A Minor Project Report

On

COMPANY NETWORK IMPLEMENTING ROUTING PROTOCOL AND LAN SWITCHING

Submitted in Partial Fulfilment of Requirements for the Award of the Degree of

Bachelor of Technology

In Computer Science Engineering

To

Guru Gobind Singh Indraprastha University, Delhi

Under the guidance of

Mr. Gourav Sharma

Submitted By:

ASHISH KUMAR SINGH
{06425602714}

DEEPAK CHOPRA
{06325602714}

Affiliated to GGSIP University, New Delhi
Approved by AICTE & Council of Architecture

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DELHI TECHNICAL CAMPUS

KNOWLEDGE PARK-III, GREATER NOIDA,

NOVEMBER – 2017

CANDIDATE’S DECLARATION

We, Ashish Kumar Singh and Deepak Chopra, (Enrollment No: 06425602714 and 06325602714), presently studying in 7th Semester, B.Tech - CSE (2014-2018 Batch), DTC, Guru Gobind Singh Indraprastha University, hereby declare that the work being presented in the Minor Project & Report entitled "**COMPANY NETWORK IMPLEMENTING ROUTING PROTOCOL AND LAN SWITCHING**" is an authentic and original record of our own work under the technical guidance/inputs of Mr. Gourav Sharma, Asst. Prof, DTC. We declare that the work in the said Minor Project has not been submitted in part or in full for any diploma or degree course of this or any other University/Institute to the best of my knowledge and belief. We will be solely responsible ourselves for any copyright infringement or plagiarism, if any, in the said work.

Date:

Place: DTC, Greater Noida

ASHISH KUMAR SINGH

(06425602714)

DEEPAK CHOPRA

(06325602714)

CERTIFICATE

This is to certify that the Minor Project Report entitled "**COMPANY NETWORK IMPLEMENTING ROUTING PROTOCOL AND LAN SWITCHING**" is an original and authentic work carried out by Ashish Kumar Singh and Deepak Chopra (Enrollment No: 06425602714 and 06325602714), a student of B.Tech-CSE (2014-2018 Batch) 7th Semester, DTC, GGS Indraprastha University, under my technical guidance/inputs to fulfill his academic requirements of the above said program. To the best of my knowledge and belief, the matter embodied in this work, in my opinion, has not been submitted in full or in part of any diploma or degree of this or any other University/Institute.

Date: **Mr. Gourav Sharma**

Place: DTC, Greater Noida (Assistant Professor, CSE)

ACKNOWLEDGEMENT

We express our sincere gratitude to Dr. Pushpa Choudhary (HOD, CSE) and Mr. Gourav Sharma Faculty Guide (A.P, CSE), Delhi Technical Campus, for his valuable guidance and timely suggestions during the entire duration of my dissertation work, without which this work would not have been possible. I would also like to convey my deep regards to all other faculty members of Computer Science Department, who have bestowed their great effort and guidance at appropriate times without which it would have been very difficult on my part to finish this work. Finally we would also like to thank our friends for their advice and pointing out our mistakes.

ABSTRACT

The project title "**COMPANY NETWORK IMPLEMENT ROUTING PROTOCOLS & LAN SWITCHING**" is actually a network based project. The enterprise network is the lifeblood of any Small to Medium Enterprise (SME) with more than one site or supply chain partner. It enables access to business information and allows for profitable and effective communication flows between employees in different enterprise sites. Network enterprise network equipment is mature and ubiquitous, but the quality of services provided by similar networks varies from city to city and from country to country. IT is a secured network often used in big organizations and other institutions to make a secured communication and sharing's of their documents, files, etc. should also be secured. As we know that there are many departments in an organization. So we desire that these departments should be separate for their good output. Then this project also includes this feature. This type of network avoids the unauthorized access it authenticate the authorized users or hosts. Implementation of logical network topology has been done. All the routers have their password to access them by any user. This network connects the different department of a company or many companies and combines them in a single network. And the implementations of router are very accurate, that they should select the excellent path for the packets and make the communication fast and secure. We have also used Adaptive Bitrate Technology in this project.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

- ✓ PING 191.168.1.2 FROM 191.168.1.3 (PC 10 to PC 4)
- ✓ DIFFERENT NETWORKS COMMUNICATING TO EACH OTHER AND LAPTOP CONNECTED TO WIRELESS ROUTER
- ✓ SAME VLANS ABLE TO COMMUNICATE
- ✓ MANAGER AND CEO COMMUNICATING WITH EACH OTHER AND WITH HR DEPARTMENT
- ✓ PCs CONNECTED WITH HELP OF HUBS ABLE TO COMMUNICATE IN NETWORK
- ✓ MANAGER AND CEO ABLE TO COMMUNICATE WITH DELHI’S SERVER

LIST OF SYMBOLS, ABBREVIATIONS AND NOMENCLATURE

N/W	Network
LAN	Local Area Network
WAN	Wide Area Network
ISDN	Integrated Services Digital Network **(**ISDN)
OSI	Open Systems Interconnection
TCP/IP	Transmission Control Protocol/Internet Protocol
NIC	Network Interface Card
MAC	Media Access Control
IETF	Internet Engineering Task Force
EXEC	EXECUTION
VTY	Virtual Telnet Type
VLAN	VIRTUAL Local Area Network
EIGRP	Enhanced Interior Gateway Routing Protocol
IGRP	Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
IOS	Internetwork Operating System
CLI	Command-Line Interface

CHAPTER 1: INTRODUCTION

The project title "**COMPANY NETWORK IMPLEMENT ROUTING PROTOCOLS & LAN SWITCHING**" is actually a network based project. IT is a secured network often used in big organizations and other institutions to make a secured communication and sharing's of their documents, files, etc. should also be secured. As we know that there are many departments in an organization. So we desire that these departments should be separate for their good output. Then this project also includes this feature. This type of network avoids the unauthorized access it authenticate the authorized users or hosts. Implementation of logical network topology has been done.

All the routers have their password to access them by any user. This network connects the different department of a company or many companies and combines them in a single network. And the implementations of router are very accurate, that they should select the excellent path for the packets and make the communication fast and secure. We have also used Adaptive Bitrate Technology in this project. Adaptive bitrate streaming is a technique used in streaming multimedia over computer networks. A distance vector protocol is implemented in the project and the routers are password protected for security purpose.

The fundamental purpose of designing this project is to provide security in your network to secure your private data and make a reliable and excellent communication in a WAN connection and reduce the organization dependency on floppy disks etc. Organizations that share data through the use of floppy disks follow a non-efficient or cost-effective method. The issue is that the business by using this method to share data leads to duplication of data which effects the growth of the business. Using this method leads to a major issue i.e. Lack of communication- all details are not possible to be conveyed at the required time. The scope of this project is to have a secure WAN network for the communication purpose of an company that eradicate data redundancy from the grass root level which shows smooth functioning of a network.

1.1 PROBLEM STATEMENT

The main aim of this project is to provide security in your network to secure your private data and make a reliable and excellent communication in a WAN connection. As we know that a company network or basically known as an organization network has many departments, so we desire that these departments should be separate for their good output. Then this project also includes this feature. This type of network avoids the unauthorized access it authenticate the authorized users or hosts. Implementation of logical network topology has been done in the project. Further the network is secured & easy to understand. Because of the easy implementation of project it is easy to troubleshoot. As the routing protocol that has been used i.e. the routing information protocol (RIP) can support upto 15 hop count we can easily extend the range of routers. Different class IP addresses are used in this project subnetting is also done to prevent the waste of IP addresses.

1.2 PURPOSE

The main purpose of this project is to create a company network have best routing protocol for the scenario given and show LAN switching.

Customers Intended:

Company: To create a better communication at different branches of the company at different locations (by creating a WAN Network for the company).

Features

Following are some important features that come along with this project these are:-

- The network is secured.
- It is easy to understand the whole network.
- Easy to troubleshoot because of its easy understanding.
- We can extend the range of slots in routers.
- Whole of the network is intelligent.
- Networking By areas

Assumption

There are some assumptions that are needed to be taken before studying the project that are:

- Routing protocol used is best for the scenario depicted.
- The Company for which the network is created is a huge company having offices at different locations.
- Company for which the network is created is expanded in a certain state e.g. Delhi as all the locations that are mentioned are in Delhi.

1.3 INTENDED AUDIENCE AND READING SUGGESTIONS

This project can be used by any upcoming startup or a well-established organisation, basically packet tracer labs are scenario based and upon the needs of a particular customer/client that is how he/she wants the network setup for their organisation. Further Wide Area Network (WAN) security can be added making this project to be used by all the top ranking organisations or company having several branches at different locations.

1.4 PROJECT SCOPE

The scope of this project is to have a secure WAN network for the communication purpose of an company that eradicate data redundancy from the grass root level which shows smooth functioning of a network.

Basically, CISCO Packet tracer labs are scenario based they can be designed for any type of scenario given by the customer/consumer according to it the suitable company network is designed for the consumer by a network associate.

Following are some features because of which this project can be opted by any of upcoming or already established company:

- This company network provides security in your network to secure your private data and make a reliable and excellent communication in a WAN connection and reduce the organization dependency on floppy disks etc.

- It is easy to understand the whole network because of its easy implementation rather than using large number of end devices minimum no of end devices are used just to make it easy for the user to understand.

- Easy to troubleshoot because of its easy understanding.

- We can extend the range of slots in routers up to 15th hop count as RIP is implemented. The 16th hop won't be reachable.

- Networking is done by areas in this project every area PC's and laptop's are having a separate class IP Address.

CHAPTER 2: OVERALL DESCRIPTION

This project consist of 5 routers the main router is the Delhi Router which is further connected to Nirman Vihar and Vaishali router which are connected to Dwarka and Ghaziabad router respectively. The main Delhi Router is Password protected and it is assumed that headquarter of the company is located there. The other offices of the company are located at different places like: Dwarka, Nirman Vihar, Ghaziabad and Vaishali.

Further to keep this project simple use of limited number of Computers and Laptops are there for the easy understanding to the users. Copper straight-through and copper cross over cables are used to connect routers with switches and switches with PCs. laptops are connected to the network with the help of wireless routers. Serial DTE (Data Terminal Equipment) cable is used to connect routers together.

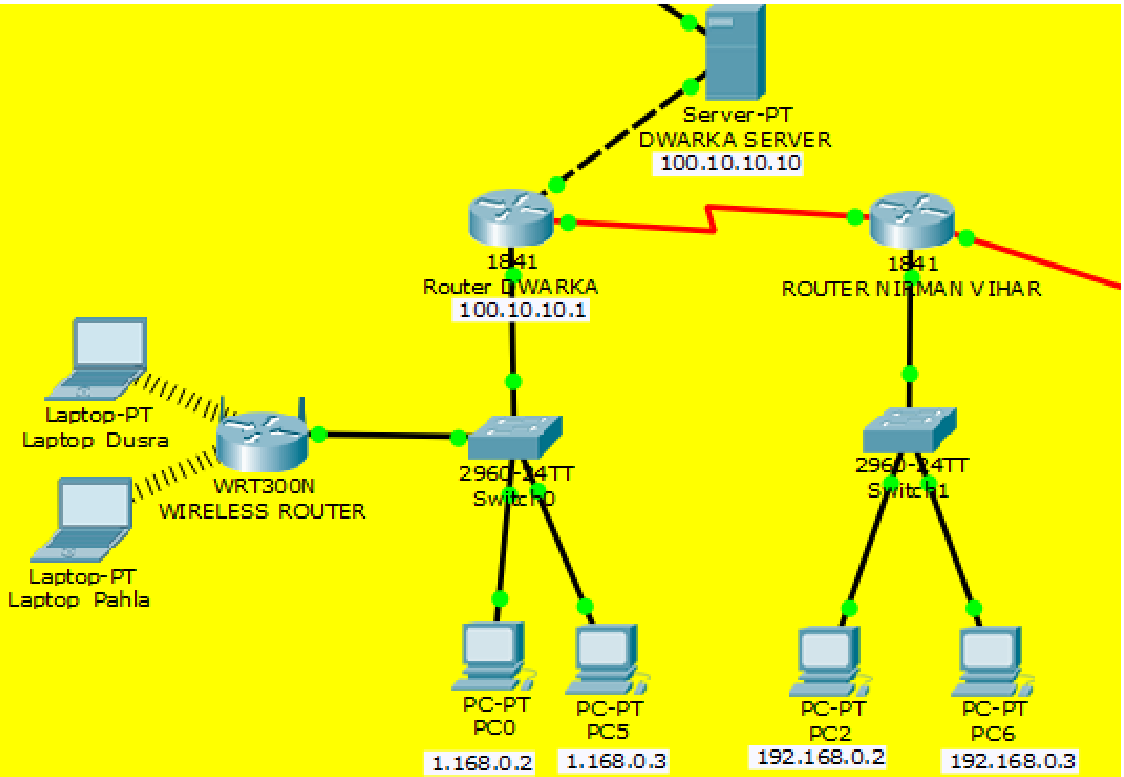


Figure 1: DWARKA & NIRMAN VIHAR ROUTER

The above figure 1 shows Router DWARKA and Router NIRMAN VIHAR which are connected to each other with the help of Serial DTE cable. These routers are further connected to 2960-24TT switches and then the corresponding end devices like computer are connected to these switches.

Note: Every PC connected in a different network has a specific class IP. No IP addresses are repeated.

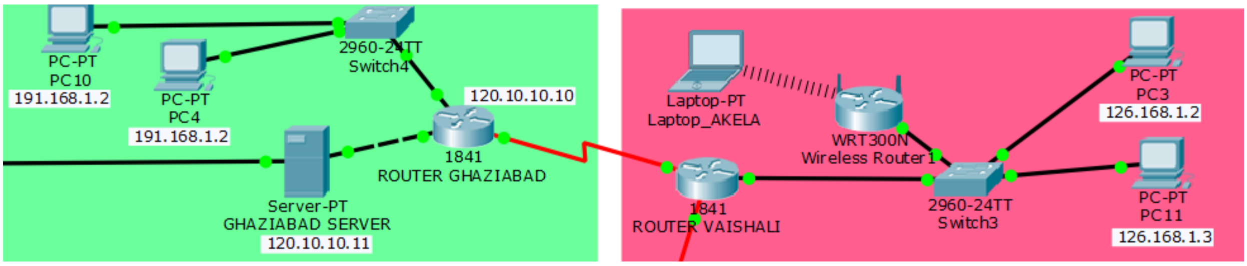


Figure 2: GHAZIABAD & VAISHALI ROUTER

The above figure 2 shows Router (1841) GHAZIABAD and Router (1841) VAISHALI which are connected to each other with the help of Serial DTE cable. Just like Dwarka and Nirman vihar here also the routers are connected to 2960-24TT switches and then the corresponding end devices like computer are connected to these switches. In the Vaishali network a Wireless Router (WRT300N) is also connected to the switch making the end device like laptop to get attach to the network via Wireless medium.

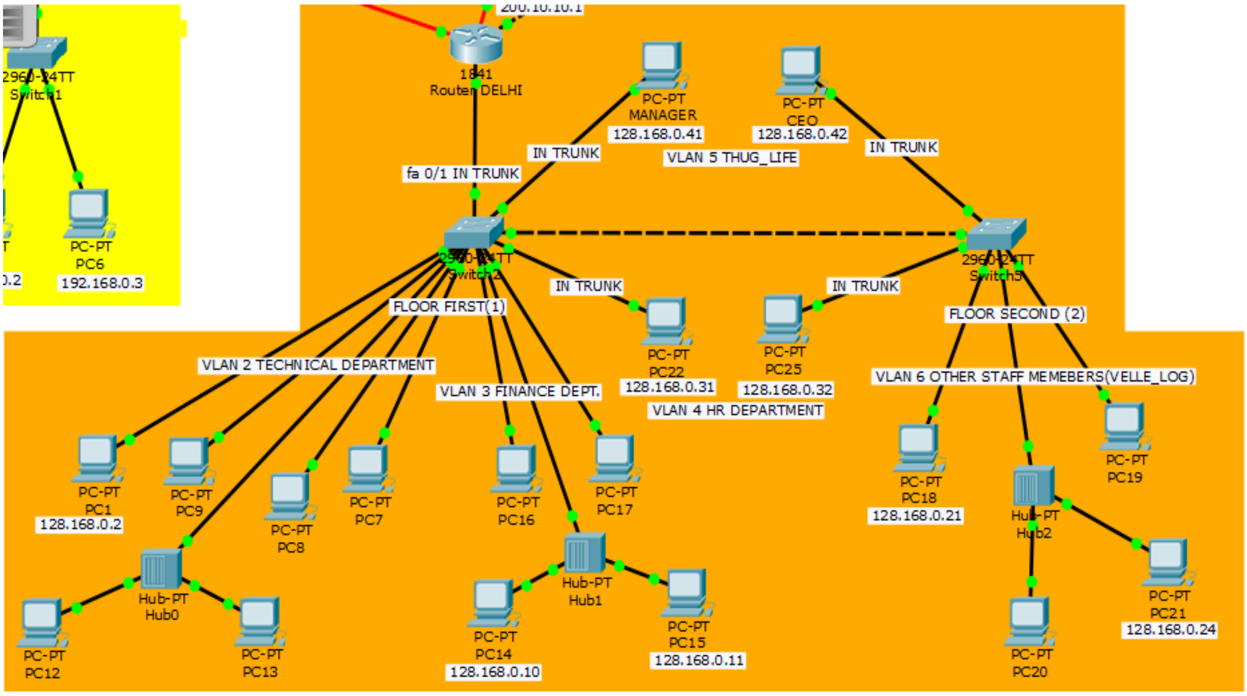


Figure 3: DELHI ROUTER (The Assumed Headquarter of the Company)

The above figure 3 shows Router (1841) Delhi that is assumed to be the main headquarter of the company. It comprises of various departments like: Technical department, HR department, Finance department and other staff members which can do there respected work in there PCs arranged (the person can be anyone who can work here- might be of a particular department or other people like trainee and interns). The headquarter as assumed to have two floors the manager CEO and HR department representatives are in Trunk in the network so then can communicate and share files in there network. Security features are added in this network separate VLANs are created for particular department so that a person in technical department cannot access the data that is present in the finance department. Different class IP Address is present in this network.

2.1 PROJECT PERSPECTIVE AND FUNCTIONS

There are different equipment's that are used while making this project those are:

2.1.1 ROUTERS

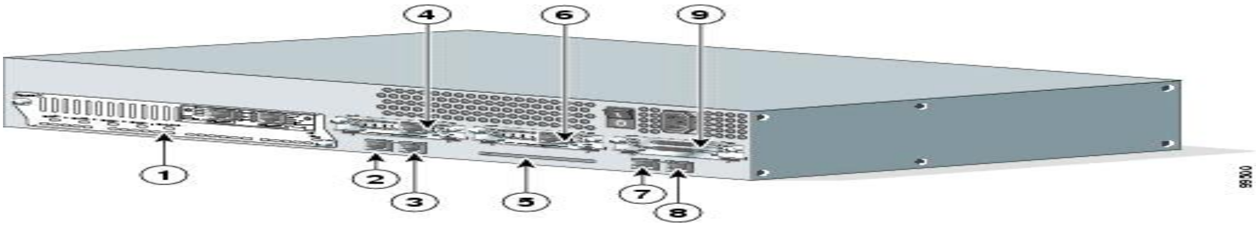


Figure 4: ROUTER AND ITS PORTS

1	Network Module	**6**	Interface Card Slot
2	FastEthernet 0/1	**7**	Console Port
3	FastEthernet 0/0	**8**	Auxiliary Port
4	Interface Card Slot	**9**	Interface Card Slot
5	Compact Flash Slot		

A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

The most familiar type of routers are home and small office routers that simply pass data, such as web pages, email, IM, and videos between the home computers and the Internet. An example of a router would be the owner's cable or DSL modem, which connects to the Internet through an ISP. More sophisticated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the Internet backbone. Though routers are typically dedicated hardware devices, use of software-based routers has grown increasingly common.

2.1.2 SWITCHES

A switch is a device used on a computer network to physically connect devices together. Multiple cables can be connected to a switch to enable networked devices to communicate with each other. Switches manage the flow of data across a network by only transmitting a received message to the device for which the message was intended. Each networked device connected to a switch can be identified using a MAC address, allowing the switch to regulate the flow of traffic. This maximises security and efficiency of the network. Because of these features, a switch is often considered more "intelligent" than a network hub. Hubs neither provide security, or identification of connected devices. This means that messages have to be transmitted out of every port of the hub, greatly degrading the efficiency of the network.

2.1.3 FIREWALL

In computing, a **firewall** is a software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. Firewalls can be defined in many ways according to your level of understanding. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

2.1.4 MODEM

A **modem** (**mo**dulator-**dem**odulator) is a device that modulates an analog carrier signal to encode digital information and demodulates the signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals, from light emitting diodes to radio. The most familiar type is a voice band modem that turns the digital data of a computer into modulated electrical signals in the voice frequency range of a telephone channel. These signals can be transmitted over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Modems are generally classified by the amount of data they can send in a given unit of time, usually expressed in bits per second (bit/s or bps), orbytes per second (B/s). Modems can also be classified by their symbol rate, measured in baud. The baud unit denotes symbols per second, or the number of times per second the modem sends a new signal. For example, the ITU V.21 standard used audio frequency shift keying with two possible frequencies, corresponding to two distinct symbols (or one bit per symbol), to carry 300 bits per second using 300 baud. By contrast, the original ITU V.22 standard, which could transmit and receive four distinct symbols (two bits per symbol), transmitted 1,200 bits by sending 600 symbols per second (600 baud) using phase shift keying.

2.1.5 NETWORK CABLES

Networking cables are used to connect one network device to other network devices or to connect two or more computers to share printer, scanner etc. Different types of network cables likeCoaxial cable, Optical fiber cable, Twisted Pair cables are used depending on the network's topology, protocol and size. The devices can be separated by a few meters (e.g. via Ethernet) or nearly unlimited distances (e.g. via the interconnections of the Internet).

While wireless may be the wave of the future, most computer networks today still utilize cables to transfer signals from one point to another. In this project maximum twisted pair is used.

2.1.6 TFTP SERVER

Trivial File Transfer Protocol (**TFTP**) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user.

Due to its simple design, TFTP can be implemented using a very small amount of memory. It is therefore useful for booting computers such as routers which may not have any data storage devices. It is an element of the Pre boot Execution Environment (PXE) network boot protocol, where it is implemented in the firmware ROM / NVRAM of the host's network card.

It is also used to transfer small amounts of data between hosts on a network, such as IP phone firmware or operating system images when a remote X Window System terminal or any other thin client boots from a network host or server. The initial stages of some network based installation systems (such as Solaris Jumpstart, Red Hat Kickstart, Symantec Ghost and Windows NT'sRemote Installation Services) use TFTP to load a basic kernel that performs the actual installation. It was used for saving router configurations on Cisco routers, but was later augmented by other protocols.

TFTP was first defined in 1980 by IEN 133. Since 1992, it has been defined by RFC 1350. There have been some extensions to the TFTP protocol documented in later RFCs (see the section on Extensions, below). TFTP is based in part on the earlier protocol EFTP, which was part of the PUP protocol suite. TFTP support appeared first as part of 4.3 BSD.

Due to the lack of security, it is dangerous to use it over the Internet. Thus, TFTP is generally only used on private, local networks.

2.2 PROJECT COMPONENTS

There are different things we need to know before understanding the project these are as follows:

2.2.1 NETWORK TOPOLOGY

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

A good example is a local area network (LAN): Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. Conversely, mapping the data flow between the components determines the logical topology of the network.

There are two basic categories of network topologies:

- Physical topologies
- Logical topologies

2.2.1.1 Physical Topology

The shape of the cabling layout used to link devices is called the physical topology of the network. This refers to the layout of cabling, the locations of nodes, and the interconnections between the nodes and the cabling. The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or fault tolerance desired, and the cost associated with cabling or telecommunications circuits.

2.2.1.2 Logical Topology

The logical topology in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. A network's logical topology is not necessarily the same as its physical topology. For example, the original twisted pair Ethernet using repeater hubs was a logical bus topology with a physical star topology layout. Token Ring is a logical ring topology, but is wired a physical star from the Media Access Unit.

2.2.1.3 Common LAN Topology

2.2.1.3.1 BUS Topology

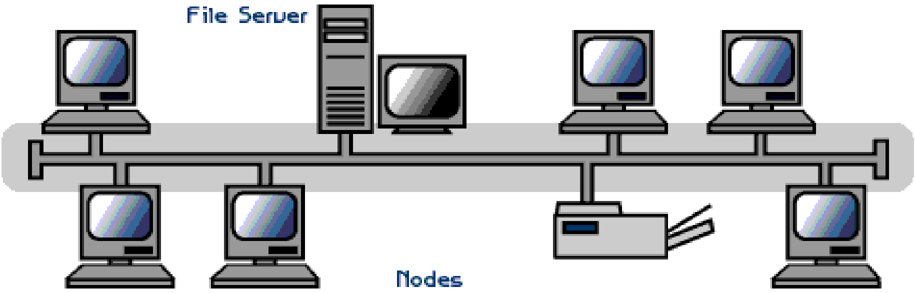


Figure 5: BUS TOPOLOGY

A **bus network** is a network topology in which nodes are connected in a daisy chain by a linear sequence of buses.The bus is the data link in a bus network. The bus can only transmit data in one direction, and if any segments severed, all network transmission ceases.

A host on a bus network is called a *station* or *workstation*. In a bus network, every station receives all network traffic, and the traffic generated by each station has equal transmission priority. Each network segment is, therefore, a collision domain. In order for nodes to transmit on the same cable simultaneously, they use a media access control technology such as carrier sense multiple access (CSMA) or a bus master.

2.2.1.3.2 RING Topology

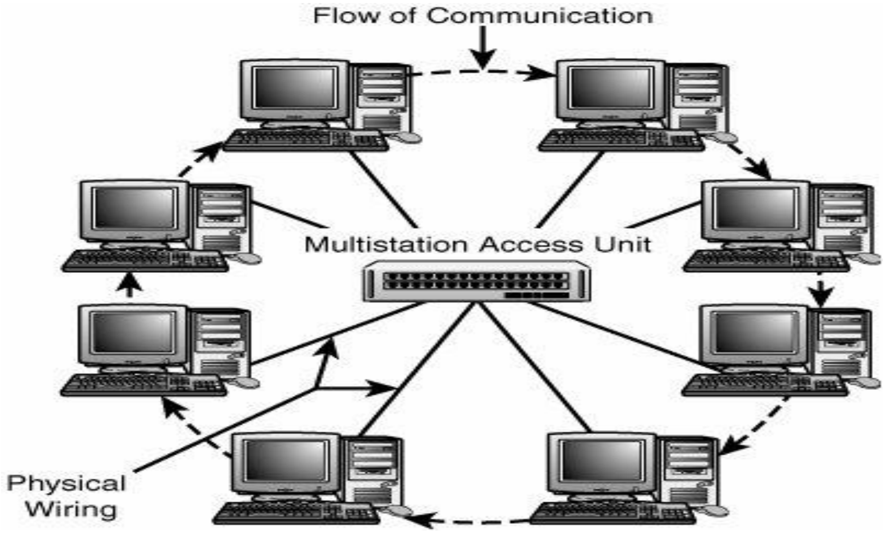


Figure 6: RING TOPOLOGY

In Ring Topology, all the nodes are connected to each-other in such a way that they make a closed loop. Each workstation is connected to two other components on either side, and it communicates with these two adjacent neighbours. Data travels around the network, in one direction. Sending and receiving of data takes place by the help of TOKEN.

Advantages of Ring Topology

- This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduces chances of collision. Also in ring topology all the traffic flows in only one direction at very high speed
- Even when the load on the network increases, its performance is better than that of Bus topology.
- There is no need for network server to control the connectivity between workstations.
- Additional components do not affect the performance of network.
- Each computer has equal access to resources.

Disadvantages of Ring Topology

- Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.
- If one workstation or port goes down, the entire network gets affected.
- Network is highly dependent on the wire which connects different components.
- MAU’s and network cards are expensive as compared to Ethernet cards and hubs.

2.2.1.3.3 STAR Topology

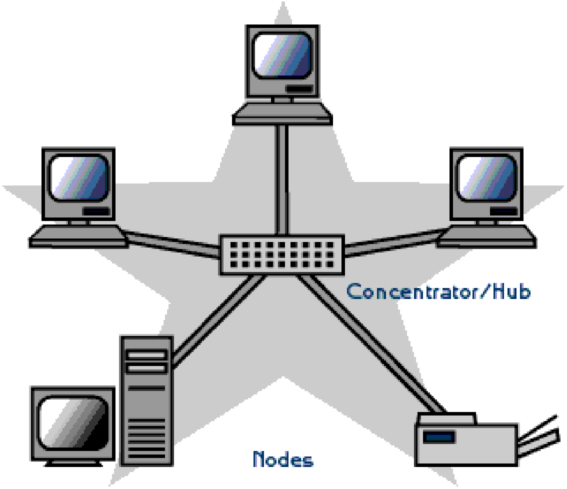


Figure 7: STAR TOPOLOGY

Star networks are one of the most common computer network topologies. In its simplest form, a star network consists of one central switch, hub or computer, which act as a conduit to transmit messages. This consists of a central node, to which all other nodes are connected; this central node provides a common connection point for all nodes through a hub. In star topology, every node (computer workstation or any other peripheral) is connected to a central node called a hub or switch. The switch is the server and the peripherals are the clients.[1] Thus, the hub and leaf nodes, and the transmission lines between them, form a graph with the topology of a star. 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 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.

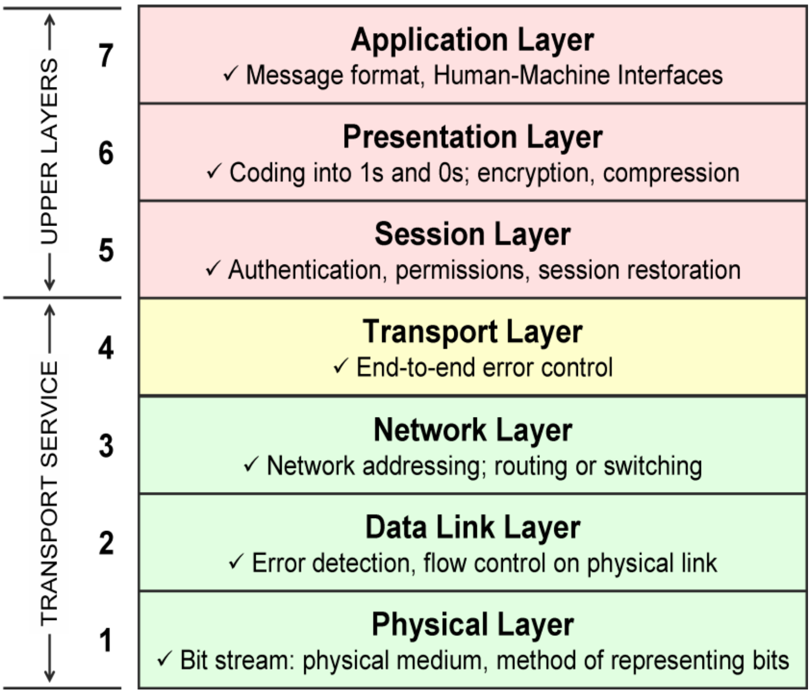
2.2.2 OSI (OPEN SYSTEM INTERCONNECTION) MODEL

OSI model is the layer approach to design, develop and implement network. OSI provides following advantages: -

- Designing of network will be standard base.
- Development of new technology will be faster.
- Devices from multiple vendors can communicate with each other.
- Implementation and troubleshooting of network will be easy.

Layer 1: The Physical Layer

The bottom layer, or Layer 1, of the OSI reference model is called the physical layer. This layer is responsible for the transmission of the bit stream. It accepts frames of data from Layer 2, the data link layer, and transmits their structure and content serially, one bit at a time. Layer 1 is also responsible for the reception of incoming streams of data, one bit at a time. These streams are then passed on to the data link layer. The physical layer, quite literally, operates on only 1s and 0s. It has no mechanism for determining the significance of the bits it transmits or receives. It is solely concerned with the physical characteristics of electrical and/or optical signalling techniques. This includes the voltage of the electrical current used to transport the signal, the media type and impedance characteristics, and even the physical shape of the connector used to terminate the media. Transmission media includes any means of actually transporting signals generated by the OSI's Layer 1 mechanisms. Some examples of transmission media are coaxial cabling, fibre-optic cabling, and twisted-pair wiring.



7 Application Layer
✓ Message format, Human-Machine Interfaces

6 Presentation Layer
✓ Coding into 1s and 0s; encryption, compression

5 Session Layer
✓ Authentication, permissions, session restoration

4 Transport Layer
✓ End-to-end error control

3 Network Layer
✓ Network addressing; routing or switching

2 Data Link Layer
✓ Error detection, flow control on physical link

1 Physical Layer
✓ Bit stream: physical medium, method of representing bits

Figure 8: OSI MODEL

Layer 2: The Data Link Layer

Layer 2 of the OSI reference model is called the data link layer. As all the layers do, it has two sets of responsibilities: transmit and receive. It is responsible for providing end-to-end validity of the data being transmitted. On the transmit side, the data link layer is responsible for packing instructions---data---into frames. A frame is a structure indigenous to the data link layer that contains enough information to make sure that the data can be successfully sent across a LAN to its destination. Implicit in this definition is that the data link layer contains its own address architecture. This addressing is only applicable to other networked devices that reside locally on the same data link layer domain.

Layer 3: The Network Layer

The network layer enables internetworking. The protocols at this layer are responsible for establishing the route to be used between the source and destination computers. This layer lacks any native transmission error detection/correction mechanisms and, consequently, is forced to rely on the end-to-end reliable transmission service of either the data link layer or the transport layer. Although some data link layer technologies support reliable delivery, many others do not. Therefore, Layer 3 protocols (such as IP) assume that Layer 4 protocols (such as TCP) will provide this functionality rather than assume Layer 2 will take care of it.

Layer 4: Transport Layer

Transport layer is responsible for connection oriented and connection less communication. Transport layer also performs other functions like

1. Error checking
2. Flow Control
3. Sequencing
4. Positive Acknowledgement Response

- **Error checking**

Transport layer generates cyclic redundancy check (CRC) and forward the CRC value to destination along with data. The other end will generate CRC according to data and match the CRC value with received value. If both are same, then data is accepted otherwise discard.

- **Flow Control**

Flow control is used to control the flow of data during communication. For this purpose following methods are used: -

- **Buffer**

Buffer is the temporary storage area. All the data is stored in the buffer memory and when communication ability is available the data is forward to another.

- **Windowing**

Windowing is the maximum amounts of the data that can be send to destination without receiving Acknowledgement. It is limit for buffer to send data without getting Acknowledgement.

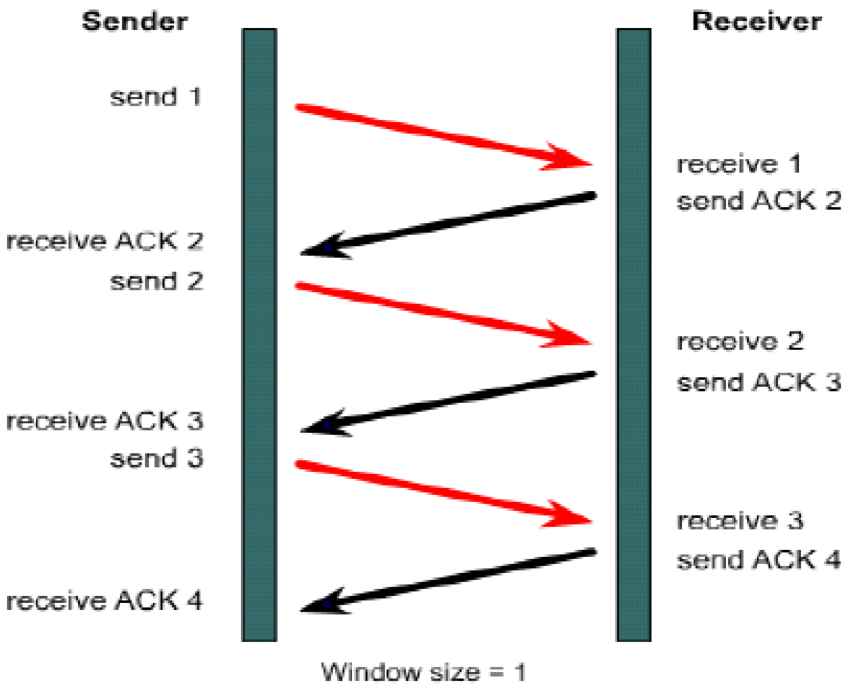


Figure 9: WINDOWING

- Multiplexing

Multiplexing means combining small data segment, which has same destination IP and same destination service.

- Sequencing

Transport layer add sequence number to data, so that out of sequence data can be detected and rearranged in proper manner.

- Positive acknowledgement and Response

When data is send to destination, the destination will reply with acknowledgement to indicate the positive reception of data. If acknowledgement is not received within a specified time then the data is resend from buffer memory.

Layer 5: Session Layer

This layer initiate, maintain and terminate sessions between different applications. Due to this layer multiple application software can be executed at the same time.

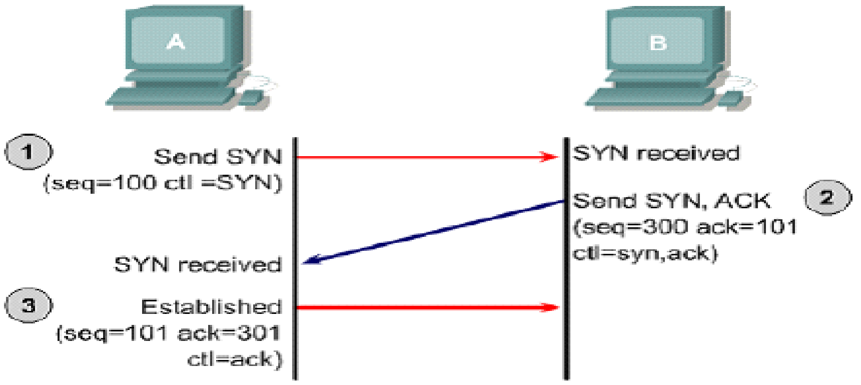
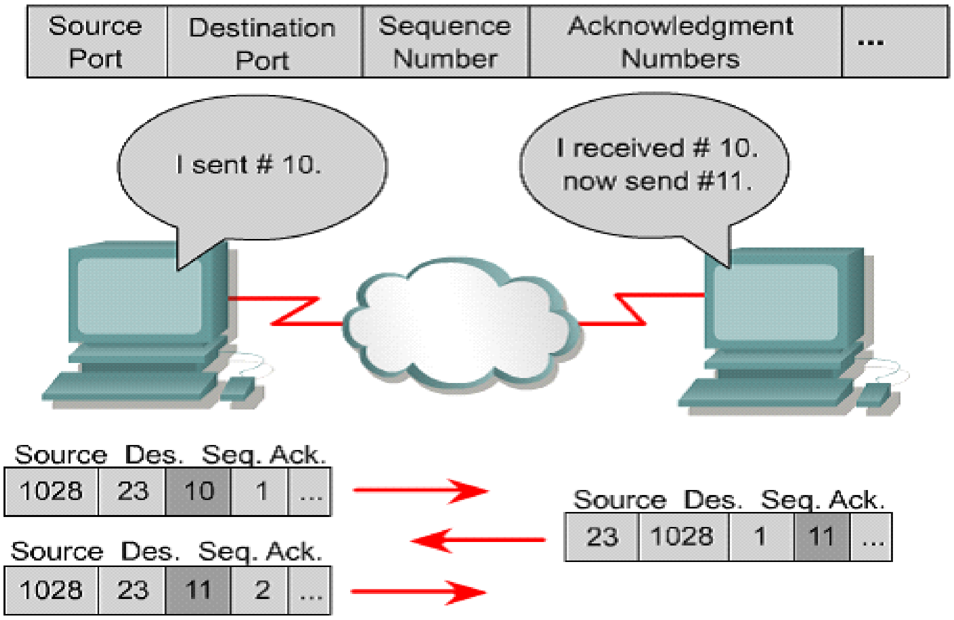


Figure 10: Connection Oriented Communication



Source Port	Destination Port	Sequence Number	Acknowledgment Numbers	...

Source	Des.	Seq.	Ack.	
1028	23	10	1	...

Source	Des.	Seq.	Ack.	
23	1028	1	11	...

Source	Des.	Seq.	Ack.	
1028	23	11	2	...

Figure 11: Connection less Communication

Layer 6: The Presentation Layer

Layer 6, the presentation layer, is responsible for managing the way that data is encoded. Not every computer system uses the same data encoding scheme, and the presentation layer is responsible for providing the translation between otherwise incompatible data encoding schemes, such as American Standard Code for Information Interchange (ASCII) and Extended Binary Coded Decimal Interchange Code (EBCDIC).

The presentation layer can be used to mediate differences in floating-point formats, as well as to provide encryption and decryption services.

Layer 7: The Application Layer

The top, or seventh, layer in the OSI reference model is the application layer. Despite its name, this layer does not include user applications. Instead, it provides the interface between those applications and the network's services. This layer can be thought of as the reason for initiating the communications session. For example, an email client might generate a request to retrieve new messages from the email server. This client application automatically generates a request to the appropriate Layer 7 protocol(s) and launches a communications session to get the needed files.

2.2.3 NETWORK CABLING

Networking cables are used to connect one network device to other network devices or to connect two or more computers to share printer, scanner etc. Different types of network cables like Coaxial cable, Optical fibre cable, Twisted Pair cables are used depending on the network's topology, protocol and size. The devices can be separated by a few meters (e.g. via Ethernet) or nearly unlimited distances (e.g. via the interconnections of the Internet).

2.2.3.1 Coaxial Cable

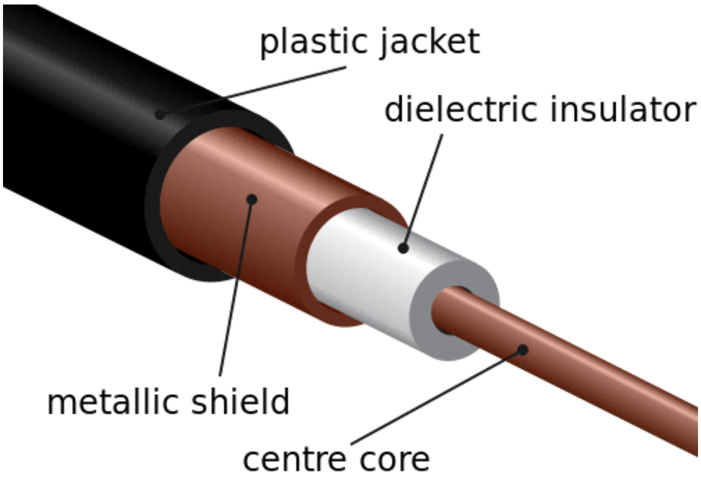


Figure 12: Coaxial Cable

Coaxial cables are a type of cable that is used by cable TV and that is common for data communications. Taking a round cross-section of the cable, one would find a single center solid wire symmetrically surrounded by a braided or foil conductor. Between the center wire and foil is a insulating dielectric. This dielectric has a large effect on the fundamental characteristics of the cable. In this lab, we show the how the permittivity and permeability of the dielectric contributes to the cable's inductance and capacitance. Also, these values affect how quickly electrical data is travels through the wire.

The two types of Coaxial Cabling are:

- **Thick Coaxial**

10BASE5 (also known as **thick Ethernet** or **thicket**) was the original commercially available variant of Ethernet**.** The name *10BASE5* is derived from several characteristics of the physical medium. The *10* refers to its transmission speed of 10 Mbit/s. The *BASE* is short for basebandsignalling as opposed to broadband, and the *5* stands for the maximum segment length of 500 meters (1,600 ft.).

Disadvantage:

Adding new stations to network was complicated by the need to accurately pierce the cable. The cable was stiff and difficult to bend around corners. One improper connection could take down the whole network and finding the source of the trouble was difficult.

- **Thin Coaxial**

10BASE2 (also known as ***cheaper net***, ***thin Ethernet***,***thinnet***, and ***thin wire***) is a variant of Ethernet that uses thin coaxial cable (RG-58A/U or similar, as opposed to the thicker RG-8 cable used in 10BASE5 networks), terminated with BNC connectors

The name *10BASE2* is derived from several characteristics of the physical medium. The *10* comes from the maximum transmission speed of 10 Mbit/s (millions of bits persecond). The *BASE* stands for baseband signaling, and the *2* supposedly refers to the maximum segment length of 200 meters, though in practical use it can only run up to 185 meters. (The IEEE rounded 185 up to 200 to come up with the name 10BASE2, for consistency with the general standard).

2.2.3.2 Twisted Pair Cable

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference(EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs. It was invented by Alexander Graham Bell.

Twisted pair cable comes in two varieties: unshielded twisted pair and shielded twisted pair.

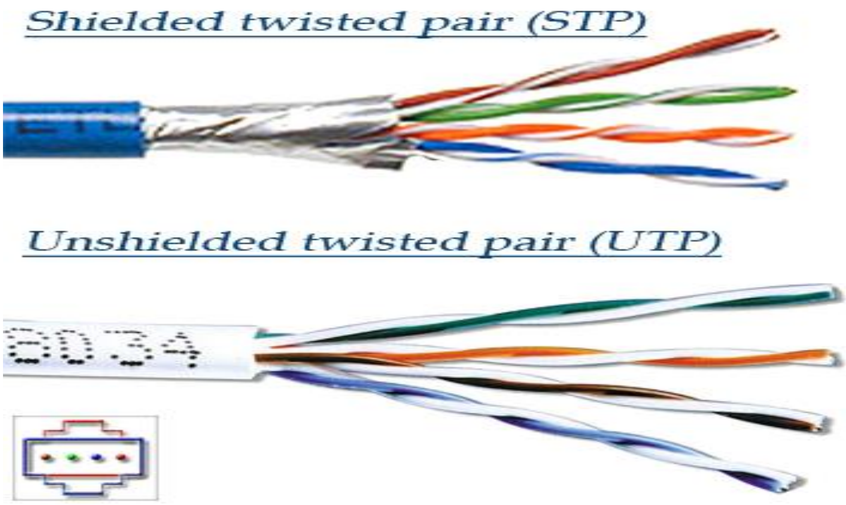


Figure 13: STP & UTP

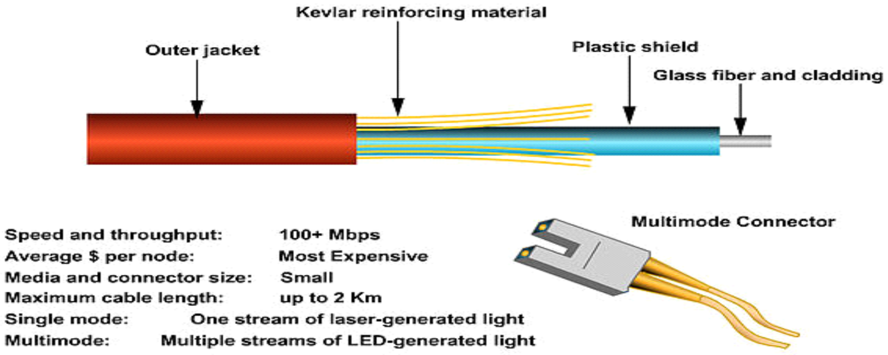
- **Unshielded Twisted Pair cable**

Unshielded Twisted Pair cable is most certainly by far the most popular cable around the world. UTP cable is used not only for networking but also for the traditional telephone (UTP-Cat 1). There are 6+ different types of UTP categories and, depending on what you want to achieve, you would need the appropriate type of cable. UTP-CAT5e is the most popular UTP cable, it came to replace the well known coaxial cable which was not able to keep up with the continuous growth for faster and more reliable networks.

- **Shielded Twisted Pair (STP) cable**

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded Twisted Pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded Twisted Pair is often used on networks using token ring topology.

2.2.3.3 Fiber Optic Cable



Speed and throughput:	100+ Mbps
Average $ per node:	Most Expensive
Media and connector size:	Small
Maximum cable length:	up to 2 Km
Single mode:	One stream of laser-generated light
Multimode:	Multiple streams of LED-generated light

Figure 14: FIBRE OPTIC CABLE

An **optical fiber cable** is a cable containing one or more optical that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

2.2.4 IP ROUTING

IP Routing is an umbrella term for the set of protocols that determine the path that data follows in order to travel across multiple networks from its source to its destination. Data is routed from its source to its destination through a series of routers, and across multiple networks

2.3.4.1 ROUTER

Unlike most LAN components, routers are intelligent. More importantly, they can operate at all layers of the OSI reference model rather than just the first two. This enables them to internetwork multiple LANs by using Layer 3 addressing.

A router must have two or more physical interfaces for interconnecting LANs and/or WAN transmission facilities. The router learns about the addresses of machines or networks that are somehow connected via each of its interfaces. The list of these addresses is kept in tables that correlate Layer 3 addresses with the port numbers that they are directly or indirectly connected to. A router uses two types of networking protocols, both of which operate at Layer 3. These are routable protocols and routing protocols. Routable protocols, also known as routed protocols, are those that encapsulate user information and data into packets. An example of a routed protocol is IP. IP is responsible for encapsulating application data for transport through a network to the appropriate destinations.

Routing protocols are used between routers to determine available routes, communicate what is known about available routes, and forward routed protocol packets along those routes. The purpose of a routing protocol is to provide the router with all the information it needs about the network to route datagram's. Routers are used to forward packets of data between devices that aren't necessarily connected to the same local network. Routing is the cumulative processes that discover paths through the network to specific destinations, compare redundant routes mathematically, and build tables that contain routing information

The router's task is easy: It has only two interfaces. Any packets received by one of its interfaces was either delivered to the other interface or discarded as undeliverable. In this particular case, the router may well have been replaced by a hub, bridge, switch, or any other Layer 2 device. The router's real value lies in determining routes to destinations on nonadjacent networks.

2.3.4.2 IP Addressing

IPv4 Address Formats

- Class A Addresses
- Class B Addresses
- Class C Addresses
- Class D Addresses
- Class E Addresses

IP addressing is accompanied by a two-tiered network address, consisting of the network's address and a host address.

- **Class A Addresses**

The Class A IPv4 address was designed to support extremely large networks. As the need for very large-scale networks was perceived to be minimal, architecture was developed that maximized the possible number of host addresses but severely limited the number of possible Class A networks that could be defined.

A Class A IP address uses only the first octet to indicate the network address. The remaining three octets enumerate host addresses. The first bit of a Class A address is always a 0. This mathematically limits the possible range of the Class A address to 127, which is the sum of 64 + 32 + 16 + 8 + 4 + 2 + 1. The leftmost bit's decimal value of 128 is absent from this equation. Therefore, there can only ever be 127 possible Class A IP networks.

The last 24 bits (that is, three dotted-decimal numbers) of a Class A address represent possible host addresses. The range of possible Class A network addresses is from 1.0.0.0 to 126.0.0.0. Notice that only the first octet bears a network address number. The remaining three are used to create unique host addresses within each network number. As such, they are set to zeroes when describing the range of network numbers.

- **Class B Addresses**

The Class B addresses were designed to support the needs of moderate- to large-sized networks. The range of possible Class B network addresses is from 128.1.0.0 to 191.254.0.0. The mathematical logic underlying this class is fairly simple. A Class B IP address uses two of the four octets to indicate the network address. The other two octets enumerate host addresses. The first 2 bits of the first octet of a Class B address are 10. The remaining 6 bits may be populated with either 1s or 0s.

This mathematically limits the possible range of the Class B address space to 191, which is the sum of 128 + 32 + 16 + 8 + 4 + 2 + 1. The last 16 bits (two octets) identify potential host addresses. Each Class B address can support 65,534 unique host addresses. This number is calculated by multiplying two to the 16th power and subtracting two (values reserved by IP). Mathematically, there can only be 16,382 Class B networks defined.

- **Class C Addresses**

The Class C address space is, by far, the most commonly used of the original IPv4 address classes. This address space was intended to support a lot of small networks. This address class can be thought of as the inverse of the Class A address space. Whereas the Class A space uses just one octet for network numbering, and the remaining three for host numbering, the Class C space uses three octets for networking addressing and just one octet for host numbering.

The first 3 bits of the first octet of a Class C address are 110. The first 2 bits sum to a decimal value of 192 (128 + 64). This forms the lower mathematical boundary of the Class C address space. The third bit equates to a decimal value of 32. Forcing this bit to a value of 0 establishes the upper mathematical boundary of the address space. Lacking the capability to use the third digit limits the maximum value of this octet to 255 - 32, which equals 223. Therefore, the range of possible Class C network addresses is from 192.0.1.0 to 223.255.254.0.

The last octet is used for host addressing. Each Class C address can support a theoretical maximum of 256 unique host addresses (0 through 255), but only 254 are usable because 0 and 255 are not valid host numbers. There can be 2,097,150 different Class C network numbers.

Note: In the world of IP addressing, 0 and 255 are reserved host address values. IP addresses that have all their host address bits set equal to 0 identify the local network. Similarly, IP addresses that have all their host address bits set equal to 255 are used to broadcast to all end systems within that network number.

- **Class D Addresses**

The Class D address class was created to enable multicasting in an IP network. The Class D multicasting mechanisms have seen only limited usage. A multicast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses. Therefore, a single station can simultaneously transmit a single stream of datagram's to multiple recipients. The need to create separate streams of datagram's, one for each destination, is eliminated. Routers that support multicasting would duplicate the datagram and forward as needed to the predetermined end systems. Multicasting has long been deemed a desirable feature in an IP network because it can substantially reduce network traffic.

The Class D address space, much like the other address spaces, is mathematically constrained. The first 4 bits of a Class D address must be 1110. Presetting the first 3 bits of the first octet to 1s means that the address space begins at 128 + 64 + 32, which equals 224. Preventing the fourth bit from being used means that the Class D address is limited to a maximum value of 128 + 64 + 32 + 8 + 4 + 2 + 1, or 239.

Therefore, the Class D addresses space ranges from 224.0.0.0 to 239.255.255.254.

This range may seem odd because the upper boundary is specified with all four octets. Ordinarily, this would mean that the octets for both host and network numbers are being used to signify a network number. There is a reason for this. The Class D address space isn't used for internetworking to individual end systems or networks. Class D addresses are used for delivering multicast datagram's within a private network to groups of IP-addressed end systems. Therefore, there isn't a need to allocate octets or bits of the address to separate network and host addresses. Instead, the entire address space can be used to identify groups of IP addresses (Classes A, B, or C). Today, numerous other proposals are being developed that would allow IP multicasting without the complexity of a Class D address space.

- **Class E Addresses**

A Class E address has been defined, but is reserved by the IETF for its own research. Therefore, no Class E addresses have been released for use in the Internet. The first 4 bits of a Class E address are always set to 1s; therefore, the range of valid addresses is from 240.0.0.0 to

255.255.255.255. Given that this class was defined for research purposes, and its use is limited to inside the IETF, it is not necessary to examine it any further.

- **IP Routing**

When we want to connect two or more networks using different n/w addresses then we have to use IP Routing technique. The router will be used to perform routing between the networks. A router will perform following functions for routing.

- **Path determination**

The process of obtaining path in routing table is called path determination.

There are three different methods to which router can learn path.

- Automatic detection of directly connected n/w.
- Static & Default routing.
- Dynamic Routing.

- **Packet forwarding**

It is a process that is by default enable in router. The router will perform packet forwarding only if route is available in the routing table.

- **Routing Process**

- The pc has a packet in which destination address is not same as the local n/w address.
- The pc will send an ARP request for default gateway. The router will reply to the ARP address and inform its Mac address to pc.
- The pc will encapsulate data, in which source IP is pc itself, destination IP is server, source Mac is pc's LAN interface and destination Mac is router's LAN interface.

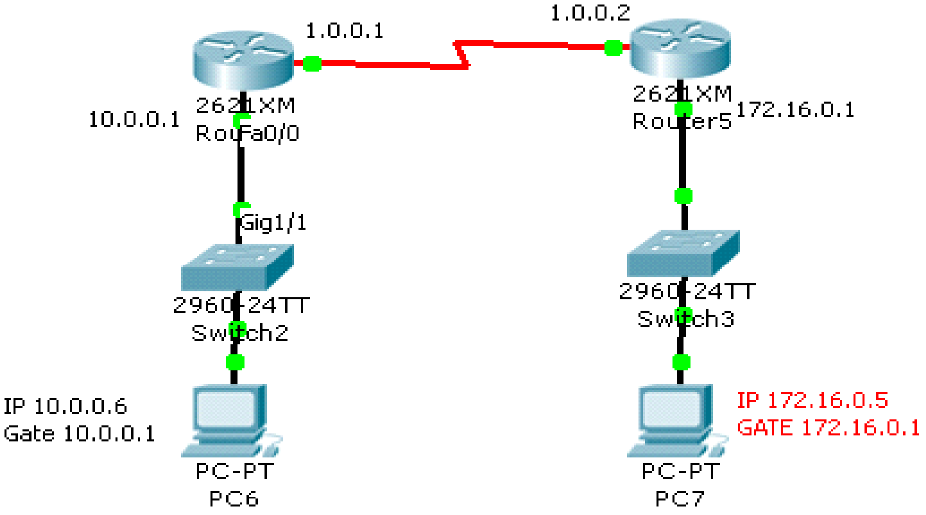


Figure 15: ROUTING PROCESS

S. MAC	D. MAC
PC1	R1
D. IP	172.16.0.5
S. IP	10.0.0.6

The router will receive the frame, store it into the buffer. When obtain packet from the frame then forward data according to the destination IP of packet. The router will obtain a route from routing table according to which next hop IP and interface is selected According to the next hop, the packet will encapsulated with new frame and data is send to the output queue of the interface.

- **Router Access Modes**

When we access router command prompt the router will display different modes. According to the modes, privileges and rights are assigned to the user.

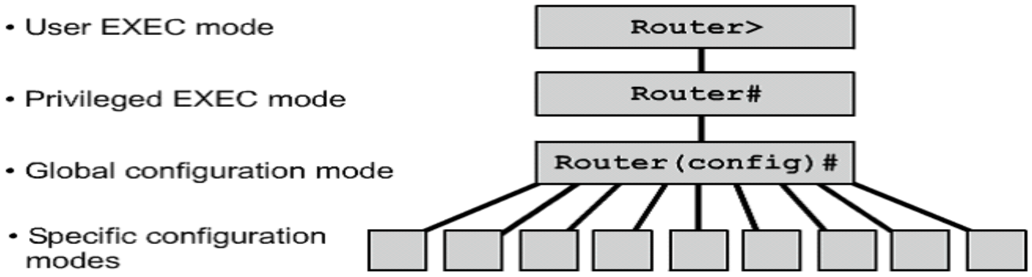


Figure 16: ROUTING ACCESS MODES

- **User mode**

In this mode, we can display basic parameter and status of the router we can test connectivity and perform telnet to other devices. In this mode we are not enable to manage & configure router.

- **Privileged mode**

In this mode, we can display all information, configuration, perform administration task, debugging, testing and connectivity with other devices. We are not able to perform here configuration editing of the router.

The command to enter in this mode is 'enable'. We have to enter enable password or enable secret password to enter in this mode. Enable secret has more priority than enable password. If both passwords are configured then only enable secret will work.

- **Global configuration**

This mode is used for the configuration of global parameters in the router. Global parameters applied to the entire router. For e.g.: - router hostname or access list of router the command enters in this mode is 'configure terminal'.

- **Line configuration mode**

This mode is used to configure lines like console, vty and auxiliary. There are main types of line that are configured.

Console router(config)#line console 0

Auxiliary router(config)#line aux 0

Telnet or vty router(config)#line vty 0 4

- **Interface configuration mode**

This mode is used to configure router interfaces. For e.g:- Ethernet, Serial, BRI etc.

Router(config)#interface <type><number>

Router(config)#interface serial 1

- **Routing configuration mode**

This mode is used to configure routing protocol like RIP, EIGRP, OSPF etc.

Router(config)#router <protocol> [<option>]

```
Router(config)#router rip
Router(config)#router eigrp 10
```

- **Configuring Password**

There are six types of password available in a router

- **Console Password**

```
router#configure terminal
router(config)#line console 0
router(config-line)#password <word>
router(config-line)#login
router(config-line)#exit
```

- **Vty Password**

```
router>enable
router#configure terminal
router(config)#line vty 0 4
router(config-line)#password <word>
router(config-line)#login
router(config-line)#exit
```

- **Auxiliary Password**

```
router#configure terminal
router(config)#line Aux 0
router(config-line)#password <word>
router(config-line)#login
router(config-line)#exit
```

- **Enable Password**

```
router>enable

router#configure terminal

router(config)#enable password <word>

router(config)#exit
```

- **Enable Secret Password**

Enable Password is the clear text password. It is stored as clear text in configuration where as enable secret password is the encrypted password with MD5 (Media Digest 5) algorithm.

```
Router>enable

Router#configure terminal

Router(config)#enable secret <word>

Router(config)#exi
```

- **Encryption all passwords**

All passwords other than enable secret password are clear text password. We can encrypt all passwords using level 7 algorithms. The command to encrypt all passwords is

```
Router#configure terminal

Router(config)#service password-encryption
```

- **Managing Configuration**

There are two types of configuration present in a router

(1) Startup Configuration

(2) Running Configuration

- Startup configuration is stored in the NVRAM. Startup configuration is used to save settings in a router. Startup configuration is loaded at the time of booting in to the Primary RAM.
- Running Configuration is present in the Primary RAM wherever we run a command for configuration; this command is written in the running configuration.

- **To save configuration**

```
Router#copy running-configuration startup-configuration

OR

Router#write
```

- **To abort configuration**

```
Router#copy startup-configuration running-configuration
```

- **To display running-configuration**

```
 Router#show running-configuration
```

- **To display startup configuration**

```
Router#show startup-configuration
```

- **Configuring HostName**

```
Router#configure terminal

Router#hostname <name>

 #exit
```

- **Configuring Interfaces**

Interfaces configuration is one of the most important part of the router configuration. By default, all interfaces of Cisco router are in disabled mode. We have to use different commands as our requirement to enable and configure the interface.

Configuring IP, Mask and Enabling the Interface

```
Router#configure terminal

Router(config)#interface <type><no>

Router(config-if)#ip address <ip><mask>

Router(config-if)#no shutdown

Router(config-if)#exit
```

2.3.4.3 TYPES OF ROUTING

- **Static Routing**

In this routing, we have to use IP route commands through which we can specify routes for different networks. The administrator will analyze whole internetwork topology and then specify the route for each n/w that is not directly connected to the router.

Steps to perform static routing

(1) Create a list of all n/w present in internetwork.

(2) Remove the n/w address from list, which is directly connected to n/w.

(3) Specify each route for each routing n/w by using IP route command.

```
Router(config)#ip route <destination n/w><mask><next hop ip>
```

Next hop IP: It is the IP address of neighbor router that is directly connected to our router.

Static Routing Example: -

```
Router#configure terminal

Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.10.2
```

Advantages of static routing

(1) Fast and efficient.

(2) More control over selected path.

(3) Less overhead for router.

(4) Bandwidth of interfaces is not consumed in routing updates.

Disadvantages of static routing

(1) More overheads on administrator.

(2) Load balancing is not easily possible.

(3) In case of topology change routing table has to be change manually.

Alternate command to specify static route: Static route can also specify in following syntax:

```
Router(config)#ip route 172.16.0.0 255.255.0.0 172.25.0.2
```

Or

```
Router(config)#ip route 172.16.0.0 255.255.0.0 serial 0
```

Backup route or loading static route

If more than one path is available from our router to destination then we can specify one route as primary and other route as backup route.

Administrator Distance is used to specify one route as primary and other route as backup. Router will select lower AD route to forward the traffic. By default static route has AD value of 1. With backup path, we will specify higher AD so that this route will be used if primary route is unavailable.

Protocols	**AD**
Directly Connected	0
Static	1
BGP	20
EIGRP	90
IGRP	100
OSPF	110
RIP	120

Syntax: - To set backup path

```
Router(config)#ip route <dest. n/w><mask><next hop><AD>
<exit interface>
```

Example: -

```
Router#configure terminal

Router(config)#ip route 150.10.0.0 255.255.0.0 150.20.0.5

Router(config)#ip route 150.10.0.0 25.255.0.0 160.20.1.1 8 (below

Router(config)#exit
```

Scenario 1

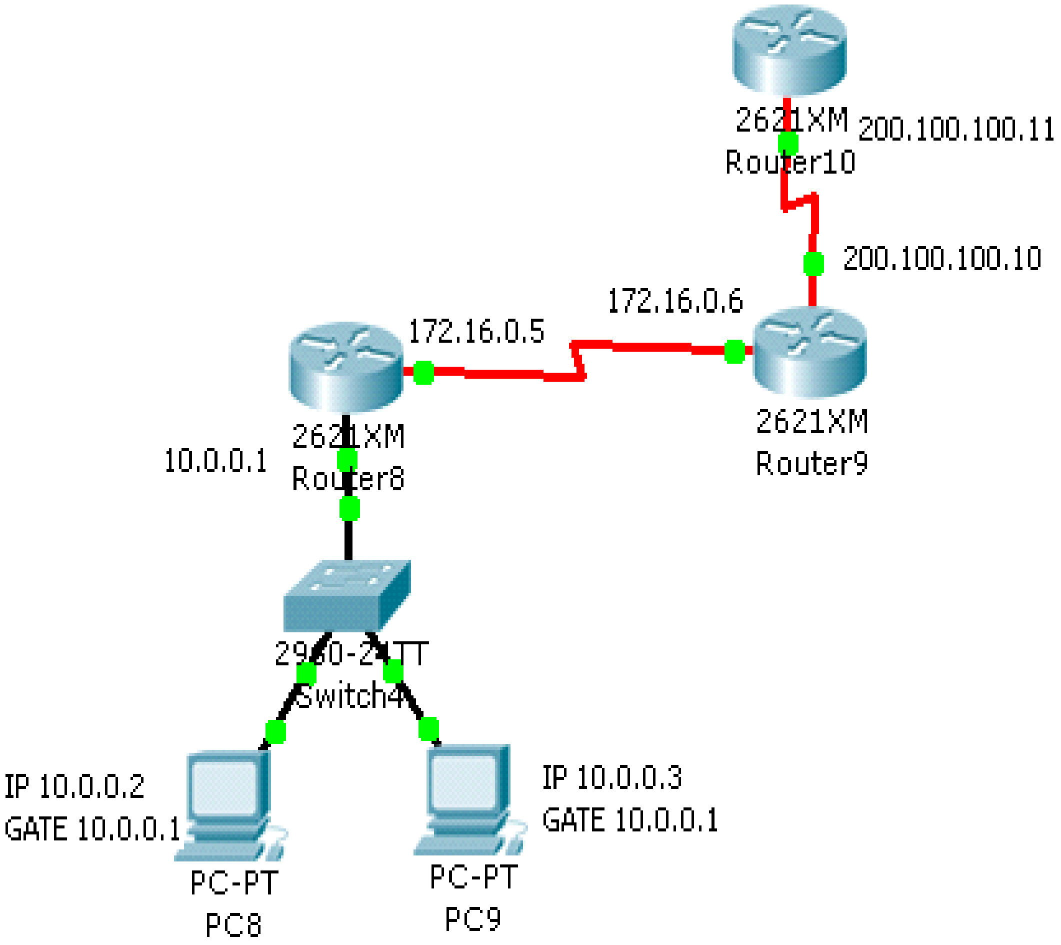


Figure 17: STATIC ROUTING

- **To display routing table**

```
Router#show ip route
```

- **To display static routes only**

Router#show ip route static

- **To display connected n/ws only**

  Router#show ip route connected

- **To check all the interface of a router**

  Router#show interface brief

- **Default Routing**

Default routing means a route for any n/w. these routes are specify with the help of following syntax: -

Router(config)#ip route 0.0.0.0 0.0.0.0 <next hop>

This type of routing is used in following scenario.

Scenario 2: -

Stub network

A n/w which has only one exit interface is called **stub network**.

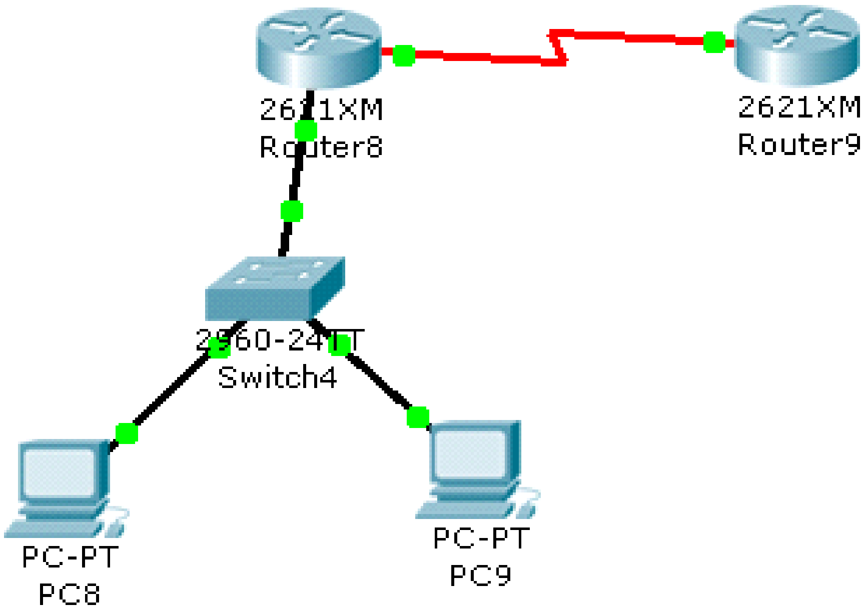


Figure 18: DEFAULT ROUTING

Internet connectivity

On Internet, million of n/ws are present. So we have to specify default routing on our router. Default route is also called gateway of last resort. This route will be used when no other routing protocol is available. If there is one next hop then we can use default routing.

- **Dynamic Routing**

In dynamic routing, we will enable a routing protocol on router. This protocol will send its routing information to the neighbor router. The neighbors will analyze the information and write new routes to the routing table.

The routers will pass routing information receive from one router to other router also. If there are more than one path available then routes are compared and best path is selected. Some examples of dynamic protocol are: - **RIP, IGRP, EIGRP, OSPF**

Types of Dynamic Routing Protocols

According to the working there are two types of Dynamic Routing Protocols.

(1) Distance Vector

(2) Link State

According to the type of area in which protocol is used there are again two types of protocol: -

(1) Interior Routing Protocol

(2) Exterior Routing Protocol

- **Distance Vector Routing**

The Routing, which is based on two parameters, that is distance and direction is called Distance Vector Routing. The example of Distance Vector Routing is RIP & IGRP.

Operation: -

(1) Each Router will send its directly connected Information to the neighbor router. This information is send periodically to the neighbors.

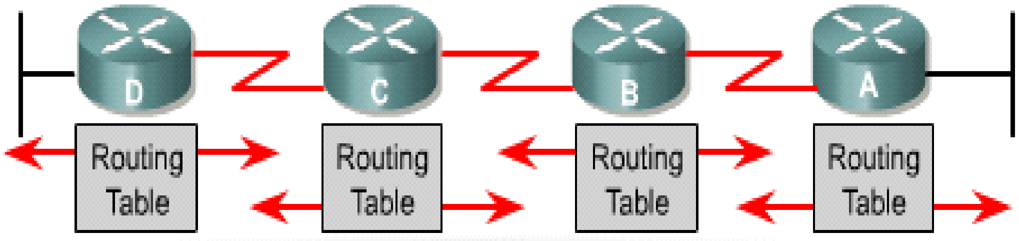


Figure 19: DISTANCE VECTOR ROUTING

(2) The neighbor will receive routing updates and process the route according to following conditions: -

(i) If update of a new n/w is received then this information is stored in routing table.

(ii) If update of a route is received which is already present in routing table then route will be refresh that is route times are reset to zero.

(iii) If update is received for a route with lower metric then the route, which is already present in our routing table. The router will discard old route and write the new route in the routing table.

(iv) If update is received with higher metric then the route that is already present in routing table, in this case the new update will be discard.

(3) A timer is associated with each route. The router will forward routing information on all interfaces and entire routing table is send to the neighbor.

There are three types of timers associated with a router route:

(i) Route update timer. It is the time after which the router will send periodic update to the neighbor.

(ii) Route invalid timer. It is the time after which the route is declared invalid, if there are no updates for the route. Invalid route are not forwarded to neighbor routers but it is still used to forward the traffic.

(iii) Route flush timer. It is the time after which route is removed from the routing table, if there are no updates about the router.

- **Metric of Dynamic Routing**

Metric are the measuring unit to calculate the distance of destination n/w. A protocol may use a one or more than one at a time to calculate the distance. Different types of metric are: -

(1) Hop Count

(2) Band Width

(3) Load

(4) Reliability

(5) Delay

(6) MTU

Hop Count It is the no. of Hops (Routers) a packet has to travel for a destination n/w.

Bandwidth Bandwidth is the speed of link. The path with higher bandwidth is preferred to send the data.

Load Load is the amount of traffic present in the interface. Paths with lower load and high throughput are used to send data.

Reliability Reliability is up time of interface over a period of time.

Delay Delay is the time period b/w a packet is sent and received by the destination.

MTU (Maximum Transmission Unit) It is the maximum size of packet that can be sent in a frame mostly MTU is set to 1500.

- **Problems of Distance Vector**

There are two main problems of distance vector routing:

- Bandwidth Consumption
- Routing Loops

(i) Bandwidth Consumption: The problem of excessive bandwidth consumption is solved out with the help of autonomous system. It exchanges b/w different routers. We can also perform route summarization to reduce the traffic.

(ii) Routing Loops: It may occur b/w adjacent routers due to wrong routing information. Distance Vector routing is also called routing by Rumor. Due to this the packet may enter in the loop condition until their TTL is expired.

Methods to solve routing loops

There are five different methods to solve or reduce the problem of routing loop.

(i) Maximum Hop Count

This method limits the maximum no. of hops a packet can travel. This method does not solve loop problem. But it reduces the loop size in the n/w. Due to this method the end to end size of a n/w is also limited.

(ii) Flash Updates/Triggered Updates

In this method a partial update is send to the all neighbors as soon as there is topology change. The router, which receives flash updates, will also send the flash updates to the neighbor routers.

(iii) Split Horizon

Split Horizon states routes that update receive from an interface cannot be send back to same interface.

(iv) Poison Reverse

This method is the combination of split Horizon and Flash updates. It implements the rule that information received from the interface cannot be sent back to the interface and in case of topology change flash updates will be send to the neighbour.

(v) Hold Down

If a route changes frequently then the route is declared in Hold Down state and no updates are received until the Hold Down timer expires.

Routing Information Protocol (RIP):

Routing Information Protocol (RIP) is a true distance-vector routing protocol.

RIP Features:

- Distance Vector Routing Protocol
- Maximum Reachable hop-count is 15
- Hop 16 is considered unreachable
- Metric is HOP COUNT
- Administrative distance 120
- Sends periodic update every 30 seconds
- Supports equal path load balancing
- Works at application layer

RIP Timers:-

RIP uses different kinds of timers to regulate its performance:

- **Route update timer** Sets the interval (typically 30 seconds) between periodic routing updates, in which the router sends a complete copy of its routing table out to all neighbours.
- **Route invalid timer** Determines the length of time that must elapse (180 seconds) before a router determines that a route has become invalid. It will come to this conclusion if it hasn’t heard any updates about a particular route for that period. When that happens, the router will send out updates to all its neighbours letting them know that the route is invalid.
- **Hold down timer** This sets the amount of time during which routing information is suppressed. Routes will enter into the hold down state when an update packet is received that indicated the route is unreachable. This continues until either an update packet is received with a better metric or until the hold down timer expires. The default is 180 seconds.
- **Route flush timer** Sets the time between a route becoming invalid and its removal from the routing table (240 seconds). Before it’s removed from the table, the router notifies its neighbours of that route’s impending demise. The value of the route invalid timer must be less than that of the route flush timer. This gives the router enough time to tell its neighbours about the invalid route before the local routing table is updated.

Configuring RIP

```
Router#confiure terminal
```

```
Router(config)#router rip
Router(config-router)#network <own net address>
Router(config-router)#network <own net address>
Router(config-router)#exit
```

RIP advanced configuration

(a) Passive Interfaces

An interface, which is not able to send routing updates but able to receive routing update only is called Passive Interface. We can declare an interface as passive with following commands:

```
Router#configure terminal
Router(config)#router rip
Router(config-router)#Passive-interface <type><no>
Router(config-router)#exit
```

(b) Configuring Timers

```
Router(config)#router rip
Router(config-router)#timers basic <update><invalid><hold down><flush>
Router(config-router)#exit
```

Example: -

```
Router(config-router)#timer basic 50 200 210 300
```

Update 50 sec

Invalid 200 sec

Hold 210 sec

Flush 300 sec

(c) To configure Load Balance

RIP is able to perform equal path cost Load Balancing. If multiple paths are available with equal Hop Count for the destination then RIP will balance load equally on all paths.

Load Balancing is enabled by default 4 paths. We can change the no. of paths. It can use simultaneously by following command: -

```
Router(config)#router rip
```

```
Router(config-router)#maximum-path <1-6>
```

(d) To display RIP parameters

```
Router#show ip protocol
```

This command displays following parameters: -

(i) RIP Timers

(ii) RIP Version

(iii) Route filtering

(iv) Route redistribution

(v) Interfaces on which update send

(vi) And receive

(vii) Advertise n/w

(viii) Passive interface

(ix) Neighbor RIP

RIP version 2

RIP version 2 supports following new features: -

(1) Support VLSM (send mask in updates)

(2) Multicast updates using address 224.0.0.9

(3) Supports authentication

Commands to enable RIP version 2

We have to change RIP version 1 to RIP version 2. Rest all communication will remain same in RIP version 2.

```
Router(config)#Router RIP

Router(config-router)#version 2

Router(config-router)#exit
```

To debug RIP routing

```
Router#debug ip rip
```

To disable debug routing

```
Router#no debug ip rip
```

2.2.5 LAN SWITCHING

Ethernet switches are used in LAN to create Ethernet n/ws. Switches forward the traffic on the basis of MAC address. Switches maintain a Mac Addressee table in which mac addresses and port no's used to perform switching decision. Working of bridge and switch is similar to each other.

Classification of switches

Switches are classified according to the following criteria: -

Types of switches based on working

(1) Store & Forward: This switch receives entire frame then perform error checking and start forwarding data to the destination.

(2) Cut through this switch starts forwarding frame as soon as first six bytes of the frame are received.

(3) Fragment-free this switch receives 64 bytes of the frame, perform error checking and then start forwarding data.

(4) Adaptive cut-through it changes its mode according the condition. If it sees there are errors in many frames then it changes to Store & Forward mode from Cut through or Fragment-free.

Types of switches based on management

(1) Manageable switches

(2) Non-Manageable switches

(3) Semi-Manageable switches

Types of switches based on OSI layer

(1) Layer 2 switches (only switching)

(2) Layer 3 switches (switching & routing)

Types of switches based on command mode (only in Cisco)

(1) IOS based

(2) CLI based

Type of switches based on hierarchical model

(1) Core layer switches

(2) Distribution layer switches

(3) Access layer switches

Qualities of switch

- No. of ports

- Speed of ports

- Type of media

- Switching or wire speed or throughput

Configuring IP and Gateway on switch

We can configure IP address on switch for web access or telnet IP address is required for the administration of the switch. If we have to access switch from remote n/w then we will configure default gateway in addition to IP address.

IP address is assigned to the logical interface of switch with following command:-

```
Switch(config)#interface vlan 1

Switch(config)#IP address <ip><mask>

Switch(config)#no sh

Switch(config)#exit
```

2.2.5.1 VLAN (Virtual LAN)

VLAN provides Virtual Segmentation of Broadcast Domain in the network. The devices, which are member of same Vlan, are able to communicate with each other. The devices of different Vlan may communicate with each other with routing. So that different.Vlan devices will use different n/w addresses.

Vlan provides following advantages: -

(1) Logical Segmentation of network

(2) Enhance network security

Creating port based Vlan

In port based Vlan, first we have to create a Vlan on manageable switch then we have to add ports to the Vlan.

Commands to create Vlan

```
Switch#configure terminal

Switch(config)#vlan <no>

[name <word>]

Switch(config)#exit optional
```

Or

```
Switch#vlan database

Switch(vlan)#vlan <no>

[name <word>]

Switch(vlan)#exit
```

Commands to configure ports for a Vlan

By default, all ports are member of single vlan that is Vlan1. We can change vlan membership according to our requirement.

```
Switch#configure terminal

Switch(config)#interface <type><no>

Switch(config-if)#switchport access vlan <no>
Switch(config-if)#exit
```

Commands to configure multiple ports in a vlan

```
Switch#configure terminal

Switch(config)#interface range <type><slot/port no (space)–(space) port no>

Switch(config-if)#switchport access vlan <no>

Switch(config-if)#exit
```

2.3 OPERATION ENVIRONMENT

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts.

Packet Tracer, which is often not feasible with physical hardware, due to costs. Packet Tracer is commonly used by CCNA Academy students, since it is available to them for free. However, 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. Packet Tracer can be useful for understanding abstract networking concepts, such as the Enhanced Interior Gateway Routing Protocol by animating these elements in a visual form. Packet Tracer is also useful in education by providing additional components, including an authoring system, network protocol simulation and improving knowledge an assessment system.

2.4 DESIGN AND IMPLEMENTATION CONSTRAINTS

While designing the scenario the main focus was on implementing the best routing protocol for the given scenario and show LAN switching. Other main focus while designing was to create a better communication at different branches of the company at different locations

This project has the following features:-

- The network is secured.
- It is easy to understand the whole network.
- Networking is done by areas.
- Easy to troubleshoot.
- We can extend the range of slots in routers.
- Networking By areas

There are some assumptions that are needed to be taken before studying the project that are:

- Routing protocol (RIP) used is best for the scenario depicted.
- The Company for which the network is created is a huge company having offices at different locations.
- Company for which the network is created is expanded in a certain state e.g. Delhi as all the locations that are mentioned are in Delhi.

CHAPTER 3: SYSTEM IMPLEMENTATION

3.1 ER DIAGRAAM

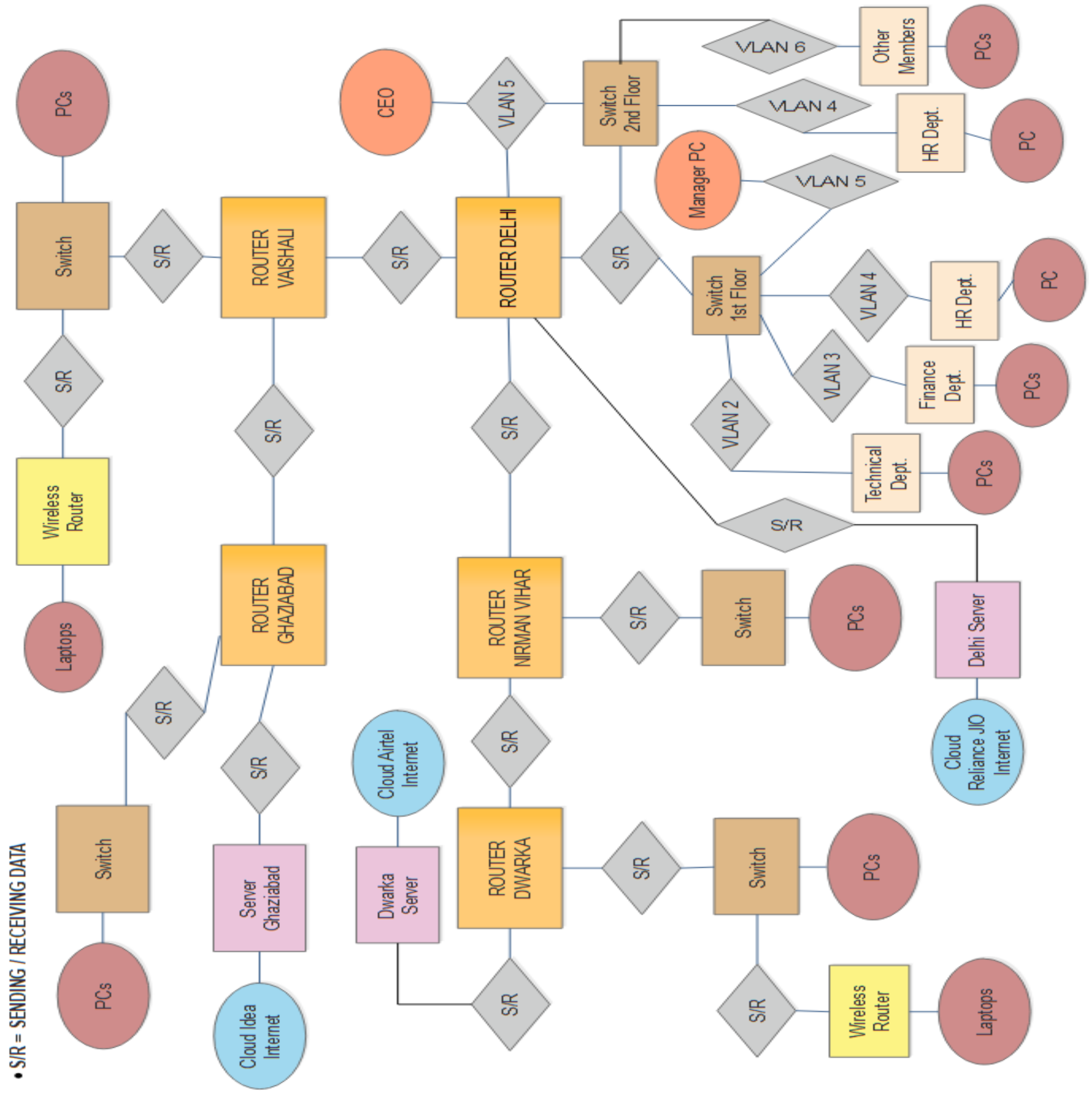


Figure 20: ER DIAGRAM OF PROJECT

Entities with their corresponding attributes:

1. **Router Dwarka**
   It contains the network under Dwarka region.

- Switches
- Wireless router
- Dwarka server (further connected to cloud Airtel Internet)
- End devices like: PC and Laptop (having a different class IP address)

2. **Router Nirman Vihar**
   It contains the network under Nirman Vihar region.

- Switch
- End device like: PC (having a different class IP address)

3. **Router Ghaziabad**
   It contains the network under Ghaziabad region.

- Switch
- Ghaziabad server (further connected to Cloud Idea Internet)
- End device like: PC

4. **Router Vaishali**
   It contains the network under Vaishali region.

- Switch
- Wireless router
- End devices like: PC and Laptop (having a different class IP address)

5. **Router Delhi**
   It contains the network under Delhi region. The headquarter of the company is assumed to be here.

- Switches
- Hubs
- Delhi server (further connected to Cloud Reliance JIO Internet)
- End device like: PCs (having a different class IP address)
- Technical, Finance, HR, Other members Department
- CEO and Manager PC (both are in trunk with HR members i.e. the manager and CEO are able to access information from HR members PC)

3.2 PROJECT PLANNING OR SCHEDULING

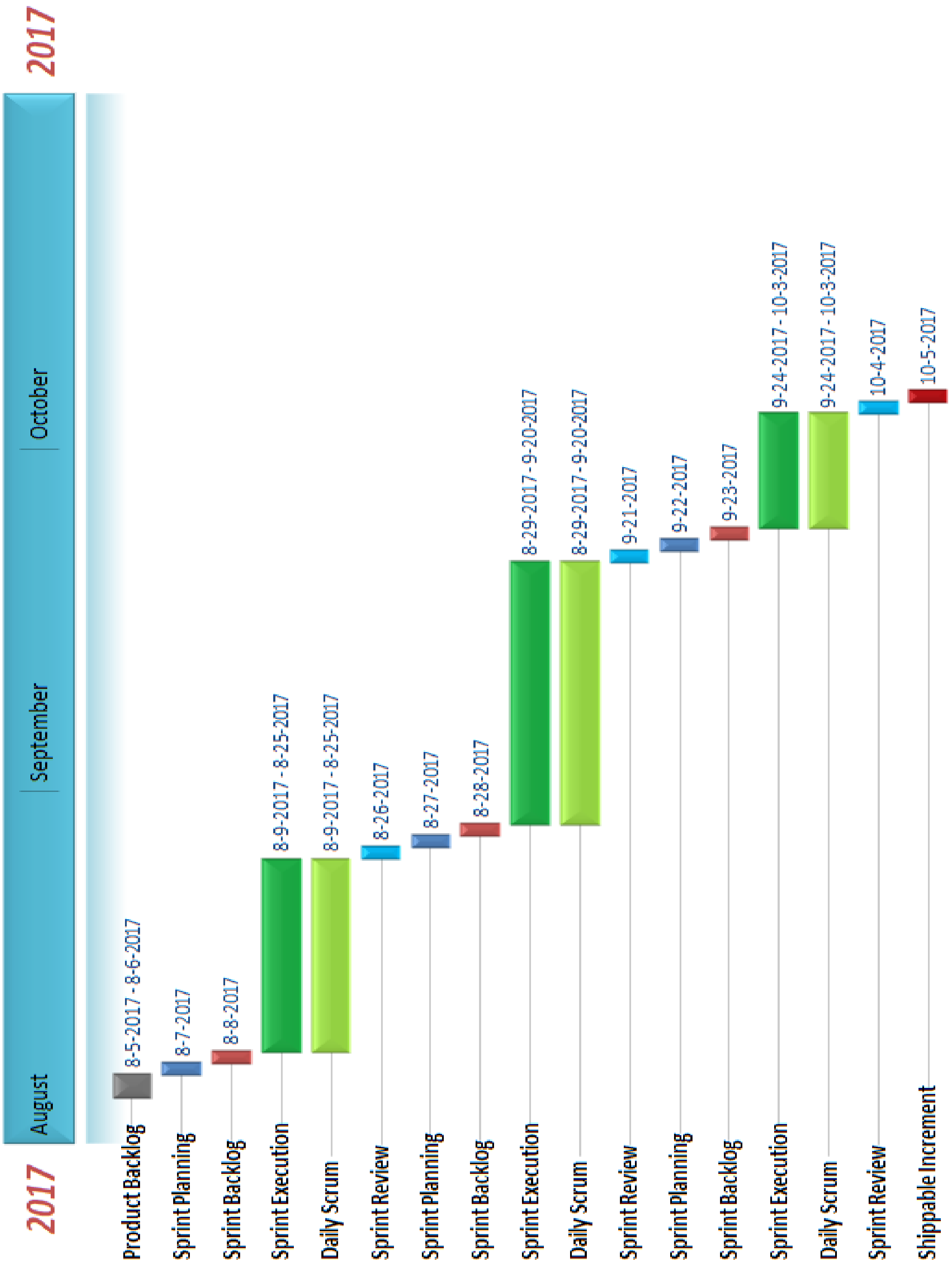


Figure 21: GANTT CHART

In Figure 4, Gantt chart uses a Software Development methodology among **Agile** Methodology, knows as **Scrum.**

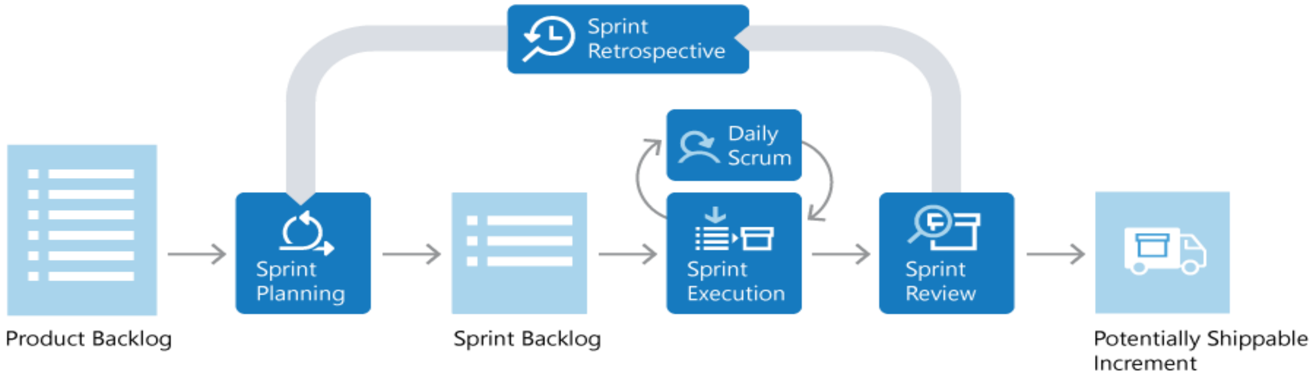


Figure 22: FLOW DEPICTION OF SCRUM

Product Backlog

The Product Backlog is a prioritized list of value the team can deliver. The Product Owner owns the backlog and adds, changes, and reprioritizes as needed. The items at the top of the backlog should always be ready for the team to execute on.

Sprint Planning and Sprint Backlog

In Sprint Planning, the team chooses the backlog items they will work on in the upcoming sprint. The team chooses backlog items based on priority and what they believe they can complete in the sprint. The Sprint Backlog is the list of items the team plans to deliver in the sprint. Often, each item on the Sprint Backlog is broken down into tasks. Once all members agree the Sprint Backlog is achievable, the Sprint starts.

Sprint Execution and Daily Scrum

Once the Sprint starts, the team executes on the Sprint Backlog. Scrum does not specify how the team should execute. That is left for the team to decide.

Scrum defines a practice called a Daily Scrum, often called the Daily Standup. The Daily Scrum is daily meeting limited to 15 minutes. Team members often stand during the meeting, to ensure it stays brief. Each team member briefly reports their progress since yesterday, the plans for today, and anything impeding their progress.

Sprint Review

The team demonstrates what they’ve accomplished to stakeholders. They demo the software and show its value.

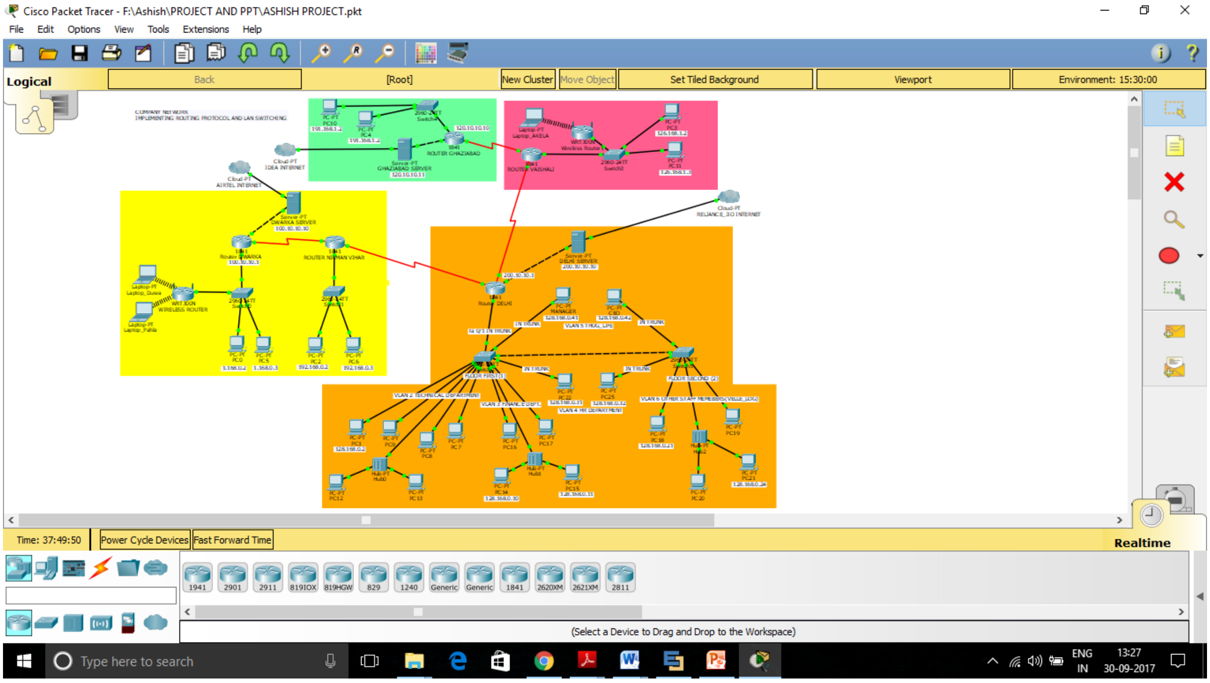
Sprint Retrospective

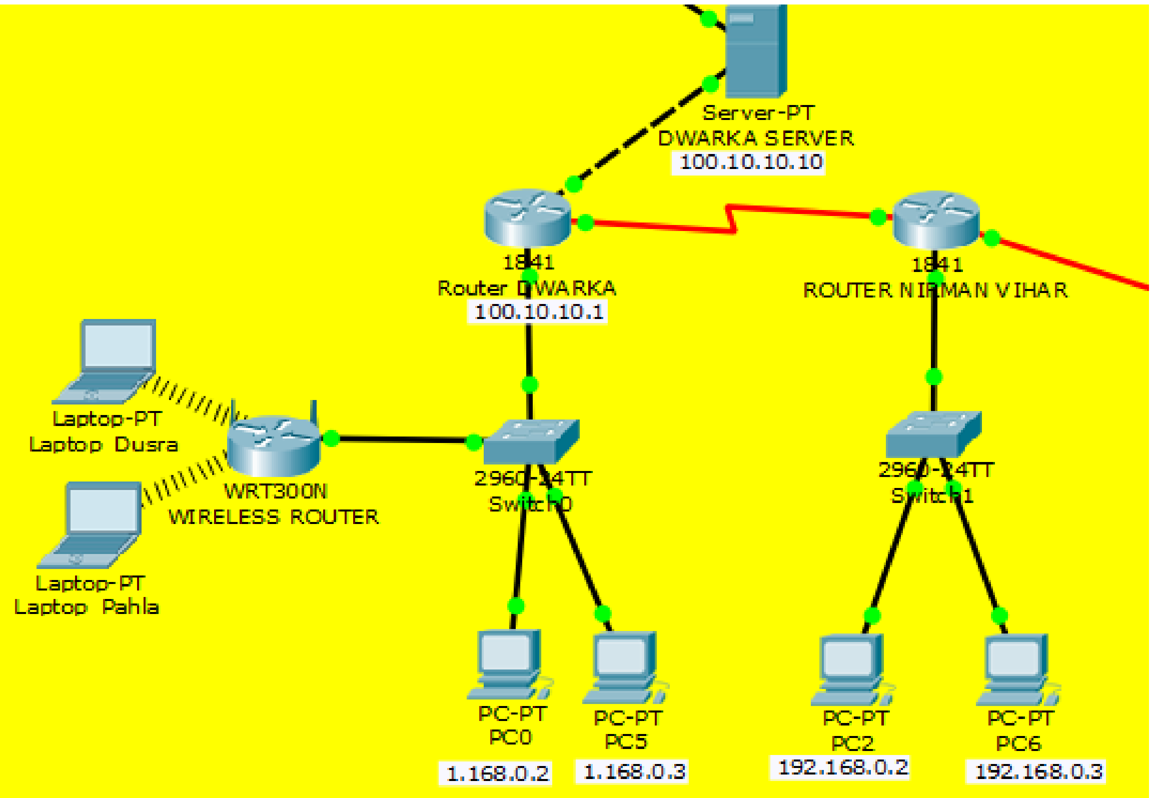
The team takes time to reflect on what went well and which areas need improvement. The outcomes of the retrospective are actions for next sprint.

Shippable Increment

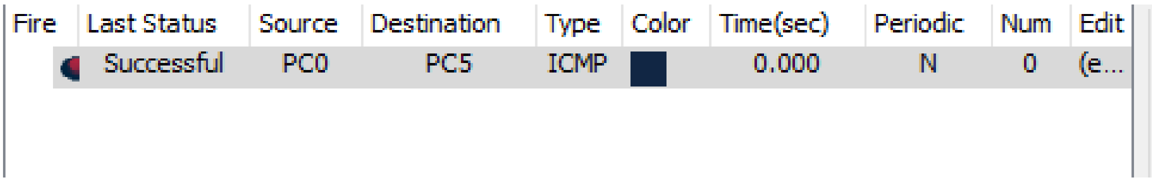
It should meet all the quality criteria set by the team and Product Owner so that it is of shippable quality and ready to dispatch to the client/customer.

3.3 PROJECT SCREENSHOTS


Cisco Packet Tracer - F:\Ashish\PROJECT AND PPT\ASHISH PROJECT.pkt
File Edit Options View Tools Extensions Help
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Environment: 15:30:00
Time: 37:49:50
Power Cycle Devices
Fast Forward Time
Realtime
1941 2901 2911 819IOX 819HGW 829 1240 Generic Generic 1841 2620XM 2621XM 2811
(Select a Device to Drag and Drop to the Workspace)
Type here to search
ENG IN
13:27
30-09-2017

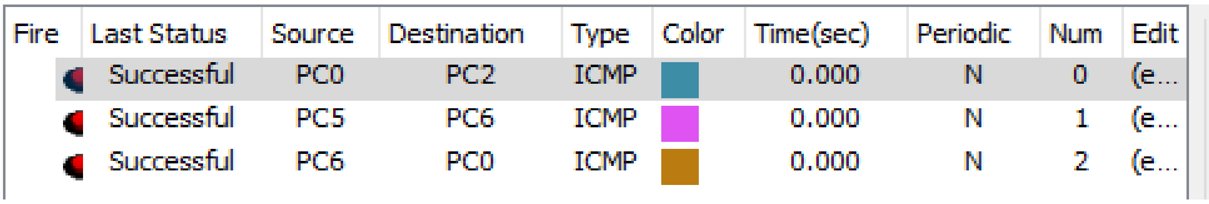


- **COMMUNICATING IN SAME NETWORK**



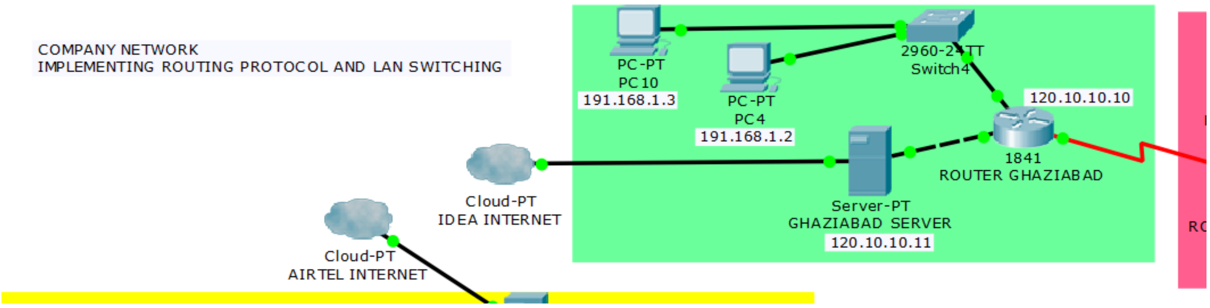
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	Successful	PC0	PC5	ICMP	■	0.000	N	0	(e...

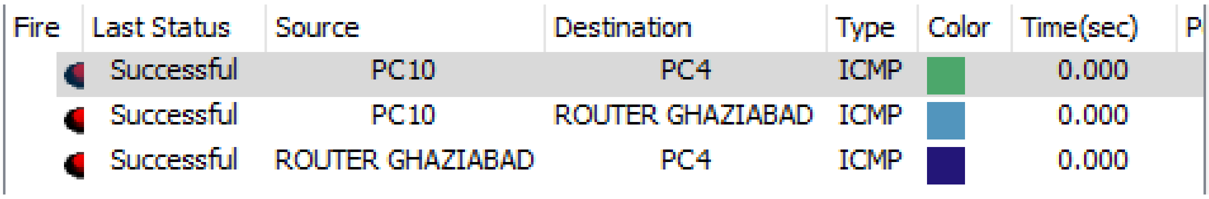
- **COMMUNICATING IN DIFFERENT NETWORK**



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	Successful	PC0	PC2	ICMP	🟦	0.000	N	0	(e...
●	Successful	PC5	PC6	ICMP	🟪	0.000	N	1	(e...
●	Successful	PC6	PC0	ICMP	🟫	0.000	N	2	(e...

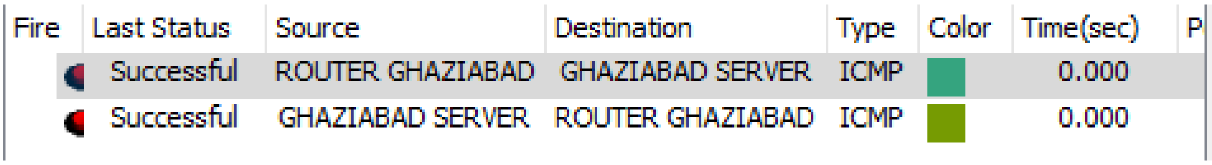
- **ANOTHER NETWORK SHOWING PC COMMUNICATING TO ROUTER AND ROUTER TO PC AND PC TO PC**





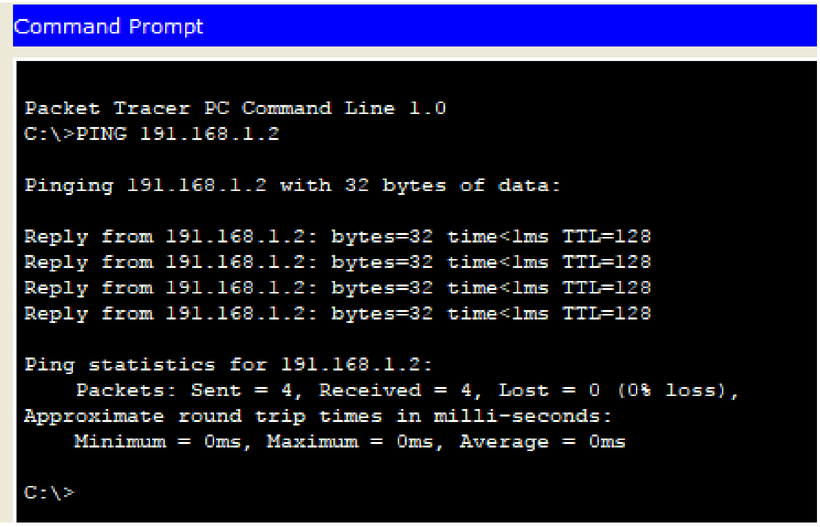
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	P
●	Successful	PC10	PC4	ICMP	🟩	0.000	
●	Successful	PC10	ROUTER GHAZIABAD	ICMP	🟦	0.000	
●	Successful	ROUTER GHAZIABAD	PC4	ICMP	🟦	0.000	

- **GHAZIABAD ROUTER COMMUNICATING WITH GAZIABAD SERVER AND VICE VERSA**



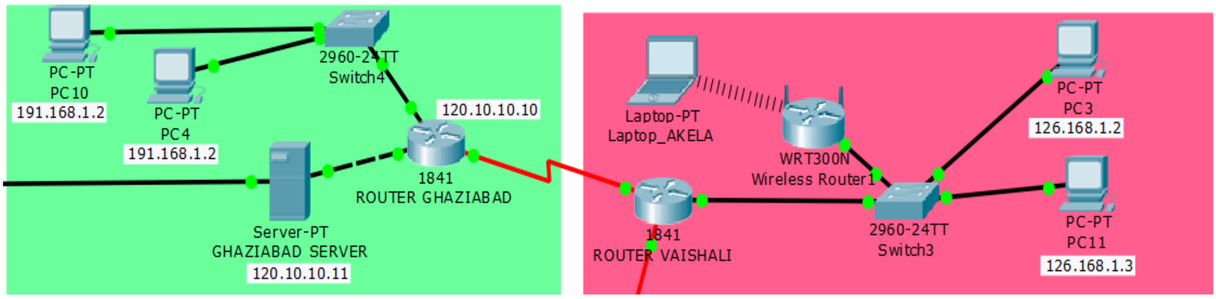
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	P
●	Successful	ROUTER GHAZIABAD	GHAZIABAD SERVER	ICMP	🟩	0.000	
●	Successful	GHAZIABAD SERVER	ROUTER GHAZIABAD	ICMP	🟩	0.000	

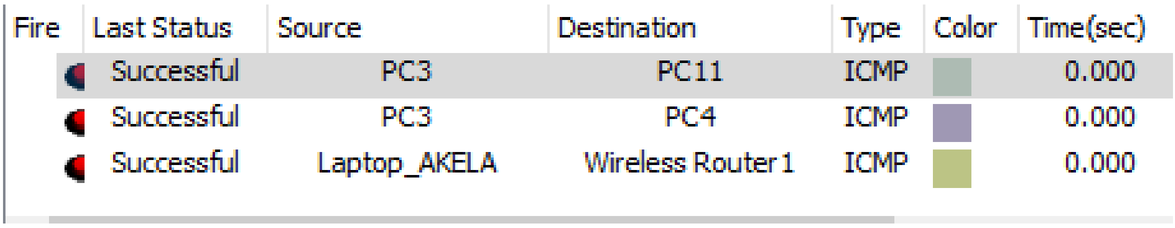
- **PING 191.168.1.2 FROM 191.168.1.3 (PC 10 to PC 4)**



```
Packet Tracer PC Command Line 1.0
C:\>PING 191.168.1.2

Pinging 191.168.1.2 with 32 bytes of data:

Reply from 191.168.1.2: bytes=32 time<1ms TTL=128
Reply from 191.168.1.2: bytes=32 time<1ms TTL=128
Reply from 191.168.1.2: bytes=32 time<1ms TTL=128
Reply from 191.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 191.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

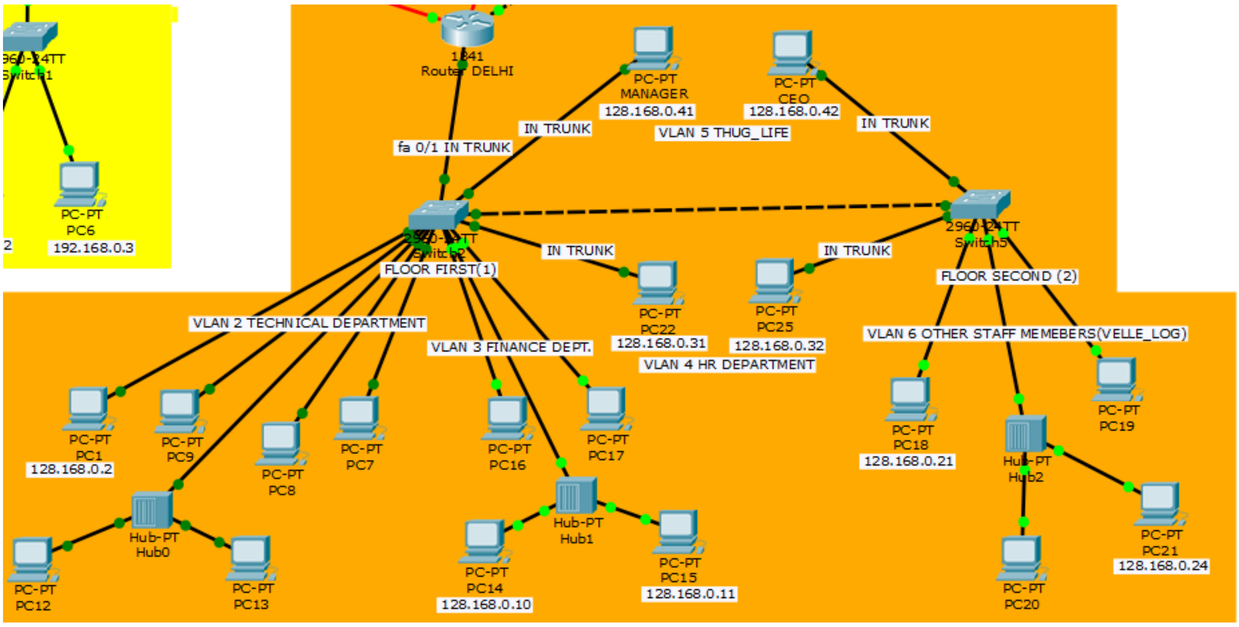
- **DIFFERENT NETWORKS COMMUNICATING TO EACH OTHER AND LAPTOP CONNECTED TO WIRELESS ROUTER**

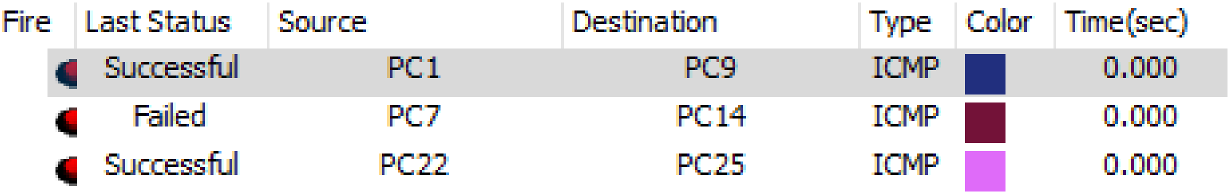




Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	PC3	PC11	ICMP	■	0.000
●	Successful	PC3	PC4	ICMP	■	0.000
●	Successful	Laptop_AKELA	Wireless Router1	ICMP	■	0.000

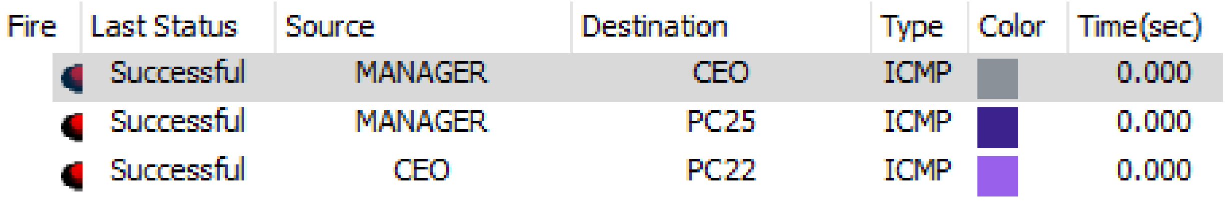
- **SAME VLANS ABLE TO COMMUNICATE**





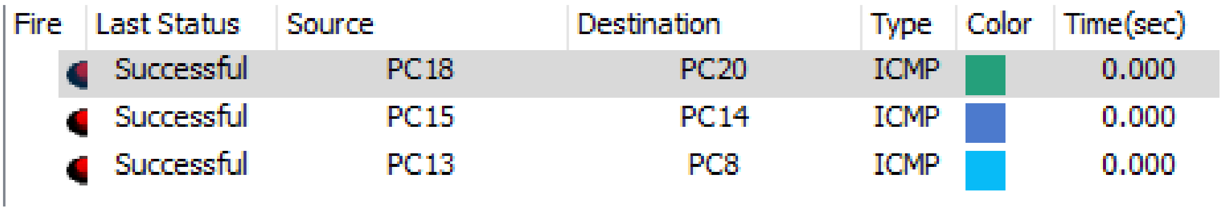
Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	PC1	PC9	ICMP	■	0.000
●	Failed	PC7	PC14	ICMP	■	0.000
●	Successful	PC22	PC25	ICMP	■	0.000

- **MANAGER AND CEO COMMUNICATING WITH EACH OTHER AND WITH HR DEPARTMENT**



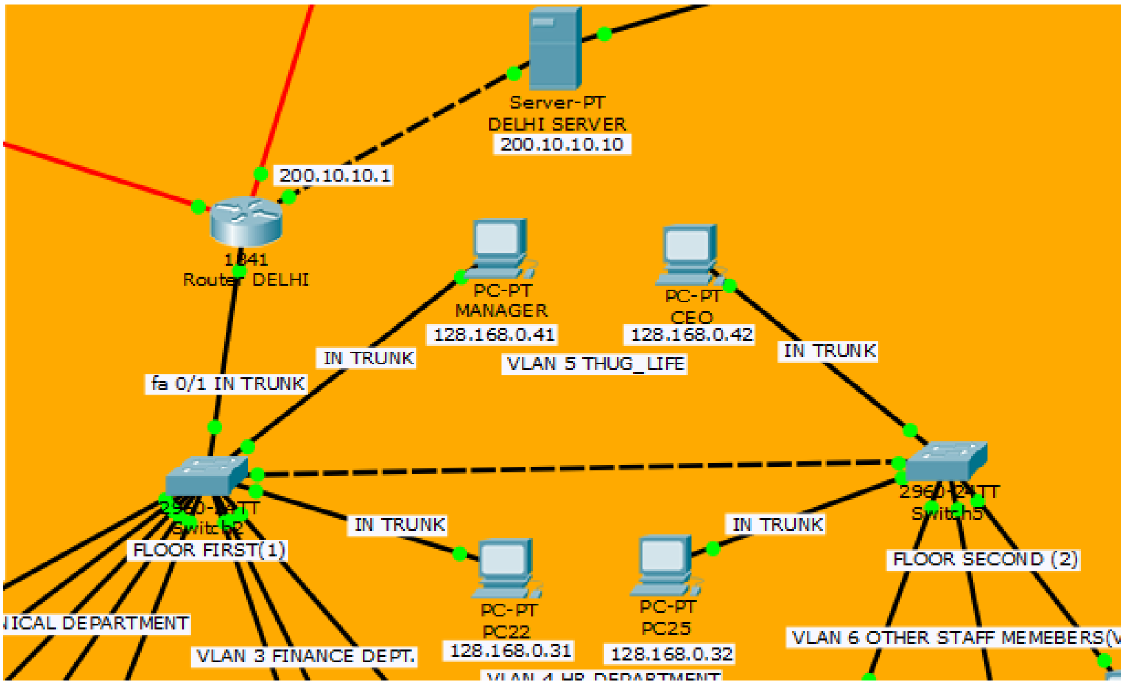
Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	MANAGER	CEO	ICMP	⬛	0.000
●	Successful	MANAGER	PC25	ICMP	🟪	0.000
●	Successful	CEO	PC22	ICMP	🟪	0.000

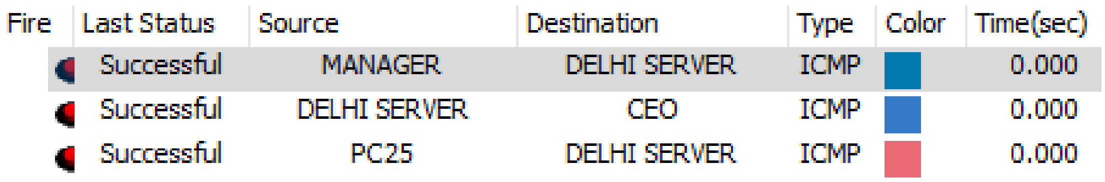
- **PCs CONNECTED WITH HELP OF HUBS ABLE TO COMMUNICATE IN NETWORK**



Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	PC18	PC20	ICMP	🟩	0.000
●	Successful	PC15	PC14	ICMP	🟦	0.000
●	Successful	PC13	PC8	ICMP	🟦	0.000

- **MANAGER AND CEO ABLE TO COMMUNICATE WITH DELHI’S SERVER**





Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	MANAGER	DELHI SERVER	ICMP	🟦	0.000
●	Successful	DELHI SERVER	CEO	ICMP	🟦	0.000
●	Successful	PC25	DELHI SERVER	ICMP	🟥	0.000

CHAPTER 4: RESULT AND DISCUSSION

As the above screenshots depicts the project having logical topology implemented this network avoids the unauthorized access as it authenticate the authorized users or hosts. The main Delhi router is password protected as it is the assumed headquarter of the organisation further subnetting helps in reducing the wastage of IP Addresses. This network connects the different department of a company that is the finance, technical, HR and other staff members department. The assumed headquarter is connected to four other small branches of the company (via router) and the data transfer from each branch to main office is efficient. The transfer of packets can be seen in simulation mode of the packet tracer. The implementations of router are very accurate for the scenario as RIP is used it will follow the distance vector protocol and provide us with the shortest path in the network making the communication fast and secure. Further Vlan’s (Virtual LAN) creation help in providing logical segmentation of network and enhancing network security. This project fulfils the requirement of providing security in network to secure the private data and make reliable and excellent communication in WAN connection and reduce organisation dependency on floppy disks etc.

REFERENCES

Books:

- *L. Parziale, D.T. Britt, C. Davis, J. Forrester, Wei Liu, C. Matthews, N. Rosselot,* "TCP/IP Tutorial and Technical Overview".
- *Rahul Banerjee*, "Internetworking Technologies - An Engineering Perspective".
- *Sudakshina Kundu*, "Fundamentals of Networking".

Web Site:

- www.cisco.com