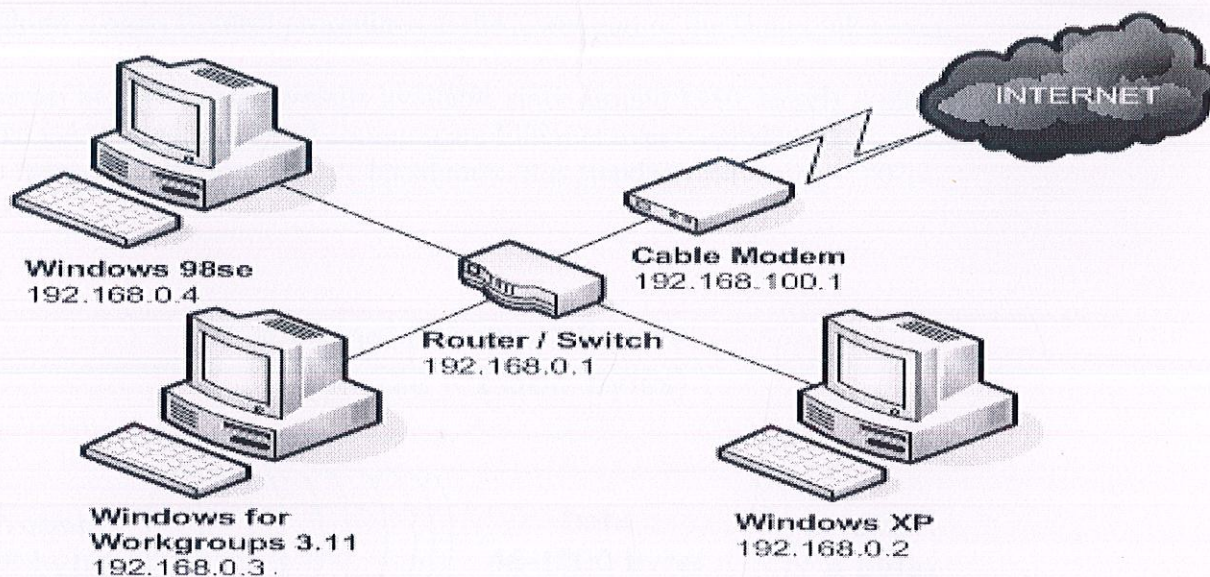


Figure 2.1 : Adapted from cbt nuggets.com

Early LAN cabling had always been based on various grades of coaxial cable. However shielded twisted pair was used in IBM's Token Ring implementation, and in 1984 StarLAN showed the potential of simple *unshielded* twisted pair by using Cat3—the same simple cable used for telephone systems. This led to the development of 10Base-T (and its successors) and structured cabling which is still the basis of most commercial LANs today. In addition, fiber-optic cabling is increasingly used in commercial applications.

As cabling is not always possible, wireless Wi-Fi is now the most common technology in residential premises, as the cabling required is minimal and it is well suited to mobile laptops and smartphones.

## 2.1 Ethernet

**Ethernet** is a family of frame-based computer networking technologies for local area networks (LAN). It defines a number of wiring and signaling standards for the Physical Layer of the standard networking model as well as a common addressing format and a variety of Medium Access Control procedures at the lower part of the Data Link Layer.

Ethernet has been commercially available since around 1980, largely replacing competing wired LAN standards. Most common are Ethernet over twisted pair to connect end systems, and fiber optic versions for site backbones. It is standardized as IEEE 802.3.

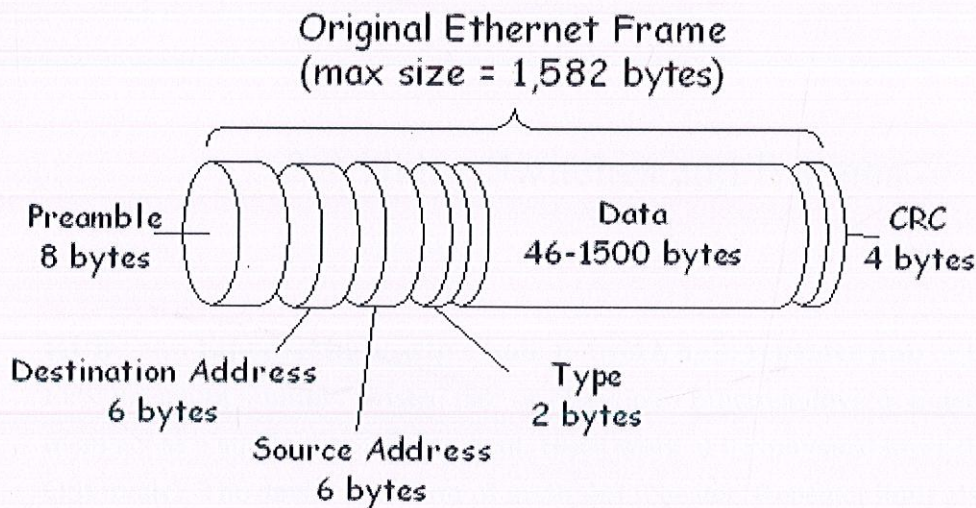


Figure 2.2 : Adapted from cbt nuggets.com

Shared cable Ethernet was always hard to install in offices because its bus topology was in conflict with the star topology cable plans designed into buildings for telephony. Modifying Ethernet to conform to twisted pair telephone wiring already installed in commercial buildings provided another opportunity to lower costs, expand the installed base, and leverage building design, and, thus, twisted-pair Ethernet was the next logical development in the mid-1980s, beginning with StarLAN.

## 2.2 CSMA/CD

**Carrier sense multiple access with collision detection (CSMA/CD)** is a computer networking access method in which:

- a carrier sensing scheme is used.
- a transmitting data station that detects another signal while transmitting a frame, stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to send that frame again.

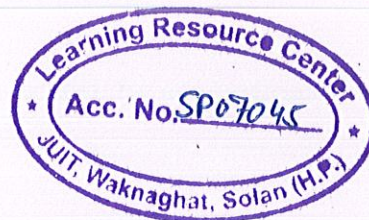
## 2.3 Hubs, Switches and Bridges

**HUB :-** An **Ethernet hub, active hub, network hub, repeater hub** or **hub** is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

**SWITCH :-** Switches may operate at one or more layers of the OSI model, including data link, network, or transport (i.e., end-to-end). A device that operates simultaneously at more than one of these layers is known as a multilayer switch.

In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fibre Channel, ATM, ITU-T G.hn and 802.11. This connectivity can be at any of the layers mentioned. While Layer 2 functionality is adequate for bandwidth-shifting within one technology, interconnecting technologies such as Ethernet and token ring are easier at Layer 3.

## BRIDGES :-



### Advantages :-

- Self-configuring
- Simple bridges are inexpensive
- Isolate collision domain
- Reduce the size of collision domain by microsegmentation in non-switched networks
- Transparent to protocols above the MAC layer
- Allows the introduction of management/performance information and access control
- LANs interconnected are separate, and physical constraints such as number of stations, repeaters and segment length don't apply
- Helps minimize bandwidth usage.

## 2.4 MAC ADDRESSING

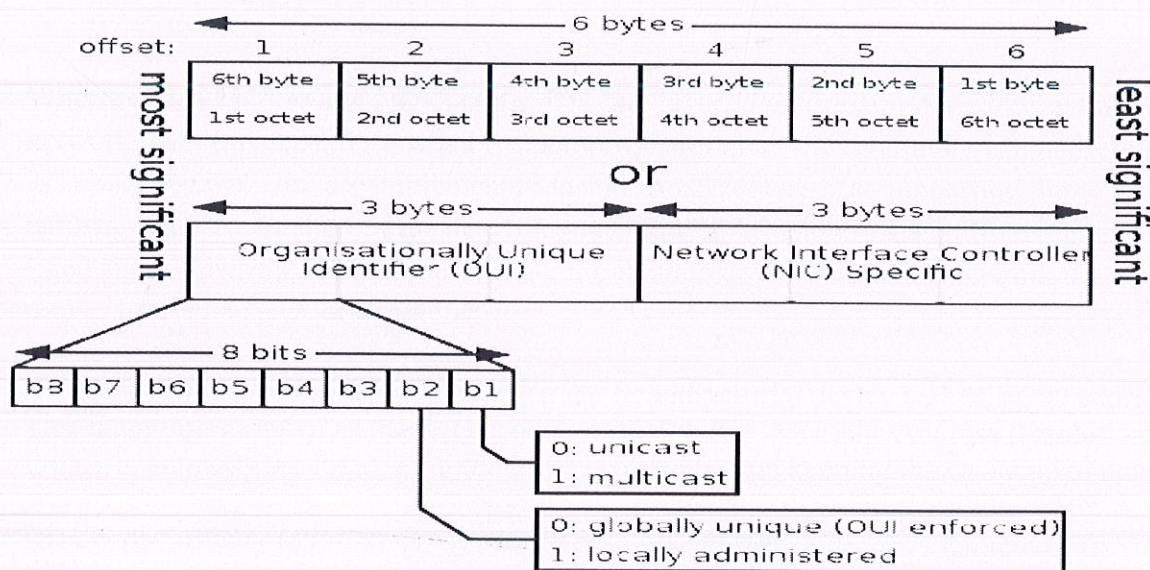


Figure 2.3 : Adapted from cbt nuggets.com

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as **hardware** addresses or **physical** addresses. 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-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body (see sidebar). The second half 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.

- **MAC vs. IP Addressing**

Whereas MAC addressing works at the data link layer, IP addressing functions at the network layer (layer 3). It's a slight oversimplification, but one can think of IP addressing as supporting the software implementation and MAC addresses as supporting the hardware implementation of the network stack. The MAC address generally remains fixed and follows the network device, but the IP address changes as the network device moves from one network to another.

IP networks maintain a mapping between the IP address of a device and its MAC address. This mapping is known as the **ARP cache** or **ARP table**. ARP, the Address Resolution Protocol, supports the logic for obtaining this mapping and keeping the cache up to date.

DHCP also usually relies on MAC addresses to manage the unique assignment of IP addresses to devices.

# CHAPTER 3

## (Network Topologies)

**Network topology** is the layout pattern of interconnections of the various elements (links, nodes, etc.) of a computer network. Network topologies may be physical or logical. Physical topology means the physical design of a network including the devices, location and cable installation. Logical topology refers to how data is actually transferred in a network as opposed to its physical design. In general physical topology relates to a core network whereas logical topology relates to basic network.

Topology can be considered as a virtual shape or structure of a network. This shape does not correspond to the actual physical design of the devices on the computer network. The computers on a home network can be arranged in a circle but it does not necessarily mean that it represents a ring topology.

Any particular network topology is determined only by the graphical mapping of the configuration of physical and/or logical connections between nodes. The study of network topology uses graph theory. Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ in two networks and yet their topologies may be identical.

A **local area network (LAN)** is one example of a network that exhibits both a physical topology and a logical topology. Any given node in the LAN has one or more links to one or more nodes in the network and the mapping of these links and nodes in a graph results in a geometric shape that may be used to describe the physical topology of the network. Likewise, the mapping of the data flow between the nodes in the network determines the logical topology of the network. The physical and logical topologies may or may not be identical in any particular network.

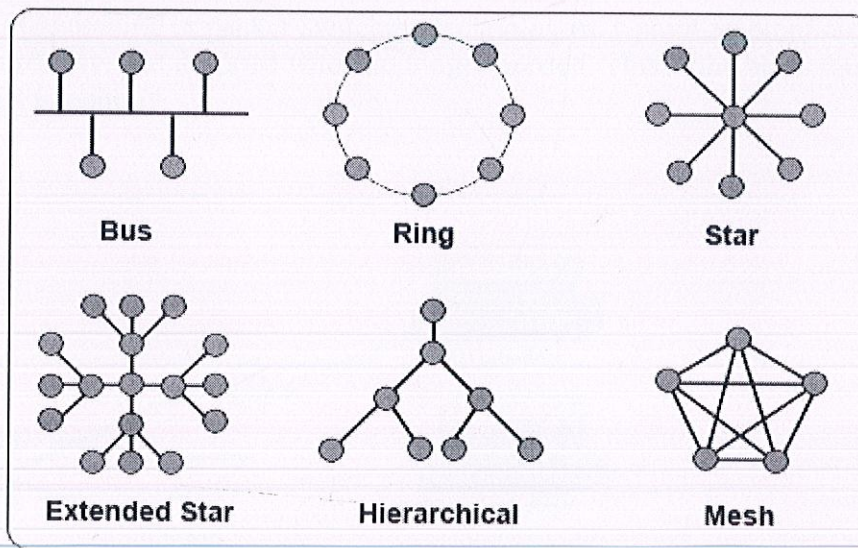


Figure 3.1 : Adapted from cbt nuggets.com



## 3.1 POINT TO POINT

The simplest topology is a permanent link between two endpoints (the *line* in the illustration at the top of the page). Switched point-to-point topologies are the basic model of conventional telephony. The value of a permanent point-to-point network is the value of guaranteed, or nearly so, communications between the two endpoints. The value of an on-demand point-to-point connection is proportional to the number of potential pairs of subscribers, and has been expressed as Metcalfe's Law.

- **Permanent (dedicated)**

Easiest to understand, of the variations of point-to-point topology, is a point-to-point communications channel that appears, to the user, to be permanently associated with the two endpoints. A children's "tin-can telephone" is one example, with a microphone to a single public address speaker is another. These are examples of *physical dedicated* channels.

- **Switched:**

Using circuit-switching or packet-switching technologies, a point-to-point circuit can be set up dynamically, and dropped when no longer needed. This is the basic mode of conventional telephony

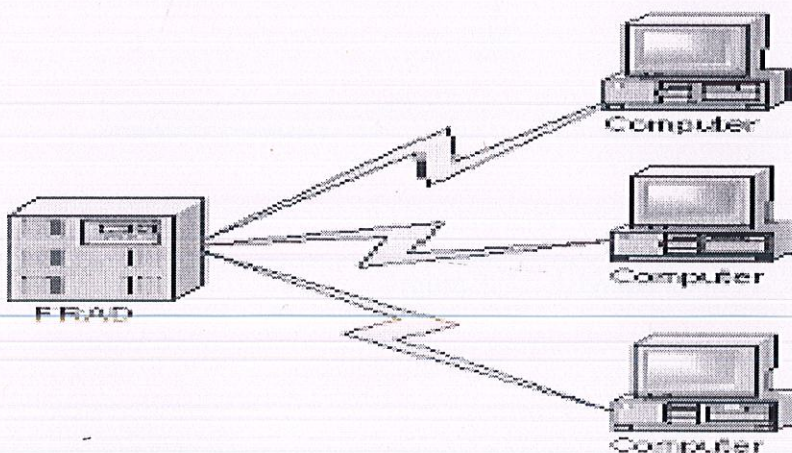


Figure 3.2 :Adapted from cbt nuggets.com

## 3.2 BUS

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable through some kind of connector. A terminator is required at each end of the bus cable to prevent the signal from bouncing back and forth on the bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the MAC address or IP address on the network that is the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data does match the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable breaks, the entire network will be down.

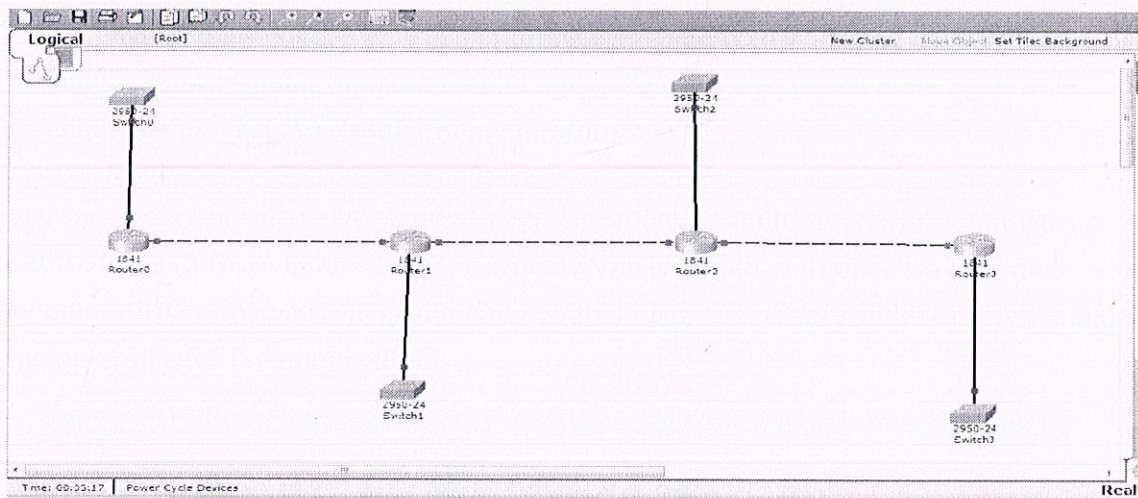


Figure 3.3 : Adapted from Packet tracer.

## 3.3 STAR

In local area networks with a star topology, each network host is connected to a central hub. In contrast to the bus topology, the star topology connects each node to the hub with a point-to-point connection. All traffic that traverses the network passes through the central hub. The hub acts as a signal booster or repeater. The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the hub represents a single point of failure.

- A point-to-point link (described above) is sometimes categorized as a special instance of the physical star topology – therefore, the simplest type of network that is based upon the physical star topology would consist of one node with a single point-to-point link to a second node, the choice of which node is the 'hub' and which node is the 'spoke' being arbitrary.

Star networks may also be described as either broadcast multi-access or nonbroadcast multi-access (NBMA), depending on whether the technology of the network either automatically propagates a signal at the hub to all spokes, or only addresses individual spokes with each communication

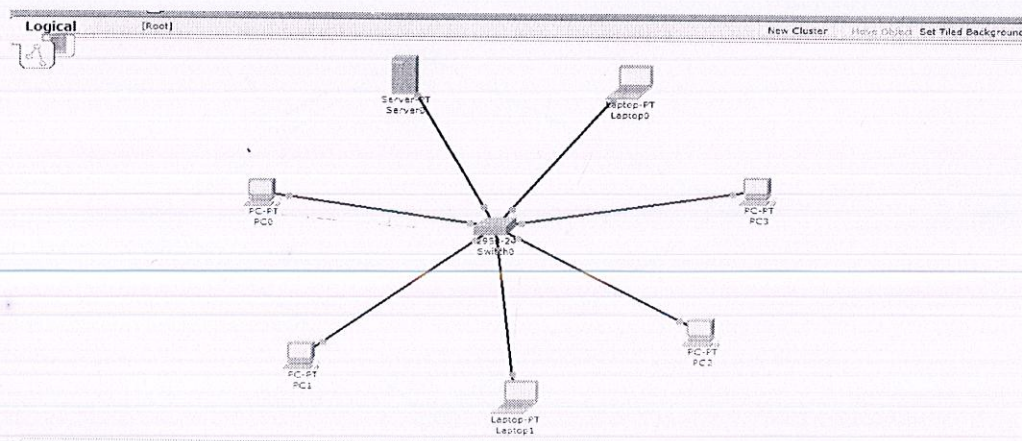


Figure 3.4 : Adapted from Packet Tracer

## 3.4 RING

A **ring network** is a network topology in which each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node - a ring. Data travels from node to node, with each node along the way handling every packet.

Because a ring topology provides only one pathway between any two nodes, ring networks may be disrupted by the failure of a single link. A node failure or cable break might isolate every node attached to the ring.

### Advantages :-

- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a bus topology under heavy network load

### Disadvantages

- One malfunctioning workstation or bad port in the MAU can create problems for the entire network
- Moves, adds and changes of devices can affect the network.

Many ring networks add a "counter-rotating ring" to form a redundant topology. Such "dual ring" networks include Spatial Reuse Protocol, Fiber Distributed Data Interface (FDDI), and Resilient Packet Ring.

- 802.5 networks -- also known as IBM Token Ring networks—avoid the weakness of a ring topology altogether: they actually use a *star* topology at the *physical* layer and a Multistation Access Unit (MAU) to *imitate* a ring at the *datalink* layer

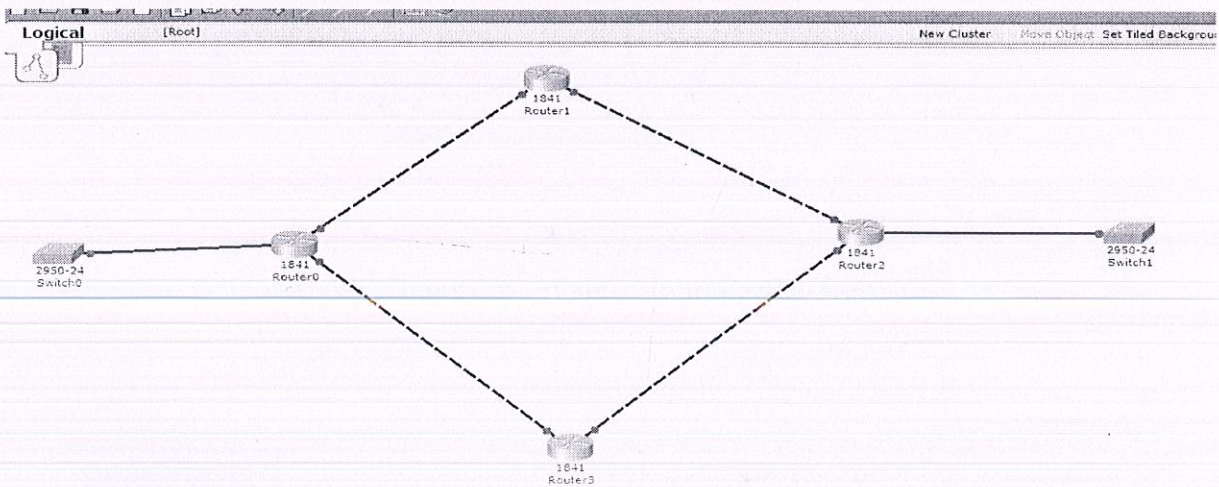


Figure 3.5 : Adapted from Packet Tracer

## 3.5 MESH

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law

The number of connections in a full mesh =  $n(n - 1) / 2$

### Partially connected :-

The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network

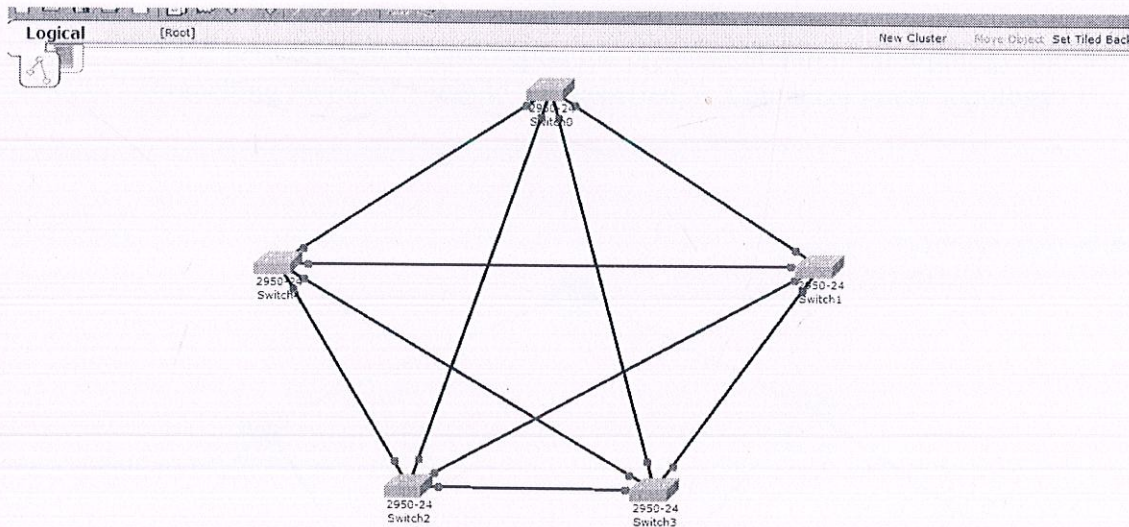


Figure 3.6 :Adapted from Packet Tracer

## 3.6 TREES

The type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy (The hierarchy of the tree is symmetrical.) Each node in the network having a specific fixed number, of nodes connected to it at the next lower level in the hierarchy, the number, being referred to as the 'branching factor' of the hierarchical tree. This tree has individual peripheral nodes.

- 1.) A network that is based upon the physical hierarchical topology must have at least three levels in the hierarchy of the tree, since a network with a central 'root' node and only one hierarchical level below it would exhibit the physical topology of a star.
- 2.) A network that is based upon the physical hierarchical topology and with a branching factor of 1 would be classified as a physical linear topology.

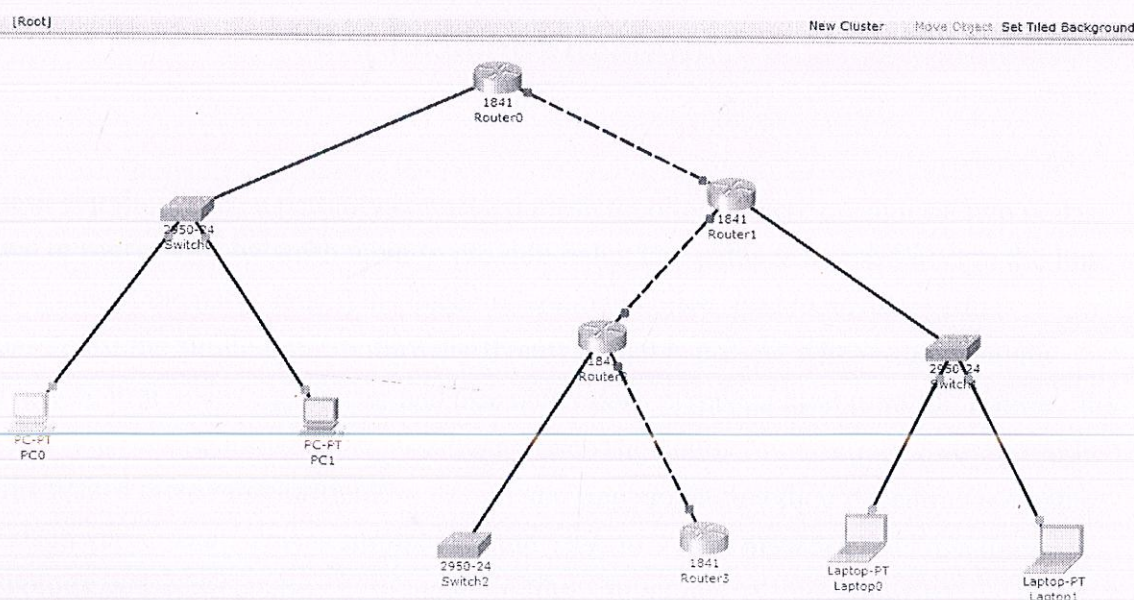


Figure 3.7 : Adapted from Packet Tracer

## 3.7 Daisy Chains

Except for star-based networks, the easiest way to add more computers into a network is by daisy-chaining, or connecting each computer in series to the next. If a message is intended for a computer partway down the line, each system bounces it along in sequence until it reaches the destination. A daisy-chained network can take two basic forms: linear and ring.

- A **linear topology** puts a two-way link between one computer and the next. However, this was expensive in the early days of computing, since each computer (except for the ones at each end) required two receivers and two transmitters.
- By connecting the computers at each end, a **ring topology** can be formed. An advantage of the ring is that the number of transmitters and receivers can be cut in half, since a message will eventually loop all of the way around. When a node sends a message, the message is processed by each computer in the ring. If a computer is not the destination node, it will pass the message to the next node, until the message arrives at its destination. If the message is not accepted by any node on the network, it will travel around the entire ring and return to the sender. This potentially results in a doubling of travel time for data.

## 3.8 Decentralization

In a **mesh topology** (i.e., a partially connected mesh topology), there are at least two nodes with two or more paths between them to provide redundant paths to be used in case the link providing one of the paths fails. This decentralization is often used to advantage to compensate for the single-point-failure disadvantage that is present when using a single device as a central node (e.g., in star and tree networks). A special kind of mesh, limiting the number of hops between two nodes, is a hypercube. The number of arbitrary forks in mesh networks makes them more difficult to design and implement, but their decentralized nature makes them very useful. This is similar in some ways to a **grid network**, where a linear or ring topology is used to connect systems in multiple directions. A multi-dimensional ring has a toroidal topology, for instance.

## 3.9 CENTRALIZATION

The **star topology** reduces the probability of a network failure by connecting all of the peripheral nodes (computers, etc.) to a central node. When the physical star topology is applied to a logical bus network such as Ethernet, this central node (traditionally a hub) rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network, sometimes including the originating node. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node only. The failure of a transmission line linking any peripheral node to the central node will result in the isolation of that peripheral node from all others, but the remaining peripheral nodes will be unaffected. However, the disadvantage is that the failure of the central node will cause the failure of all of the peripheral nodes also,

If the central node is *passive*, the originating node must be able to tolerate the reception of an echo of its own transmission, delayed by the two-way round trip transmission time (i.e. to and from the central node) plus any delay generated in the central node. An *active* star network has an active central node that usually has the means to prevent echo-related problems.

A **tree topology** (a.k.a. **hierarchical topology**) can be viewed as a collection of star networks arranged in a hierarchy. This tree has individual peripheral nodes (e.g. leaves) which are required to transmit to and receive from one other node only and are not required to act as repeaters or regenerators. Unlike the star network, the functionality of the central node may be distributed.

As in the conventional star network, individual nodes may thus still be isolated from the network by a single-point failure of a transmission path to the node. If a link connecting a leaf fails, that leaf is isolated; if a connection to a non-leaf node fails, an entire section of the network becomes isolated from the rest.

In order to alleviate the amount of network traffic that comes from broadcasting all signals to all nodes, more advanced central nodes were developed that are able to keep track of the identities of the nodes that are connected to the network. These network switches will "learn" the layout of the network by "listening" on each port during normal data transmission, examining the data packets and recording the address/identifier of each connected node and which port it's connected to in a lookup table held in memory. This lookup table then allows future transmissions to be forwarded to the intended destination only.



CHAPTER 4  
(Routing Protocols)

## 4.1 Routing Information Protocol

*RIP* is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP). It uses the distance-vector routing algorithm. It was first defined in RFC 1058 (1988). The protocol has since been extended several times, resulting in RIP Version 2 (RFC 2453). Both versions are still in use today, although they are considered to have been made technically obsolete by more advanced techniques such as Open Shortest Path First (OSPF) and the OSI protocol IS-IS. RIP has also been adapted for use in IPv6 networks, a standard known as RIPng (RIP next generation) protocol, published in RFC 2080.

RIP is a distance-vector routing protocol, which employs the hop count as a routing metric. The hold down time is 180 seconds. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

RIP implements the split horizon, route poisoning and holddown mechanisms to prevent incorrect routing information from being propagated. These are some of the stability features of RIP. It is also possible to use the so called RMTI (Routing Information Protocol with Metric-based Topology Investigation) algorithm to cope with the count to infinity problem. With its help, it is possible to detect every possible loop with a very small computation effort.

Originally each RIP router transmitted full updates every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant. As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times. It was thought, as a result of random initialization, the routing updates would spread out in time, but this was not true in practice. Sally Floyd and Van Jacobson showed in 1994 that, without slight randomization of the update timer, the timers synchronized over time. In most current networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS (the latter two being link-state routing protocols), and (without RMTI) a hop limit severely limits the size of network it can be used in. However, it is easy to configure, because RIP does not require any parameters on a router unlike other protocols .

RIP is implemented on top of the User Datagram Protocol as its transport protocol. It is assigned the reserved port number 520.

## 4.2 Versions of RIP

### RIP version 1

The original specification of RIP, defined in RFC 1058, uses classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size. There is also no support for router authentication, making RIP vulnerable to various attacks. The RIP version 1 works when there is only 16 hop counts (0-15). If there are more than 16 hops between two routers it fails to send data packets to the destination address.

### RIP version 2

Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993 and last standardized in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all *Must Be Zero* protocol fields in the RIPv1 messages are properly specified. In addition, a *compatibility switch* feature allows fine-grained interoperability adjustments.

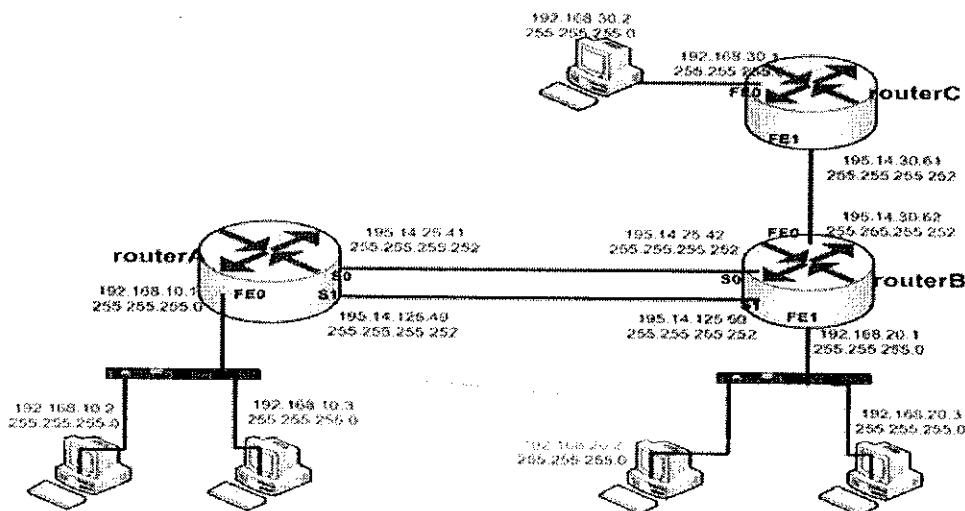


Figure 4.1: Adapted from cbnuggets.com

## RIPng

RIPng (RIP next generation), defined in RFC 2080, is an extension of RIPv2 for support of IPv6, the next generation Internet Protocol. The main differences between RIPv2 and RIPng are:

- Support of IPv6 networking.
- While RIPv2 supports RIPv1 updates authentication, RIPng does not. IPv6 routers were, at the time, supposed to use IPsec for authentication.
- RIPv2 allows attaching arbitrary tags to routes, RIPng does not;

RIPv2 encodes the next-hop into each route entries, RIPng requires specific encoding of the next hop for a set of route entries.

## 4.3 OSPF v/s IS-IS

**Open Shortest Path First (OSPF)** is an adaptive 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). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340(2008). Research into the convergence time of OSPF can be found in Stability Issues in OSPF Routing (2001).

OSPF is perhaps the most widely-used interior gateway protocol (IGP) in large enterprise networks. IS-IS, another link-state routing protocol, is more common in large service provider networks. The most widely-used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet.

**Intermediate System To Intermediate System (IS-IS)**, is a routing protocol designed to move information efficiently within a computer network, a group of physically connected computers or similar devices. It accomplishes this by determining the best route for datagrams through a packet-switched network. The protocol was defined in ISO/IEC 10589:2002 as an international standard within the Open Systems Interconnection (OSI) reference design. Though originally an ISO standard, the IETF republished the protocol as an Internet Standard in RFC 1142. IS-IS has been called "the de facto standard for large service provider network backbones."

## 4.4 IGRP

**Interior Gateway Routing Protocol (IGRP)** is a distance vector interior routing protocol (IGP) invented by Cisco. It is used by routers to exchange routing data within an autonomous system.

IGRP is a proprietary protocol. IGRP was created in part to overcome the limitations of RIP (maximum hop count of only 15, and a single routing metric) when used within large networks. IGRP supports multiple metrics for each route, including bandwidth, delay, load, MTU, and reliability to compare two routes these metrics are combined together into a single metric, using a formula which can be adjusted through the use of pre-set constants. The maximum hop count of IGRP-routed packets is 255 (default 100), and routing updates are broadcast every 90 seconds (by default).

IGRP is considered a classful routing protocol. Because the protocol has no field for a subnet mask, the router assumes that all interface addresses within the same Class A, Class B, or Class C network have the same subnet mask as the subnet mask configured for the interfaces in question. This contrasts with classless routing protocols that can use variable length subnet masks. Classful protocols have become less popular as they are wasteful of IP address space.

CHAPTER 5  
(CISCO IOS)

## 5.1 Configuration of Network devices using Cisco IOS

- The Internetwork Operating System
- A command line method of configuring a cisco device.
- Software that is consistent through nearly all cisco devices.
- Learn it once, use it many times.
- More powerful than any graphic interface.

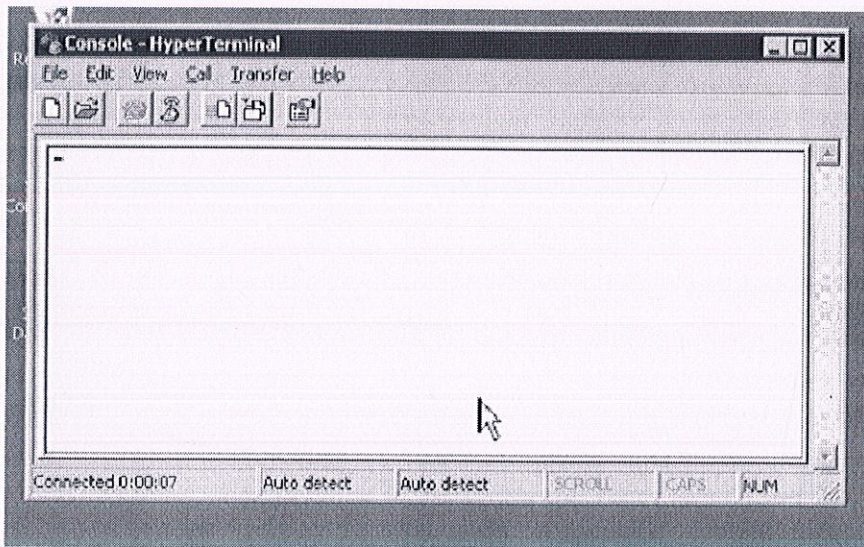


Fig 5.1: Adapted from cbt nuggets.com

# Connecting the switch and configuring the terminal program you are going to use :-

- A. Get a console cable
- B. Plug the serial end into the back of your pc
- C. Plug the RJ45 end into console port of switch
- D. Get a terminal program like hyper terminal, tera terminal etc.
- E. Set it to connect via COM PORT with :-
  - Baud rate - 9600
  - Data bits - 8
  - Parity - none
  - Stop bits - 1
  - Flow control - none

## Cisco Routers

Main keys - ?, TAB, Spacebar, Enter

Always use “?” for help

You can shortcut any command that exists, as long as you’ve typed enough for it to be unique.

### Modes :-

- Switch> User mode (base monitoring made limited, user executes.)
- Switch# Privileged mode (verification only, no configuration, private execution.)
- Switch(config)# Global configuration mode (configurations and changes)

Example –

```
Switch>enable
Switch#configure t
Switch(config)# hostname PT_SWITCH
PT_SWITCH(config)# interface fast Ethernet 0/1
PT_SWITCH(config-if)#end
```

This sets switch name to PT\_SWITCH and accesses fast Ethernet port no 0/1.

NOTE – “end” moves the control back to privilege mode directly whereas “exit” moves back one step at a time.



While dealing with cisco switches we need to have an idea about the physical indicators, VLAN, commands etc.

## 5.2 Working with CISCO Switches

Physical Indicators :-

- System – green light is good, yellow is bad.
- RPS – is reluctant power supply, 2<sup>nd</sup> power supply, green light if available
- Stat – default
- VBL – indicates utilization currently
- Duplex – shows ports configured with full duplex by green light
- Speed – indicates speed

Cisco devices shows its memory in a way – 21567/1279 k

It partitions its memory, as to calculate its actual memory you add the two partitions.

Press “CTRL + C” to get out of configuration wizard if you typed “yes” while startup of the cisco router.

Now we will have a look at the different commands that are used and a look at some of the more useful ones.

## 5.3 Commands

- Switch(config)# ip address A.B.C.D E.F.G.H  
A.B.C.D is the ip address.  
E.F.G.H is the subnet mask.
- Switch(config)#ip default gateway A.B.C.D  
This sets the switch default gateway as A.B.C.D
- Switch#Show running-configuration  
This shows every command put in yet, but is in RAM, means, if the power is lost, data is lost. So now we learn how to save information in RAM.
- Switch#copy running-configuration startup-config
- Destination filename [startup-config]? PIYUSH
- Switch#Show startup-config
  
- Switch(config)#motd Hello World!  
This sets the default message of the day to "Hello World!" which is displayed at the startup everytime the router/switch is switched on.

Chapter 6  
(Configuration and Implementation)

## 6.1 Packet Tracer, The platform

**Packet Tracer** is a Cisco router simulator that can be utilized in training and education, but also in research for simple computer network simulations. The tool is created by Cisco Systems and provided for free distribution to faculty, students, and alumni who are or have participated in the Cisco Networking Academy. The purpose of Packet Tracer is to offer students and teachers a tool to learn the principles of networking as well as develop Cisco technology specific skills.

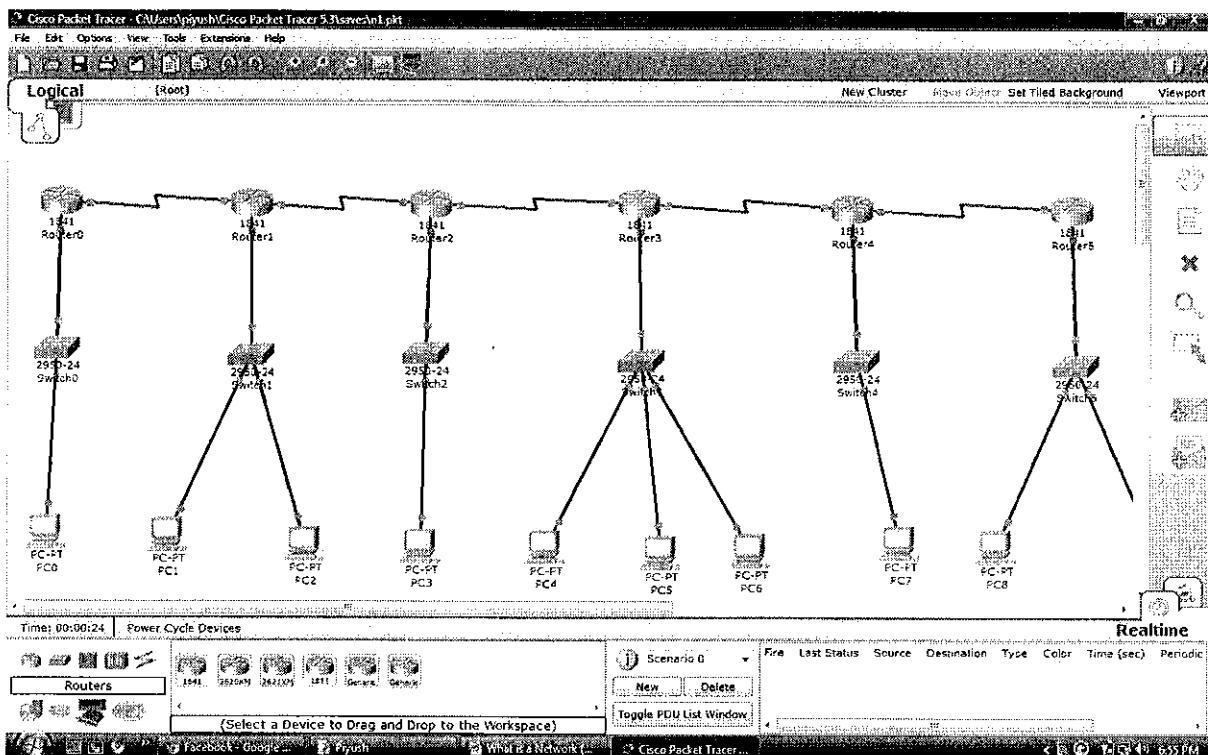


Fig 6.1: Adapted from packet tracer

Packet Tracer is commonly used by Cisco Networking Academy students working towards Cisco Certified Network Associate (CCNA) certification. Due to functional limitations, it is intended by Cisco to be used only as a learning aid, not a replacement for Cisco routers and switches.

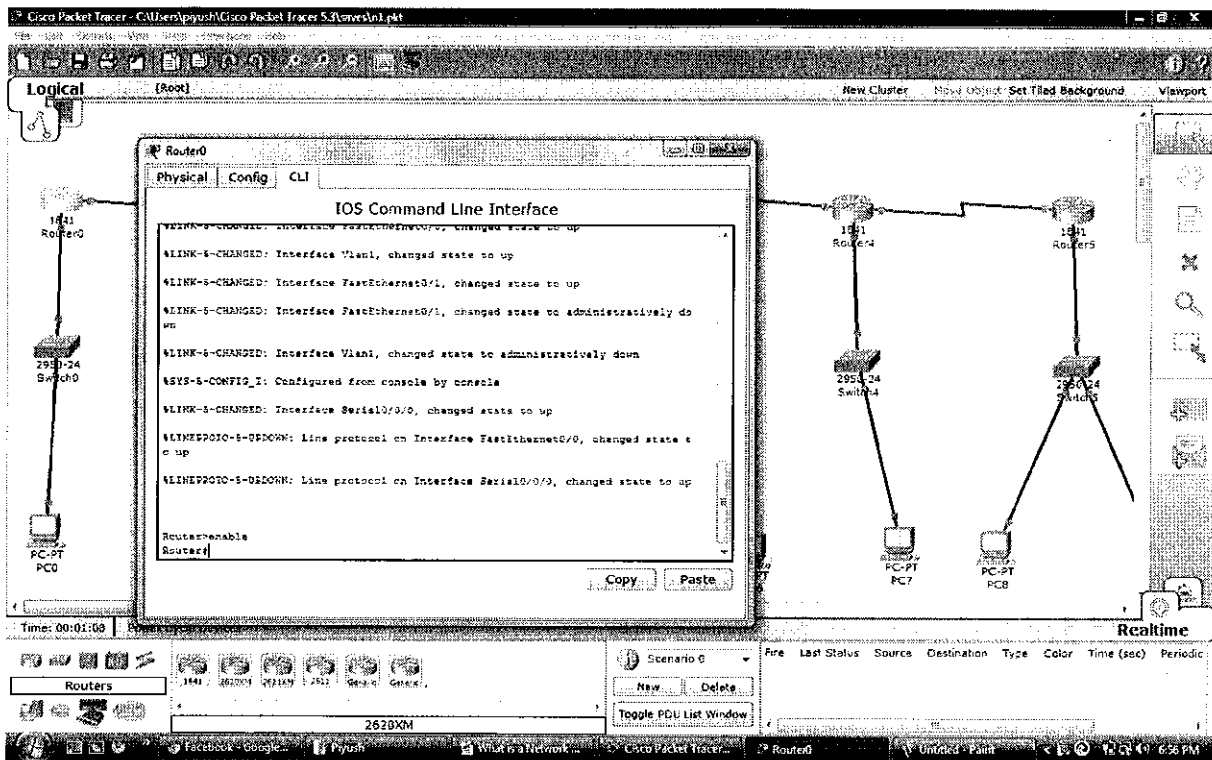


Fig 6.2: Adapted from packet tracer

This is the screenshot of the cisco packet tracer IOS. The CLI i.e Command Line Interface is a virtual terminal program which accepts the Cisco IOS language. All the commands are entered in the cli. Shifting from one mode to the other is also done via the cli. Different routers and switches are configured using this virtual cli that the packet tracer offers. There is also an easier option to configure the network devices offered by the packet tracer i.e the automatic config mode that does not require the user to know all the commands. But this mode is not helpful in the future since eventually when you work practically with cisco devices or other network devices you need to know all useful IOS commands.

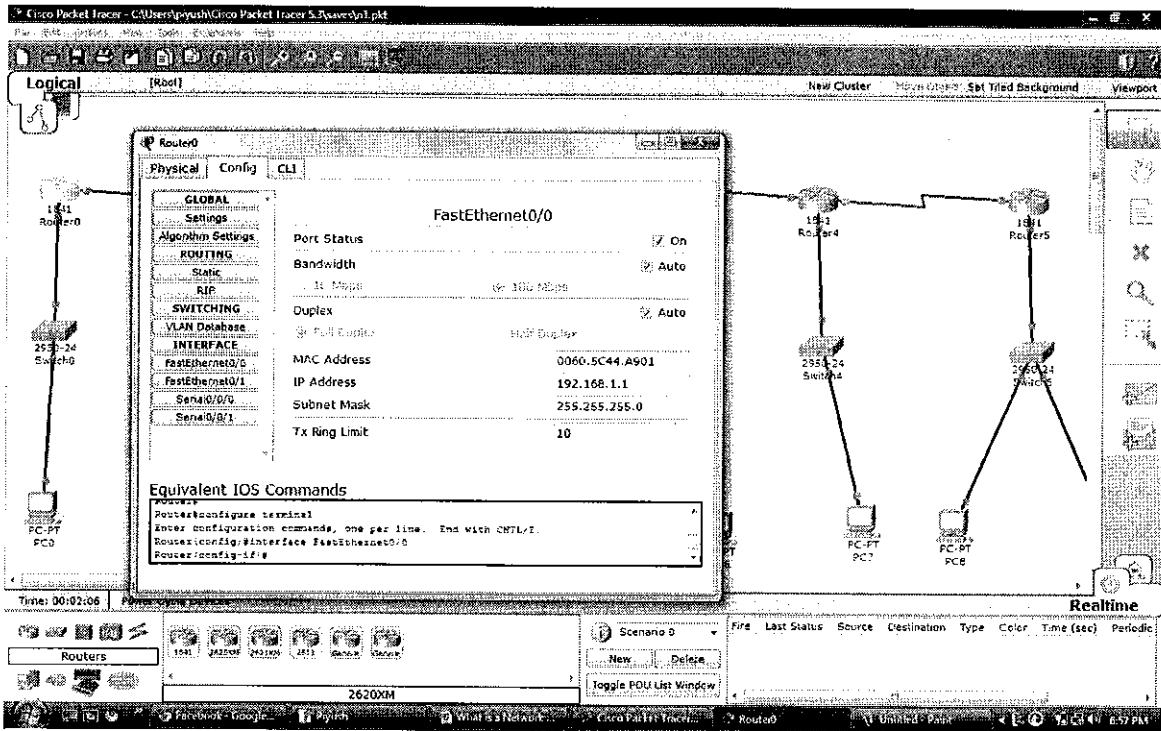


Fig 6.3: Adapted from packet tracer

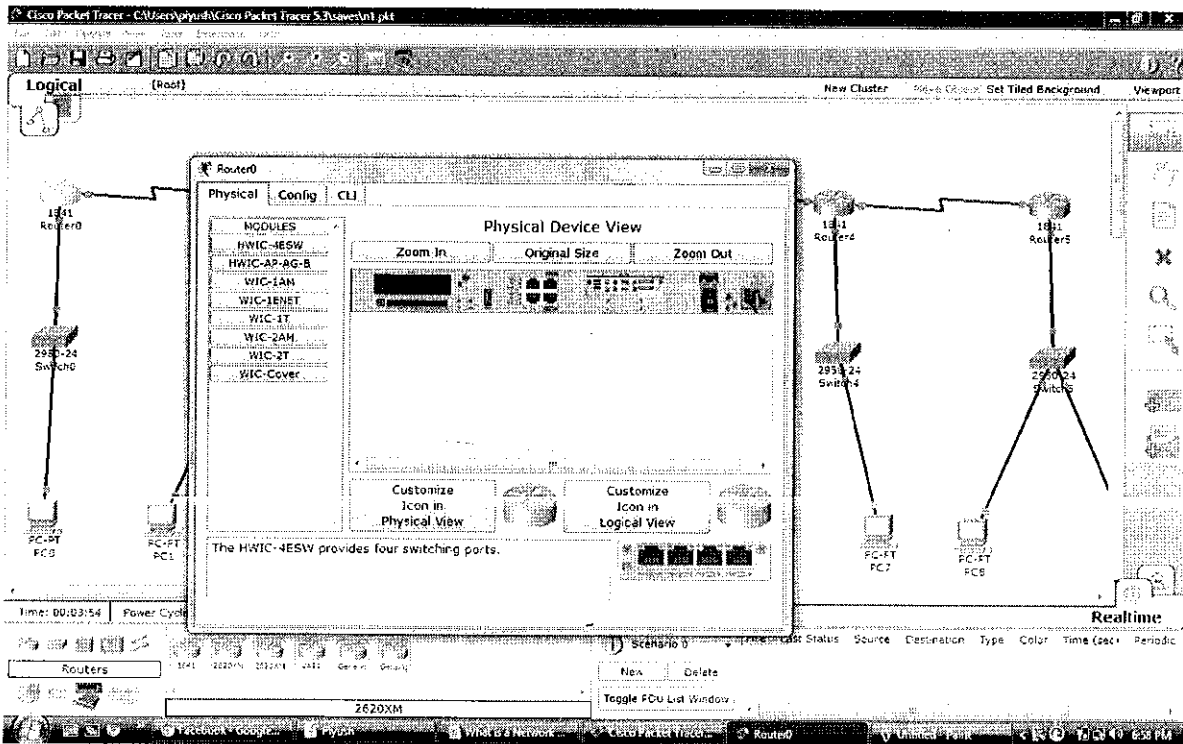


Fig 6.4: Adapted from packet tracer

## System requirements

---

- CPU: Intel Pentium 300 MHz or equivalent
- OS: Microsoft Windows 2000, Windows XP, Vista Home Basic, Vista Home Premium, Fedora 7, or Ubuntu 7.10
- RAM: 96 MB
- Storage: 250 MB of free disk space
- Screen resolution: 800 x 600 or higher
- Macromedia Flash Player 6.0 or higher
- Language fonts supporting Unicode encoding (if viewing in languages other than English)
- Latest video card drivers and operating system updates

## Observation and Results

These ping results were obtained by pinging 32 bytes of data.

Case I : When data ping was done from one network to another.

Ping statistics for 1<sup>st</sup> ping:

**Packets: Sent=4, Received=3, Lost=1 (25% loss),**  
**Approximate round trip times in milli-seconds:**  
**Minimum=15ms, Maximum=21ms, Average=17ms**

Ping statistics for 2<sup>nd</sup> ping:

**Packets: Sent=4, Received=4, Lost=0 (0% loss),**  
**Approximate round trip times in milli-seconds:**  
**Minimum=12ms, Maximum=14ms, Average=12ms**

Case II: When ping was done within the same network.

Ping Statistics for 1<sup>st</sup> ping:

**Packets: Sent=4, Received=4, Lost=0 (0% loss),**  
**Approximate round trip times in milli-seconds:**  
**Minimum=5ms, Maximum=10ms, Average=7ms**

We noticed that when ping was done within the same network, data variations were minimal for 1<sup>st</sup>, 2<sup>nd</sup> & 3<sup>rd</sup> ping.




# Chapter 8

## (Conclusion)

## Conclusion

Packet tracer is the best network simulator out there. Its main purpose is that the students get to practice network simulations that include configuration and implementation of the network. We, investigate about different kinds of network devices, and impact of the configuration changes as the topology changes. We carried out our experiment with various routing protocols about the journey of the packet. We applied some basic security features but concluded that the software isn't enough to practice network security. This project could be taken to a different level such as working with real devices in a real environment.



## References

- **Multimedia Contents Adaptation by Modality Conversion with User Preference in Wireless Network**

Publication year: 2011

**Source:** Journal of Network and Computer Applications, In Press, Accepted Manuscript, Available online 19 May 2011.

- **A survey on security issues in service delivery models of cloud computing •**  
**Review article Journal of Network and Computer Applications, Volume 34, Issue 1, January 2011, Pages 1-11**  
**Subashini, S.; Kavitha, V.**

- **Innovations in multi-agent systems**

Volume 30, Issue 3, 2007, Pages 1089-1115

Tweedale, J.; Ichalkaranje, N.; Sioutis, C.; Jarvis, B.; Consoli, A.; Phillips-Wren, G.

- [www.cbtnuggets.com](http://www.cbtnuggets.com).

- [www.google.com](http://www.google.com)

- Andrew S. Tanenbaum, "Computer Networks," Fourth Edition, Pearson Education, 2005.

- Behrouz A. Forouzan, "Data Communications and Networking," Fourth Edition, McGraw-Hill.

- Various other Networking Journals