NETWORK DRIVE MAPPING, SHARING,TESTING AND AN IMPLEMENTATION BY WRITING A PROGRAM TO RETRIEVE THE DATA FILE FROM A NETWORK DRIVE OF ANOTHER COMPUTER.

BY

SAKIL AHMED

ID: 102-33-205

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Electrical and Electronics Engineering.

Supervised By
DR. M. SHAMSUL ALAM
Professor and Dean
Faculty of Engineering
Daffodil International University

Co- Supervised By
M. AKHTER UZ ZAMAN
Assistant Professor
Department of EEE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH

SEPTEMBER 2014

APPROVAL

This Project Report entitled "**NETWORK DRIVE MAPPING, SHARING,TESTING AND AN IMPLEMENTATION BY WRITING A PROGRAM TO RETRIEVE THE DATA FILE FROM A NETWORK DRIVE OF ANOTHER COMPUTER.**" By Sakil Ahmed has been submitted to the department of Electrical and Electronics Engineering of Daffodil International University in partial fulfillment of the requirements for the degree of Bachelor of Science in Electrical and Electronics Engineering.

Board of Examiners

DR. M. SHAMSUL ALAM **Dean & Chairman**
Professor and Dean
Faculty of Engineering
Daffodil International University

Prof. DR. MD. FAYZUR RAHMAN **Internal**
Professor and Head
Department of Electrical and Electronics Engineering
Daffodil International University

DECLARATION

I hereby declare that, this project has been done by me under the supervision of, **Professor Dr. M**. **Shamsul Alam**, **Dean, Faculty of Engineering, Daffodil International University** & co-supervision of **M. Akhter Uz Zaman, Assistant Professor, Department of Electrical and Electronics Engineering, Daffodil International University**. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

DR. M. SHAMSUL ALAM
Professor and Dean
Faculty of Engineering
Daffodil International University

Co- Supervised by:

M. AKHTER UZ ZAMAN
Assistant Professor
Department of EEE
Daffodil International University

Submitted by:

SAKIL AHMED

ID: 102-33-205

Department of EEE

Daffodil International University

ACKNOWLEDGEMENT

At first I want to express my heartiest thanks and gratefulness to the almighty God for His divine blessing makes me possible to complete this project successfully.

I feel grateful and wish my profound indebtedness to **Professor Dr. M. Shamsul Alam, Dean**, **Faculty of Engineering, Daffodil International University** & my Co-Supervisor **M. Akhter Uz Zaman**, **Assistant Professor, Department of EEE Daffodil International University**. Deep Knowledge & keen interest of my supervisors in the field of wired network & basic computer networking influenced me to carry out this project .Their endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

I would like to express my heartiest gratitude to **Professor Dr. Md. Fayzur Rahman,** Head of **Department of EEE**, for his kind help to finish our project and also to the other faculty members and the staffs of EEE department of Daffodil International University.

I would like to thank my entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patience of my parents.

ABSTRACT

In this project I basically worked on the very basic of computer networking. I have done root level of the networking process how the things are done behind the interface. I have discussed about different types of networks, those are used in various geographical areas. Here I discussed about OSI and TCP/IP model and about their layers that are used in networking process. I also discussed about the different network protocols and topologies. The project is basically aimed to measure the ease use of network diagram software particularly to help users to create a network diagram for multiple reasons. This project captured network file sharing and network drive mapping in a home network. The aim of this project is to share file and folder in the home network so by that everyone in the network can read and write the file.

TABLE OF CONTENTS

CHAPTERS

LIST OF FIGURES

FIGURES

CHAPTER 1: INTRODUCTION OF COMPUTER NETWORK

WHAT IS A COMPUTER NETWORK?

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.

Networks are used to:

Facilitate communication via email, video conferencing, instant messaging, etc.

Enable multiple users to share a single hardware device like a printer or scanner.

Enable file sharing across the network.

Allow for the sharing of software or operating programs on remote systems.

Make information easier to access and maintain among network users.

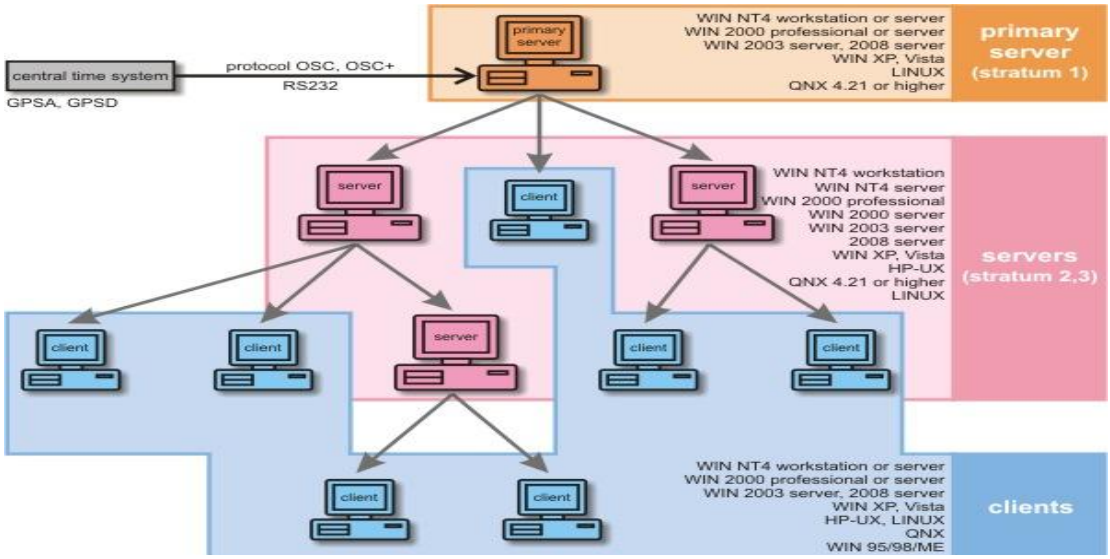


Figure1.1: Computer Network

BASIC ELEMENTS OF A COMPUTER NETWORK

The basic elements of computer networks

1. End devices also known as host: The sources and destinations of the communication. These devices act as the interface between the end users and the underlying network. Examples: Computers, mobile phones etc.

2. Intermediary devices: Devices that give network access to the attached end devices and transport the messages between hosts. Usually, transparent to the end users. Also, these devices accomplish communication functions in order to ensure the success of the communication process. Examples: Hubs, switches, routers, modems, firewalls, etc.

3. Transmission media: The physical media that connects the devices, enabling the exchange of messages between them. It may be wired or wireless.

4. Services: Network-aware software applications (e.g., a web browser) that request network resources (e.g., data) in order to enjoy the end user of the application some provided service (e.g., World Wide Web).

5. Processes: Software that runs on network devices in order to support the communication functions - in accordance with the established, also in software, communication rules or protocols - and facilitate the provision of services to the end users. In contrast with the services, processes are transparent to the end users.

6. Messages: Well-known applications. Includes telephone calls, e-mail, web pages, etc.

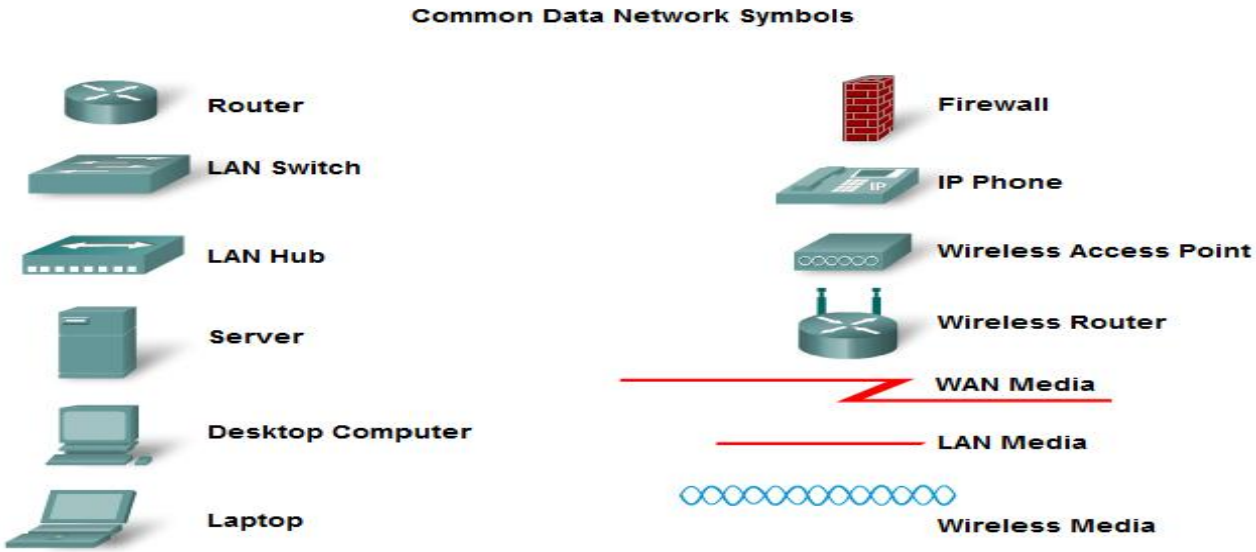


Figure 1.2: Basic Computer Network Elements

TYPES OF NETWORKS

There are many types of networks, including:

Local Area Networks (LAN)

Wide Area Networks (WAN)

Campus Area Networks (CAN)

Metropolitan Area Networks (MAN)

Home Area Networks (HAN)

Global Area Networks (GAN)

Wireless Local Area Networks (WLAN)

LOCAL AREA NETWORK

A local area network (LAN) is a computer network within a small geographical area such as a home, school, computer laboratory, office building or group of buildings.

A LAN is composed of inter-connected workstations and personal computers which are each capable of accessing and sharing data and devices, such as printers, scanners and data storage devices, anywhere on the LAN. LANs are characterized by higher communication and data transfer rates and the lack of any need for leased communication lines.

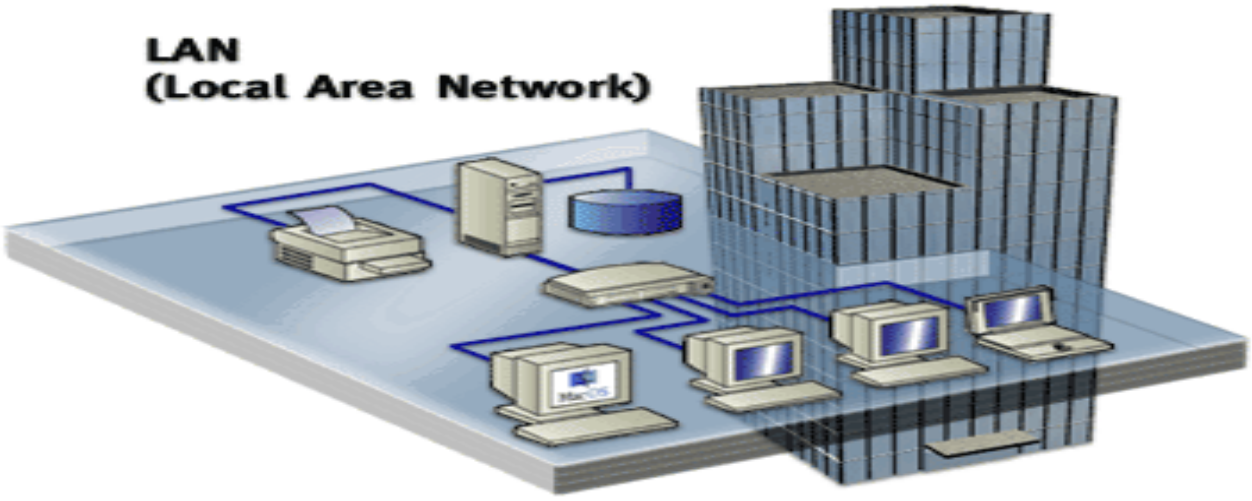


Figure1.3: Local Area Network (LAN)

WIDE AREA NETWORK

A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LAN) and metro area networks (MAN). This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.

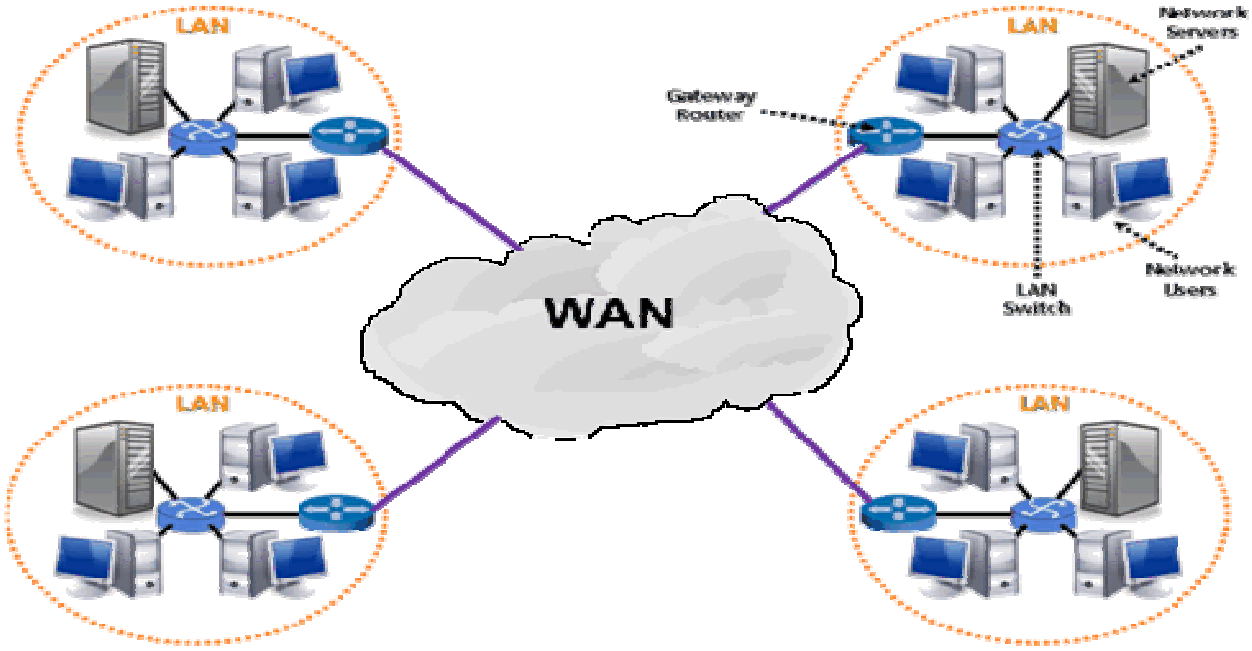


Figure1.4: Wide Area Network (WAN)

CAMPUS AREA NETWORK

A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area. A CAN is smaller than a wide area network (WAN) or metropolitan area network (MAN).

A CAN is also known as a corporate area network (CAN).In most cases, CANs own shared network devices and data exchange media.

CAN benefits are as follows:

Cost-effective

Wireless, versus cable

Multi departmental network access

Single shared data transfer rate (DTR)

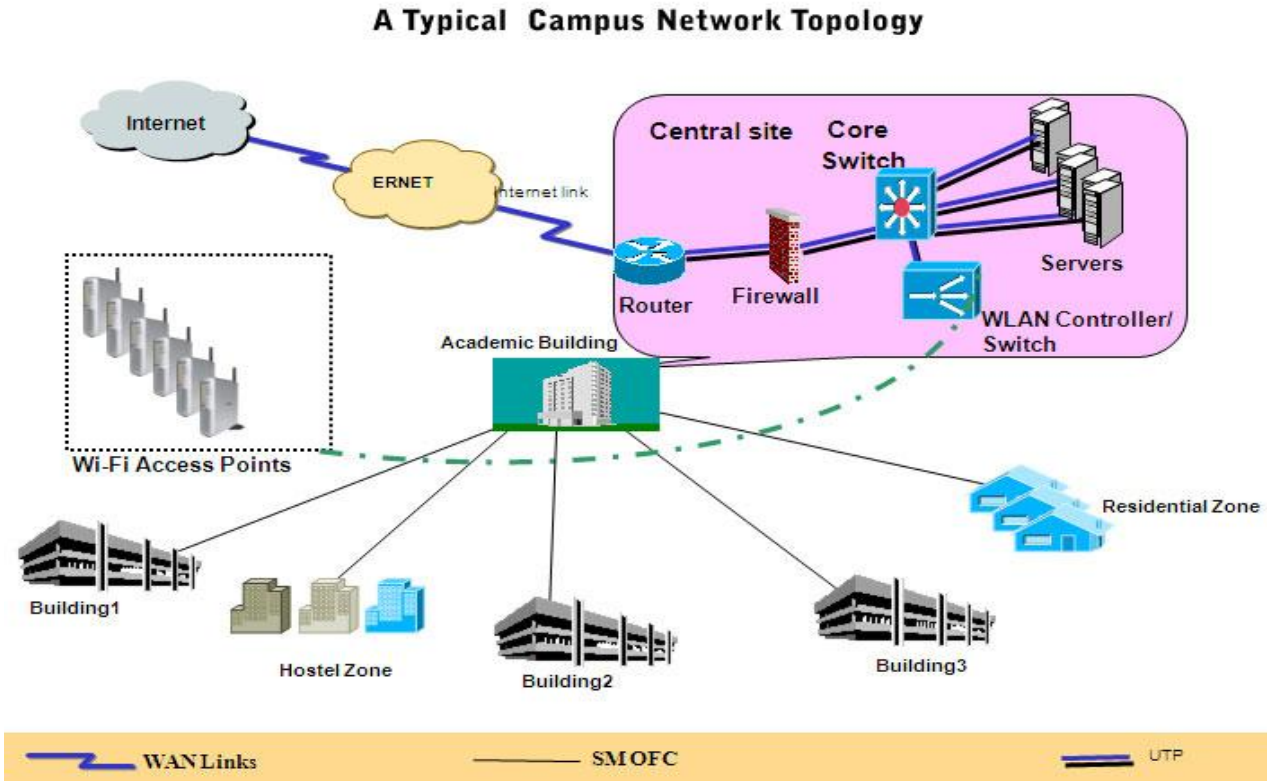


Figure1.5: Campus Area Network (CAN)

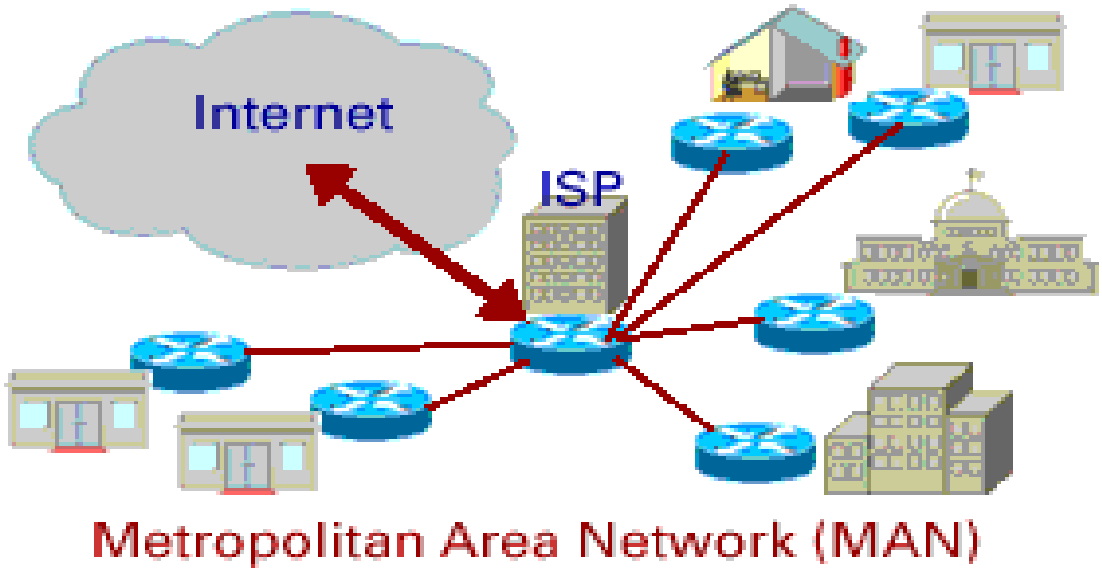
METROPOLITON AREA NETWORK

A metropolitan area network (MAN) is a computer network larger than a local area network covering an area of a few city blocks to the area of an entire city, possibly also including the surrounding areas.

MANs are extremely efficient and provide fast communication via high-speed carriers, such as fiber optic cables. A MAN is optimized for a larger geographical area than LAN ranging from

several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking local networks.

Figure1.6: Metropolitan Area Network (MAN)



HOME AREA NETWORK (HAN)

A Home Area Network is a type of local area network that develops from the need to facilitate communication and interoperability among digital devices present inside or within the close vicinity of a home. Devices capable of participating in this network–smart devices such as network printers and handheld mobile computers–often gain enhanced emergent capabilities through their ability to interact. These additional capabilities can then be used to increase the quality of life inside the home in a variety of ways, such as automation of repetitious tasks, increased personal productivity, enhanced home security, and easier access to entertainment.

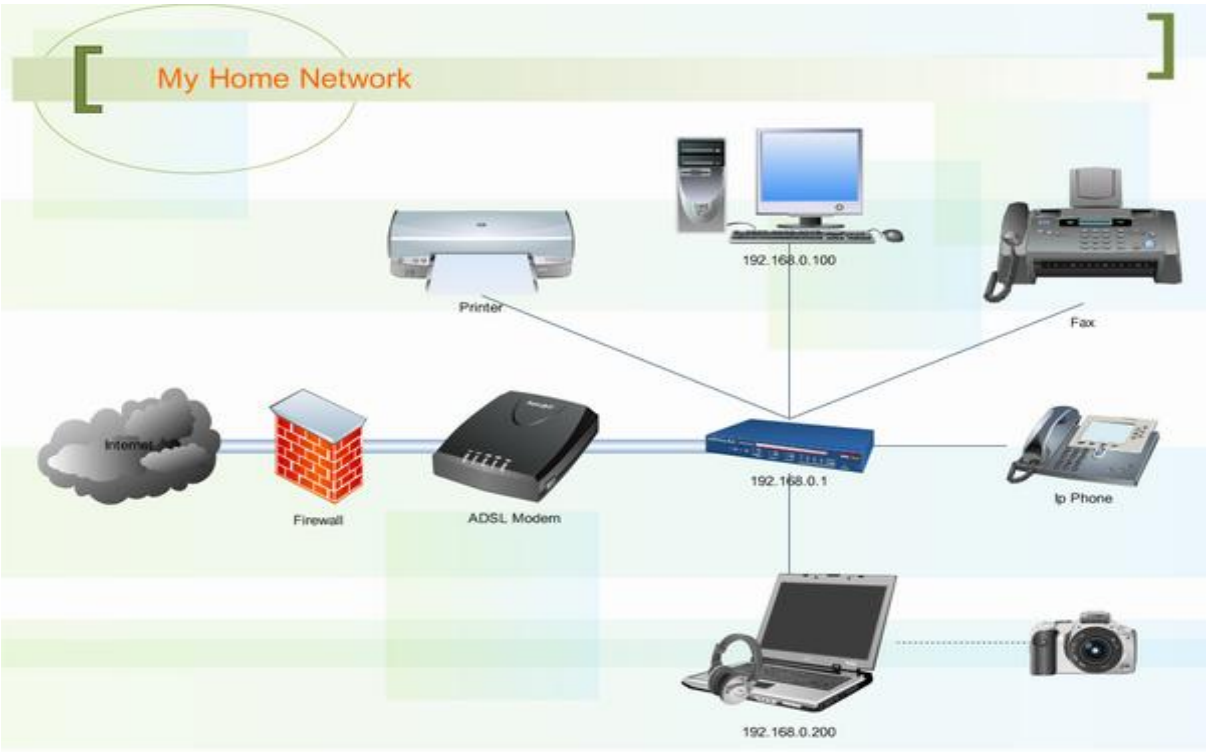


Figure1.7: Home Area Network (HAN)

GLOBAL AREA NETWORK

A global area network (GAN) refers to a network composed of different interconnected networks that cover an unlimited geographical area. The term is loosely synonymous with Internet, which is considered a global area network.

Unlike local area networks (LAN) and wide area networks (WAN), GANs cover a large geographical area.
Because a GAN is used to support mobile communication across a number of wireless LANs, the key challenge for any GAN is transferring user communications from one local coverage area to the next.

The most sought-after GAN type is a broadband GAN. The broadband GAN is a global satellite Internet network that uses portable terminals for telephony. The terminals connect laptop computers located in remote areas to broadband Internet.

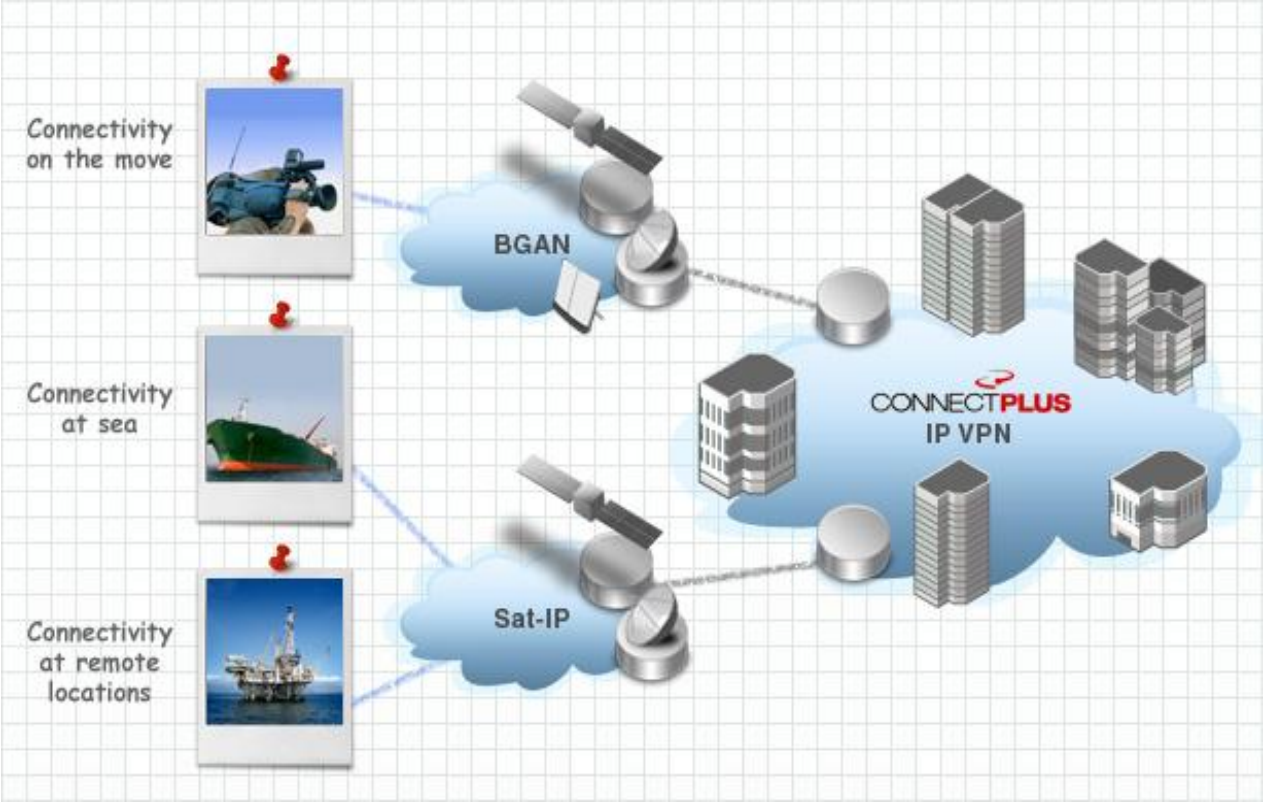


Figure1.8: Global Area Network (GAN)

1.3.7 WIRELESS LOCAL AREA NETWORK

A WLAN provides wireless network communication over short distances using radio or infrared signals instead of traditional network cabling.

A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter.

Network security remains an important issue for WLANs. Random wireless clients must usually be prohibited from joining the WLAN. Technologies like WAP raise the level of security on wireless networks to rival that of traditional wired networks.

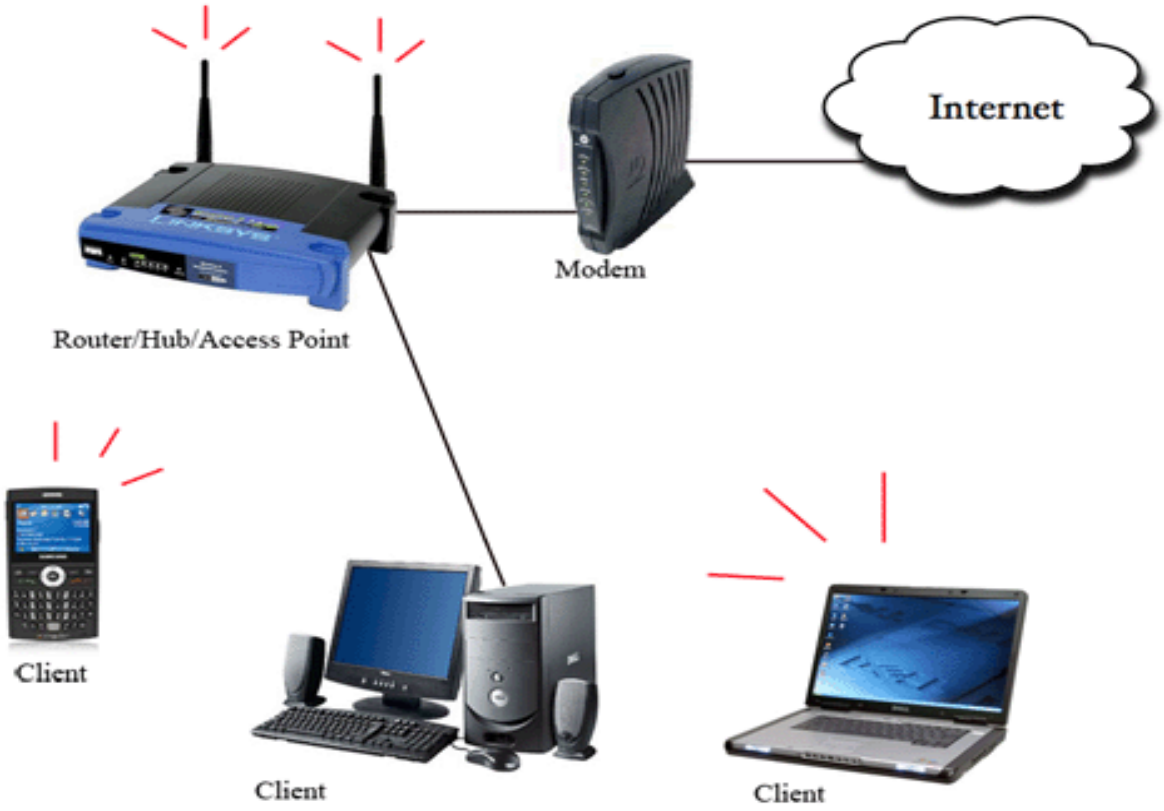


Figure1.9: Wireless Local Area Network (WLAN

CHAPTER 2: NETWORK LAYER AND IT'S FUNCTION

2.1 NETWORK MODEL

A computer network connects two or more devices together to share information and services. Multiple networks connected together form an internetwork.

Internetworking present challenges - interoperating between products from different manufacturers requires consistent standards. Network reference models were developed to address these challenges.

There are two basic types of networking models: protocol models and reference models.

Transmission Control Protocol (TCP) model:

A protocol model provides a model that closely matches the structure of a particular protocol suite. The hierarchical set of related protocols in a suite typically represents all the functionality required to interface the human network with the data network. The TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite.

The Open Systems Interconnection (OSI) model:

A reference model provides a common reference for maintaining consistency within all types of network protocols and services. A reference model is not intended to be an implementation specification or to provide a sufficient level of detail to define precisely the services of the network architecture. The primary purpose of a reference model is to aid in clearer understanding of the functions and process involved.

2.1.1 THE OPEN SYSTEMS INTERCONNECTION (OSI) MODEL:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

As a reference model, the OSI model provides an extensive list of functions and services that can occur at each layer. It also describes the interaction of each layer with the layers directly above and below it.

The Open Systems Interconnect (OSI) model has seven layers.

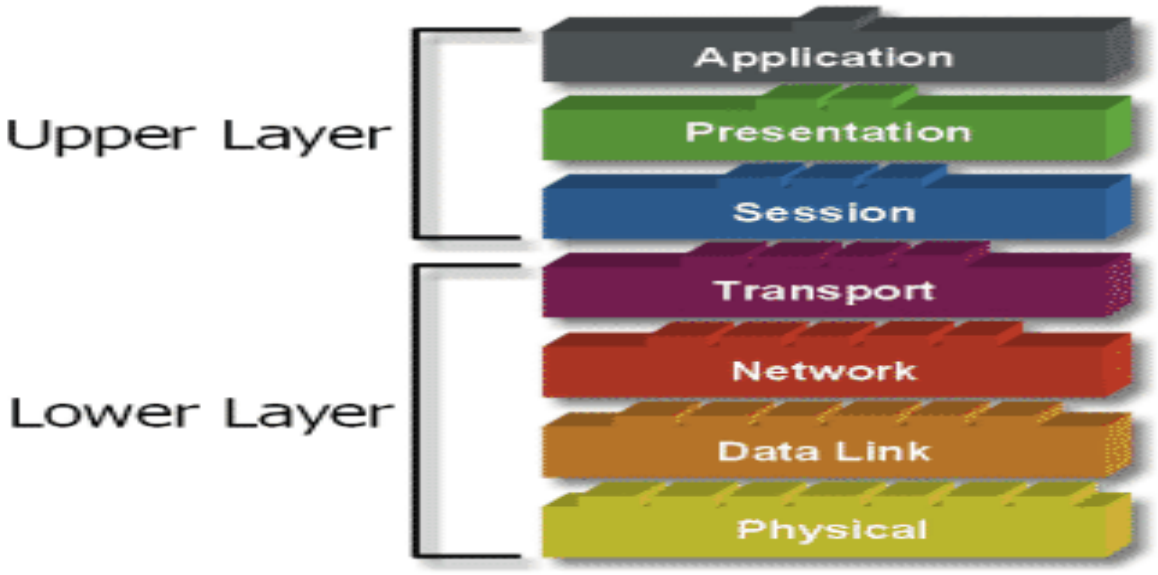


Figure2.1: The Open Systems Interconnect (OSI) model Layer

2.1.2 TRANSMISSION CONTROL PROTOCOL (TCP) MODEL:

In computer science and in Information and communications technology, the Internet protocol suite is the computer networking model and communications protocols used by the internet and similar computer networks. It is commonly known as TCP/IP, because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), were the first networking protocols defined in this standard.

TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.

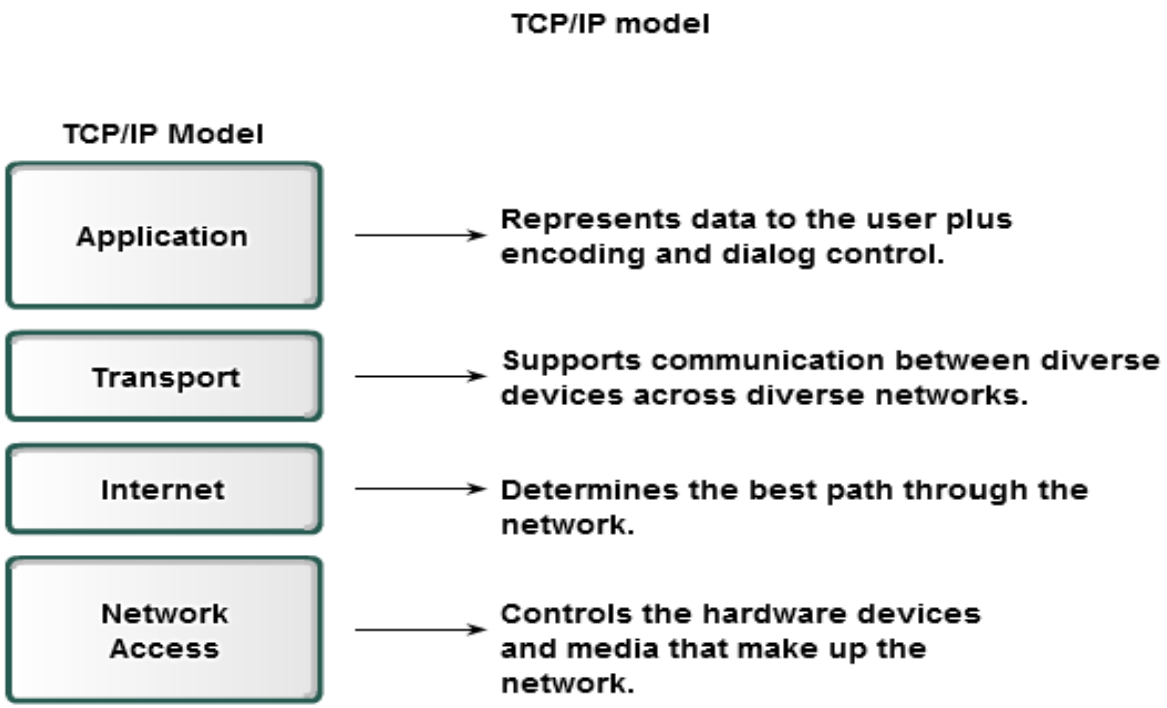


Figure2.2: Transmission Control Protocol (TCP) Layer

2.2 FUNCTION OF NETWORK LAYERS

2.2.1 Application Layer Functions

The Application layer, Layer seven, is the top layer of both the OSI and TCP/IP models. It is the layer that provides the interface between the applications we use to communicate and the underlying network over which our messages are transmitted.

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

2.2.2 Presentation Layer Function

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The Presentation layer has three primary functions:

Coding and conversion of Application layer data to ensure that data from the source device can be interpreted by the appropriate application on the destination device.

Compression of the data in a manner that can be decompressed by the destination device.

Encryption of the data for transmission and the decryption of data upon receipt by the destination.

2.2.3 Session Layer Function

The session layer allows session establishment between processes running on different stations.

As the name of the Session layer implies, functions at this layer create and maintain dialogs between source and destination applications. The Session layer handles the exchange of information to initiate dialogs, keep them active, and to restart sessions that are disrupted or idle for a long period of time.

It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

2.2.4 Transport Layer Function

The Transport layer provides for the segmentation of data and the control necessary to reassemble these pieces into the various communication streams.

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

Its primary responsibilities to accomplish this are:

Tracking the individual communication between applications on the source and destination hosts

Segmenting data and managing each piece

Reassembling the segments into streams of application data

Identifying the different applications

Tracking Individual Conversations

Any host may have multiple applications that are communicating across the network. Each of these applications will be communicating with one or more applications on remote hosts. It is the responsibility of the Transport layer to maintain the multiple communication streams between these applications.

Segmenting Data

As each application creates a stream data to be sent to a remote application, this data must be prepared to be sent across the media in manageable pieces. The Transport layer protocols describe services that segment this data from the Application layer. This includes the encapsulation required on each piece of data. Each piece of application data requires headers to be added at the Transport layer to indicate to which communication it is associated.

Reassembling Segments

At the receiving host, each piece of data may be directed to the appropriate application. Additionally, these individual pieces of data must also be reconstructed into a complete data stream that is useful to the Application layer. The protocols at the Transport layer describe the how the Transport layer header information is used to reassemble the data pieces into streams to be passed to the Application layer.

Identifying the Applications

In order to pass data streams to the proper applications, the Transport layer must identify the target application. To accomplish this, the Transport layer assigns an application an identifier. The TCP/IP protocols call this identifier a port number. Each software process that needs to access the network is assigned a port number unique in that host. This port number is used in the transport layer header to indicate to which application that piece of data is associated.

The Transport layer is the link between the Application layer and the lower layer that are responsible for network transmission. This layer accepts data from different conversations and passes it down to the lower layers as manageable pieces that can be eventually multiplexed over the media.

Applications do not need to know the operational details of the network in use. The applications generate data that is sent from one application to another, without regard to the destination host type, the type of media over which the data must travel, the path taken by the data, the congestion on a link, or the size of the network.

Additionally, the lower layers are not aware that there are multiple applications sending data on the network. Their responsibility is to deliver data to the appropriate device. The Transport layer then sorts these pieces before delivering them to the appropriate application.

Data Requirements Vary

Because different applications have different requirements, there are multiple Transport layer protocols. For some applications, segments must arrive in a very specific sequence in order to be processed successfully. In some cases, all of the data must be received for any of it to be of use. In other cases, an application can tolerate some loss of data during transmission over the network.

2.2.5 Network Layer Function

The Network layer, or OSI Layer 3, provides services to exchange the individual pieces of data over the network between identified end devices. To accomplish this end-to-end transport, Layer 3 uses four basic processes:

Addressing

Encapsulation

Routing

Decapsulation

Addressing

First, the Network layer must provide a mechanism for addressing these end devices. If individual pieces of data are to be directed to an end device, that device must have a unique address. In an IPv4 network, when this address is added to a device, the device is then referred to as a host.

Encapsulation

Second, the Network layer must provide encapsulation. Not only must the devices be identified with an address, the individual pieces - the Network layer PDUs - must also contain these addresses. During the encapsulation process, Layer 3 receives the Layer 4 PDU and adds a Layer 3 header, or label, to create the Layer 3 PDU. When referring to the Network layer, we call this PDU a packet. When a packet is created, the header must contain, among other information, the address of the host to which it is being sent. This address is referred to as the destination address. The Layer 3 header also contains the address of the originating host. This address is called the source address.

After the Network layer completes its encapsulation process, the packet is sent down to the Data Link layer to be prepared for transportation over the media.

Routing

Next, the Network layer must provide services to direct these packets to their destination host. The source and destination hosts are not always connected to the same network. In fact, the packet might have to travel through many different networks. Along the way, each packet must be guided through the network to reach its final destination. Intermediary devices that connect the networks are called routers. The role of the router is to select paths for and direct packets toward their destination. This process is known as routing.

During the routing through an internetwork, the packet may traverse many intermediary devices. Each route that a packet takes to reach the next device is called a hop. As the packet is forwarded, its contents (the Transport layer PDU), remain intact until the destination host is reached.

Decapsulation

Finally, the packet arrives at the destination host and is processed at Layer 3. The host examines the destination address to verify that the packet was addressed to this device. If the address is correct, the packet is decapsulated by the Network layer and the Layer 4 PDU contained in the packet is passed up to the appropriate service at Transport layer.

Unlike the Transport layer (OSI Layer 4), which manages the data transport between the processes running on each end host, Network layer protocols specify the packet structure and processing used to carry the data from one host to another host. Operating without regard to the application data carried in each packet allows the Network layer to carry packets for multiple types of communications between multiple hosts.

2.2.6 Data Link Layer Function

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node "has the right" to use the physical medium.

2.2.7 Physical Layer Function

The OSI Physical layer provides the means to transport across the network media the bits that make up a Data Link layer frame. This layer accepts a complete frame from the Data Link layer and encodes it as a series of signals that are transmitted onto the local media. The encoded bits that comprise a frame are received by either an end device or an intermediate device.

The delivery of frames across the local media requires the following Physical layer elements:

The physical media and associated connectors

A representation of bits on the media

Encoding of data and control information

Transmitter and receiver circuitry on the network devices

At this stage of the communication process, the user data has been segmented by the Transport layer, placed into packets by the Network layer, and further encapsulated as frames by the Data Link layer. The purpose of the Physical layer is to create the electrical, optical, or microwave signal that represents the bits in each frame. These signals are then sent on the media one at a time.

It is also the job of the Physical layer to retrieve these individual signals from the media, restore them to their bit representations, and pass the bits up to the Data Link layer as a complete frame.

The media does not carry the frame as a single entity. The media carries signals, one at a time, to represent the bits that make up the frame.

There are three basic forms of network media on which data is represented:

Copper cable

Fiber

Wireless

The representation of the bits - that is, the type of signal - depends on the type of media. For copper cable media, the signals are patterns of electrical pulses. For fiber, the signals are patterns of light. For wireless media, the signals are patterns of radio transmissions.

CHAPTER 3: NETWORK PROTOCOLS

3.1WHAT IS A NETWORK PROTOCOLS

At the human level, some communication rules are formal and others are simply understood, or implicit, based on custom and practice. For devices to successfully communicate, a network protocol suite must describe precise requirements and interactions.

Networking protocols suites describe processes such as:

The format or structure of the message

The process by which networking devices share information about pathways with other networks

How and when error and system messages are passed between devices

The setup and termination of data transfer sessions

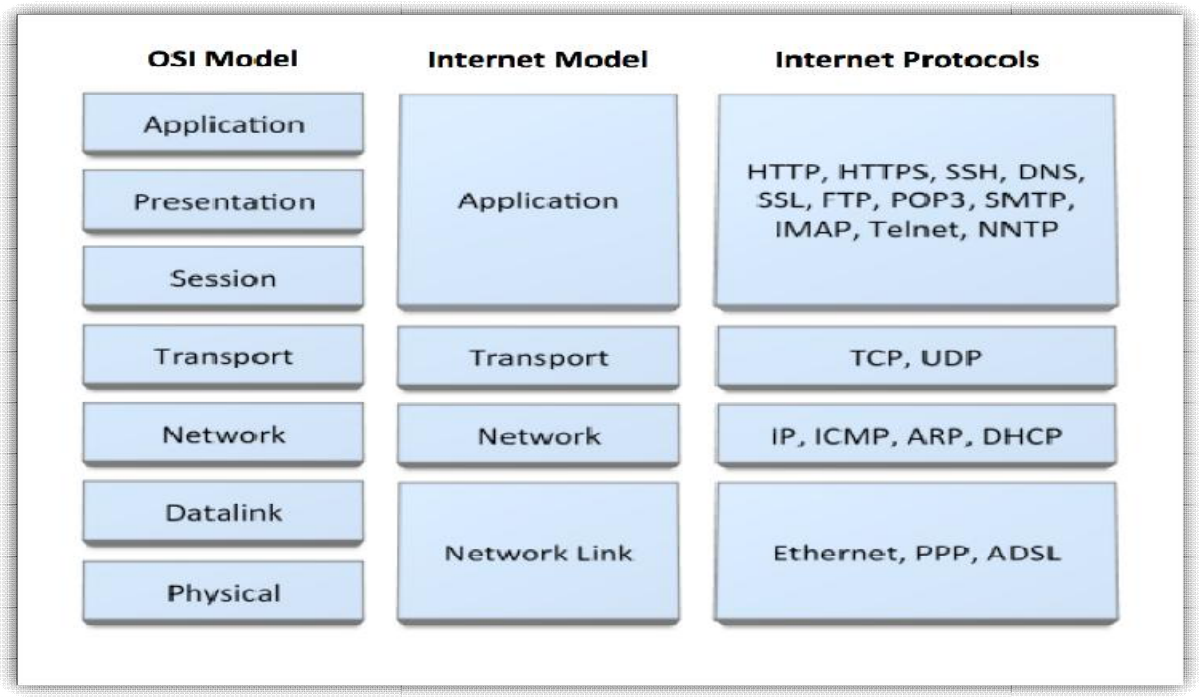


Figure3.1: Protocols of different layers

APPLICATION LAYER PROTOCOLS

Email Protocols: Simple Mail Transfer Protocols (SMTP), Post Office Protocol (POP)

File Transfer: File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Secure File Transfer Protocol (SFTP), Secure Shell (SSH),

Terminal Services: TELNET, Remote Desktop

Formatting: Hypertext Transfer Protocol(HTTP)

Translating: Domain Name System (DNS)

SMTP/POP

SMTP stands for Simple Mail Transfer Protocol. SMTP is used when email is delivered from an email client, such as Outlook Express, to an email server or when email is delivered from one email server to another. SMTP uses port 25.

POP3 stands for Post Office Protocol. POP3 allows an email client to download an email from an email server. The POP3 protocol is simple and does not offer many features except for download. Its design assumes that the email client downloads all available email from the server, deletes them from the server and then disconnects. POP3 normally uses port 110.

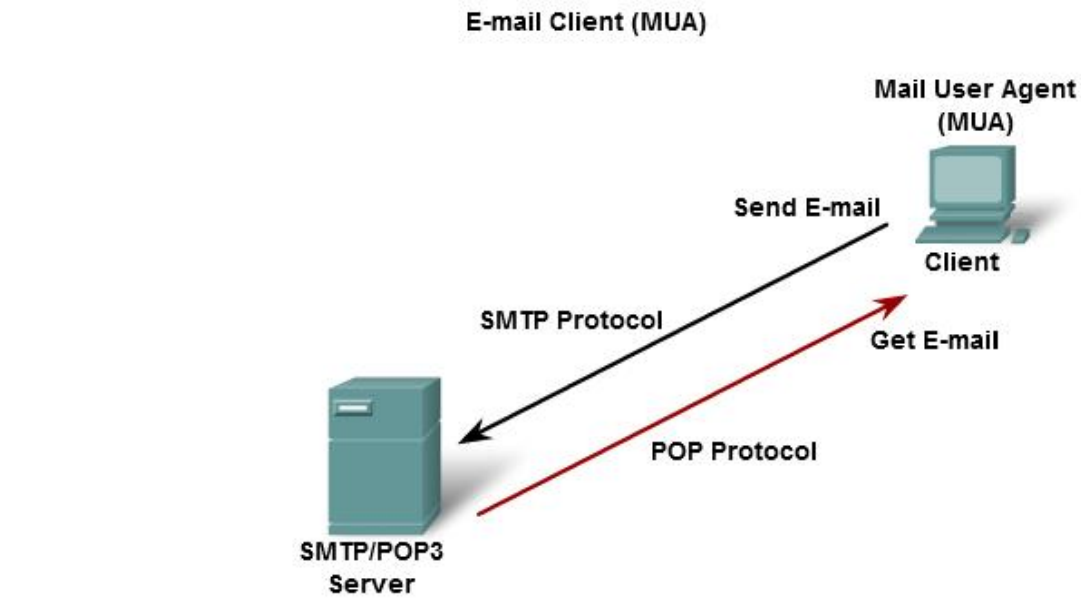


Figure3.2: SMTP/POP

FTP

The File Transfer Protocol (FTP) is another commonly used Application layer protocol. FTP was developed to allow for file transfers between a client and a server. An FTP client is an application that runs on a computer that is used to push and pull files from a server running the FTP daemon (FTPd).

To successfully transfer files, FTP requires two connections between the client and the server: one for commands and replies, the other for the actual file transfer.

The client establishes the first connection to the server on TCP port 21. This connection is used for control traffic, consisting of client commands and server replies.

The client establishes the second connection to the server over TCP port 20. This connection is for the actual file transfer and is created every time there is a file transferred.

The file transfer can happen in either direction. The client can download (pull) a file from the server or, the client can upload (push) a file to the server.

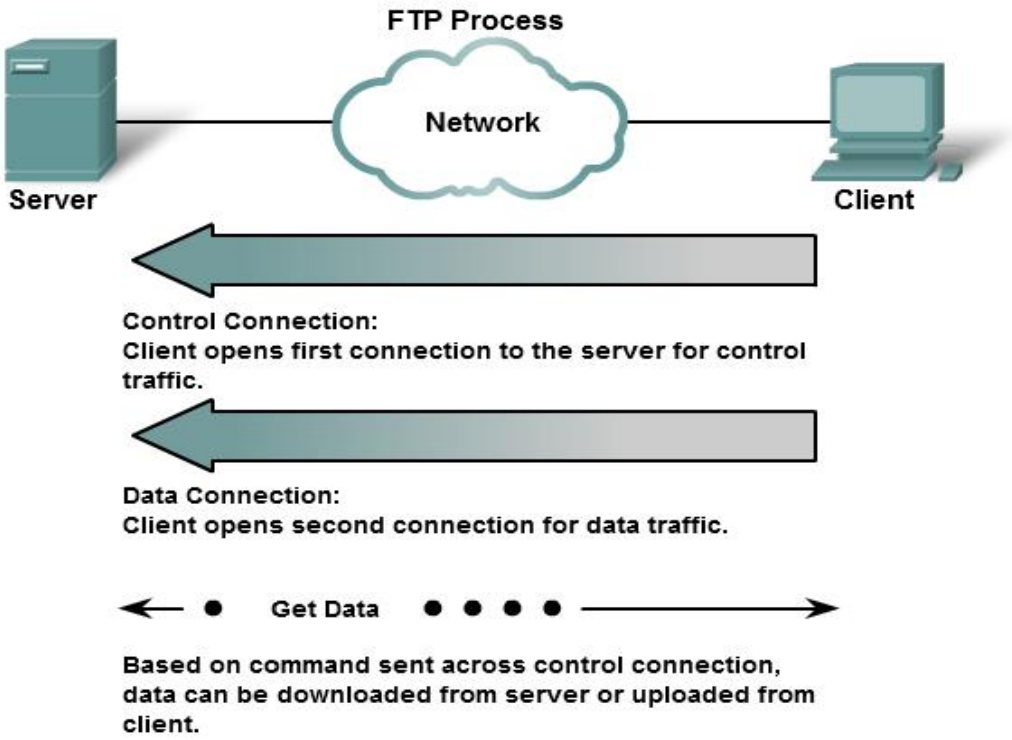


Figure3.3: FTP

TELNET

Telnet is a network protocol used on the internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Telnet provides a standard method of emulating text-based terminal devices over the data network. Both the protocol itself and the client software that implements the protocol are commonly referred to as Telnet. Appropriately enough, a connection using Telnet is called a Virtual Terminal (VTY) session, or connection. Rather than using a physical device to connect to the server, Telnet uses software to create a virtual device that provides the same features of a terminal session with access to the server command line interface (CLI).

To support Telnet client connections, the server runs a service called the Telnet daemon. A virtual terminal connection is established from an end device using a Telnet client application. Most operating systems include an Application layer Telnet client. On a Microsoft Windows PC, Telnet can be run from the command prompt. Other common terminal applications that run as Telnet clients are HyperTerminal, Minicom, and TeraTerm.

Once a Telnet connection is established, users can perform any authorized function on the server, just as if they were using a command line session on the server itself. If authorized, they can start and stop processes, configure the device, and even shut down the system.

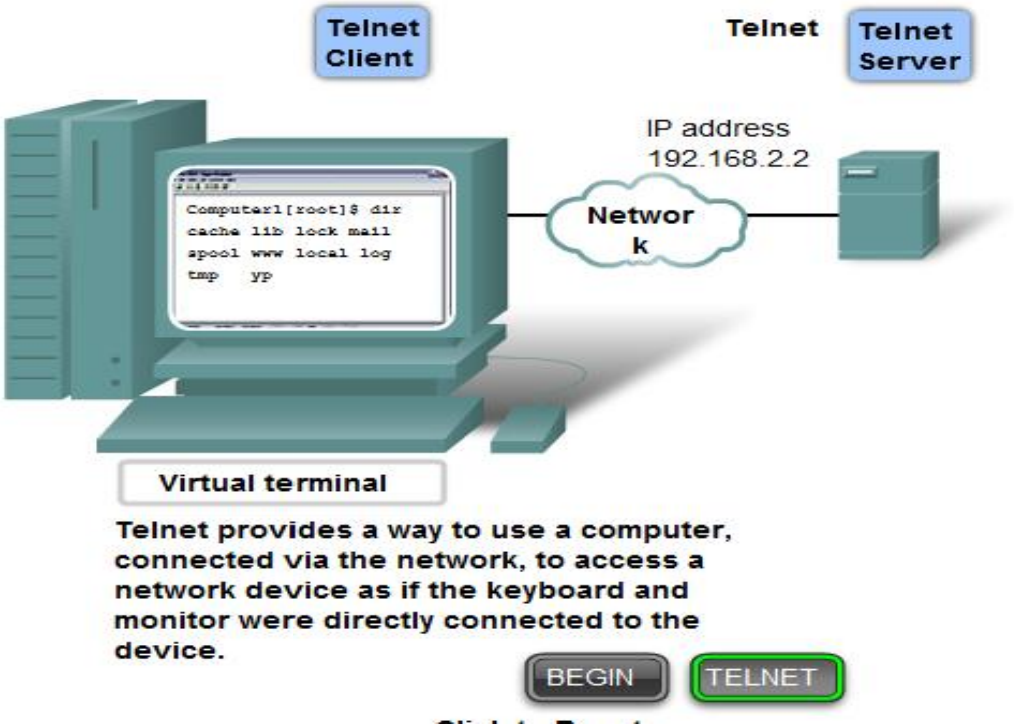


Figure3.4: TELNET

HOW TELNET WORKS

Telnet uses software, installed on your computer, to create a connection with the remote host. The Telnet client (software), at your command, will send a request to the Telnet server (remote host). The server will reply asking for a user name and password. If accepted, the Telnet client will establish a connection to the host, thus making your computer a virtual terminal and allowing you complete access to the host's computer.

Telnet requires the use of a user name and password, which means you need to have previously set up an account on the remote computer. In some cases, however, computers with Telnet will allow guests to log on with restricted access.

TELNET CONNECTION

The telnet commands allow you to communicate with a remote computer that is using the Telnet protocol. You can run telnet without parameters in order to enter the telnet context, indicated by the Telnet prompt (telnet>). From the Telnet prompt, use the following commands to manage a computer running Telnet Client.

The telnet admin commands allow you to remotely manage a computer running Telnet Server. These commands are run from the command prompt.

A telnet connection is a network connection established with a remote computer using the telnet command.

For example, if a command line like below is used,

Telnet [// dibas chakma 23]

Then telnet will inform the user that a connection is being established, like that:

Trying 192.168.2.2

Connected to dibas chakma

Login:

Password:

To establish the connection telnet will usually ask the user to type a login name and a password like in the example above. Here, Login prompts for the user name, which is a name given by the system administrator, Password prompts for the password, which is a confidential name known only by the user.

Here 23 is the default telnet port.

HTTP

Short for Hypertext Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed. HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input.

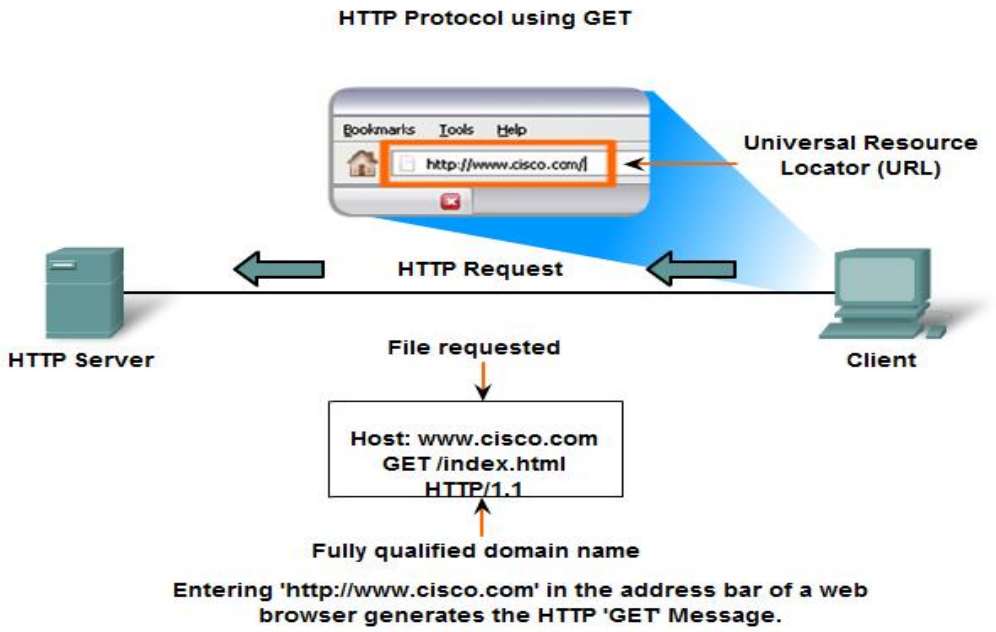


Figure3.5: HTTP

DNS

In data networks, devices are labeled with numeric IP addresses, so that they can participate in sending and receiving messages over the network. However, most people have a hard time remembering this numeric address. Hence, domain names were created to convert the numeric address into a simple, recognizable name.

On the Internet these domain names, such as www.cisco.com, are much easier for people to remember than 198.132.219.25, which is the actual numeric address for this server. Also, if Cisco decides to change the numeric address, it is transparent to the user, since the domain name

will remain www.cisco.com. The new address will simply be linked to the existing domain name and connectivity is maintained. When networks were small, it was a simple task to maintain the mapping between domain names and the addresses they represented. However, as networks began to grow and the number of devices increased, this manual system became unworkable.

The Domain Name System (DNS) was created for domain name to address resolution for these networks. DNS uses a distributed set of servers to resolve the names associated with these numbered addresses.

The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data formats. DNS protocol communications use a single format called a message. This message format is used for all types of client queries and server responses, error messages, and the transfer of resource record information between servers.

TRANSPORT LAYER PROTOCOLS

Transmission Control Protocol (TCP): A connection-oriented reliable protocol for packet delivery from an application to another.

User Datagram Protocol (UDP): Connectionless unreliable packet delivery.

TRANSMISSION CONTROL PROTOCOL (TCP)

TCP is a connection-oriented protocol.TCP incurs additional overhead to gain functions. Additional functions specified by TCP are the same order delivery, reliable delivery, and flow control. Each TCP segment has 20 bytes of overhead in the header encapsulating the Application layer data, whereas each UDP segment only has 8 bytes of overhead.

When two applications want to communicate to each other reliably, they establish a connection and send data back and forth over that connection. This is analogous to making a telephone call. You should send data back and forth over the connection by speaking to one another over the phone lines. Like the phone company, TCP guarantees that data sent from one end of the connection actually gets to the other end and in the same order it was sent. Otherwise, an error is reported.

Applications that use TCP are:

Web Browsers

E-mail

File Transfers

USER DATAGRAM PROTOCOL (UDP)

UDP is a simple, connectionless protocol, described in RFC 768. It has the advantage of providing for low overhead data delivery. The pieces of communication in UDP are called datagram's. These datagram's are sent as "best effort" by this Transport layer protocol.

Applications that use UDP include:

Domain Name System (DNS)

Video Streaming

Voice over IP (VoIP)

NETWORK LAYER PROTOCOLS

The Internet Protocol (IPv4 and IPv6)

Address Resolution Protocol (ARP)

WHAT IS IP?

Any device that wants to communicate with other devices via the Internet must have a unique and appropriate IP address. IP addresses are used to identify the sending and receiving devices. There are currently two IP versions: IP version 4 (IPv4) and IP version 6 (IPv6). The main difference between the two is that the length of an IPv6 address is longer (128 bits compared with 32 bits for an IPv4 address). IPv4 addresses are most commonly used today.

IPV4 ADDRESSES

For Internet Protocol version 4 (IPv4), each TCP/IP host is identified by a logical IP address. The IP address is a Network layer address and has no dependence on the Data-Link layer address (such as a MAC address of a network adapter). A unique IP address is required for each host and network component that communicates using TCP/IP. This address can be assigned manually or by using Dynamic Host Configuration Protocol (DHCP).

Each IP address includes a network ID and a host ID.

The network ID (also known as a network address) identifies the systems that are located on the same physical network bounded by IP routers. All systems on the same physical network must have the same network ID. The network ID must be unique to the network.

The host ID (also known as a host address) identifies a workstation, server, router, or other TCP/IP host within a network. The host address must be unique to the network ID.

IPV4 Address Syntax

An IP address consists of 32 bits .Instead of expressing IPV4 addresses 32 bits at a time using binary notation, it is standard practice to segment the 32 bits of an IPV4 address into four 8-bit fields called octets. Each octet is converted to a decimal number (base 10) from 0-255 and separated by a period (a dot). This format is called dotted decimal notation. The following table provides an example of an IP address in binary and dotted decimal formats.

Binary Format	Dotted Decimal Notation
11000000 10101000 00000011 00011000	192.168.3.24

For example, the IPv4 address of 11000000101010000000001100011000 is:

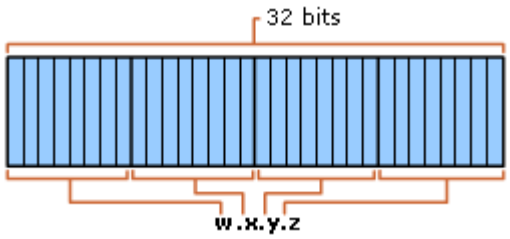
Segmented into 8-bit blocks: 11000000 10101000 00000011 00011000

Each block is converted to decimal: 192 168 3 24

The adjacent octets are separated by a period: 192.168.3.24

The notation *w.x.y.z* is used when referring to a generalized IP address, and is shown the following figure.

IP Address



Types of IPV4 Addresses

The Internet standards define the following types of IPv4 addresses:

Unicast. Assigned to a single network interface located on a specific subnet on the network and used for one-to-one communications.

Multicast. Assigned to one or more network interfaces located on various subnets on the network and used for one-to-many communications.

Broadcast. Assigned to all network interfaces located on a subnet on the network and used for one-to-everyone-on-a-subnet communications.

IPV6 ADDRESSES

The IPv6 128-bit address is divided along 16-bit boundaries. Each 16-bit block is then converted to a 4-digit hexadecimal number, separated by colons. The resulting representation is called colon-hexadecimal. This is in contrast to the 32-bit IPv4 address represented in dotted-decimal format, divided along 8-bit boundaries, and then converted to its decimal equivalent, separated by periods.

The following is a sample IPv6 address in binary form:

00100001110110100000000011010011000000000000000000010111100111011

00000010101010100000000011111111111111100010100010011100010110 10

The 128-bit address is divided along 16-bit boundaries:

0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

Each 16-bit block is converted to hexadecimal and delimited with colons. The result is:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

IPv6 representation can be further simplified by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit. With leading zero suppression, the address representation becomes:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

Types of IPV6 Addresses

IPv6 addresses are broadly classified into three categories:

1) Unicast addresses A Unicast address acts as an identifier for a single interface. An IPv6 packet sent to a Unicast address is delivered to the interface identified by that address.

2) Multicast addresses A Multicast address acts as an identifier for a group/set of interfaces that may belong to the different nodes. An IPv6 packet delivered to a Multicast address is delivered to the multiple interfaces.

3) Anycast addresses Anycast addresses act as identifiers for a set of interfaces that may belong to the different nodes. An IPv6 packet destined for an Anycast address is delivered to one of the interfaces identified by the address.

PING

Ping is the name of a standard software utility (tool) used to test network connections. It can be used to determine if a remote device (such as Web or game server) can be reached across the network and, if so, the connection's latency. Ping tools are part of Windows, Mac OS X and Linux as well as some routers and game consoles.

Most ping tools use Internet Control Message Protocol (ICMP). They send request messages to a target network address at periodic intervals and measure the time it takes for a response message to arrive. These tools typically support options like

How many times to send requests .

How large of a request message to send .

How long to wait for each reply .

The output of ping varies depending on the tool. Standard results includes .

IP address of the responding computer .

Length of time (in milliseconds) between sending the request and receiving the response .

An indication of how many network hops between the requesting and responding computers .

Error messages if the target computer did not respond .

CHAPTER 4: NETWORK TOPOLOGY AND CATEGORIES OF NETWORK

4.1 NETWORK TOPOLOGY

The topology of a network is the arrangement or relationship of the network devices and the interconnections between them. Network topologies can be viewed at the physical level and the logical level.

Physical Topology

The physical topology is an arrangement of the nodes and the physical connections between them. The representation of how the media is used to interconnect the devices is the physical topology.

Logical Topology

A logical topology is the way a network transfers frames from one node to the next. This arrangement consists of virtual connections between the nodes of a network independent of their physical layout. These logical signal paths are defined by Data Link layer protocols. The Data Link layer "sees" the logical topology of a network when controlling data access to the media. It is the logical topology that influences the type of network framing and media access control used.

4.1.1 POINT TO POINT TOPOLOGY

A point-to-point topology connects two nodes directly together, as shown in the figure. In data networks with point-to-point topologies, the media access control protocol can be very simple. All frames on the media can only travel to or from the two nodes. The frames are placed on the media by the node at one end and taken off the media by the node at the other end of the point-to-point circuit.

In point-to-point networks, if data can only flow in one direction at a time, it is operating as a half-duplex link. If data can successfully flow across the link from each node simultaneously, it is a full-duplex link.

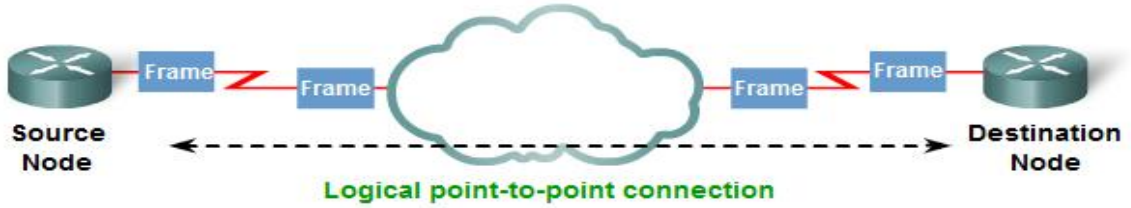


Figure 4.1: Point to Point Topology

4.1.2 MULTI ACCESS TOPOLOGY

A logical multi-access topology enables a number of nodes to communicate by using the same shared media. Data from only one node can be placed on the medium at any one time. Every node sees all the frames that are on the medium, but only the node to which the frame is addressed processes the contents of the frame.

Having many nodes share access to the medium requires a Data Link media access control method to regulate the transmission of data and thereby reduce collisions between different signals. The media access control methods used by logical multi-access topologies are typically CSMA/CD or CSMA/CA. However, token passing methods can also be used.

A number of media access control techniques are available for this type of logical topology. The Data Link layer protocol specifies the media access control method that will provide the appropriate balance between frame control, frame protection, and network overhead.

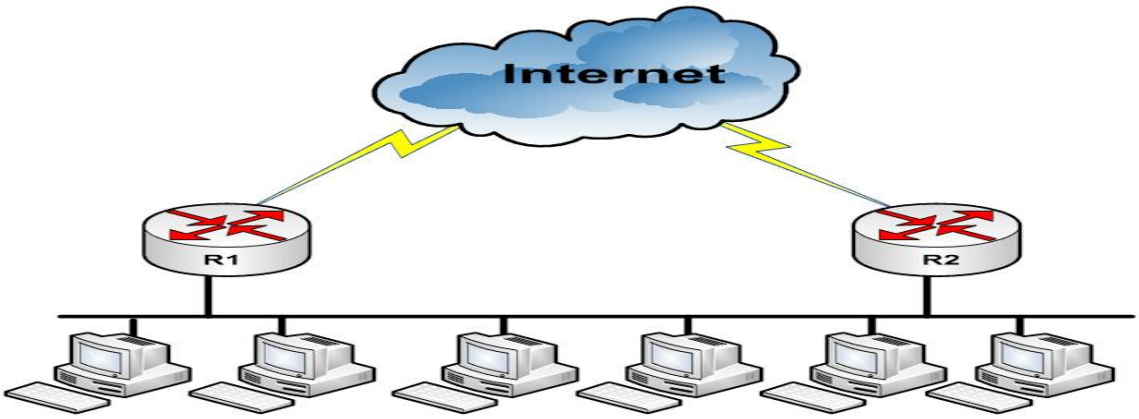


Figure 4.2: Multi Access Topology

4.1.3 RING TOPOLOGY

In a logical ring topology, each node in turn receives a frame. If the frame is not addressed to the node, the node passes the frame to the next node. This allows a ring to use a controlled media access control technique called token passing.

Nodes in a logical ring topology remove the frame from the ring, examine the address, and send it on if it is not addressed for that node. In a ring, all nodes around the ring- between the source and destination node examine the frame.

There are multiple media access control techniques that could be used with a logical ring, depending on the level of control required. For example, only one frame at a time is usually carried by the media. If there is no data being transmitted, a signal (known as a token) may be placed on the media and a node can only place a data frame on the media when it has the token.

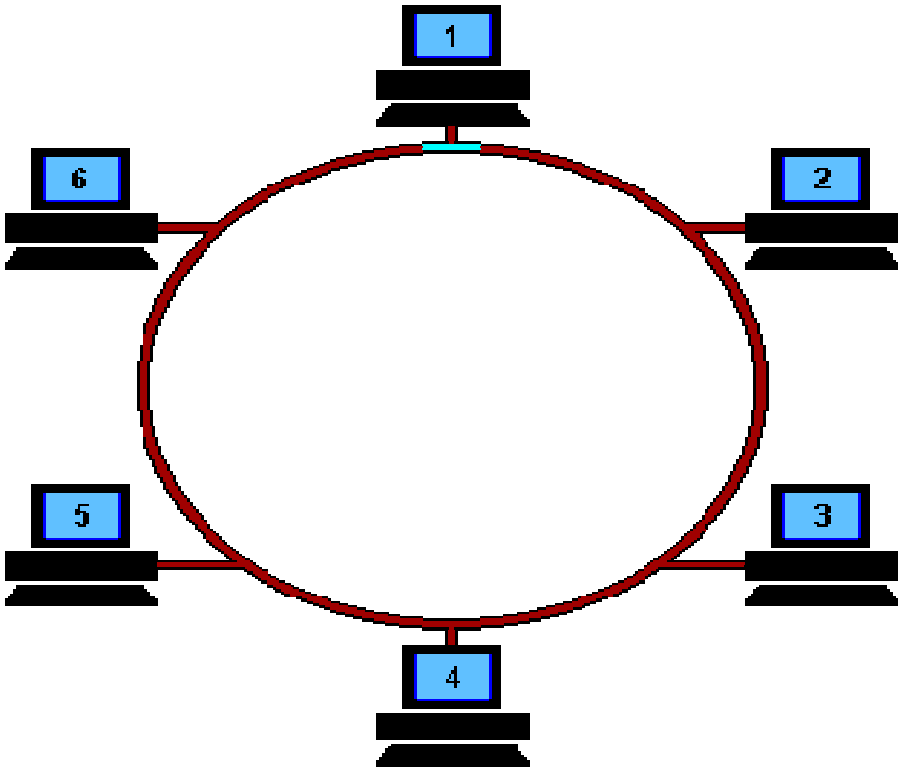


Figure 4.3: Ring Topology

4.2 CATEGORIES OF NETWORK

Network can be divided into two categories:

Peer-to-Peer Network

Server-based Network

4.2.1 PEER-TO-PEER NETWORK

In a peer-to-peer network, two or more computers are connected via a network and can share resources (such as printers and files) without having a dedicated server. Every connected end device (known as a peer) can function as either a server or a client. One computer might assume the role of server for one transaction while simultaneously serving as a client for another. The roles of client and server are set on a per request basis.

A simple home network with two connected computers sharing a printer is an example of a peer-to-peer network. Each person can set his or her computer to share files, enable networked games, or share an Internet connection.

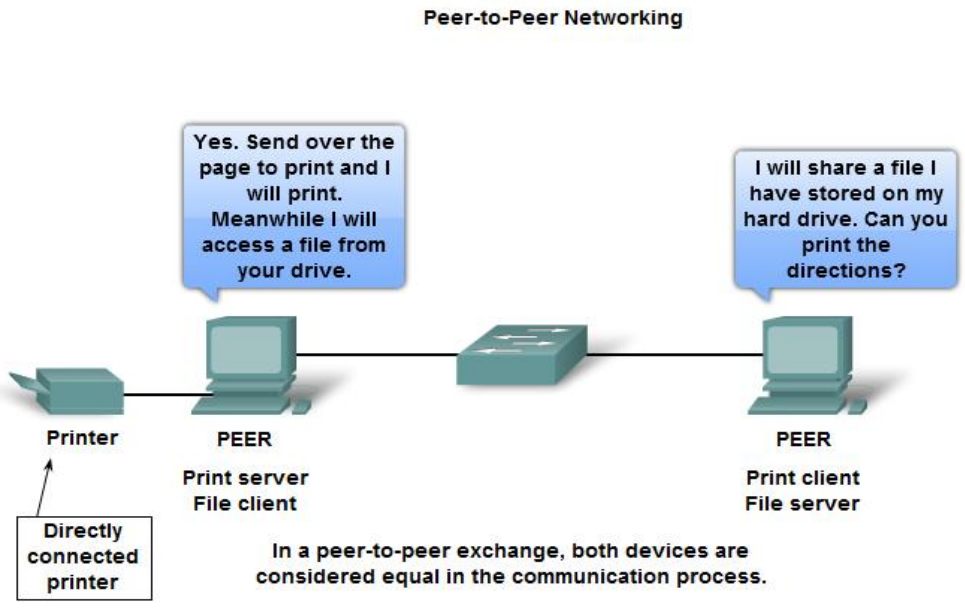


Figure 4.4: Peer-to-Peer Network

Peer-to-Peer Applications

A peer-to-peer application (P2P), unlike a peer-to-peer network, allows a device to act as both a client and a server within the same communication. In this model, every client is a server and every server a client. Both can initiate a communication and are considered equal in the communication process. However, peer-to-peer applications require that each end device provide a user interface and run a background service.

4.2.2 SERVER-BASED NETWORK

In a server-based network, the server is the central location where users share and access network resources. This dedicated computer controls the level of access that users have to shared resources. Shared data is in one location, making it easy to back up critical business information. Each computer that connects to the network is called a client computer. In a server-based network, users have one user account and password to log on to the server and to access shared resources. Server operating systems are designed to handle the load when multiple client computers access server-based resources.

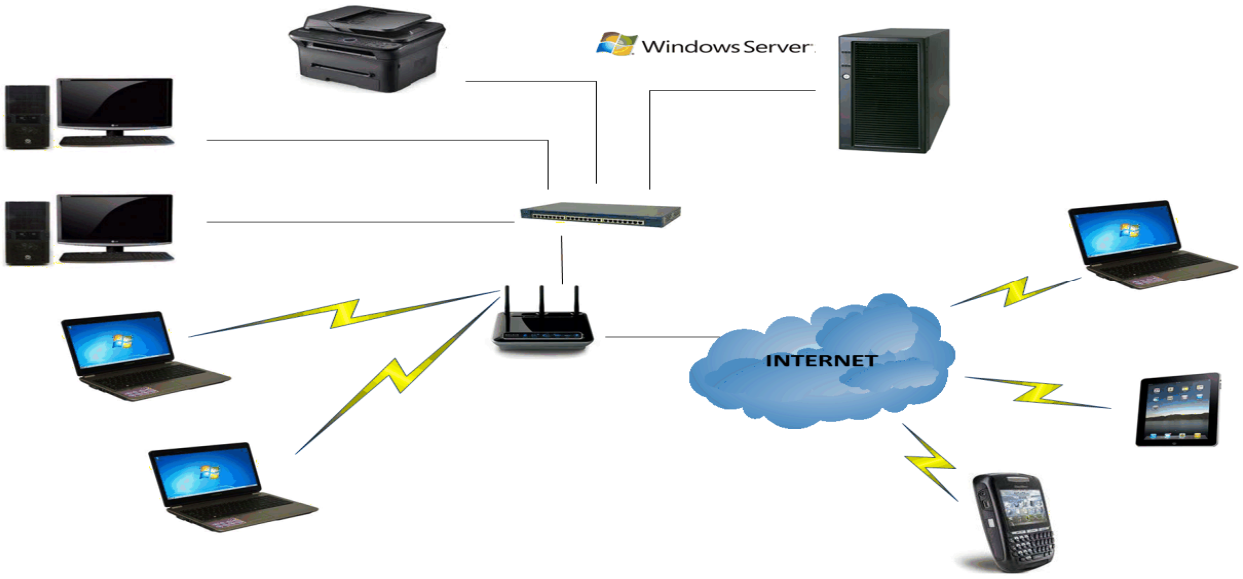


Figure 4.5: Server-Based Network

4.3 ETHERNET CABLE

An Ethernet cable is one of the most popular forms of network cable used on wired networks. Ethernet cables connect devices on local area networks such as PCs.

A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal.

A crossover cable directly connects two network devices of the same type to each other over Ethernet. Ethernet crossover cables are commonly used when temporarily networking two devices in situations where a network router, switch or hub is not present.

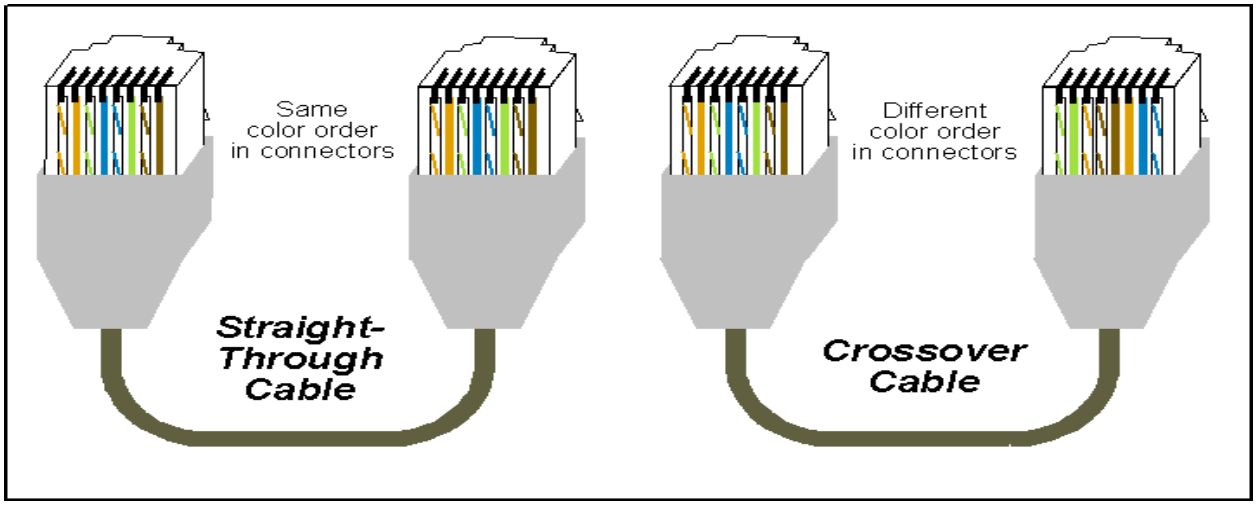


Figure 4.6: Ethernet Cable

4.4 ROUTER

A router is a networking device, commonly specialized hardware, that forwards data packet between computer networks. This creates an overlay internetwork, as 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.

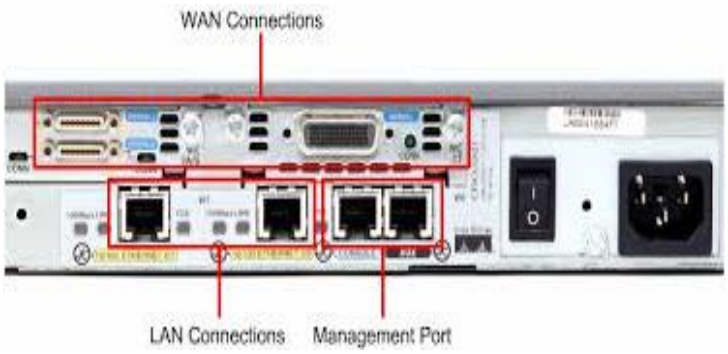


Figure 4.7: Router

4.5 SWITCH

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 maximize 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.

Figure 4.8: switch

4.6 FIREWALLS

Firewalls are computer network devices that protect a network from other less trusted networks. They are essentially network access control devices that permit and deny different types of traffic to travel into and out of an organization's network. Most often, firewalls are placed at the network boundary to protect an organization from the great, unwashed masses on the Internet.

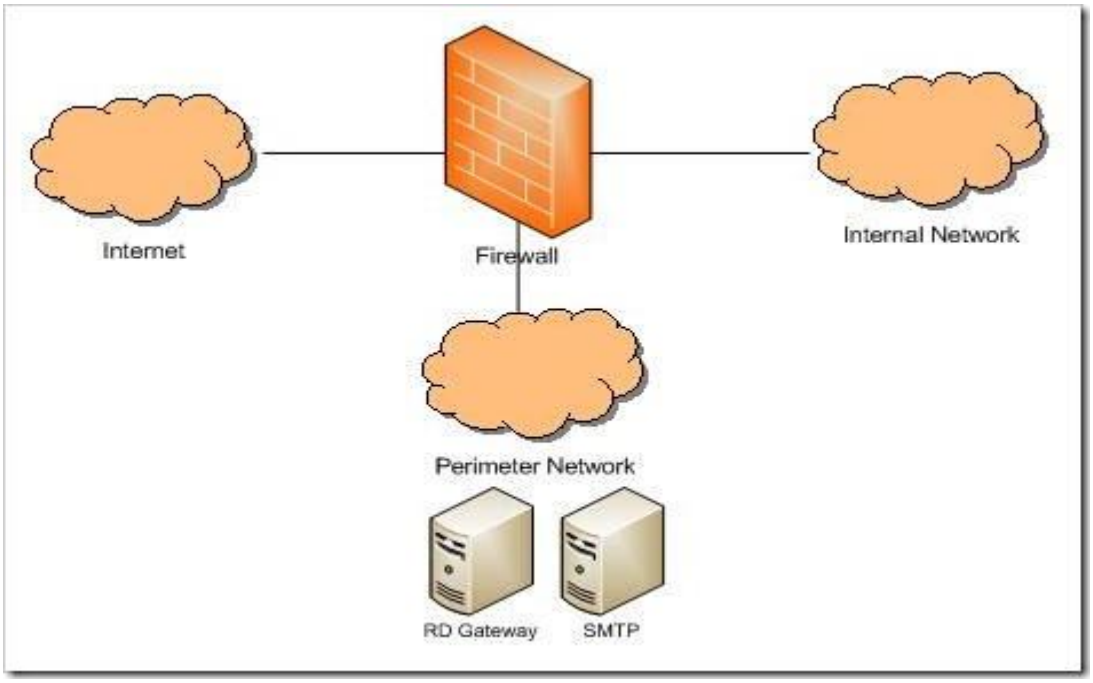


Figure 4.9: Firewalls

4.7 INTERNET CONNECTION

In order to connect a LAN to the Internet, a network connection via an Internet service provider (ISP) must be established. When connecting to the Internet, terms such as upstream and downstream are used. Upstream describes the transfer rate with which data can be uploaded from the device to the Internet; for instance, when video is sent from a network camera. Downstream is the transfer speed for downloading files; for instance, when video is received by a monitoring PC.

CHAPTER 5: NETWORK FILE/FOLDER SHARING, MAPPING CONCEPT AND IMPLEMENTATION

5.1 .WHAT IS FILE/FOLDER SHARING

File sharing is the practice of distributing or providing access to digital media, such as computer programs, multimedia (audio, images and video), documents or electronic books. Sharing a file or folder allows to access data on that drive from other computers on the same network.

5.2. DRIVE MAPPING

Drive mapping is how operating systems, such as Microsoft Windows associate a local drive letter (A through Z) with a shared storage area to another computer over a network.

After a drive has been mapped, a software application on a client's computer can read and write files from the shared storage area by accessing that drive, just as if that drive represented a local physical hard disk drive.

Mapping (sometimes called "mounting") a drive means you assign a drive letter on your computer to the server path. You can then connect to the server without having to remember and type the path every time

5.3. STEPS

SHARING FILE/FOLDER

The first step is to create a folder/file that would be shared. Then complete the below step's.

WHAT IS SHARING WITH EVERYBODY, NOBODY, SPECIFIC PEOPLE

Nobody. This option makes an item private so only you have access.

Specific people. This option opens the File Sharing wizard, so you can choose particular people to share with.

Everybody: This option opens the file sharing wizard, so everyone can have the access permission.

THE PURPOSE OF PERMISSION

In Windows, who gets to see a file can be set, but what recipients can do with it. These are called sharing permissions. There are two options:

Read. The "look, don't touch" option. Recipients can open, but not modify or delete a file.

Read/Write. The "does anything" option. Recipients can open, modify, or delete a file.

5.4 IMPLEMENTATION

Folder Sharing:

At first I have to create a local area network .Because networking connection is required for file and folder sharing and mapping. So I need some network elements such as

Computers with LAN Card.

Ethernet cables.

Hub or Switch.

Straight Ethernet cable is necessary for switch to pc connection.

At first I have to on the switch, then connect the pc and switch by the straight Ethernet cable.

Both the computers have the same operating system. After connecting both the pc with the switch a LAN connection is created.

Now click the START button and again click the CONTROL PANEL, go to NETWORK AND INTERNET

Then I set the ip addresses in both pcs as below.

Here I have use ipv4 addresses in both pcs with the subnet mask.

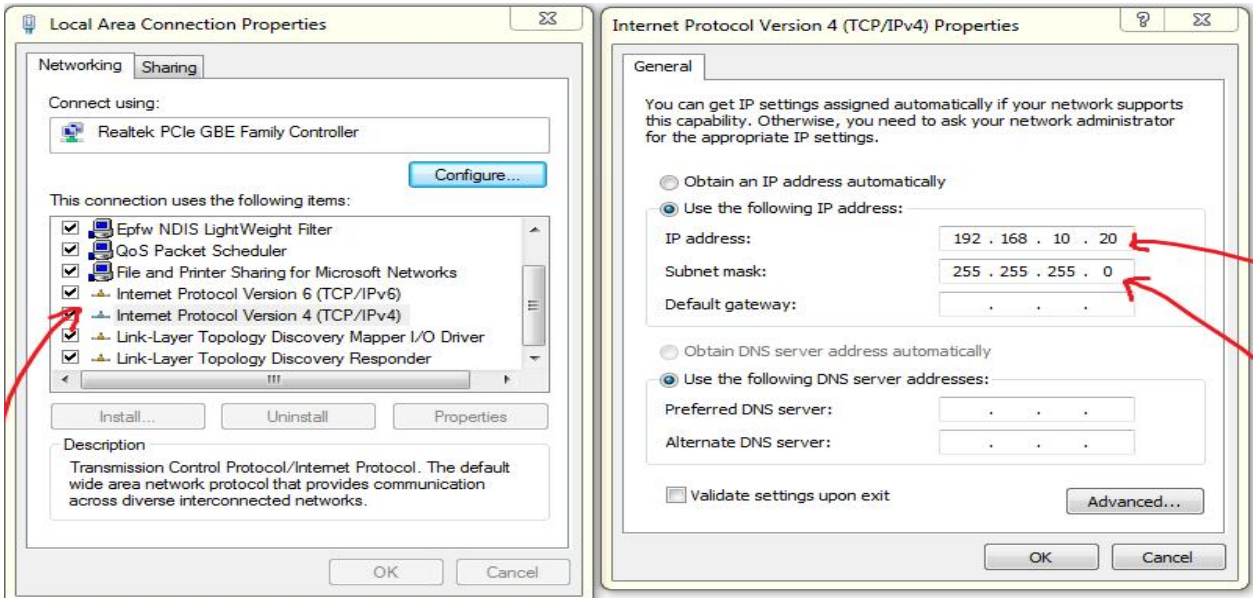


Figure5.1: PC 1 IP Setting

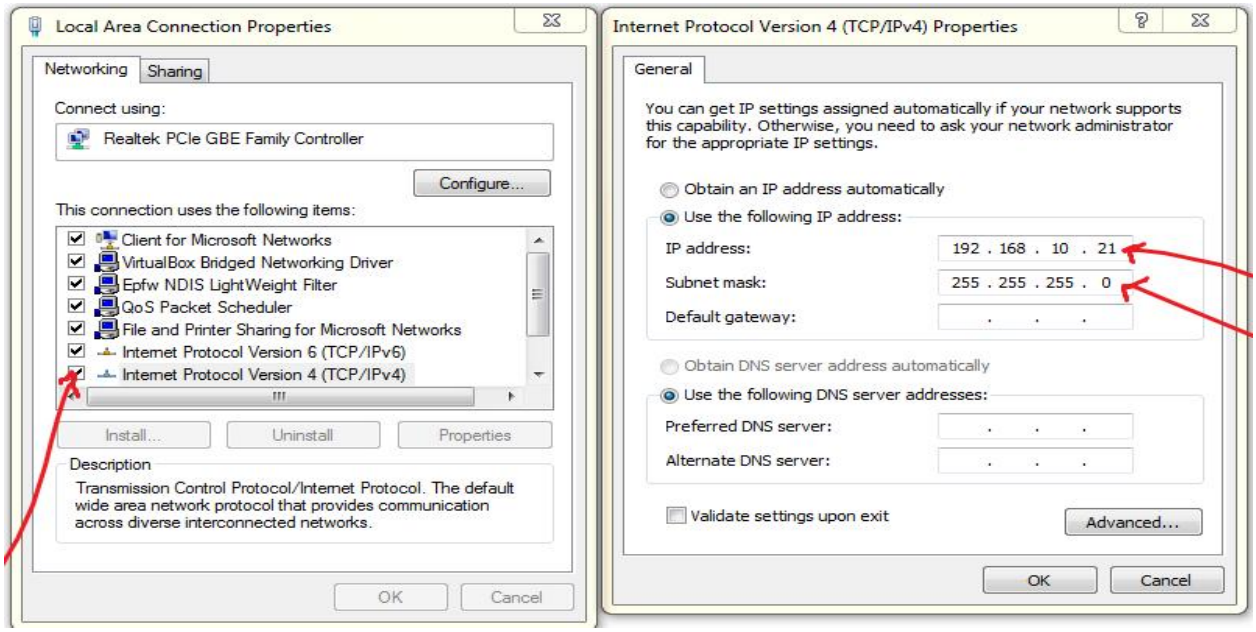
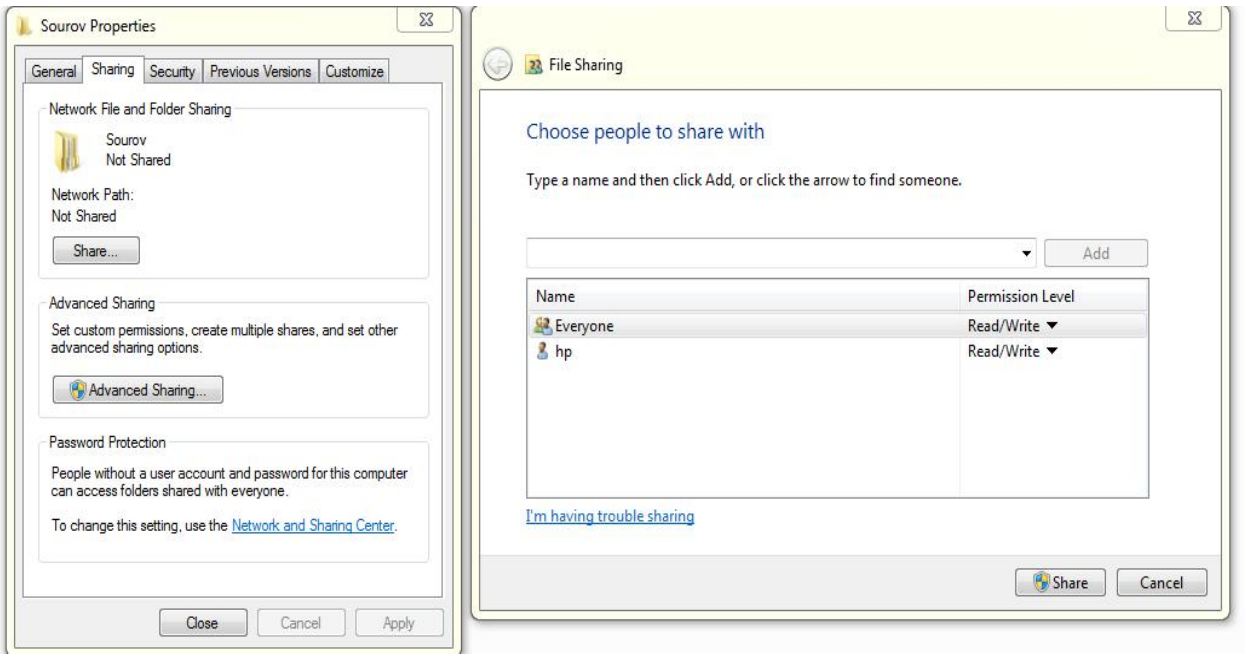
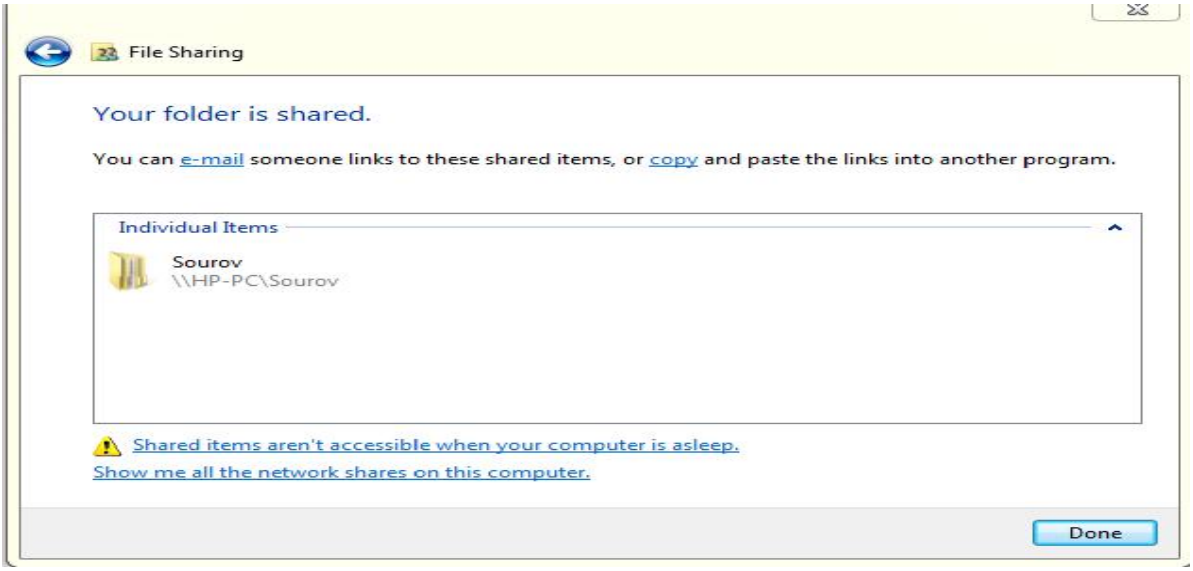


Figure5.2: pc 2 ip setting

Then I have created a drive or folder name is MY ZONE (F:) . Then create a folder sourov into MY ZONE (F:).

\\HP-PC\Sourov i want to share this file over our LAN. Now click the Share button select Everyone and give Read/Write permission. At last click Share and done.





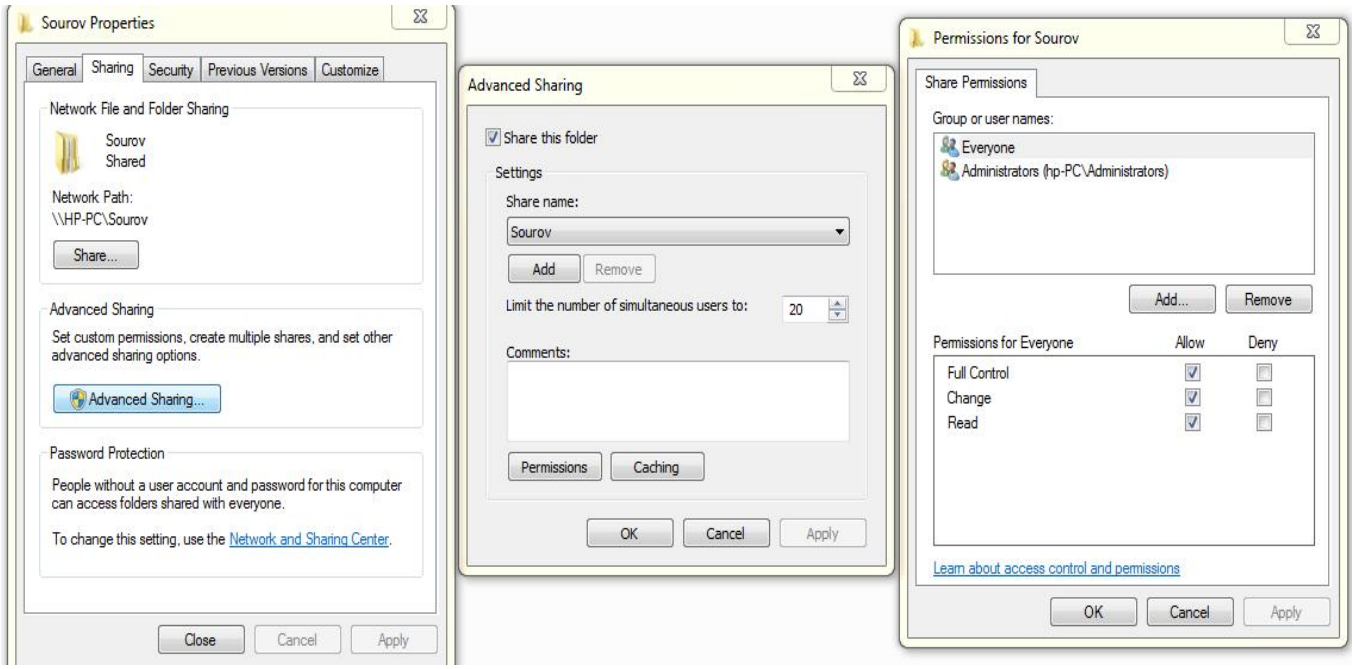


Figure5.3: **HP-PC\sourov** folder sharing from pc 1.

Drive Mapping:

Before drive mapping I have to share the drive we want to mapping as before.

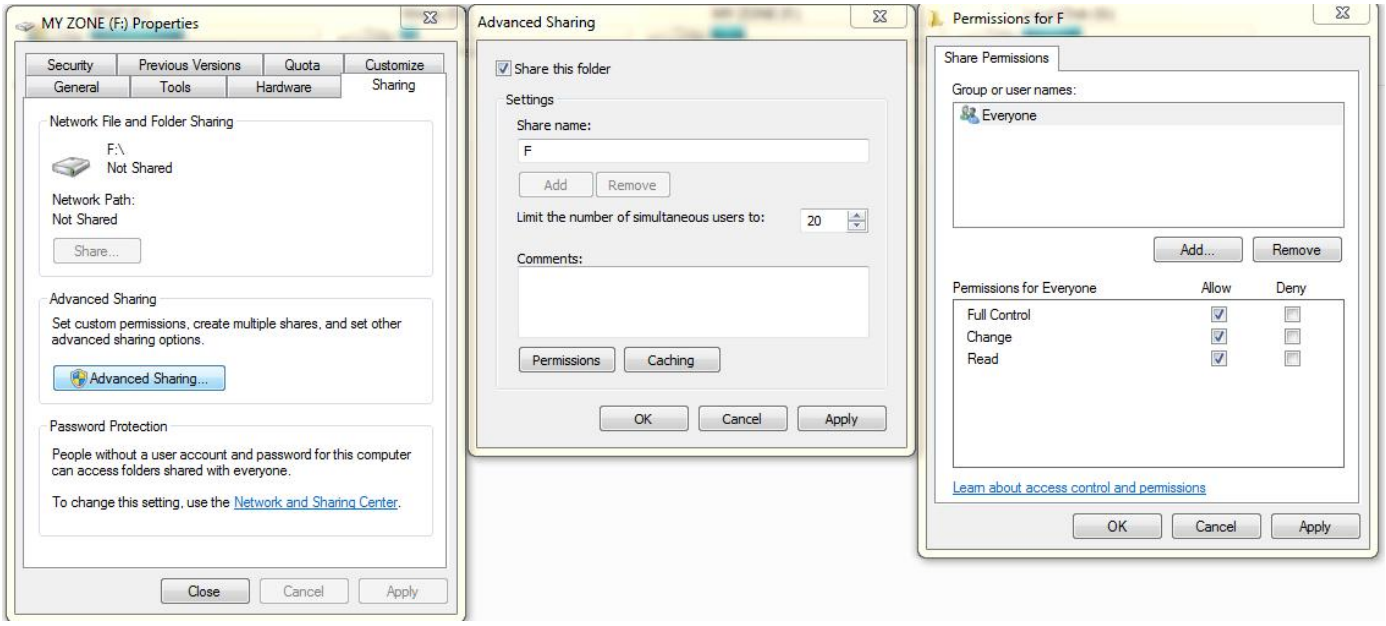


Figure5.4: **HP-PC\MYZONE** (F:) folder sharing from pc 1.

Then click the Start button then click Computer and click Map network drive

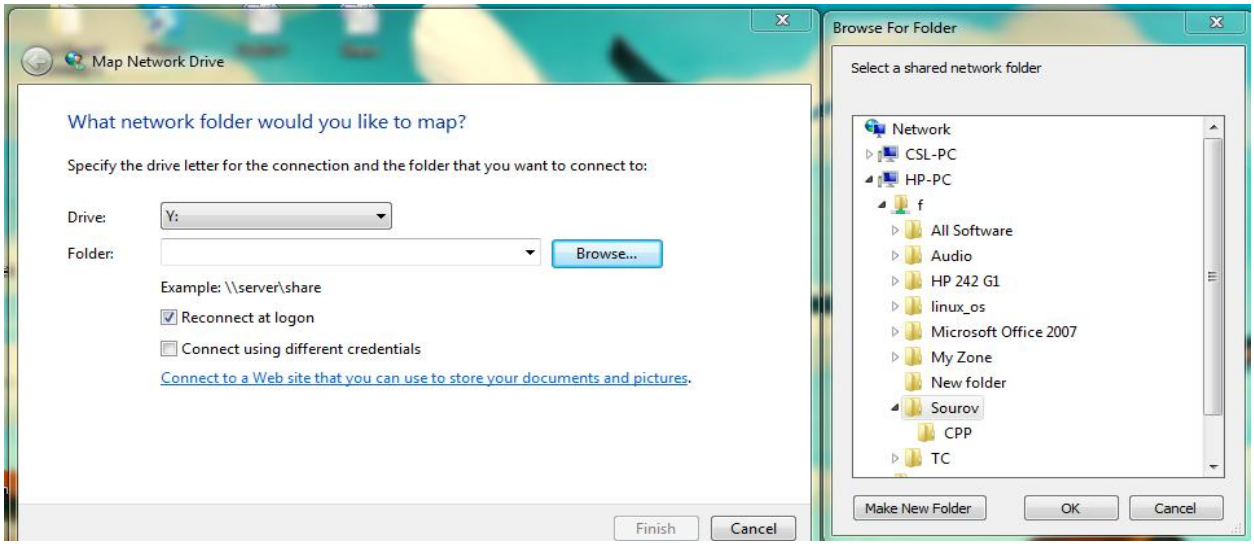


Figure5.4:Drive mapping sourov (**HP-PC**) (Y:)

Now check the sharing and mapping file and folder from pc 2.

At first ping pc1 from pc2 then I get the sharing file

//192.168.10.20 write to the search box.

Pc2 can read, write all the folders sharing from pc1 because pc1 gives the permission.

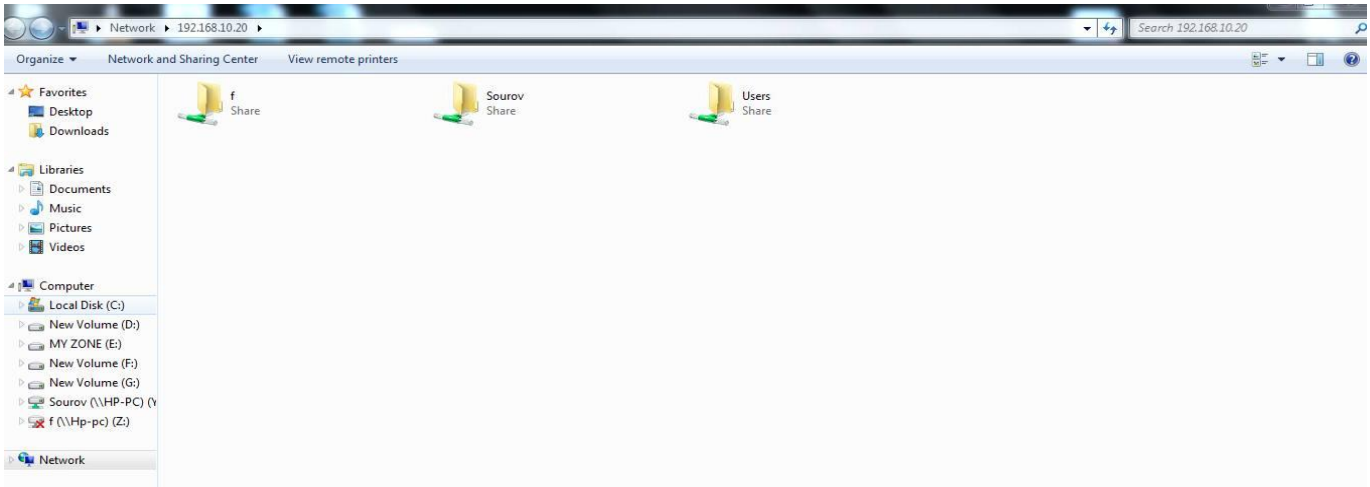


Figure5.5: Sharing File From pc1 is showing on pc2

The driver which is mapped automatically show on the pc2

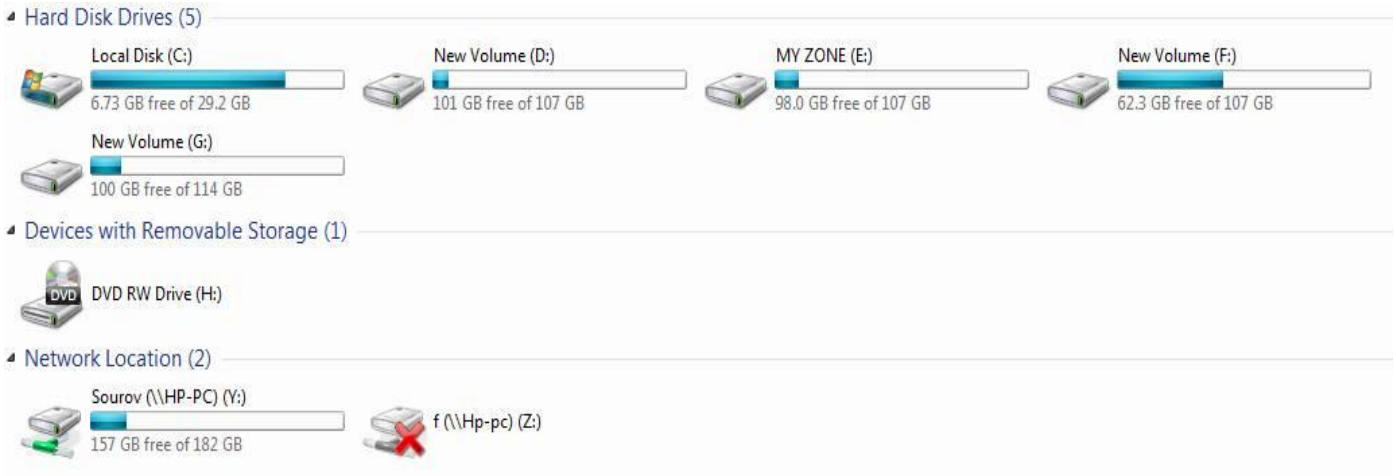


Figure5.6: Mapping Folder From pc1 is showing on pc2

As the same process I have shared and mapped the MY ZONE(E) drive. In this drive I have TC software.

Then I run a C program in the software. When I run the program in pc1 then the output of that program is shown in pc2 Y:\data\ folder. After drive mapping I have created a data folder in Y drive.

The program that I used in PC1 for implementation is" writing a program" to create a data file on a network drive of PC2.

```
#include<stdio.h>
#include<stdlib.h>
#include<string.h>
#include<conio.h>
typedef struct
{
    int  ROLL;
    char NAME[12];
    float GPA;
    }
    student;
    int main()
    {
       clrscr();
       student STD;
       FILE *WFP;
       if (!(WFP=fopen("TESTFILE.TXT","w")))
```

```
{
printf("TESTFILE.TXT can't open....");
exit(1);
};
printf("\nRoll Number(any -ve number to finish)>");
scanf("%d",&STD.ROLL);
while(STD.ROLL>=0)
{
printf("\nNAME>");
scanf("%s",STD.NAME);
printf("\nGrade Point Average>");
scanf("%f",&STD.GPA);
fprintf(WFP,"%d\n",STD.ROLL);
fprintf(WFP,"%s\n",STD.NAME);
fprintf(WFP,"%f\n",STD.GPA);
printf("\nRoll Number(any -ve number to finish)>");
scanf("%d",&STD.ROLL);
};
fclose(WFP);
getch();
return 0;
```

After ran I gave some data in the output

Roll No: 10

Student Name: sourov

Average Grade: 3.5

This output showed in the drive that is mapped

Y:\data in this folder I have shown the write file

10

sourov

3.5

This is the final output of write program ,which I ran in PC1 in E drive .

And the output has shown in Y:\data folder in PC2.

Then I mapped a drive from PC2 the drive is MY ZONE(E):

The program is “writing a program to retrieve the data file from a different network drive of another computer”.

```
#include<stdio.h>
#include<stdlib.h>
#include<string.h>
#include<conio.h>

//student record structure
typedef struct{
            int    ROLL;
            char   NAME[12];
            float  GPA;
            }student;
int main()
{
       //variable declaration
       clrscr();
       student STD;

FILE *RFP;            //declaring file pointer

if(!(RFP=fopen("E:\\data\\TESTFILE.TXT","r"))){
      printf("TESTFILE.TXT can't open...");
      exit(1);};

//retrieve roll number first
fscanf(RFP,"%d",&STD.ROLL);

while(!feof(RFP)){
          //reading rest of the record
          fscanf(RFP,"%s", STD.NAME);
          fscanf(RFP,"%f",&STD.GPA);

          //display on screen
          printf("\nRoll Number>");
          printf("%d",STD.ROLL);
          printf("\nName>");
          printf("%s",STD.NAME);
          printf("\nGrade poit Average>");
          printf("%f",STD.GPA);

          //reading first field of record
          fscanf(RFP,"%d",&STD.ROLL);
          };
   fclose(RFP);               // closing the file
   getch();
   getch();
   getch();
   return 0;
```

Then I ran a program from PC2 by TC software .

The output had to show in Y:\data folder in PC1 .

CHAPTER 6: FINDINGS

6.1 SUCCESS

Finally I am able to sharing and mapping file/folder from one pc to another over a LAN. It's a great benefit for a small work station where disk space is at a premium. By sharing the file I can back up file easily to all the pc in the same network. By this process I can easily share a printer for the whole LAN. For a small LAN network folder sharing is very popular, but for a large network mapping is essential. By sharing file from one pc I can read and write from another. But it's a basic data sharing process. I have successfully done the program which is called "write program". I ran this program from PC1 and created a data file on a network drive of PC2.

6.2 ADVANTAGES OF FILE SHARING

In a file sharing environment, a large number of users can access a program as though it were on their local machines, when actually the program resides on a single file server. This is a great benefit to small workstations, where disk space is at a premium. A user can have access to a much larger program repertoire than could fit on a private disk.

By having a resource resides physically on a single server, then distributed throughout the network, you can greatly simplify administration. First, you reduce the number of copies of various programs that need to be maintained on the network. Second, you reduce the problems involved in performing backups for a number of machines dispersed over a wide geographical area. By keeping files in a single location, this task becomes comparable to backing up a single machine.

Centralizing files on a few file servers not only simplifies administration, it helps maintain consistency of shared data files. When changes are made to a shared file, they become available to all users immediately.

As an alternative to centralizing files on a few file servers, files may be shared. When a single computer runs out of capacity, more computers can be added to a configuration. Files can be moved to the new computers, while a consistent view of the file system from the user's perspective is maintained.

More available space for users to access programs

Easier to back up files

Reduce number of programs on any given network

Simply administration

Helps maintain consistency of shared data files

6.3 DISADVANTAGES OF FILE SHARING

Security problems

Potentially breaking copyright laws

Duplication of data

Data inconsistency

Data Redundancy

6.4 FAILURE

I have ran the “read program” but I did not get the output successfully.

SUMMARY:

This paper only presents some network categories, protocols and basic data sharing over a LAN. It should be noted that I can share data over a network in various way. This is a very simple and basic way. But this way is very good for small or home area network. This is a basic sharing technique, small file and document can be shared by this. However it is the base of all sharing method.

REFERENCE:

- http://www.businessdictionary.com/definition/computer-network.html#ixzz38XgEsTWQ
- http://www.webanswers.com/technology-computers/computer-terminology/what-are-the-basic-elements-of-computer-network-8773cf
- http://www.techopedia.com/definition/5526/local-area-network-lan
- https://www.google.com.bd/search?q=local+area+network&client=firefox-a&hs=TvF&rls=org.mozilla:en-US:official&tbm=isch&tbo=u&source=univ&sa=X&ei=uCzTU8_3DNKdugTS3ICADg&ved=0CC0QsAQ&biw=1366&bih=664#imgdii=_
- http://www.techopedia.com/definition/5409/wide-area-network-wan
- http://en.wikipedia.org/wiki/Campus_network
- http://en.wikipedia.org/wiki/Metropolitan_area_network
- http://en.wikipedia.org/wiki/Home_network
- http://compnetworking.about.com/cs/wirelessproducts/g/bldef_wlan.htm
- https://www.google.com.bd/search?q=TCP/IP+model&client=firefox-a&hs=P42&rls=org.mozilla:en-US:official&tbm=isch&tbo=u&source=univ&sa=X&ei=lLHZU6CFI8i8uASBjoDYCA&ved=0CB8QsAQ&biw=1366&bih=664#imgdii=_
- http://en.wikipedia.org/wiki/OSI_model
- http:///C:/CISCO_CCNA/Exploration1/theme/cheetah.html?c1lang=en&c1id=en0600000000&c2lang=&c2id=&chapter=3
- http:///C:/CISCO_CCNA/Exploration1/theme/cheetah.html?c1lang=en&c1id=en0600000000&c2lang=&c2id=&chapter=3.1.1
- http:///C:/CISCO_CCNA/Exploration1/theme/cheetah.html?c1lang=en&c1id=en0600000000&c2lang=&c2id=&chapter=4.1.1
- http:///C:/CISCO_CCNA/Exploration1/theme/cheetah.html?c1lang=en&c1id=en0600000000&c2lang=&c2id=&chapter=5.1.1
- http:///C:/CISCO_CCNA/Exploration1/theme/cheetah.html?c1lang=en&c1id=en0600000000&c2lang=&c2id=&chapter=7.1
- http:///C:/CISCO_CCNA/Exploration1/theme/cheetah.html?c1lang=en&c1id=en0600000000&c2lang=&c2id=&chapter=8.1
- http://en.wikipedia.org/wiki/POP_before_SMTP
- http://www.ncftp.com/ncftpd/doc/misc/ftp_and_firewalls.html
- http:///C:/CISCO_CCNA/Exploration1/theme/cheetah.html?c1lang=en&c1id=en0600000000&c2lang=&c2id=&chapter=3.3.4
- http://technet.microsoft.com/en-us/library/cc785220(v=ws.10).aspx

- http://technet.microsoft.com/en-us/library/cc757152(v=ws.10).aspx
- http://technet.microsoft.com/en-us/library/cc527483%28v=ws.10%29.aspx
- http://www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing
- https://www.google.com.bd/search?q=multiaccess+topology&client=firefox-a&hs=6uh&rls=org.mozilla:en-US:official&channel=sb&tbm=isch&tbo=u&source=univ&sa=X&ei=cMnlU5LHLJPh8AXBloHAAg&ved=0CDkQsAQ&biw=1366&bih=657#facrc=_&imgdii=_&imgrc=5yIhSWNvp0cDQM%253A%3BuXm7-KnPlH4-MM%3Bhttp%253A%252F%252Fwww.howtonetwork.net%252Fmembers%252Fimages%252FCCNPImages%252FBSCITheory%252Fmod3fig3.png%3Bhttp%253A%252F%252Fwww.howtonetwork.net%252Fmembers%252F1077.cfm%3B739%3B471
- http:///C:/CISCO_CCNA/Exploration1/theme/cheetah.html?c1lang=en&c1id=en0600000000&c2lang=&c2id=&chapter=3.2.1
- http://www.google.com.bd/imgres?imgurl=&imgrefurl=http%3A%2F%2Fwww.datacottage.com%2Fnch%2Ftroperation.htm&h=0&w=0&tbnid=AMG2lwzxtSAOhM&zoom=1&tbnh=232&tbnw=217&docid=yHXc_5Ei1BxQtM&tbm=isch&client=firefox-a&ei=5cjlU4KhBoneoAT9nYHIDg&ved=0CAIQsCUoAA
- http://www.webopedia.com/TERM/R/router.html
- http://www.webopedia.com/TERM/S/switched_Ethernet.html
- http://www.thefreedictionary.com/peer-to-peer+network
- http://www.neat.com/support/neatcloud-faq/sharing-files-folders/
- http://support.microsoft.com/kb/301281
- http://windows.microsoft.com/en-us/windows/file-sharing-essentials#1TC=windows-
- http://www.7tutorials.com/homegroup-feature-how-it-works
- http://www.howtogeek.com/school/windows-network-sharing/lesson4/all/
- http://it.med.miami.edu/x1783.xml
- http://www.it.cornell.edu/services/guides/computer/howto/map_win7.cfm