SURESH GYAN VIHAR UNIVERSITY
Accredited by NAAC with ‘A+’ Grade

Bachelor of Computer Application

(B.C.A.)

Computer Networking

Semester-iv

Author- Archana P. Kothawade

SURESH GYAN VIHAR UNIVERSITY
Centre for Distance and Online Education
Mahal, Jagatpura, Jaipur-302025

Published by:
S. B. Prakashan Pvt. Ltd.
WZ-6, Lajwanti Garden, New Delhi: 110046
Tel.: (011) 28520627 | Ph.: 9205476295
Email: info@sbprakashan.com | Web.: www.sbprakashan.com

Every effort has been made to avoid errors or omissions in the publication. In spite of this, some errors might have crept in. Any mistake, error or discrepancy noted may be brought to our notice and it shall be taken care of in the next edition. It is notified that neither the publishers nor the author or seller will be responsible for any damage or loss of any kind, in any manner, therefrom.

For binding mistakes, misprints or for missing pages, etc., the publishers' liability is limited to replacement within one month of purchase by similar edition. All expenses in this connection are to be borne by the purchaser.

Designed & Graphic by : S. B. Prakashan Pvt. Ltd.

Printed at :

Syllabus

Computer Networking

Learning Objectives

- The course introduces main concepts of networking; application areas; classification; reference models; transmission environment; technologies; routing algorithms; IP, UDP and TCP protocols; reliable data transferring methods; application protocols; network security; management systems; perspectives of communication networks.
- Students will be able to gain knowledge about the above given components and application of the same in real work situations.

UNIT I

INTRODUCTION: Network applications, network hardware, network software, reference models: OSI, TCP/IP, Internet, Connection oriented network - X.25, frame relay. THE PHYSICAL LAYER: Theoretical basis for communication, guided transmission media, wireless transmission, the public switched telephone networks, mobile telephone system.

UNIT - II

THE DATA LINK LAYER: Design issues, error detection and correction, elementary data link protocols, sliding window protocols, example data link protocols - HDLC, the data link layer in the internet. THE MEDIUM ACCESS SUBLAYER: Channel allocations problem, multiple access protocols, Ethernet, Data Link Layer switching, Wireless LAN, Broadband Wireless, Bluetooth

UNIT - III

THE NETWORK LAYER: Network layer design issues, routing algorithms, Congestion control algorithms, Internetworking, the network layer in the internet (IPv4 and IPv6), Quality of Service.

UNIT – IV

THE TRANSPORT LAYER: Transport service, elements of transport protocol, Simple Transport Protocol, Internet transport layer protocols: UDP and TCP.

UNIT - V

THE APPLICATION LAYER: Domain name system, electronic mail, World Wide Web: architectural overview, dynamic web document and http. APPLICATION LAYER PROTOCOLS: Simple Network Management Protocol, File Transfer Protocol, Simple Mail Transfer Protocol, Telnet.

References

- A. S. Tanenbaum (2003), Computer Networks, 4th edition, Pearson Education/ PHI, New Delhi, India.

- Behrouz A. Forouzan (2006), Data communication and Networking, 4th Edition, Mc Graw-Hill, India.
- Kurose, Ross (2010), Computer Networking: A top-down approach, Pearson Education, India.

Contents

1. Basics of Computer Networks **38**

1. Introduction 1-1
   - *1.1 What is Computer Network? 1-2*
   - *1.2 Goals of Networks 1-3*
   - *1.3 Applications of Networking 1-4*
   - *1.4 Network Structure 1-5*
   - *1.5 Components of Network 1-5*
   - *1.6 Computer Network Criteria 1-6*
2. Topology 1-7
   - *2.1 What is Topology? 1-8*
   - *2.2 Types of Topology 1-8*
3. Types of Networks 1-15
   - *3.1 LAN - Local Area Networks 1-15*
   - *3.2 WAN- Wide Area Network 1-17*
   - *3.3 MAN - Metropolitan Area Network 1-19*
   - *3.4 Internet 1-20*
   - *3.5 Transmission Technology 1-23*
4. Communication Types 1-25
   - *4.1 Synchronous Transmission 1-25*
   - *4.2 Asynchronous Transmission 1-27*
5. Modes of Communication 1-29
6. Types of Network 1-30
   - *6.1 Peer to Peer LAN's 1-31*
   - *6.2 Client server LAN's 1-32*
7. Protocols and Standards 1-34
   - *7.1 Protocols 1-34*
   - *7.2 Standards 1-37*

2. Network Models **30**

1. Introduction 2-1
2. Design Issues of the Layer 2-2
3. Protocol Hierarchies 2-3
4. ISO-OSI Reference Model 2-4
5. Terminology 2-9
   - *5.1 SAP 2-9*
   - *5.2 Connection Oriented Services 2-11*
   - *5.3 Connectionless Services 2-13*
   - *5.4 Peer Entities 2-15*
6. Internet Model (TCP/IP) 2-15
   - *6.1 Overview of TCP/IP Architecture 2-16*
   - *6.2 OSI Reference Model and TCP/IP 2-17*
   - *6.3 Layers 2-17*
7. Addressing 2-20
   - *7.1 Types of Addressing 2-20*
   - *7.2 Physical Address 2-21*
   - *7.3 Logical Address 2-21*
   - *7.4 Port Address 2-22*
8. IP Addressing 2-22
   - *8.1 Assigning IP Address 2-24*
   - *8.2 Automatically Assigned Addresses 2-25*
   - *8.3 Classful Addressing 2-26*
   - *8.4 Classless Addressing 2-29*

3. Transmission Media **20**

1. Introduction 3-1
2. Classification of Transmission Media 3-2
   - *2.1 Guided Media / Wired Transmission 3-2*
   - *2.2 Unguided Media / Wireless Transmission 3-10*
3. Propagation Methods 3-16
   - *3.1 Ground Wave Propagation 3-17*
   - *3.2 Sky Wave Propagation 3-17*
   - *3.3 Space or Line-of-Sight Propagation 3-18*

4. Wired and Wireless LANs **40**

1. Introduction 4-1
2. IEEE Standards 4-2
3. Standard Ethernet 4-4
4. Fast Ethernet 4-7
   - *4.1 MAC Sublayer 4-8* *4.2 Physical Layer 4-8*
5. Giga Ethernet 4-9
   - *5.1 MAC Sublayer 4-10* *5.2 Physical Layer 4-11*
6. Network Interface Cards (NIC) 4-12
   - *6.1 Components of NIC 4-14*
   - *6.2 Functions of NIC 4-15*
   - *6.3 Types of NIC 4-16*
7. Wireless LAN 4-29
   - *7.1 IEEE 802.11 Architecture 4-30*
   - *7.2 Frame Types 4-31*
   - *7.3 Frame Formats 4-32*
   - *7.4 MAC Sublayer 4-32*
   - *7.5 Addressing Mechanism 4-34*
   - *7.6 Bluetooth Technology 4-35*

5. Network Connectivity Devices **24**

1. Categories of Connectivity Devices 5-1
   - *1.1 Hub 5-1*
   - *1.2 Repeaters 5-4*
   - *1.3 Bridges 5-6*
   - *1.4 Routers 5-11*
   - *1.5 Switches 5-13*
   - *1.6 Gateways 5-15*
2. Network Security Devices 5-18
   - *2.1 Firewall 5-19* *2.2 Proxy Server 5-21*

6. Internet Basics **26**

1. Concept of Intranet and Extranet 6-1
   - *1.1 Intranet 6-1* *1.2 Extranet 6-5*
2. Internet Information Server (IIS) 6-6
3. Web Server 6-8
4. WWW (World Wide Web) 6-12
   - *4.1 WWW Architecture 6-12* *4.2 Web Documents 6-15*
5. Search Engines 6-16
6. Internet Service Providers (ISP) 6-18
7. HTTP 6-20
   - *7.1 HTTP Transaction 6-20*
   - *7.2 Persistent HTTP connections 6-23*
   - *7.3 Non-persistent HTTP Connection 6-24*

***

Chapter 1

Basics of Computer Networks

1. Introduction

Computers are used as an information tool. It was developed with the concept of independent operation. The individuals use computer networks almost daily to conduct personal and professional business. This trend is accelerating as more people discover the power of computers and communication networks both for businesses and for homes. The day-to-day transactions at department stores, banks, reservation counters and other business are all dependent upon computer networks. The information age is equally dependent on the computer and the computer network.

1.1 What is Computer Network?

A computer network is a number of computers interconnected by one or more transmission paths. Network is a group of two or more computer systems linked together.

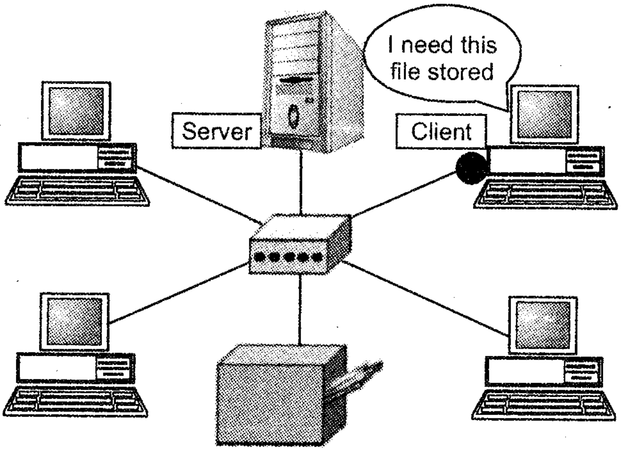


Figure 1.1: A simple network

All the networks must have the following:

i. Something to share (data)

ii. A physical pathway or transmission media (cable)

iii. Rules of communication (Protocols)

A network consists of two or more computers that are linked in order to share resources (such as printers and CD-ROMs), exchange files or allow electronic communications. The computer on a network may be linked through cables, satellites or infrared light beams.

Definition

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

1.2 Goals of Networks

The goals of computer networking are to provide services and to reduce equipment costs. It enables computers to share their resources by offering services to other computers.

Following are some main goals of computer network:

i. **Resource sharing:** Multiple users can share hardware like scanners and printers. They can also share software resources such as programs, databases, and files simultaneously. This reduces cost by reducing the number of hardware items bought. Resources are available to all users on the network without regard to the physical location of the resources and users.

3

Apr. 2012, 2011 – *5M*
Explain Goals and Applications of Computer Networks.

Oct. 2011 – *5M*
List various goals of Networking.

ii. **High reliability:** Provides high reliability by having alternative sources of supply. Information can be replicated on two or more machines, so that if one machine fails, the other one can be used to access it. Very important in applications where loss of information is not tolerable, *for example*, banking and military applications, air traffic control, nuclear reactor etc.

iii. **Saving money:** Small computers have a much better price/performance ratio than large ones.

The cost of building network is less because of cheap hardware. All users can share costly devices such as printers, scanners or Xerox machines by connecting them in the network.

iv. **Scalability:** The ability to increase system performance gradually as the workload grows just by adding more devices is called scalability. We can extend network just by adding more computers, printers etc. without affecting overall performance.

v. **Powerful communication medium:** Now-a-days it becomes easy for people living in different locations of the world to work together using computer networks. They can exchange documents, reports, e-mails on-line without any delay. They can share ideas, views through videoconferencing without considering actual distance between them.

vi. **Protecting information**: Networking provides the protection to the data by providing passwords and usernames, encryption of data etc., i.e., data is more secure.

vii. **Distribution of workload:** If any one of the computer get saturated due to a heavy workload, then its work is distributed among other computers having no or very little workload on the network.

viii. **Preserving information:** Information can be backed up to a central location. It is difficult to maintain regular backups in stand alone computers. It keeps back up of data on server.

1.3 Applications of Networking

The use of networking allows a very flexible working environment. Employees can work at home by using terminals tied through networks into computers at the office, thus accounting for flexibility in working hours. Some of these are summarized below:

i. **Access to remote programs information**

Access to remote programs involves interaction between a person and a remote database. Access to remote information comes in many forms like:

a. Home shopping, paying telephone, electricity bills, e-banking, online share market etc.

b. Newspaper is available online and is personalized. Digital library consisting of books magazines, scientific journals etc. are also easily available.

c. World Wide Web which contains information about arts, business, cooking, government, history etc.

ii. **Person to person communication**

Person to person communication includes:

a. Electronic-mail (e-mail)

b. Real time email, i.e., video conferencing allows remote users to communicate with no delay by seeing and hearing each other.

c. World wide new groups in which one person posts a message and all other subscribers to the newsgroup can read it or give their feedbacks.

iii. **Interactive entertainment**

Interactive entertainment includes:

a. Multiperson real time simulation games.

b. Video on demand

c. Participation in live TV programmes like quiz, contest, discussions etc.

1.4 Network Structure

In any network there are collection of machines which are intended for application user programs. Any network should have following elements:

i. **Host:** Hosts are the machines intended for running user application. They are also called as end system because they are the end users.

ii. **Communication subnet:** Hosts are connected with each other by communication subnet. The job of the subnet is to carry messages from host to host. The subnet plays an important role in network addressing which is needed in internetworking. Depending upon the boundary of the communication subnet, network is classified as:

LAN: Local Area network

WAN: Wide Area network

MAN: Metropolitan Area network

Following *figure* shows relation between hosts and subnets:

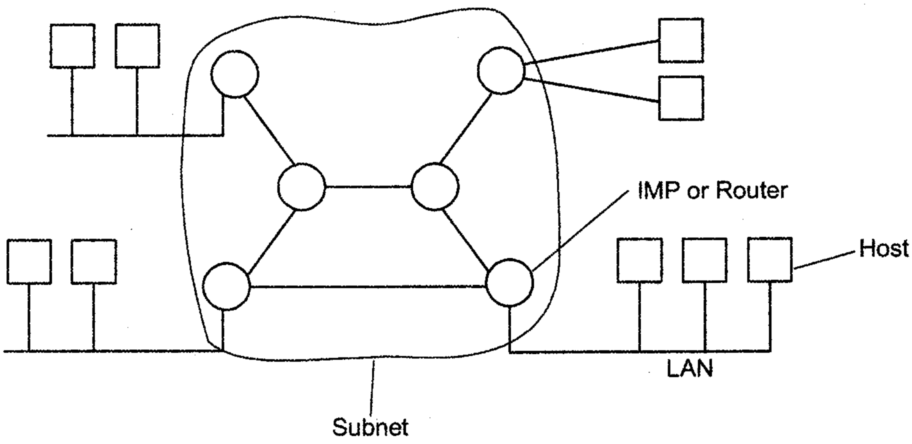


Figure 1.2

1.5 Components of Network

A data communication is exchange of data between 2 machines. A data communication system is made up of five components.

They are as follows:

i. **Sender:** This is a device which sends the data message. It can be a computer, workstation, telephone handset and so on.

ii. **Receiver:** This is a device which receives the message. It can be a computer, workstation, telephone handset and so on.

iii. **Message:** The message is nothing but the data or information which is to be communicated. It may have texts, numbers, pictures, sound or video or combination of anything from these.

iv. **Medium:** The transmission medium is the physical path by which a message travels from sender to receiver. It may be twisted pair wise, coaxial cable, fiber optic cable and so on.

v. **Protocol:** It is a set of rules required for data communication. It represents the agreement between the two communicating devices. The job of protocol is similar to that of a translator.

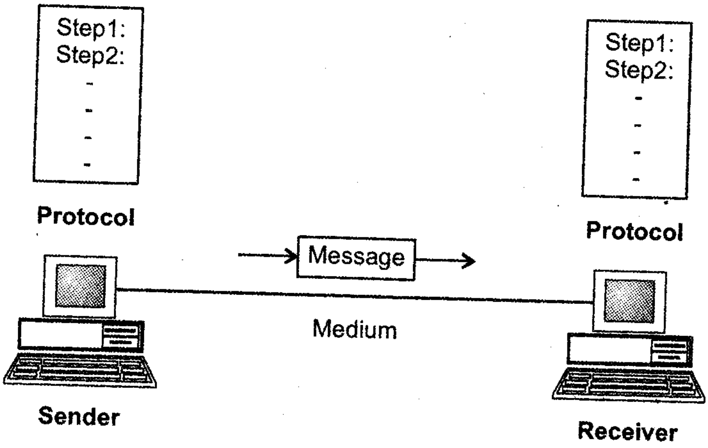


Figure 1.3: Data communication system components

1.6 Computer Network Criteria

Network is a broad term similar to system. Network is a communication system which supports many users. A 'computer network' is a system which allows communication among the computers connected in the network. A network must be able to meet certain criteria.

The most important of them are:

i. **Performance:** Performance is measured in terms of transit time and response time.

a. *Transit time:* It is defined as the amount of time required for a message to travel from one device to the other.

b. *Response time:* It is the time elapsed between enquiry and response.

Other factors deciding the performance are as follows:

a. Number of users.

b. Types of transmission medium

c. Capability of connected hardware.

d. Efficiency of software

ii. **Reliability:** The network reliability is important because it decides the frequency at which network failure takes place.

It also decides the time taken by the network to recover and its robustness in the catastrophe.

iii. **Security:** Security of the network is considered as the important aspect for improving the network performance. The network security may be affected due to viruses and unauthorized access of other users. To provide network security:

- Avoid opening unknown e-mail attachments which may contain virus.
- Use anti-virus software for securing the systems from virus.
- Firewalls can be implemented for detecting and preventing unauthorized access of other users in the network.
- Use backup tools to store the important data on removable media like CD or ZIP disks. This helps to secure your data.
- Turn off the system and remove the network cable when not in use, to avoid unauthorized interference in the systems.

2. Topology

In communication networks, a topology is a usually schematic description of the arrangement of a network, including its nodes and connecting lines.

2

Apr. 12, Oct. 11 – *5M*
Write a note on network topologies.

There are two ways of defining network geometry: the physical topology and the logical (or signal) topology. The physical topology of a network is the actual geometric layout of workstations.

2.1 What is Topology?

4

Oct. 11, Apr. 10 – *5M*
Define topology. Explain its various types.

Apr. 2011 – *5M*
What is Topology? Explain its types.

Apr. 2010 – *5M*
Define Network Topology. List different types of topologies. Explain any one in detail.

A network topology is the shape or the physical connectivity of the network. The topology refers to the physical layout of the computers, servers, hubs, cabling etc.

Following are the most commonly used meanings of topology:

a. A topology defines the arrangement of nodes, cables and connectivity devices that make up the network.

b. A topology is a map of computers which allows how to connect the computers with each other.

2.2 Types of Topology

Types of Topology
i. Bus topology
ii. Star topology
iii. Ring topology
iv. Mesh topology
v. Hierarchical / tree topology

Following are some basic types of topology:

i. Bus topology

A topology that allows all network nodes to receive the same message through the network cable at the same time is called **"bus topology"**.

The bus pattern connects the computer to the same communication line. In bus topology, all nodes/stations are connected to a common link/medium. In this, communication goes both directions along the line. It is a multipoint network connection type of topology.

In bus topology, one long cable acts as a backbone to link all the devices in a network. Various workstations (or nodes) are connected to the bus by drop line and tap.

A drop line is a cable through which workstation (or node) connects to the bus. A drop line is a connection running between a device and the main cable.

A tap is a point where dropline connects to the network cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

Following figure shows bus topology with dropline and taps:

The bus topology is usually used when a network installation is small, simple or temporary as shown in *figure 1.4*

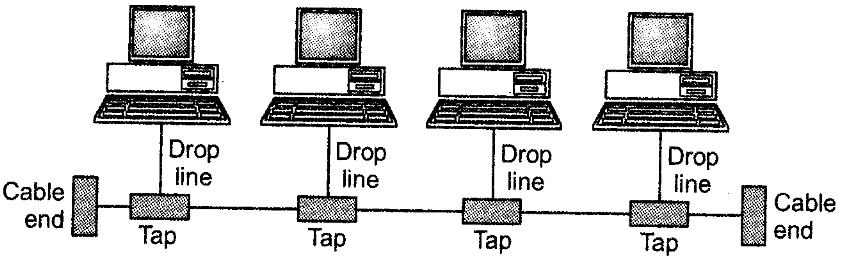


Figure 1.4: Bus topology

When one computer sends a signal to, all the computers on the network receives the information but only the one whose address matches will accept the encoded information while all the others rejects the message.

The speed of the bus topology is slow as only one computer can send a message at a time. A computer must wait until the bus topology requires proper termination at both the ends of the cable.

Without termination at both the ends of the cable, it returns back and travels back up the cable.

Bus topology is the cheapest way of connecting computers to join a workgroup or departmental LAN.

Advantages

a. Easy installation: It is very easy to install and connect a computer or peripheral to a bus.

b. Requires less cabling length as drop lines are available.

c. Cheaper or less cost due to less cabling length.

d. Does not affect the other computers in bus, if any one computer or device fails.

e. Fast as compared to other topologies.

Disadvantages

a. Cannot connect a large number of computers.

b. Fault isolation is difficult. A fault or break in the bus cable stops all transmission. Difficult to identify the problem if the entire network shuts down.

c. Collision may occur.

d. Signal reflection at the taps can cause degradation in quality.

e. When backbone (main cable) fails, whole transmission of a network fails.

f. Terminators are required at both ends of the backbone cable.

g. Limited number of stations are possible and spaces between two stations are also considered.

h. Only one cable is used for whole transmission. It has huge workload and ultimately it becomes slow.

Usage

Ethernet and local talk network uses the bus topology.

ii. Star topology

A star topology links the computers by individual cables to a central unit, usually a hub, as shown in *figure 1.5.*

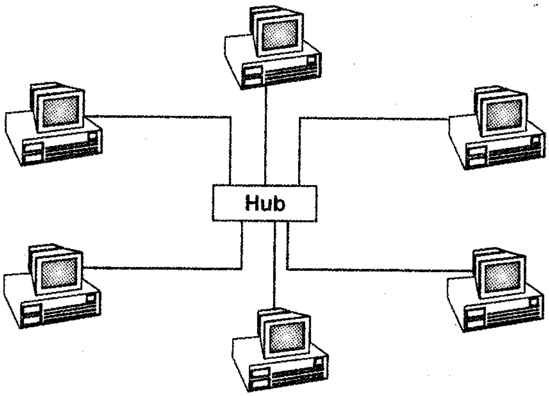


Figure 1.5: Star topology

When a computer component transmits a signal to the network, the signal travels to the hub.

Then, the hub broadcasts the signal to all other components connected to the hub.

A star network can be expanded by placing another star hub.

Note

1. Ethernet 10 base T is a popular network based on the star topology.
2. Intelligent hubs with microprocessor that implement features in addition to repeating network. Signals provide for centralized monitoring and management of the network.
3. It is the most flexible and the easiest to diagnose when there is a network fault.

Advantages

a. Failure of a single computer or cable doesn't bring down the entire network.

b. It is easy to modify and add new computers to a star network without disturbing the rest of the network.

c. The centralized networking equipment can reduce costs in the long run by making network management much easier.

Disadvantages

a. If the central hub fails, the whole network fails to operate.

b. It is slightly more expensive than bus topology.

iii. Ring topology

In Ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in *figure 1.6.*

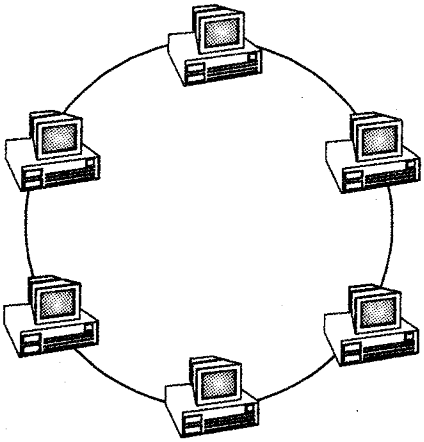


Figure 1.6: Ring topology

Rings are used in high performance networks where large bandwidth is necessary.

Every computer is connected to the next computer in the ring and each transmits what it receives from the previous computer hence the ring is an active network. The message flow around the ring is in one direction.

Ring networks also do token passing. A short message called a token is passed around the ring until the computer wishes to send information to another computer. The computer modifies the token, adds an electronic address and data and sends it around the ring. Each computer receives the token and the information and passes it to the next computer until the electronic address matches the address of a computer or the token returns to its origin. The receiving computer returns a message to the originator indicating that the message has been received. The sending computer then creates another token and places it on the network, allowing another computer station to capture the token and begin transmitting. The token circulates until a station/computer is ready to send and capture the token. Faster networks circulate several tokens at once.

Note

Token ring networks are defined by JEEE 802.5 standard.

Advantages

a. One computer cannot monopolize the network, as every computer is given equal access to the token.

b. A ring is relatively easy to install and reconfigure.

c. Fault isolation is easy.

Disadvantages

a. Failure of one computer affects the whole network.

b. It is difficult to troubleshoot.

c. Adding and removing computers disrupts the network.

d. Traffic is in one direction only.

iv. Mesh topology

In mesh topology every device has a dedicated point to point link to every other device as shown in *figure 1.7.*

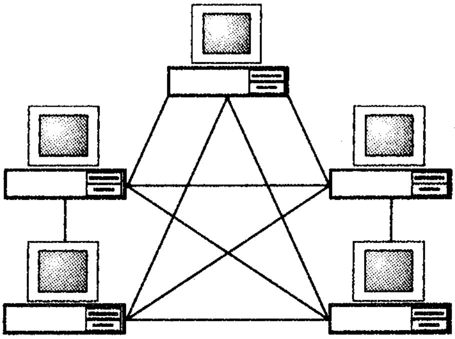


Figure 1.7: Mesh topology

The term dedicated means that the link carries traffic only between two devices it connects. A fully connected mesh network therefore has n(n–1)/2 physical channels to link n devices. To accommodate that many links every device on the network must have n–1 input/ output ports. In a mesh topology each computer on a network has redundant data paths as shown in *figure 1.7.*

1 **Oct. 2012 – *5M***
Explain Star and Mesh Topology with its advantages and disadvantages.

The mesh topology provides fault tolerance – if a wire, hub, switch or other component fails, data can travel along an alternate path. The mesh topology is most often used in large backbone of a single switch or router and can result in a large portion of the network going down.

Note

Mesh topology is usually implemented as a backbone connecting the main computer of a hybrid network that can include several other topology.

Advantages

a. It is more reliable compared to others.

b. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating traffic problems.

c. It is robust because the failure of any one computer does not bring down the entire network.

d. It provides security message sent along a dedicated line.

Disadvantages

a. Since every computer is connected to every other computer, installation and reconfiguration is difficult.

b. Cabling cost is more.

c. Hardware required to connect each link to input/output and cable is expensive.

v. Tree topology

A tree topology is a variation of a star. As in a star, nodes in a tree are linked to a central hub that controls the traffic to the network.

Here all computers are not connected to the central hub, but are connected to a secondary hub which in turn is connected to the central hub as shown in *figure 1.8.*

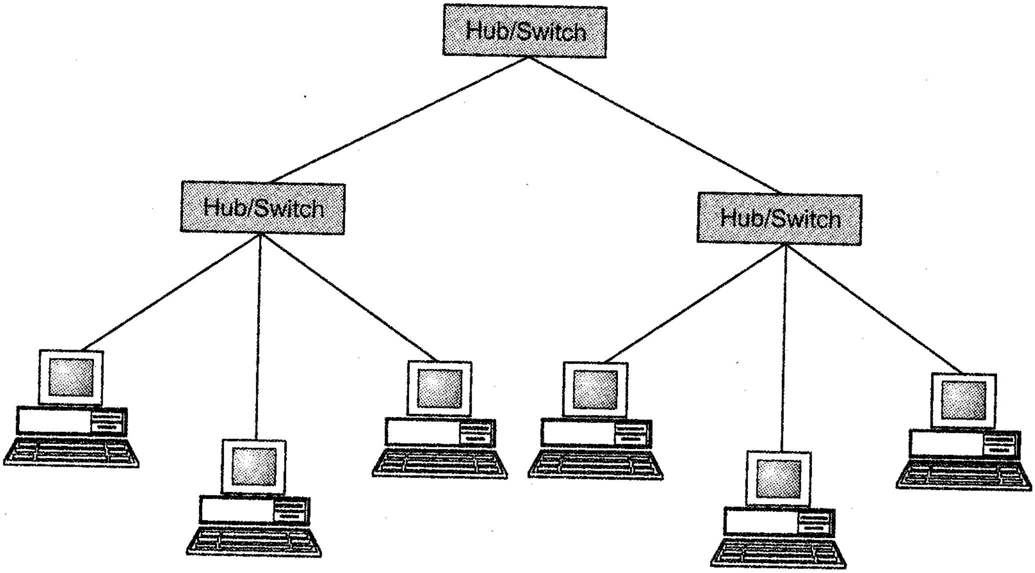


Figure 1.8 : Tree topology

The central hub in the tree is the active hub which contains repeater. The repeater amplifies the signal and increases the distance a signal can travel.

The secondary hubs may be active or passive. A passive hub provides a simple physical connection between the attached devices.

Advantages

a. Failure of one or more nodes does not affect the entire network.

b. It is easier to isolate a defective node.

c. It is easier to add new nodes or branches to the network.

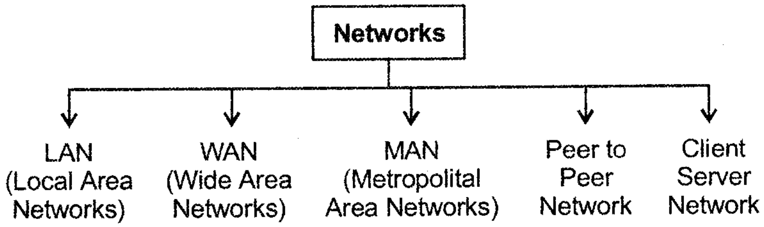
Disadvantages

a. The cabling cost is more.

b. If the central hub fails the system or network breaks down.

c. Installation can become costly and complex.

3. Types of Networks



3.1 LAN - Local Area Networks

LAN can be thought as a combination of hardware and software that enables computers to share resources across a network that spans a short distance.

It is the interconnection of computers located at different places at a short distance.

LAN lets the user to communicate with other users, share files and share peripherals.

3

Oct. 12, Apr. 10 – *5M*
Define Network. What are the types of Network? Explain.

Apr. 2011 – *5M*
Explain Network Classification.

It is usually a privately owned and links the devices in a single office, building or campus of upto few kilometers in size as shown in *figure 1.9*

LANs are typically owned, controlled and managed by a single person or organization. They also use certain specific connectivity technologies, primarily ethernet or token ring.

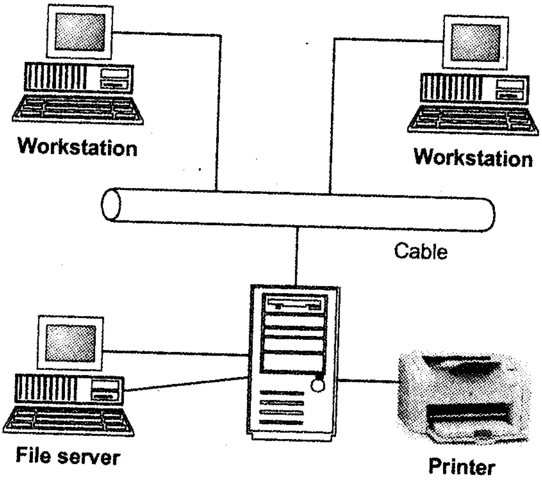


Figure 1.9: LAN

▶ Features of LAN

i. **Resource sharing:** It allows workstations to share peripherals like hard disks, plotters, printers, tapedrives etc.

ii. **Productivity:** It increases productivity as people have timely access to the equipment and information required to perform their job.

iii. **Communication:** It helps in providing fast responses and transmitting urgent notes, messages and circulars.

iv. **Management:** LAN manages and caters to ever increasing need of the organization and its people. It helps in improving efficiency and provides security by giving authority with responsibility.

▶ Advantages

i. It provides a cost effective multiuser computer environment.

ii. It is flexible and growth oriented.

iii. It offers email as an built in facility.

iv. It allows sharing of central storage and printer.

v. High rate of data transmission is possible.

vi. Allows file/record locking.

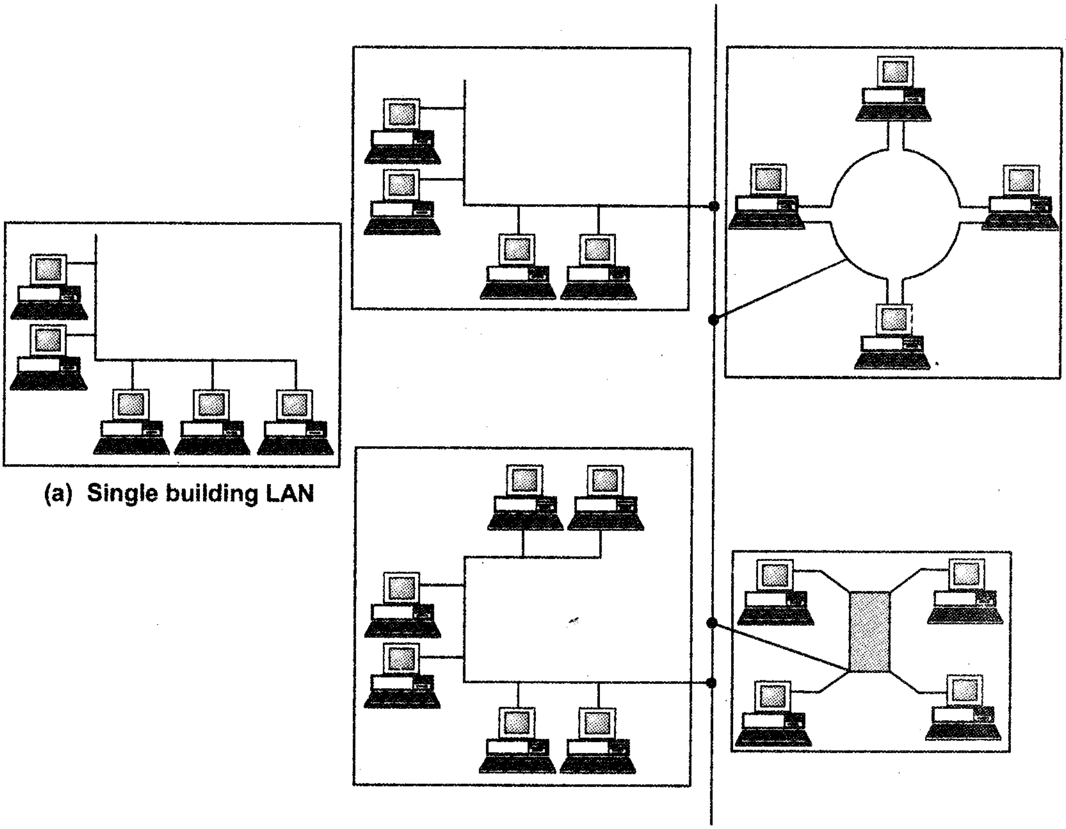
vii. It provides security.

viii. It provides data integrity.

▶ Disadvantages

i. Used for small geographical area / Limited area.

ii. Limited computers are connected in LAN.



(a) Single building LAN

(b) Multiple building LAN

Figure 1.10: Features of LAN

3.2 WAN- Wide Area Network

A WAN spans a large geographical area often a country or continent.

When the computers to be connected to each other are at widely separated locations a LAN cannot be used. A WAN must be installed.

It is cheaper and more efficient to use the phone network for the links.

Most wide area networks are used for transferring large blocks of data between it users.

It contains a collection of machines intended for running user programs called as hosts. The host are connected by a communication subset. The job of the subset is to carry messages from host to host.

The network contains number of transmission lines, each one connecting a pair of routers. Routers are used to connect the networks as well as route the data packets.

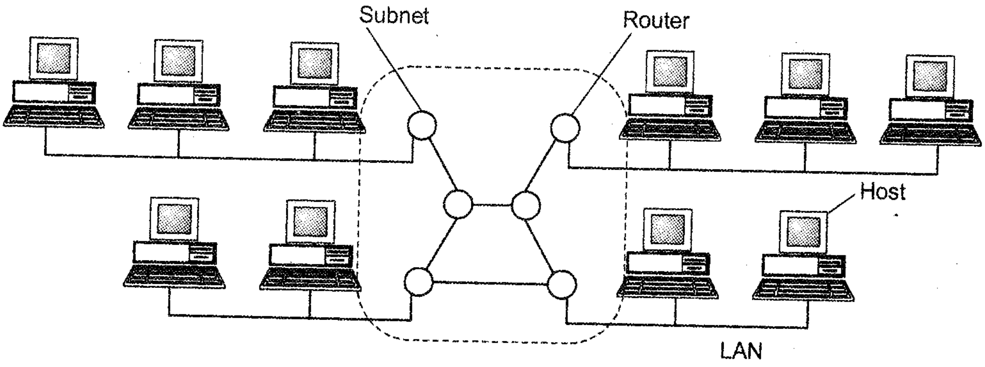


Figure 1.11: WAN

▶ Advantages

i. Allows many people to use the same network from many different locations.

ii. Large geographical area, covered.

iii. Cost effective.

▶ Disadvantages

i. Open to attacks from hackers.

ii. Can be expensive.

iii. Slow speed than LAN .

iv. Not easy for design and installation.

v. Maintaining is too difficult because where the exact fault is not identified quickly.

vi. Operates on low data rates.

vii. Each station cannot transmit the data.

3.3 MAN - Metropolitan Area Network

MAN can be defined as a large LAN, as a collection of interconnected LANs, operating over a metropolitan sized area.

It covers a city, the best known example of MAN is the cable television network available in many cities. In MAN there is connectivity of number of LANs into a large network so that resources may be shared LAN to LAN.

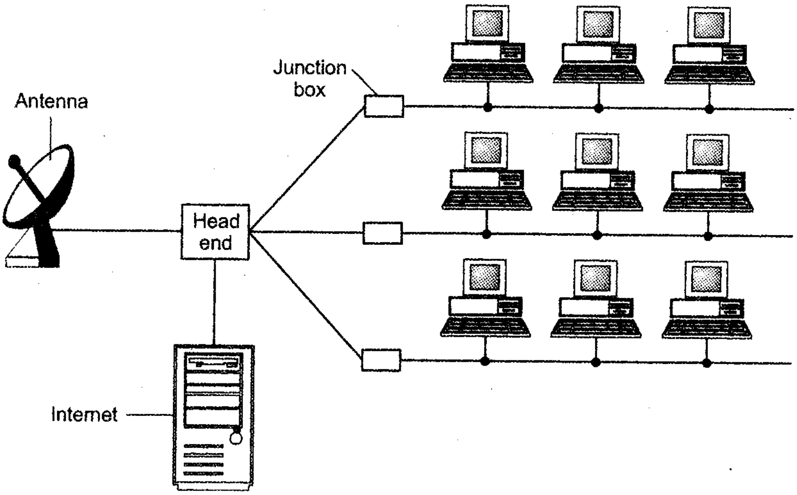


Figure 1.12: MAN based on cable TV

▶ Advantages

MAN can cover a wider area than a LAN. MAN networks are usually operated at airports, or a combination of several pieces at a local school. By running a large network connectedness, information can be disseminated more widely, rapidly and significantly. Public libraries and government agencies typically use a MAN.

▶ Disadvantages

MAN will only apply if the personal computer or a terminal can compete. If a personal computer is used as a terminal, move the file (file transfer software) allows users to retrieve files (downloaded) from the hose or hose to deliver the data (upload). Download files means open and retrieve data from a personal computer to another and deliver the data to the computer pertaining requested by the user.

▶ Comparison of LAN and WAN

	LAN	WAN
i.	The LAN is owned by a person, college etc. It is a privately owned network.	WAN can be private or it can be public leased type network.
ii.	LAN is designed to operate over a small physical area such as office, factory or group of buildings.	WAN is used for the network that spans over a large distance such as system spanning states, countries etc.
iii.	LANs are easy to design and easy to maintain.	WAN is not so easy to design and maintain.
iv.	LAN can operate on very high data rates.	WAN operates on low data rates.
v.	The communication medium used for interconnection is a simple co-axial cable.	The communication medium used in WAN can be PSTN or satellite links due to longer distances involved.
vi.	Due to shorter distances, problems such as propagation delay do not exist.	Due to long distances, the problem such as satellite links exists.
vii.	In LAN each station can transmit and receive data over the communication medium.	In WAN each station cannot transmit data.
viii.	LAN operates on the principle of broadcasting.	WAN operates on the principle of switching.

3.4 Internet

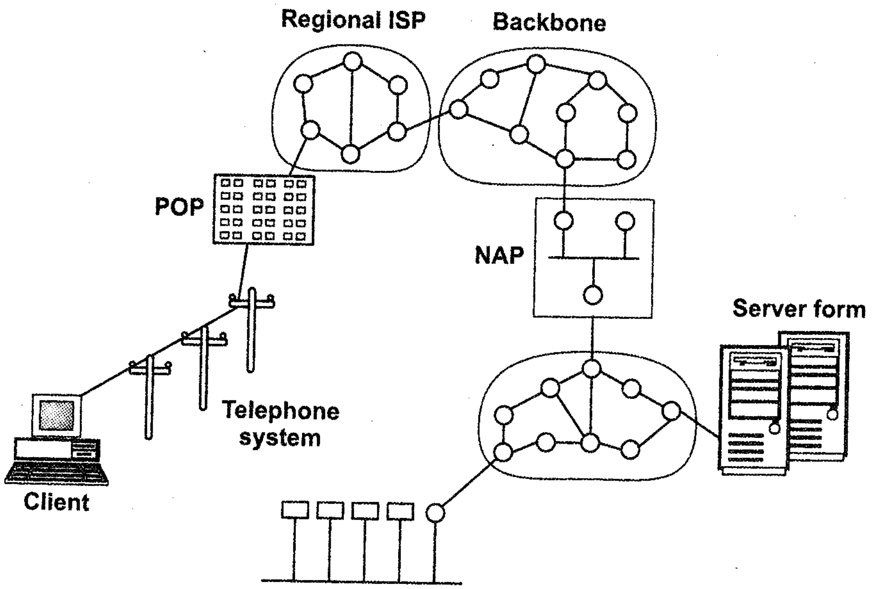


Figure 1.13: Overview of the internet

Internet means nothing but internetwork.

Internetworking involves connecting of two or more distinct computer networks or network segments via a common routing technology. The result is called as internetwork.

Any interconnection among or between public, private, commercial industrial or government networks may also be defined as internetwork. In modern practice, the interconnected networks use the internet protocol.

There are atleast three variants of internetwork, depending on who administers and who participates in them:

i. **Intranet:** An Intranet is a set of networks, using the Internet protocol and IP-based tools such as web browsers and file transfer an application that is under the control of a single administrative entity.

   Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

ii. **Extranet:** An extranet is a network that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations.

   Technically, an extranet may also be categorized as LAN, WAN, MAN or other types of network. An extranet cannot consist of a single LAN it must have with at least one connection with an external network.

iii. **Internet:** Internet is the extensive, worldwide computer network available to the public. An internet is a more general term for any set of interconnected computer networks that are connected by internetworking.

   a. The internet, or simply the net, is the physical available worldwide system of inter connected computer networks that transmit data by packet switching using standardized Internet Protocol (ISP) and many other protocols.

   b. It is made up of thousands of smaller commercial, academic and government networks.

   c. It carries various information and services, such as electronic mail, on-line chat and interlinked web pages and other documents of the world wide web.

   d. Hypertext is viewed using a program called a web browser which retrieves pieces of information, called 'documents' or 'web pages' from web servers and displays them, typically on a computer monitor.

   e. One can then follow hyperlinks on each page to the other documents or even send information back to the server to interact with it.

f. The act of following hyperlinks is often called 'surfing' or 'browsing' the web. Web pages are often arranged in collections of related material called 'Web sites'.

g. Typical network schematic is shown in figure.

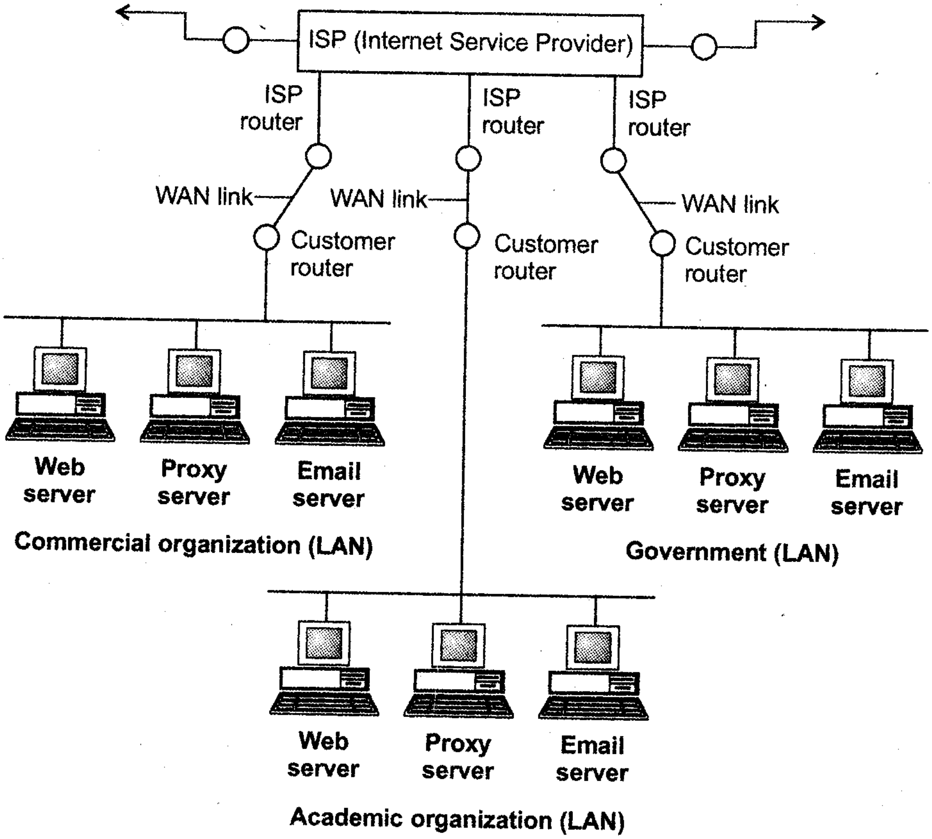


Figure 1.14: Typical internet connection components

Functions

1. Function of web server is to host website.
2. Function of proxy server is to provide internet connectivity to the different machines with private IP addresses.
3. Email server is used to provide different email accounts for email transactions.
4. Thus, routers are used to interconnect different LANs to form internet.
5. Organization router and IsPs router are interconnected to form internet.

6. Customer router to ISP router link can be
   - Dial up line
   - Leased line
   - ISDN line etc.

3.5 Transmission Technology

Transmission technology means the way in which two devices are connected through connecting links. There are two different ways to connect the devices. *They are as follows:*

i. **Point to point connection:** In point to point connection, the computer is connected directly to another device/computer by a dedicated communication channel/link. As shown in *figure 1.15.*

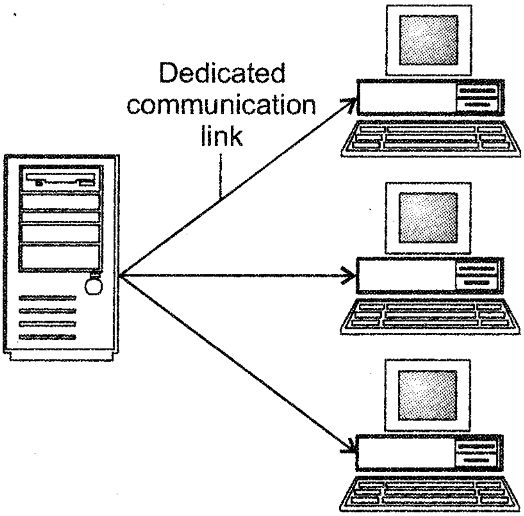


Figure 1.15: Point to point connection

Point to point can be an inefficient and costly configuration if a terminal is not active enough to keep the line busy.

ii. **Multipoint connection:** In this method, three or more devices are connected to the same line. This means it has a single communication channel that is shared by all the computers on the network.

It uses communication channel more efficiently and reduces the amount of inter cabling needed, thus lowering the cost.

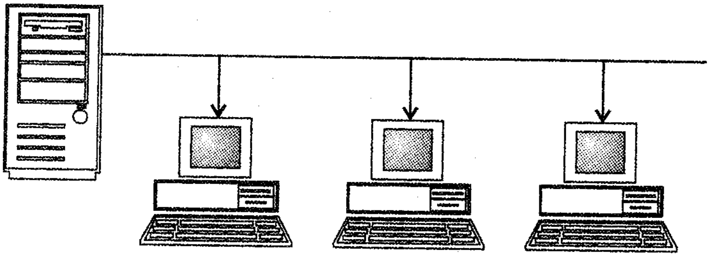


Figure 1.16: Multipoint connection

▶ Comparison of Broadcast and Point to Point Networks

Broadcast Network

2

Apr. 12, Oct. 11 – *5M*
Compare broadcast and point to point networks.

Broadcast networking refers to a type of networking that is done on shared-media networks such as Ethernet where multiple nodes are attached to the same LAN. It is a one-to-many method of transmitting information. All the devices attached to the network that receive the broadcast are part of the same broadcast domain.

A transmission on a broadcast network consists of frames that include the MAC (Medium Access Control) address of the destination node. Network interface cards have built-in MAC addresses that are programmed at the factory. A sender puts the destination system MAC address in a frame and transmits it on the network. Each node listens to traffic on the network and reads the destination address in the frames. If a node receives a frame that has been addressed to it, it accepts the frame. Other nodes ignore the frame. There is also a *broadcast address* that is used to address frames to every node on the network.

Applications that produce broadcast messages include ARP (used by hosts to locate IP addresses on a network), routing protocols like RIP, and network applications that advertise their services on the network.

Point to Point Network

In point to point network, a *point-to point* link is an unshared connection between two systems. On a point-to-point link, there is no contention for the cable because it connects only the sender and receiver, not a number of shared devices.

A point-to-point network is one of the simplest networks because it only involves two nodes. Each node is connected to the other with one connection line. This is one of the cheapest and most effective network architectures because it doesn't involve the cost of redundancies and it doesn't add the complexity of needing several nodes functioning to make a connection.

However, the point-point-to network is impractical from a networking standpoint because rarely is only one connection between two nodes adequate. The point-to-point network can be compared to two soup cans connected by a string. Although there is nothing to interrupt the connection, there is no ability for the network to branch out and make more connections.

A good example of a point-to-point network is a computer that is connected to a local printer by a USB cable. Although highly reliable, there is no way for either node to connect to anything else using that one USB connection. Also, without any redundancy, the entire connection is dependent on the USB cable as well.

4. Communication Types

Types of Communication
i. Synchronous
ii. Asynchronous

In data communication, timing control of the reception of bits is important. There are two methods of timing control for the reception of bits. *They are:*

5

Apr. 13, Oct. 10 – *5M*
Write a short note on: Modes of Communication

Apr. 2013 – *5M*
Explain Synchronous and Asynchronous communication in detail.

Apr. 2011 – *5M*
Explain Synchronous Transmission.

Oct. 2010 – *5M*
Explain Synchronous Communication in detail.

4.1 Synchronous Transmission

In this type of transmission blocks of characters are transmitted in timed sequences.

It is carried out under the control of a common master clock. Here the transmitted bits are synchronized to a reference clock.

No start and stop bits are used, instead the bytes are transmitted as a block in a continuous stream of bits, as shown in *figure 1.17.*

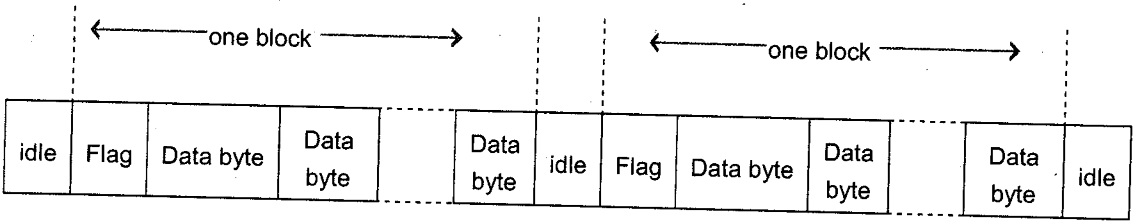


Figure 1.17: Synchronous transmission

The receivers operate at exactly the same clock frequency as that of transmitter.

This is essential for error free reception of data. Flag is a sequence of fixed number of bits which is prefixed to each block as shown in *figure 1.17*. Flag is useful in identifying the start of a block.

Here the bit stream to be transmitted is combined into longer 'frames' which may contain more than one byte.

There is no gap between it and the next one.

▶ Block Diagram of Synchronous Transmission

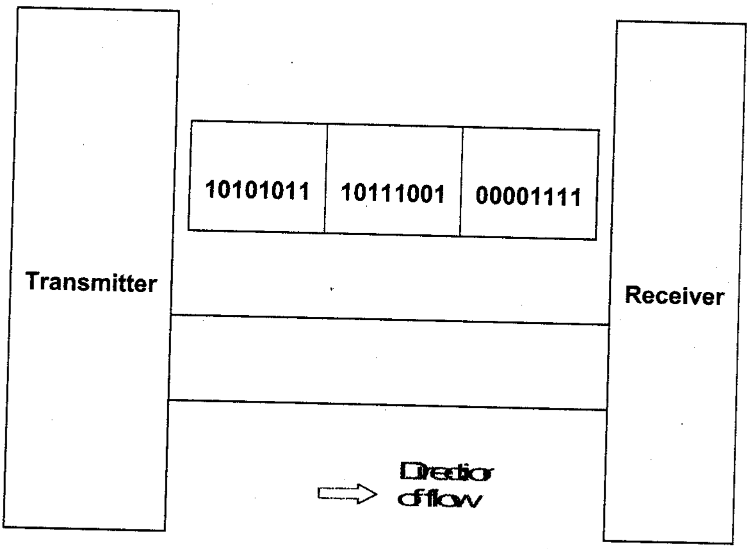


Figure 1.18

▶ Advantages

i. Speed is increased.

ii. Due to the absence of gaps between the data units and absence of start and stop bits.

a. Start and stop bits are not needed.

b. Timing errors are reduced due to synchronization.

▶ Disadvantages

i. The timing is very important.

ii. The transmitter and receiver have to operate at same clock frequency.

4.2 Asynchronous Transmission

In this transmission system, one character is sent at a time.

The transfer of data is controlled by start bit and stop bit.

Each character is surrounded by bits that signal the beginning and end of the character.

The start bit is always '0' and stop bit is always '1'. As shown in *figure 1.19.*

Start Stop

	0	data byte	1	idle time	0	data byte	1	idle time	0	

Figure 1.19: Asynchronous transmission

▶ Block Diagram of Asynchronous Transmission

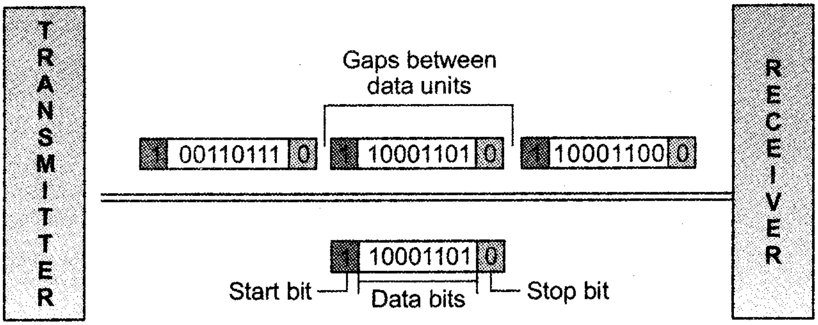


Figure 1.20

▶ Advantages

i. Synchronization between the transmitter and receiver is not necessary.

ii. It is easy to implement.

iii. It is a easy and cheap scheme.

iv. It is an effective scheme.

▶ Disadvantages

i. Additional bits called start and stop bits are required to be used.

ii. It is difficult to determine the sampling instants hence the timing error can take place.

▶ Comparison of Synchronous and Asynchronous Transmission

	Parameter	Asynchronous transmission	Synchronous transmission
i.	Synchronization	Not needed	Needed
ii.	Start and stop bit	Used	Not used
iii.	Gap between data blocks	Present	Absent
iv.	Speed	Low	High
v.	Application	Communication between a computer and keyboard.	Communication between two computers.

▶ Differentiate Synchronous and Asynchronous Communication

1

Oct. 2011 – *5M*
Differentiate synchronous and asynchronous communication.

	Synchronous communication	Asynchronous communication
i.	Synchronous communication is a data transfer method in which a continuous stream of data signal is accompanied by timing signals (generated by an electronic clock) to ensure that the transmitter and the receiver are in step (synchronized) with one another.	Asynchronous communication is transmission of data without the use of an external clock signal, where data can be transmitted intermittently rather than in a steady stream.
ii.	A synchronous operation blocks a process till the operation completes.	An asynchronous operation is non-blocking and only initiates the operation.

iii.	The notion of synchronous operations requires an understanding of what it means for an operation to complete. In the case of remote assignment, both the send and receive is complete when the message has been delivered to the receiver. In the case of remote procedure call, the send, receive, and reply is complete when the result has been delivered to the sender, assuming there is a return value. Otherwise, the send and receive is complete when the procedure finishes execution.	In asynchronous operations, the caller could discover completion by polling, by software interrupt, or by waiting explicitly for completion later. An asynchronous operation needs to return a call/transaction id if the application needs to be later notified about the operation. At notification time, this id would be placed in some global location or passed as an argument to a handler or wait call.
iv.	Hardware is more expensive.	Cheap, timing is not as critical as for synchronous transmission, therefore hardware can be made cheaper.
v.	Slightly more complex.	Simple, doesn't require synchronization of both communication sides.

5. Modes of Communication

Based on whether the system communicates only in one direction or otherwise, the communication systems are classified as,

1

Oct. 2011 – *5M*
Define following:
i. Simplex
ii. Half Duplex
iii. Full Duplex
iv. Computer Network
v. Gateways

i. **Simplex system:** In simplex mode, the communication is unidirectional, as on a one way street. Only one of the two devices on a link can transmit, the other can only receive.

Examples are TV and radio broadcasting, pager, keyboard and traditional monitors are also simplex devices.

In simplex signals are sent in only one direction.

Not used in true networks because stations on a network generally needs communication both ways.

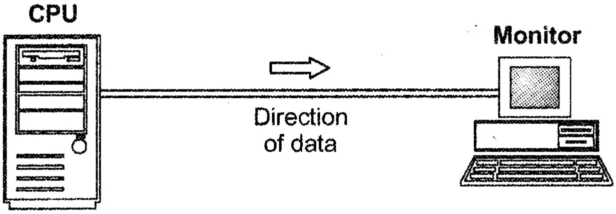


Figure 1.21: Simplex system

ii. **Half duplex system:** Each station can both transmit and receive, but not at the same time (not simultaneously).

Both end devices can send and receive but not simultaneously. When one device is sending, the other can only receive and vice versa. The entire capacity of a channel is taken over by device which is transmitting at that time.

For example, Walkie-talkie, Communication through traditional Ethernet networks.

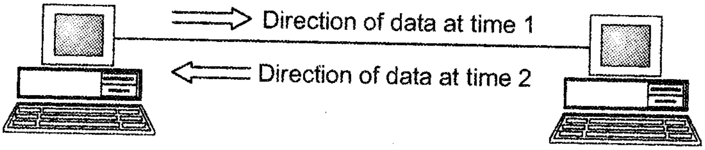


Figure 1.22: Half duplex system

iii. **Full duplex system:** In this mode, both stations can transmit as well as receive simultaneously. It is like a two way street with traffic flowing in both directions at the same time. In this mode, signal going in either direction share the capacity of the link.

Sharing can be done in two ways:

- Link must contain two physically separate transmission paths, one for sending and other for receiving.
- Capacity of channel is divided between signals traveling in both directions.

Examples, telephone networks

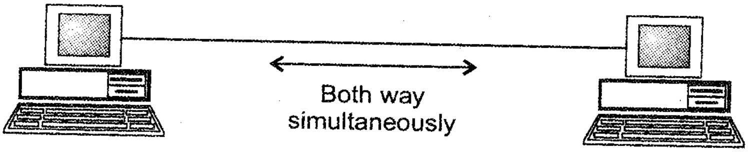


Figure 1.23: Full duplex system

6. Types of Network

There are two major types of network systems. They are as follows:

i. Peer to Peer LAN's

ii. Client/Server LAN's

6.1 Peer to Peer LAN's

It allows users to share resources and files located on their computers and to access shared resources found on other computers.

However, they do not have a file server or a centralized management source, as shown in *figure 1.24.*

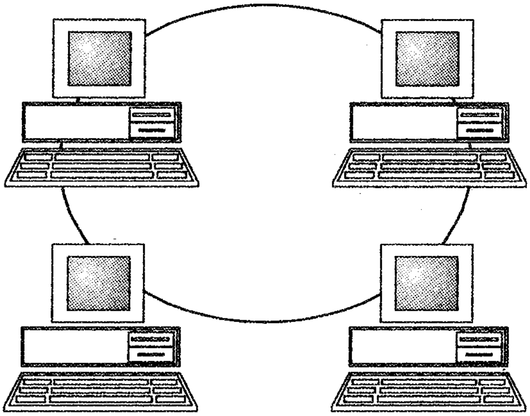


Figure 1.24: Peer to peer network

i. In peer to peer network, all computers are considered equal, they all have the same abilities to use the resources available on the network.

ii. Peer to peer networks are designed primarily for small to medium local area networks.

iii. In peer to peer network, there are no dedicated servers or hierarchy among the computer.

Peer to peer networks are good choices for environments where:

a. There are fewer than 10 users.

b. The users are all located in the same general area.

c. Security is not an issue.

d. The organization and the network will have limited growth future.

▶ Advantages

i. Easy set up and lower cost.

ii. No extra investment in server hardware or software is required.

iii. No network administrator is required.

iv. Ability of users to control resource sharing.

▶ Disadvantages

i. Lack of centralization

ii. Does not provide the security available on a client/ server network.

iii. Users are supposed to manage their own computers.

6.2 Client server LAN's

3

Apr. 2012 – *5M*
Explain server based LANs and peer to peer LANs.

Apr. 11, Oct. 10 – *5M*
Write a short note on: Server based and Peer-to-peer LANs.

i. It allows the network to centralize functions and applications in or more dedicated file servers, as shown in *figure 1.25.*

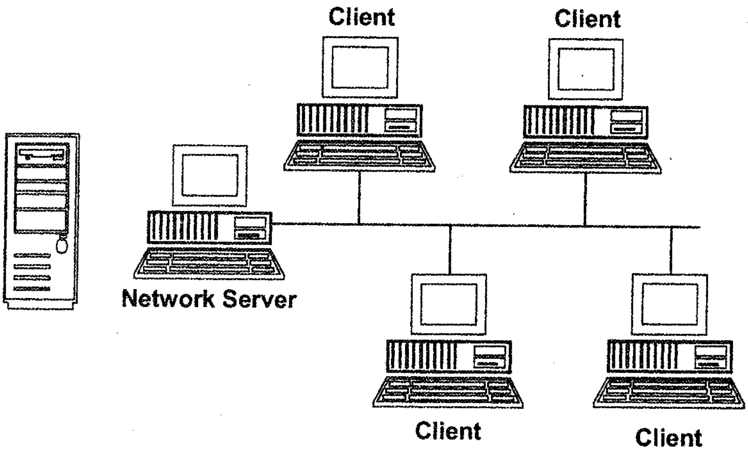


Figure 1.25: Client / server network

ii. The server becomes the heart of the system, providing access to the resources and providing security.

iii. Each client has access to the resources available on the server.

iv. The network operating system provides the mechanism to integrate all the components of the network and allows multiple users to share the same resources simultaneously.

v. In client/server computing, processes are divided between the client and the server. This relationship is based on a series of requests and responses.

Client: Requests services or information from another computer/server.

Server: Responds to the clients request by sending the result of the request back to the client computer.

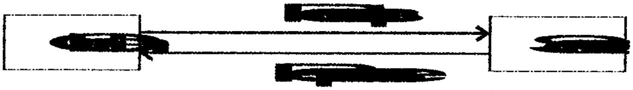


Figure 1.26: Communication of client with server

a. In a client/server setting, the client's computer runs a software application called as a client program. This software allows a computer to act as a client. The client program:

1. Enables the user to send a request for information to the server.
2. Formats the request so that the server can understand it.
3. Formats the response from the server in a way that the user can read.

b. In client/server setting, the server runs a software application called as server program. This software allows a computer to act as a server.

The server program:

1. Receives a request from a client and processes the request.
2. Responds by sending the requested information back to the client.

▶ Comparison between Peer to Peer versus Client Server Networks

	Peer to peer networks	Client server networks
i.	Each PC is an equal participant on the network.	One PC acts as the Network controller.
ii.	Access to the network is not centrally controlled.	Network access and security are centrally controlled.
iii.	Can operate on a basic PC operating system.	Needs a special operating system.
iv.	Less expensive.	More expensive.
v.	Are generally simpler.	Are generally more complex but give the user more control.
vi.	Size of network is good for 10 or fewer computers.	Size of network is limited only by server and network hardware.

vii.	Any time the network can be established.	Initial planning is required for network established.
viii.	It tends to overburden user workstations by having them play the role of server to other users.	It allows user workstations to function as unburdened clients.
ix.	It is unable to provide system-wide services since the typical workstation will run a standard desktop operating system incapable of hosting any major service (e.g., a post office).	It can provide sophisticated system-wide services.
x.	A peer-to-peer network is often a reasonable choice in a home network or other environment where significant growth in numbers of users or quantity of computer-based work is not expected, where security is not a serious concern, and where there is little or no need for major system-wide services.	The client-server architecture is usually the correct choice, even in a small business, where growth is anticipated, security matters, and sophisticated server-based services will be beneficial to productivity.

7. Protocols and Standards

7.1 Protocols

A protocol is a set of rules that governs the communication between computers on a network. A protocol is a set of rules and conventions. These rules include guidelines that regulate the following characteristics of a network access method, allowed physical topologies, types of cabling and speed of data transfer. It is very important for networking that without a protocol, network is meaningless. The sender and the receiver, the two parties in data communication must agree on a common set of rules, i.e., protocols before they can communicate with each other. Protocol defines, What is communicated? How is it communicated? And when is it communicated?

Key elements of the protocols are:

i. **Syntax:** Syntax refers to the structure or the format of the data, meaning the order in which they are presented. *For example*, a simple protocol might expect the first 8 bits to be the address of sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

ii. **Semantics:** Semantics means the meanings of each section of bits, or how to interpret a particular pattern. It also gives the information about what action is to be taken based on the interpretation. e.g. The semantics could define that if the last two bits of the receivers address field contain a 00, it means that the sender and the receiver are on the same network.

iii. **Timing:** Timing refers to the arrangement between the sender and the receiver about the data transmission rates and duration.

The purpose of a network is to exchange information among computers, and protocols are the rules by which computers communicate. Let us consider a general example that clears the idea about protocol.

Let us assume that railway stations are nodes just like computers in the computer network.

Railway tracks is the communication path just like seven layers of OSI model (we will see this in unit 2). Suppose someone wants to go from one station to another he will go in correct railway train to go to his destination station. So just like a railway train, which carries passenger, protocol is a communication media, which carries or exchanges data among computers.

Definition

A protocol is a set of rules for communication or sending information over a network as shown in *figure 1.27.*

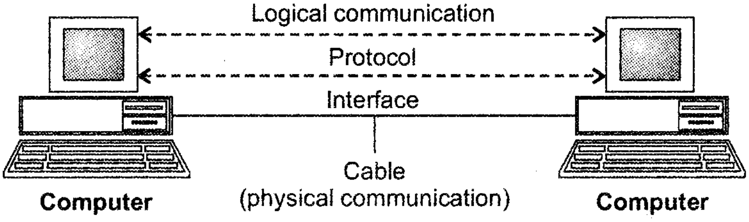


Figure 1.27: Protocols - logical communication

▶ The Function of Protocols

Protocols are rules and procedure for communicating. The following points have to be kept in mind when thinking about protocols:

i. For a computer network, there is not a single protocol, there are many protocols. While each protocol allows basic communication, they have different purposes and accomplish different tasks. Each protocol has its own advantages and restrictions.

ii. Some protocols work, the layer at which a protocol works describes its function.

iii. Several protocols may work together in what is known as a protocol stack or suite.

▶ How Protocols Work?

The entire technical operation of transmitting data over the network has to be broken down into discrete systematic steps. At each step, certain actions take place which cannot take place at any other step. Each step has its own rules and procedures, or protocol.

i. **The sending computer:** At the sending computer, the protocol

a. Breaks the data into smaller sections, called packets that the protocol can handle.

b. Adds addressing information to the packets so the destination computer on the network will know that the data belongs to it.

c. Prepares the data for actual transmission through the network adapter card and out onto the network cable.

ii. **The receiving computer:** At the receiving computer a protocol carries out the same series of steps in reverse order. The receiving computer

a. Takes the data packets of the cable.

b. Brings the data packets into the computer adapter card.

c. Strips the data packets of all the transmitting information added by the sending computer.

d. Copies the data from the packets to a buffer for reassembly.

e. Passes the reassembled data to the application in a usable form.

Both the sending and the receiving computers need to perform each step the same way so that the data will look same when it is received as it did when it was sent.

▶ Protocol Stacks

A protocol stack is a combination of protocols. Each layer specifies a different protocol for handling a function or subsystem of the communication process. Each layer has its own set of rules.

Application Layer	Initiates a request or accepts a request.
Presentation Layer	Adds formatting, display and encryption information to packet.
Session Layer	Adds traffic flow information to determine when the packet gets sent.
Transport Layer	Adds error-handling information.
Network Layer	Sequencing and address information is added to the packet.
Datalink Layer	Adds error-checking information and prepares data for giving on to the physical connection.
Physical Layer	Packet sent as a bit stream.

Figure 1.28: The OSI model showing the layer of protocols

7.2 Standards

Standards are essential for maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunication technology and processes.

3

Oct. 12, 11, 10 – *5M*
Write note on Protocols and Standards.

Standards provide guidelines to manufacturers, vendors, government agencies and other service providers to ensure the kind of interconnectivity necessary in todays market place and in international communication.

Data communications standards can be classified into two types:

i. **Defacto standards:** Defacto standards that have not been approved by an organized body, but have been adopted as standards through widespread use. These standards are often established originally by the manufacturer.

Defacto standard is further divided into proprietary and non- proprietary standards. The proprietary standards are invented and owned by an organization who first uses them, and which gain popularity. It is closed, because they close-off communication with devices/systems of other vendors.

Non-proprietary standards are those that are developed by an organization/ committee/group, which become popular and vendors start supporting them. These are open because anybody adhering to those automatically gains access to all others following those standards.

ii. **De jure standards:** De jure standards have been legislated by an official body. These are usually led by governments or government-appointed agencies.

▶ Standard Stack

In computer industry, there are several stacks as standard protocol models. Following are some of the most important standard protocol models.

i. ISO/OSF protocol suite

ii. IBM systems network architecture

iii. Digital DEC net

iv. Novell Netware

v. Apple Talk

vi. Internet protocol suite, TCP/IP.

PU Questions

5 Marks

[Apr. 2013 – *5M*] 1. Explain Synchronous and Asynchronous communication in detail.

[Apr. 2013 – *5M*] 2. Define Computer Network. State any goals and applications of Computer Network.

[Apr. 13, Oct. 10 – *5M*] 3. Write a short note on Modes of Communication.

[Oct. 2012 – *5M*] 4. Define following:

i. Repeaters ii. Topology iii. Broadcasting
iv. Half duplex v. Simplex

[Oct. 2012 – *5M*] 5. Explain IEEE 802.3 (Ethernet) in detail.

[Oct. 2012 – *5M*] 6. Explain Star and Mesh Topology with its advantages and disadvantages.

[Oct. 2012 – *5M*] 7. Write short notes on Acynchronous communication.

[Oct. 2012, 2011 – *5M*] 8. Write a note on protocols and standards.

[Oct. 12, Apr. 10 – *5M*] 9. Define Network. What are the types of Network? Explain.

[Apr. 2012 – *5M*] 10. Explain the goals and applications of computer networks.

[Apr. 2012 – *5M*] 11. Explain server based LANs and peer to peer LANs.

[Apr. 2012 – *5M*] 12. Write short notes on Synchronous communication.

[Apr. 12, Oct. 11 – *5M*] 13. Compare broadcast and point to point networks.

[Apr. 12, Oct. 11 – *5M*] 14. Write a note on network topologies.

[Oct. 2011 – *5M*] 15. Differentiate synchronous and asynchronous communication.

[Oct. 2011 – *5M*] 16. Define following: i. Simplex ii. Half Duplex
iii. Full Duplex iv. Computer Network
vi. Gateways

[Oct. 11, Apr. 10 – *5M*] 17. Define topology. Explain its various types.

[Oct. 2011 – *5M*] 18. List various goals of Networking.

[Apr. 2011 – *5M*] 19. Explain Goals and Applications of Computer Networks.

[Apr. 2011 – *5M*] 20. Explain Network Classification.

[Apr. 2011 – *5M*] 21. Explain Synchronous Transmission.

[Apr. 2011 – *5M*] 22. What is Topology? Explain its types.

[Apr. 11, Oct. 10 – *5M*] 23. Write a short note on Server based and Peer-to-peer LANs.

[Oct. 2010 – *5M*] 24. Define Network Topology. List different types of topologies. Explain any one in detail.

[Oct. 2010 – *5M*] 25. Write note on Protocols and Standards.

[Oct. 2010 – *5M*] 26. Explain Synchronous Communication in detail.

Chapter 2

NETWORK MODELS

1. Introduction

Network's architecture can be described in two ways: peer to peer and client server. A peer to peer network is a grouping of personal computers that all share information between each other. Peer to peer networks usually comprise of less than ten computers. Designing the architecture of a system requires a model. A model helps in visualizing and understanding the structure of the system.

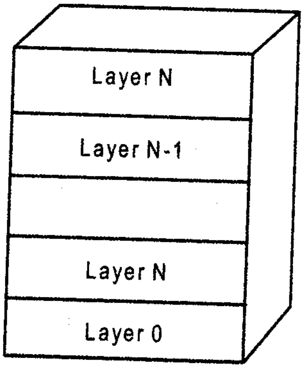


Figure 2.1: Layered architecture of a computer network

Each layer has an active element, a piece of hardware or software, which carries out the layer functions. It is called layer entity.

2. Design Issues of the Layer

2

Apr. 2012, 2011 – *5M*
What are the design issues of the layer?

i. There should be a mechanism for identifying senders and receivers. Since a network has many computers, some form of addressing is needed in order to identify machines.

ii. Another design issue is the rules for data transfer. In some cases, data transfer is simplex, in others it may be half duplex or full duplex.

iii. Since the physical channels are imperfect, error control is very important. Both ends must agree upon the error detecting and correcting methods to be used. Moreover, the receiver must have some way of telling the sender which messages have been received correctly and which have not.

iv. In some communication channels, the messages are not delivered in the same order that they are sent. So, some provisions have to be made so that the receiver can put them back in order. One scheme is to have sequence numbers.

v. Flow control is another design issue. A fast sender should not be allowed to swap a slow receiver with data. Therefore, some form of feedback from the receiver is needed.

vi. When the message is very long, it cannot be accepted by all processors. Thus, there should be mechanisms to disassemble, transmit and then reassemble the long messages.

On the other hand, if the data units are very small, it is inefficient to transmit them separately. Here, several small messages to the same destination are gathered into a single message, transmitted and then separated at the other end.

vii. Multiplexing and demultiplexing needs to be done to share a single communication channel among several unrelated conversations. This is required if it is expensive or inconvenient to set up a separate connection for each pair of communicating processes.

viii. Routing is another design issue, when there exist multiple paths from source to destination.

3. Protocol Hierarchies

To reduce the design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layer, shielding those layers from the details of how the offered services are actually implemented. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.

The fundamental idea is that a particular piece of software/hardware provides a service to its users but keeps the details of its internal state and algorithms hidden from them.

Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in these conversations are collectively known as layer n protocol. Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.

A five-layer network is illustrated in *figure 2.2*.

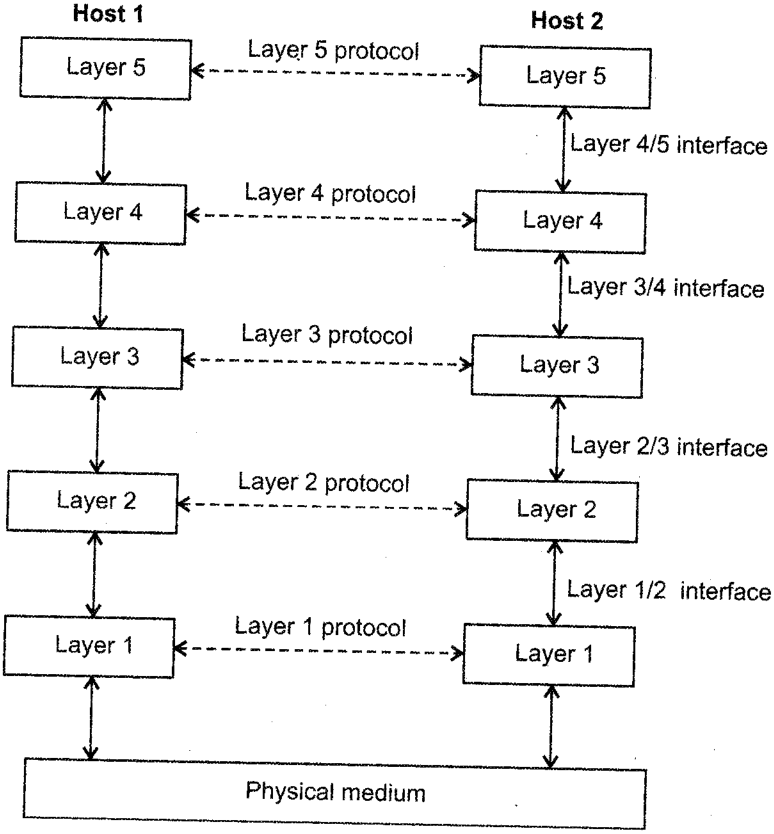


Figure 2.2: Layers, protocols and interfaces

In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each layer passes data and control information to the layer immediately below it until the lowest layer is reached. Between each pair there is an interface which defines which primitive operations and services the lower layer makes available to the upper one.

4. ISO-OSI Reference Model

Actually all networks in use today are based on the Open System Interconnection (OSI) standard. OSI was developed by the International Organization for Standardization (ISO), a global federation of national standards organizations representing approximately 130 countries.

The OSI reference model is the hierarchical structure of seven layers that defines the requirements for communication between two computers. The model was defined by the international standards organization. It was conceived to allows interoperability across the various platforms offered by vendors. The model allow all network elements to operate together, regardless of who built them. By the late 1970's ISO was recommending the implementation of the OSI model as a networking standard, unfortunately, TCP/IP had been in use for years.

The OSI model was created with the following principles in mind:

i. A layer should be created where a different level of abstraction is necessary, so that each layer can perform a well defined function.

ii. Function of each layer should confirm to the internationally standardized protocols.

iii. Layer boundaries should be such that minimum information flows across the interfaces. Also the number of layers should not be so large that distinct functions have to be thrown together in the same layer out of necessity and at the same time it should not be very small for the architecture to become useless after a certain time period.

Following points summarize the OSI model:

a. The OSI is a model consisting of seven layers such as

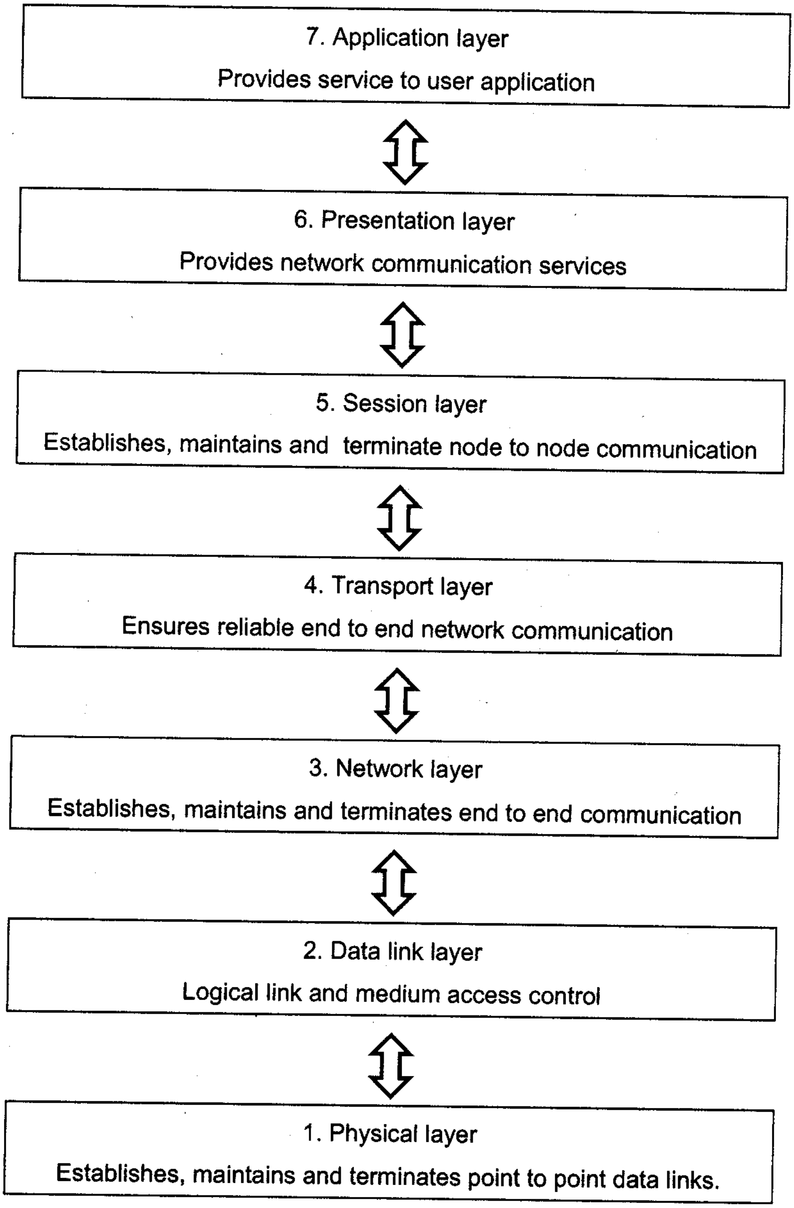
- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data link layer
- Physical layer

b. The OSI model is a model consisting of seven layers and it is used for the communication between two computers.

c. OSI model organizes communication protocols into seven layers and each layer is used to perform specific functions.

Layers in the OSI Model

The OSI is a model consisting of 7 layers as shown below:



7. Application layer

Provides service to user application

6. Presentation layer

Provides network communication services

5. Session layer

Establishes, maintains and terminate node to node communication

4. Transport layer

Ensures reliable end to end network communication

3. Network layer

Establishes, maintains and terminates end to end communication

2. Data link layer

Logical link and medium access control

1. Physical layer

Establishes, maintains and terminates point to point data links.

Figure 2.3: OSI model

▶ Functions of Layers of ISO-OSI Model

Level	Name of the layer	Functions
1	Physical layer	Make and break connections, define voltages and data rates, convert data bits into electrical signal. Decide whether transmission is simplex, half duplex or full duplex.
2	Data link layer	Synchronization, error detection and correction. To assemble outgoing messages into frames.
3	Network layer	Routing of the signals, divide the outgoing message into packets, to act as network controller for routing data.
4	Transport layer	Decides whether transmission should be parallel or single path, multiplexing, splitting or segmenting the data, to break data into smaller units for efficient handling.
5	Session layer	To manage and synchronize conversation between two systems. It controls logging ON or OFF, user identification, billing and session management.
6	Presentation layer	It works as a translating layer.
7	Application layer	Retransferring files of information, login, password checking etc.

▶ Functions of Different Layers

2

Oct. 2012 – *5M*
What are the functions of each layer in ISO/OSI Reference Model?

Oct. 2011 – *5M*
Draw ISO/OSI Model and state functions of each layer.

Layer 1: The Physical Layer

Defines network transmission media, signaling methods, synchronization architecture and cabling topologies. Defines how Network Interface Cards (NICs) interact with the media (cabling).

Functions of physical layer are as follows:

i. To activate, maintain and deactivate the physical connection.

ii. To define voltages and data rates needed for transmission.

iii. To convert the digital bits into electrical signal.

iv. To decide whether the transmission is simplex, half duplex or full duplex.

Layer 2: Data Link Layer

i. Specifies how data bits are grouped into frames and specifies frame formats.

ii. Responsible for error correction, flow control, hardware addressing and how devices such as hubs, bridges, repeaters etc operates.

iii. The project 820 specifications divides this layer into two sublayers.

a. MAC (Media Access Control): MAC deals with network access and network control.

b. LLC (Logical Link Control): LIC operates above MAC and is concerned with sending and receiving the user message.

iv. It establishes and maintains links between communicating devices.

Layer 3: **Network Layer:** Defines logical host addresses, creates packet headers, and routes packets across an internetwork using routers and switches. Strips the headers from the packets at the receiving end. This layer is responsible for the entire route of a packet, from source to destination.

Functions of network layer are as follows:

i. To route the signals through various channels to the other end.

ii. To act as the network controller by deciding which route data should take.

iii. To divide the outgoing messages into packets and to assemble incoming packets into messages for the higher levels.

Layer 4: **Transport Layer:** Sequences packets so that they can be reassembled at the destination in the proper order. Generates acknowledgements and retransmits packets. Assembles packets after they are received. If a duplicate packet arrives, the transport layer recognizes it as duplicate and discards it.

Functions of transport layer are as follows:

i. It decides if the data transmission should take place on parallel paths or single path.

ii. It does the functions such as multiplexing, splitting or segmenting of the data.

iii. It guarantees transmission of data from one end to the other.

iv. It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.

Layer 5: **Session Layer:** Defines how connections can be established, maintained and terminated. Also performs name resolution functions. This layer enables applications running at two workstations to co-ordinate their communication into a single session.

Functions of session layer are as follows:

i. This layer manages and synchronizes conversations between two different applications. This is the level at which the user will establish system to system connection.

ii. It controls logging ON and OFF, user identification, billing and session management.

iii. In the transmission of data from one system to the other, at the session layer streams of data are marked and resynchronized properly so that the ends of massages are not cut prematurely and data loss is avoided.

iv. It allows process to add check points.

Layer 6: **Presentation Layer:** Translates data to be transmitted by applications into a format suitable for transport over the network.

Functions of presentation layer are as follows:

i. It makes sure that the information is delivered in such a form that the receiving system will understand and use it.

ii. The form and syntax of two communicating systems can be different.

iii. Under such conditions the presentation layer provides the 'translation'.

Layer 7: **Application Layer:** It interfaces user application with network functionality, controls how applications access the network and generates error messages.

Functions of application layers are as follows:

i. It provides services to user applications such as manipulation of information in various ways, retransferring the files of information etc. to the user settling above this layer.

ii. The functions such as LOGIN or password checking are also performed by the application layer.

5. Terminology

5.1 SAP

▶ History of SAP

SAP, started in 1972 by five former IBM employees in Mannheim, Germany, states that it is the world largest inter-enterprise software company and the world's fourth largest independent software supplier, overall.

4

Apr. 2013, 2011, 2010, Oct. 2010 – *5M*
Write short note on SAP.

The original name for SAP was German:

Systeme, Anwendungen, Produkte, German for 'Systems Applications and Products.' The original SAP idea was to provide customers with the ability to interact with a common corporate database for a comprehensive range of applications. Gradually, the applications have been assembled and today many corporations, including IBM and Microsoft, are using SAP products to run their own businesses.

SAP applications built around their latest R/3 system, provides the capability to manage financial, asset and cost accounting, production operations and materials, personnel, plants and archived documents. The R/3 system runs on a number of platforms including windows 2000 and uses the client/server model. The latest version of R/3 includes a comprehensive internet-enabled package.

▶ What is SAP?

SAP is the leading enterprise information and management package worldwide. Use of this package makes it possible to track and manage, in real time, sales, production, finance, accounting and human resources in an enterprise.

▶ SAP Application Modules

SAP has several layers. The basic system is the heart of the data operations and should be not evident to higher level or managerial users. Other customizing and implementation tools also exist. The heart of the system from a managers viewpoint are the application modules. All these modules may not be implemented in a typical company but they are all related and are listed below:

i. **FI: Financial Accounting:** Designed for automated management and external reporting of general ledger, accounts receivable, accounts payable and other sub ledger accounts with a user defined chart of accounts. As entries are made relating to sales production and payments journal entries are automatically posted. This connection means that the 'books' are designed to reflect to real situation.

ii. **CO: Controlling:** Represents the company's flow of cost and revenue. It is a management instrument for organizational decisions. It too is automatically updated as events occur.

iii. **AM: Asset Management:** Designed to manage and supervise individual aspects of fixed assets including purchase and sale of assets, depreciation and investment management.

iv. **PS: Project System:** is designed to support the planning, control and monitoring of long term, highly complex projects with defined goals.

v. **WF: Workflow:** links the integrated SAP application modules with cross application technologies, tools and services.

vi. **IS: Industry Solutions:** It combines the SAP application modules and additional industry specific functionality. Special techniques have been developed for industries such as banking, oil and gas, etc.

vii. **HR: Human Resources:** is a complete integrated system for supporting the planning and control of personnel activities.

viii. **PM: Plant Maintenance:** In a complex manufacturing process maintenance means more than sweeping the floors. Equipment must be serviced and rebuilt. These tasks affect the production plans.

ix. **MM: Materials Management:** supports the procurement and inventory functions occurring in day to day business operations.

x. **QM: Quality Management:** is a quality control and information system supporting quality planning, inspection, and control for manufacturing and procurement.

xi. **PP: Production Planning:** is used to plan and control the manufacturing activities of a company. This module includes, bills of material, routings, work centers, sales and operations planning etc.

xii. **SD: Sales and Distribution:** Helps to optimize all the tasks and activities carried out in sales, delivery and billing. Key elements are pre-sales support, inquiry processing, quotation processing, sales order processing, delivery processing, billing and sales information system.

5.2 Connection Oriented Services

In a **connection-oriented network**, there is a guaranteed delivery of data: any data that is not received by the destination system is re-sent by the sending device. Communication between sending and receiving device continues until the transmission has been verified. Because the connection-oriented protocol has higher overhead, it places greater demand on the bandwidth.

It is modeled after the telephone system. To talk to someone, we pick up the phone, dial the number, talk and then hang up.

Similarly, to use a connection oriented network service, the service user first establishes a connection, uses the connection and then releases the connection. The essential aspect of a connection is that it acts like a tube. Here, the sender pushes objects (bits) in at one end, and the receiver takes out at the other end.

▶ Advantages

i. These services provide guaranteed delivery of data.

ii. This service is more reliable than connectionless services.

iii. Some connection-oriented services will monitor for lost packets and handle resending them.

There are two types of connection-oriented services-reliable and unreliable connection-oriented services. In reliable connection-oriented service, it sends acknowledgement signal to each byte of sender.

iv. When receiver gets errorneous bytes. Sender needs to only retransmit that byte.

v. Reliable connection-oriented service is very useful when quality of data is needed of the system, whereas unreliable connection-oriented service is very useful when urgent data is required to the system.

vi. Reliable connection-oriented service is suitable for such environment where quality of data is more important than fast data.

Unreliable connection-oriented service is suitable for such environment where speed of data transfer is more important than quality of the data.

▶ Disadvantages

i. A connection must be required with this before passing the data.

ii. These services have more overhead than connectionless service.

iii. Is a complex method for data transferring.

iv. Reliable connection-oriented service is very time consuming system because if receiver gets errorneous packet, sender needs to retransmit all 1 kilo bytes packet.

v. Reliable connection-oriented service is a lengthy process, spends more cost for confirmation and positive response and speed of data transmission is low.

vi. In unreliable connection-oriented service, retransmission is not allowed, and if channel is noisy then poor quality data is accepted by the receiver.

5.3 Connectionless Services

In **connection less network**, the information sent has no confirmation that data has been received. If there is error in transmission there is no mechanism to resend the data, so transmission by the connectionless is no guarantee that the data is received by the destination. Connectionless communication requires far less overhead than connection oriented communication. It is popular in applications such as streaming audio and video where small number packets might represent a significant problem.

It is modeled after the postal system. Each message (letter) carries the full destination address, and each one is routed through the system independent of all the others.

Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive.

	Service	Example
Connection oriented	Reliable message stream	Sequence of pages.
	Reliable byte stream	Remote login
	unreliable connection	Digitized voice
Connectionless	unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Requested reply	Database query

Figure 2.4: Six different types of services

▶ Advantages

i. Does not require any connection.

ii. This service is very simple and easy for data transfer.

iii. Used for periodic burst data transfer.

iv. Less overhead than connection-oriented services.

Connectionless services are of three types:

a. Unreliable connectionless service

b. Acknowledged datagram connectionless service

c. Request reply connectionless service

v. Unreliable connectionless services has advantages as:

   a. Speed of data transmission is good.

   b. Not time consuming.

   c. It will not send any receipt or acknowledgement signals.

   d. Cost is low.

   e. Physical connection is not required between sender and receiver.

vi. Acknowledged datagram connectionless service has advantages as:

   a. Speed of transmission is good.

   b. Reliable and gives assurance of data transmission.

   c. Quality of data transmission is very good.

   d. Cost of this is low as compared to connection-oriented system.

   e. Physical connection between sender and receiver is not required.

vii. Request-reply connectionless service has advantages as:

   a. Is reliable and gives assurance of data transmission.

   b. Quality of data transmission is good.

   c. Cost is low.

   d. No physical connection between sender and receiver is required.

▶ Disadvantages

i. Less reliable than connection-oriented services.

ii. No guarantee for delivery of data.

iii. It provides minimal services.

iv. Order of data arrival is not sequential.

v. In unreliable connectionless service, retransmission is not allowed.

In acknowledged datagram connectionless service and request - reply connectionless service, retransmission is allowed but it is time consuming.

2

Apr. 13, Oct. 10 – *5M*
What are different advantages and disadvantages of Connection Oriented and Connectionless Oriented Models?

▶ Compare Connection Oriented and Connectionless Services

	Connection oriented services	Connectionless services
i.	It establishes physical link between sender and receiver.	There is no direct physical link between sender and receiver.
ii.	It is time consuming.	It is very fast.
iii.	It provides some level of delivery guarantee.	It does not provide delivery guarantee.
iv.	Maximum time is required in establishing the connection between the sender and receiver.	No time wasting for connection of sender and receiver.
v.	It is a very costly system (expensive).	It is not costly (cheap).
vi.	Bandwidth of physical line is wasted if sender and receivers are not communicated with each other.	Bandwidth of channel is not wasted at all.
vii.	It does not require data sequencing process.	It requires data sequencing algorithms at receiver's side because data does not come sequentially.

1

Apr. 2011 – *5M*
Compare Connection Oriented and Connectionless Services.

5.4 Peer Entities

A five layer network is illustrated in *figure 2.2*. The entities comprising the corresponding layers on different machines are called peers. The peers may be processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol.

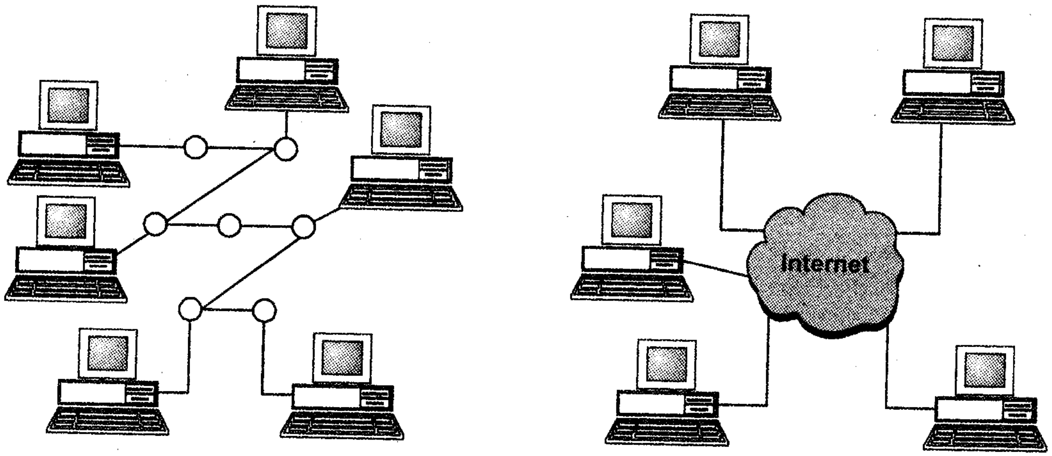
6. Internet Model (TCP/IP)

TCP/IP, a pair of protocol known as transmission control protocol/ internetworking protocol one of the most popular and powerful protocols currently in use. It is the protocol that defines how data transmissions are performed across the Internet.

1

Oct. 2012 – *5M*
Write a short note on TCP/IP Model.

Under TCP/IP, an Internet appears as if it were a single huge network as shown in *figure 2.5*, connecting a wide variety of machines of different sizes and types. Internally the Internet is an interconnection of thousands of independent physical networks.

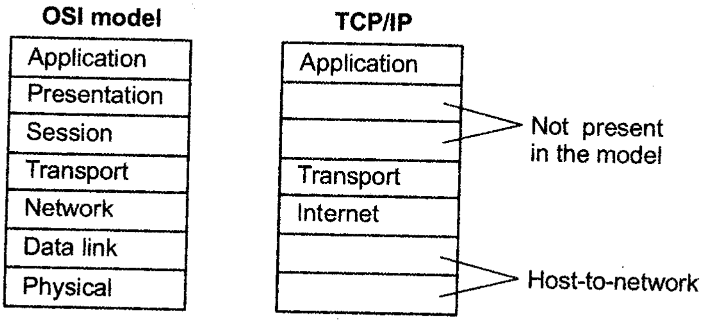


(a) Internet without TCP/IP

(b) Internet under TCP/IP

Figure 2.5: Internet model (TCP/IP)

6.1 Overview of TCP/IP Architecture



OSI model	TCP/IP
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data link	
Physical	

Figure 2.6: TCP/IP reference model

i. Transmission control protocol and Internet Protocol (TCP/IP) was developed by the department of Defence's Projects Research Agency (ARPA, DARPA) under its project on network interconnection.

ii. It is a set of protocols that allow communication across multiple diverse network.

iii. ARPA originally created TCP/IP to connect military networks together, but later on this protocol was also given to government agencies and universities free of cost.

iv. TCP/IP is the most widely used protocol for interconnecting computers and it is the protocol of the Internet.

6.2 OSI Reference Model and TCP/IP

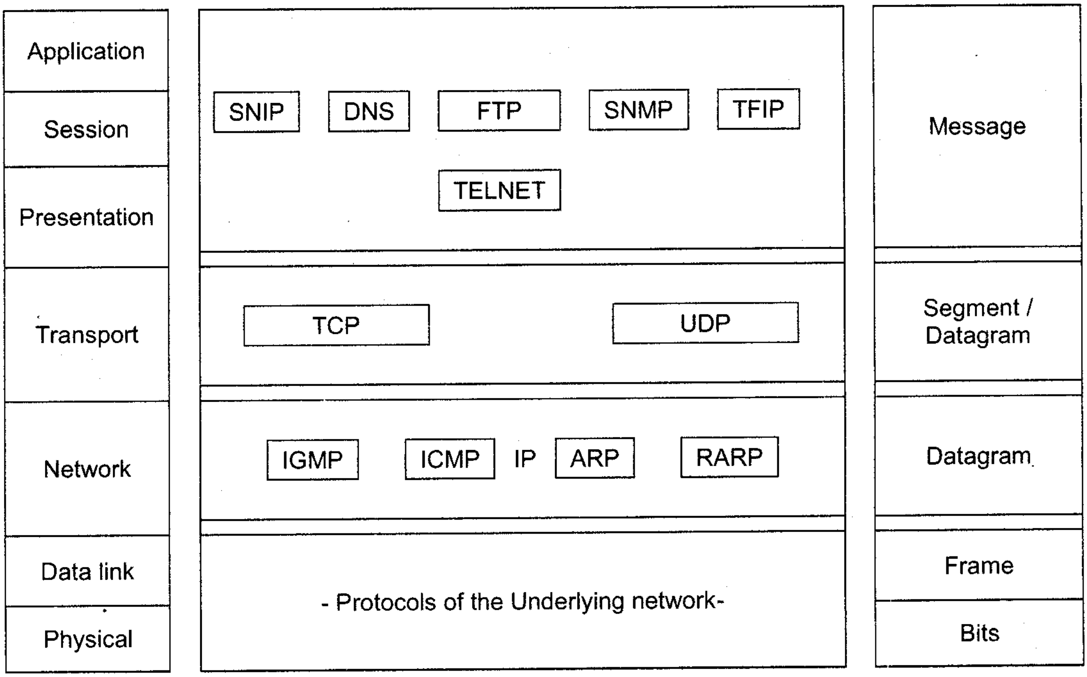


Figure 2.7: Comparison of OSI and TCP/IP

6.3 Layers

TCP/IP consists of five layers, they are:

Layer 1: Physical Layer

i. This is the first layer. This is the only layer in which the actual communication takes place.

ii. All the other layers in the protocol are there to direct and modify the behavior of the physical layer.

iii. This layer defines electrical and mechanical interface between the hosts on the internet.

iv. This includes the cabling system and electrical signaling. TCP/IP has been designed to operate independent of the type of physical and electrical media used.

Layer 2: **Data Link Layer:** The TCP/IP data link layer defines the formatting, framing and sequencing of data placed on the NIC (Network Interface Card).

Layer 3: **Network Layer**

i. The network layer is often referred to as the internet layer or the Internet Protocol (IP) Layer.

ii. The IP provides the basic datagram service of routing packets around the network and is implemented in all computers on internet.

iii. The main task of IP is addressing of computers as well as fragmentation and reassembly of datagrams. IP makes best 'effort' to move data to its destination but it contains no function for end to end message reliability.

Protocols: IP, ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).

Layer 4: **Transport Layer:** The transport layer of TCP/IP ensures reliable and efficient end to end transportation of data between host computers for the layers above it.

Two end to end protocols are defined in this layer:

i. *TCP (Transmission Control Protocol):* TCP is reliable connection-oriented protocol. It ensures end-to-end, error free delivery. It also handles reassembling of packets at the receiver and flow control to ensure that a fast sender does not slow down the receiver.

ii. *UDP (User Datagram Protocol):* Which is an unreliable connectionless protocol. It is mainly used in client-server, request–reply and one shot applications where prompt delivery is more important than accurate delivery.

Layer 5: **Application Layer:** This model does not have a session or presentation layer. The application layer contains all higher-level protocols for commonly required user service like email (SMTP), File Transfer (FTP), Remote Terminal Access (TELNET), Domain Name System (DNS) for mapping host names to network addresses, access to the world wide web (HTTP), etc.

▶ Comparison of OSI and TCP/IP Model

The main similarities between the two models include the following:

i. **They share similar architecture:** Both of the models share a similar architecture. This can be illustrated by the fact that both of them are constructed with layers.

ii. **They share a common application layer:** Both of the models share a common 'application layer'. However in practice this layer includes different services depending upon each model.

iii. **Both models have comparable transport and network layers:** This can be illustrated by the fact that whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.

▶ Differences between ISO-OSI and TCP-IP Reference Models

2

Apr. 13, Oct. 10 – *5M*
Write differences between ISO-OSI and TCP-IP reference Models.

	ISO-OSI reference model	TCP-IP model
i.	ISO-OSI has seven layers.	TCP-IP has four layers.
ii.	Services are clearly mentioned in OSI model.	Services are not clearly mentioned in TCP/IP model.
iii.	OSI model is useful in describing networks, but protocols are too general.	TCP/IP model is weak, but protocols are specific and widely used.
iv.	It is a conceptual model. Designers didn't know what functionality to put in the layers.	It is a practical model. Designers know the functionality of each layer and used in real world networks.
v.	Model is general and easier to replace protocols.	Model is not general, and difficult to replace protocols.
vi.	Model has to adjust when networks do not match the service specifications.	Model need not adjust too much in this scenario.
vii.	Model describes any type of network.	Not useful for describing any other networks, only describes TCP/IP.
viii.	Network layer supports both connection-oriented and connectionless service.	Network layer supports only connectionless service.
ix.	Transport layer supports only connection-oriented service.	Transport layer supports both connection oriented as well as connectionless services.
x.	It is general purpose network and so suitable for all networks.	It is not suitable for all the networks.

7. Addressing

A network address serves as a unique identifier for a computer on a network. When set up correctly, computers can determine the addresses of other computers on the network and use these addresses to send messages to each other.

One of the best known forms of network addressing is the Internet Protocol (IP) address. IP addresses consist of four bytes (32 bits) that uniquely identify all computers on the public Internet.

Another popular form of address is the Media Access Control (MAC) address. MAC addresses are six bytes (48 bits) that manufacturers of network adapters burn into their products to uniquely identify them.

7.1 Types of Addressing

i. **Unicast:** Unicast is a single destination node. It is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver.

   Unicast transmission, in which a packet is sent from a single source to a specified destination, is still the predominant form of transmission on LANs and within the Internet. All LANs (e.g., Ethernet) and IP networks support the unicast transfer mode, and most users are familiar with the standard unicast applications (e.g., http, smtp, ftp and telnet) which employ the TCP transport protocol.

ii. **Broadcast:** Broadcast is used to send information to all nodes on the network. It is the term used to describe communication where a piece of information is sent from one point to all other points. In this case there is just one sender, but the information is sent to all connected receivers.

   Broadcast transmission is supported on most LANs (e.g., ethernet) and may be used to send the same message to all computers on the LAN (e.g., the Address Resolution Protocol (ARP) uses this to send an address resolution query to all computers on a LAN). Network layer protocols (such as IPv4) also support a form of broadcast that allows the same packet to be sent to every system in a logical network (in IPv4 this consists of the IP network ID and an all 1's host number).

iii. **Multicast:** Multicast is used to send information to some subnet of nodes on the network. It is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there may be one or more senders, and the information is distributed to a set of receivers (there may be no receivers or any number of receivers).

One example of an application which may use multicast is a video server sending out networked TV channels. Simultaneous delivery of high quality video to each of a large number of delivery platforms will exhaust the capability of even a high bandwidth network with a powerful video clip server.

The multicast mode is useful if a group of clients require a common set of data at the same time, or when the clients are able to receive and store (cache) common data until needed. Where there is a common need for the same data required by a group of clients, multicast transmission may provide significant bandwidth savings (upto 1/N of the bandwidth compared to N separate unicast clients).

7.2 Physical Address

A physical address is a binary number in the form of logical high and low states on an address bus that corresponds to a particular cell of primary storage(also called main memory) or to a particular register in a memory-mapped I/O (Input/Output) device. Frames need to be transmitted to different systems on a network. Data link layer adds a HEADER to frames. Header defines the physical address of sender (source address) and receiver address (destination address). Frame is intended for a device outside the network.

7.3 Logical Address

If a packet is going from one network to another, another addressing system is required to help to distinguish source and destination systems. Layer adds header to the data coming from upper layers that among other things include LOGICAL ADDRESS of the sender and receiver.

7.4 Port Address

Port address is a feature of a network device that translates TCP or UDP communications made between a host and port on an outside network. It allows a single IP address to be used for many internal hosts. Port address can automatically modify the IP packets destination or source host IP and port fields belonging to its internal hosts.

▶ Difference of Physical, Logical and Port Address

i. Logical address is IP address which is not fixed and it regularly changes and it depends upon the Network layer.

ii. Physical address is called as MAC address which is fixed for every system and it depends upon the network layer.

iii. Port address is used for each process from client to server and it depends on the transport layer.

8. IP Addressing

An IP address is a binary number that uniquely identifies computers and other devices on a TCP/IP network.

- An IP address is a unique global address for a network interface.
- **An IP address**
  i. is a **32 bit long** identifier
  ii. encodes a network number (**network prefix**) and a **host number**

An IP address can be private - for use on a Local Area Network (LAN) - or public - for use on the Internet or other Wide Area Network (WAN). IP addresses can be determined statically - assigned to a computer by a system administrator - or dynamically - assigned by another device on the network on demand.

An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.

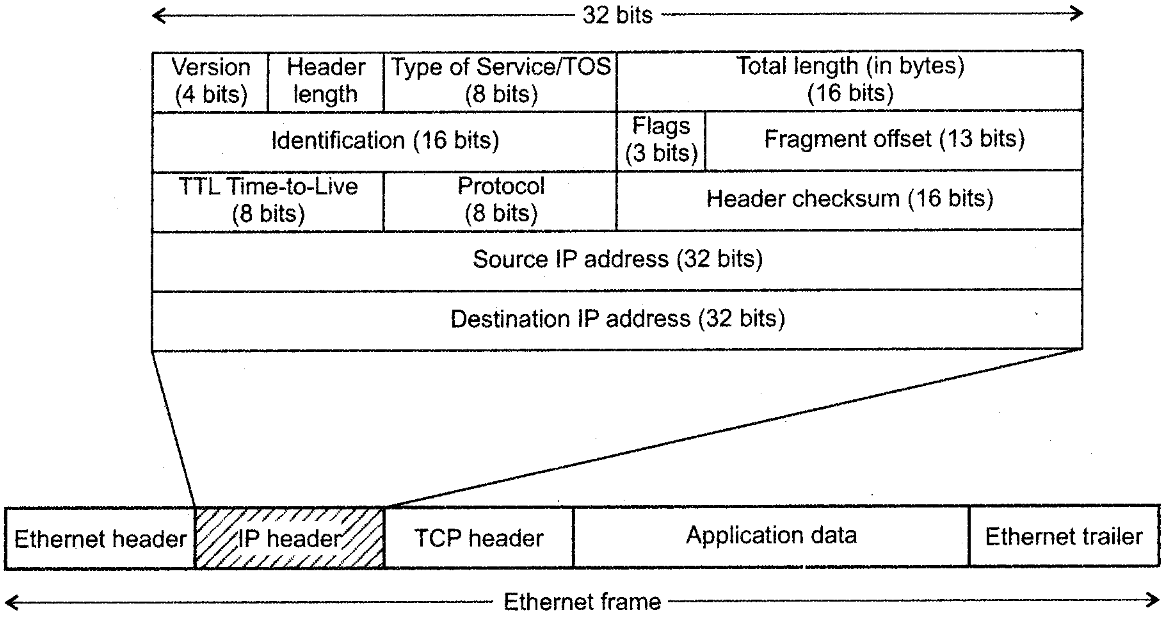

32 bits
Version (4 bits)
Header length
Type of Service/TOS (8 bits)
Total length (in bytes) (16 bits)
Identification (16 bits)
Flags (3 bits)
Fragment offset (13 bits)
TTL Time-to-Live (8 bits)
Protocol (8 bits)
Header checksum (16 bits)
Source IP address (32 bits)
Destination IP address (32 bits)
Ethernet header
IP header
TCP header
Application data
Ethernet trailer
Ethernet frame

Figure 2.8

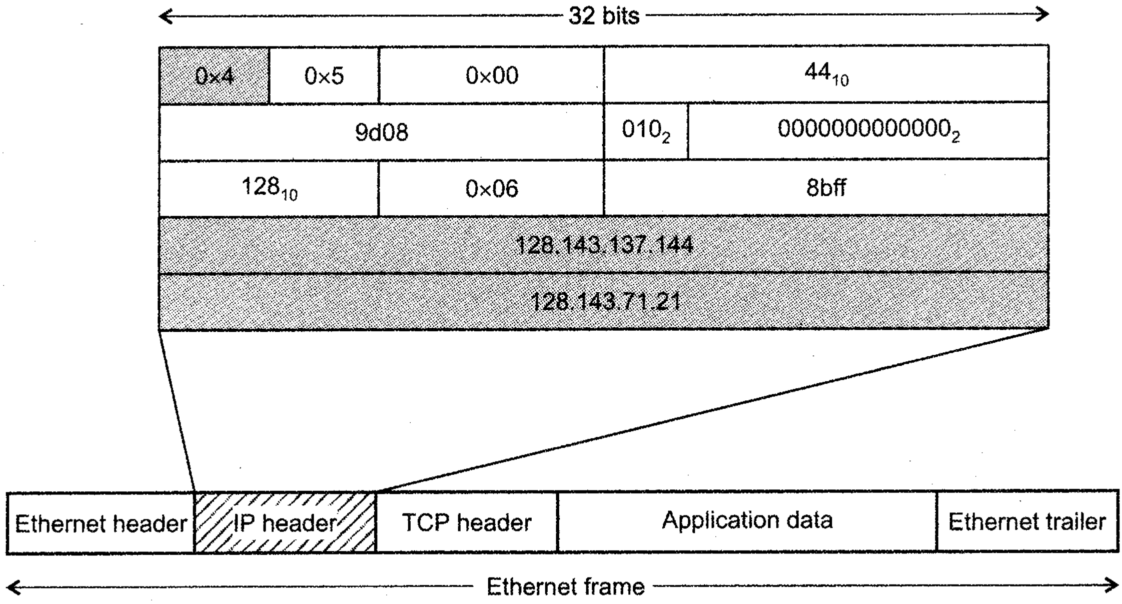


Figure 2.9

8.1 Assigning IP Address

Each device connected to the internet must have a physical address (as specified by NIC), but it must also have an address field that identifies the connection of a host to its network. An internet address has the following format:

Class type	Netid	Hostid

The first byte of IP address defines its class. Different classes have been defined to accommodate different types of organizations. There are five different classes, labeled A-E. Here are the layouts of the address for the five classes of addresses.

It is numerically the lowest. One byte is used to identify the Network ID and the remaining 3 bytes are used to determine the host. It can accommodate a large number of hosts compared to class B and class C. This is due to the reason that class B address provides a two byte host ID field and class C network provides a single byte host ID field.

Class D is reserved for multicast addressing. Multicasting refers to sending the same message to a group of hosts rather than an individual. Broadcasting refers to sending a message to all available hosts. Class E addresses are reserved for further use.

▶ Dotted-decimal Notation

It is difficult to remember and read 32 bit internet address. Hence it is easy and convenient to write the IP address in decimal form with decimal points, separating the bytes. This notation is known as dotted-decimal notation. The following example shows 32 bit pattern of an address and its dotted decimal form.

10000000 00001010 00000101 00001111
128.10.5.15

Hence by looking at first byte of the address in decimal form itself, allows us to determine the class to which the particular addresses belongs. The following *figure* denotes the address range used in different class of networks.

There are 5 classes available:

i. **Class A:** This class of IP addresses starts with binary number 0. The network is identified by the first octet. IP address 127.0.0.1 is a special IP reserved for internal loopback testing.

	From				To			
	Netid	Hostid			Netid	Hostid		
Class A	0	.0	.0	.0	127	.255	.255	.255

ii. **Class B:** This class of IP addresses starts with binary number 10. The network is identified by the first two octet. The network ID is 178.95 where as node ID is 234.23.

From

	Netid		Hostid	
Class B	128	.0	.0	.0

To

Netid		Hostid	
191	.255	.255	.255

iii. **Class C:** The binary number starts with 110. The network is identified by first three octet. The network ID is 210.233.99 whereas node ID is 145.

From

	Netid			Hostid
Class C	192	.0	.0	.0

To

Netid			Hostid
223	.225	.255	.255

iv. **Class D:** The binary digit starts with 1110. These classes of ID's are reserved for multicost purpose.

From

	Group Address			
Class D	224	.0	.0	.0

To

Group Address			
239	.255	.255	.255

v. **Class E:** The binary digit starts with 1111. This class of IP address are reserved for testing purpose and not assigned for public usage.

From

	Undefined			
Class E	240	.0	.0	.0

To

Undefined			
255	.255	.255	.255

Class type	Range	Starts with bit string
A	0 to 127	0
B	128 to 191	1 0
C	192 to 223	1 1 0
D	224 to 239	1 1 1 0
E	240 to 255	1 1 1 1 0

8.2 Automatically Assigned Addresses

There are several IP addresses that are automatically assigned when you setup a home network. These default addresses are what allow your computer and other network devices to communicate and broadcast information over your network.

Most commonly assigned network addresses in a home network are:

192.168.1.0	0 is the automatically assigned network address.
192.168.1.1	1 is the commonly used address used as the gateway.
192.168.1.2	2 is also a commonly used address used for a gateway.
192.168.1.3 – 254	Addresses beyond 3 are assigned to computers and devices on the network.
192.168.1.255	255 is automatically assigned on most networks as the broadcast address.

If you have ever connected to your home network, you should be familiar with the gateway address or 192.168.1.1, which is the address you use to connect to your home network router and change its settings.

8.3 Classful Addressing

All the classes of IP address such that A, B, and C comes in classful. A classful network is a network addressing architecture used in the Internet from 1981 until the introduction of Classless Inter-Domain Routing in 1993. The method divides the address space for Internet Protocol Version 4 (IPv4) into five address classes. Each class, coded in the first four bits of the address, defines either a different network size, i.e. number of hosts for unicast addresses (classes A, B, C), or a multicast network (class D). The fifth class (E) address range is reserved for future or experimental purposes.

In classful addressing, the network address (the first address in the block) is the one that is assigned to the organization. The range of addresses can automatically be inferred from the network address.

There were three address *classes* to choose from: A, B, or C, corresponding to 8-bit, 16-bit, or 24-bit prefixes. No other prefix lengths were allowed, and there was no concept of nesting a group of 24-bit prefixes, *for example,* within a 16-bit prefix.

An address was slotted into one of three address classes based on its high-order bits.

Addresses beginning with 0 were considered class A; addresses beginning 10 were class B; addresses beginning 110 class C. Two other classes were also defined, class D addresses beginning 1110 and class E addresses beginning 1111, though neither of these two address classes were normally used. For humans, the easiest way to distinguish between different address classes is to use the first decimal number in the IP address:

First octet	Address class
0-127	Class A
128-191	Class B
192-223	Class C
224-239	Class D
240-255	Class E

▶ Problems with Classful IP Addresses

The original classful address scheme had a number of problems:

Problem 1: Too few network addresses for large networks

Class A and Class B addresses are gone

Problem 2: Two-layer hierarchy is not appropriate for large networks with Class A and Class B addresses.

Fix #1: Subnetting

Problem 3: **Inflexible.** Assume a company requires 2,000 addresses

Class A and B addresses are overkill

Class C address is insufficient (requires 8 Class C addresses)

Fix #2: Classless Interdomain Routing (CIDR)

Problem 4: **Exploding Routing Tables:** Routing on the backbone Internet needs to have an entry for each network address. In 1993, the size of the routing tables started to outgrow the capacity of routers.

Classless Interdomain Routing (CIDR)

Problem 5: The Internet is going to outgrow the 32-bit addresses.

IP Version 6

▶ Basic Idea of Subnetting

i. Split the host number portion of an IP address into a subnet number and a (smaller) host number.

ii. Result is a 3-layer hierarchy

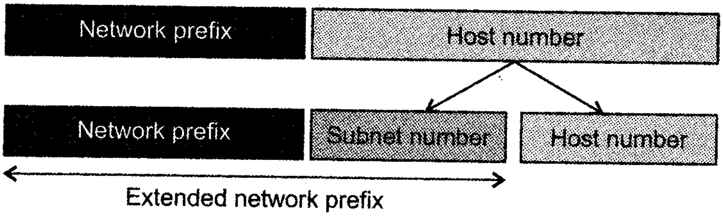


Figure 2.10

Then:

i. Subnets can be freely assigned within the organization.

ii. Internally, subnets are treated as separate networks.

iii. Subnet structure is not visible outside the organization.

Subnet Masks

Routers and hosts use an **extended network prefix (subnet mask)** to identify the start of the host numbers

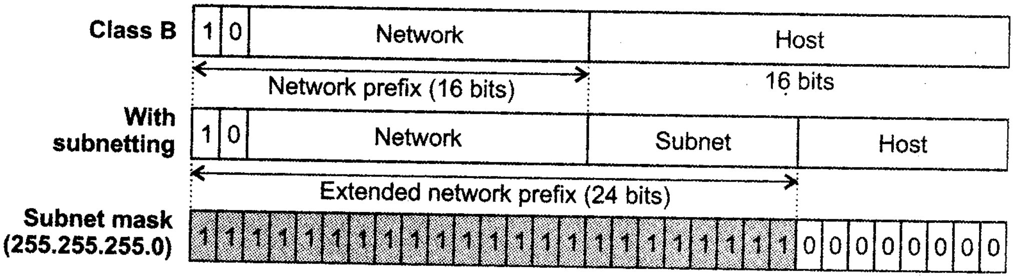


Figure 2.11

ıere are different ways of subnetting. Commonly used netmasks for university networks with 16 ʻefix (Class B) are 255.255.255.0 and 255.255.0.0

Advantages of Subnetting

i. With subnetting, IP addresses use a 3-layer hierarchy:

- Network
- Subnet
- Host

ii. Improves efficiency of IP addresses by not consuming an entire address space for each physical network.

iii. Reduces router complexity. Since external routers do not know about subnetting, the complexity of routing tables at external routers is reduced.

Note

Length of the subnet mask need not be identical at all subnetworks.

8.4 Classless Addressing

As the early internet began to grow dramatically, three main problems arose with the original 'classful' addressing scheme. These difficulties were addressed partially through subnet addressing, which provides more flexibility for the administrators of individual networks on an internet. Subnetting, however, doesn't really tackle the problems in general terms. Some of these issues remain due to the use of classes even with subnets.

All IP addresses other than the above prefix length are called classless. While development began on IP version 6 and its roomy 128-bit addressing system in the mid-1990s, it was recognized that it would take many years before widespread deployment of IPv6 would be possible. In order to extend the life of IP version 4 until the newer IP version 6 could be completed, it was necessary to take a new approach to addressing IPv4 devices. This new system calls for eliminating the notion of address classes entirely, creating a new *classless addressing* scheme sometimes called Classless Inter-Domain Routing (CIDR).

Routing protocol	Routing updates include subnet mask	Supports VLSM	Ability to send supernet routes
Classful	No	No	No
Classless	Yes	Yes	Yes

PU Questions

5 Marks

[Apr. 2013 – 5M] 1. Explain connection oriented and connection less models with advantages and disadvantages.

[Apr. 2013 – 5M] 2. Compare ISO/OSI reference model and TCP/IP.

[Apr.13,11,10,Oct.10 – 5M] 3. Write a short note on SAP.

[Oct. 2012 – 5M] 4. What are the functions of each layer in ISO/OSI Reference Model?

[Oct. 2012 – 5M] 5. Write a short note on TCP/IP Model.

[Apr. 2012 – 5M] 6. What are the functions of following layers in ISO-OSI reference model?

i. Physical Layer ii. Data Link Layer

iii. Network Layer

[Apr. 2012, 2011 – 5M] 7. What are the design issues of the layer?

[Oct. 2011 – 5M] 8. Draw TCP/IP model and state function of each layer.

[Apr. 2011 – 5M] 9. Draw ISO/OSI Model and state functions of each layer.

[Apr. 2011 – 5M] 10. Compare Connection Oriented and Connectionless Services.

[Oct. 2010 – 5M] 11. What are different advantages and disadvantages of Connection Oriented and Connectionless Oriented Models?

[Oct. 2010 – 5M] 12. Write differences between ISO-OSI and TCP-IP reference Models.

[Oct. 2010 – 5M] 13. Write short note on Functions of each layer in ISO-OSI Reference Model.

[Apr. 2010 – 5M] 14. Write down classification of IP Addresses with example.

[Apr. 2010 – 5M] 15. Explain OSI Reference Model.

Chapter 3

TRANSMISSION MEDIA

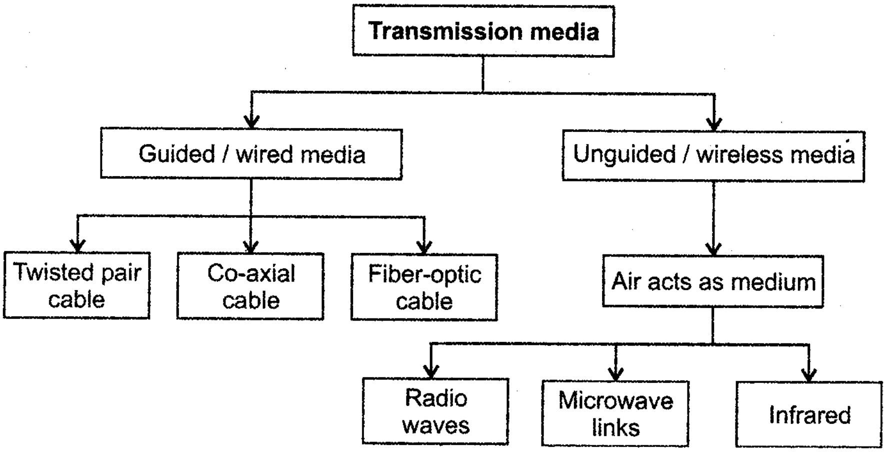
1. Introduction

Transmission media is a medium though which data can be transmitted over long distances. The speed or rate at which data is transmitted over a communication channel is denoted by a parameter called **bandwidth**. Transmission media having higher bandwidths are used now-a-days for better performance. This section introduces the characteristics of various transmission media used for connecting computers.

Different media have different properties and are used in different environments for different purpose. The purposes of the physical layer is to transport a raw bit stream from one computer to another.

2. Classification of Transmission Media

We can classify the transmission media into two categories.



▶ Comparison

	Guided transmission media	Unguided transmission media
i.	Guided indicate, medium is contained within physical boundary.	Unguided medium does not have any Physical boundary.
ii.	Transmission takes place through wire.	It is a wireless transmission.

2.1 Guided Media / Wired Transmission

Guided Media is a communication Medium which allows the data to get guided along it. For this the media needs to have a point to point physical connection.

In this type of media, the signal energy is contained and guided within a solid media. The examples of wired media are copper pair wires, coaxial cables and fiber optic cables.

▶ Types of Wired Media

Types of Wired Media
i. Co-axial cable
ii. Twisted pair cable
iii. Fiber optic cable

i. Co-axial cable

The common transmission medium is the coaxial cable (called as coax). The name 'coax' comes from its two-conductor construction in which the conductors run concentrically with each other along the axis of the cable. This has been largely replaced by twisted pair cabling for local area network installations within buildings and by fiber optic cabling for high speed network backbones. It supports both analog and digital signal.

1
Oct. 2011 – *5M*
Write a short note on coaxial cable.

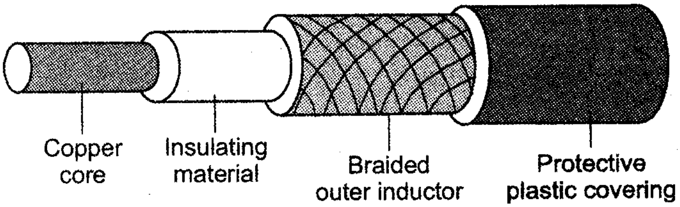


Figure 3.1: Co-axial cable

Physical description

a. The construction of co-axial cable is as shown in *figure 3.1.* It consists of two concentric conductors separated by a dielectric material.

b. A co-axial cable consists of a stiff copper wire as the core, this is surrounded by an insulating material.

c. The insulator is encased by a cylindrical conductor, often as a closely woven braided mesh.

d. The outer conductor is then covered in a protective plastic sheath.

e. The construction of the co-axial cable gives it a good combination of high bandwidth and excellent noise immunity.

f. Higher data rates are possible on shorter cables.

g. It is available for either baseband or broadband transmission.

   1. *Baseband:* Baseband transmission passes digital signals from one workstation to next upto distances of 13,000 feet at speed of 10 mb/sec.

2. *Broadband:* Broadband transmission passes voice, video and other data signals and hence is commonly used for television transmission. It passes signals upto a distance of 36 miles at a speed of around 5 mb/sec.

   1 mile = 1.61 km

   1 mile = 4991 feet

   Several coaxial cable standards are used in computer networking. The most common types meet one of the following ohm and size standards:

   - 75 ohm RG - 6 (used for satellite TV)
   - 50 ohm RG - 8 and RG - 11 (used in thick Ethernet specifications)
   - 50 ohm RG - 58 (used in thin Ethernet specifications)
   - 75 ohm RG - 59 (used for cable TV and cable modems)
   - 93 ohm RG - 62 (used for ARC net specifications)

Performance

The attenuation is much higher in coaxial cables than twisted pair cable. In other words, although co-axial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Applications

a. Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals.

b. Cable TV networks also use coaxial cables.

c. It is used in traditional ethernet LANS.

Connector for coaxial cable

a. Coaxial cable is an important type of guided transmission media. It has higher bandwidth as compared to that of twisted pair cable.

b. To connect coaxial cable to a device, we need coaxial cable connector.

c. The most common type of connector used for coaxial cables is the Bayone-Neill Concelman or BNC connectors.

   Figure 3.2 shows the various types of BNC connectors. The BNC connectors are available in three different types:

   1. BNC connector

2. BNC-T connector

3. BNC terminator

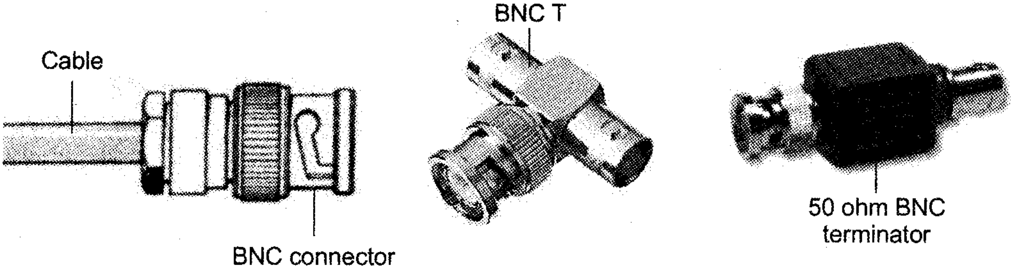


Figure 3.2: BNC connectors of different types

1. *BNC connector:* The BNC connector is used to connect the end of the cable to a device such as TV set.

2. *BNC-T connector:* The BNC-T connector is used in Ethernet networks for branching out a cable for connection to a network of other devices.

3. *BNC terminator:* The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

ii. Twisted pair cable

A pair of wire twisted together form a twisted pair. They have more noise immunity than the two wire open lines.

2

Apr. 2012, 2010 – *5M*
Explain Twisted Pair Cable in detail.

This is the oldest and still the most common transmission medium used for communication. It consists of two insulated copper wires typically about 1 mm thick. The wires are twisted together in a helical form to eliminate a lot of the noise and interference associated with cabling system.

There are two types of twisted pair cable. They are:

a. Shielded Twisted Pair (STP)

b. Unshielded Twisted Pair (UTP)

a. *Shielded Twisted Pair (STP):* IBM has produced a version of twisted pair cable for its use called shielded twisted pair. It has a metal foil or braided-mesh covering that encases each pair of insulated conductors.

b. *Unshielded Twisted Pair (UTP):* The most common twisted pair cable used in communication is referred to as Unshielded Twisted Pair (UTP). It comes in seven categories out of which category 6 and 7 are not still in use, most used is category 5 and category 3.

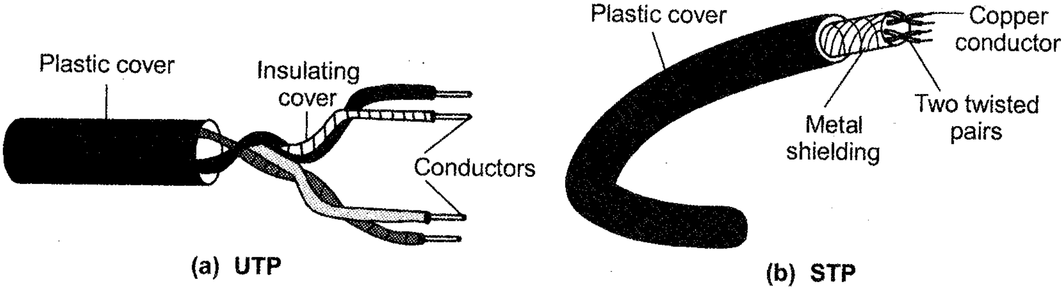


Figure 3.3: UTP AND STP

Need for twisting the wires

Twisting of wires will reduce the effect of noise or external interference.

Number of twists per unit length will determine the quality of cable. More twists means better quality.

Connectors for twisted pair cable

a. The UTP cable is most commonly used cable in computer communication.

b. The most common UTP connector is RJ45 where RJ is the short form of Registered Jack. It is male-female type keyed connector as shown in *figure 3.4.*

c. This connector can be inserted in only one way.

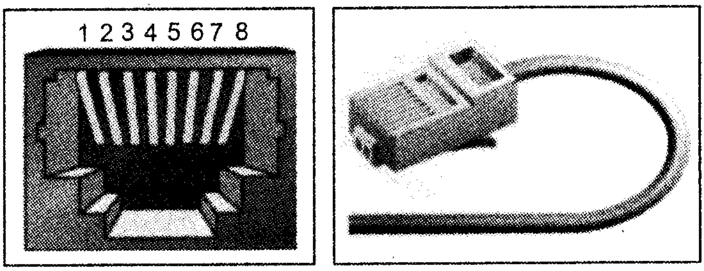
Applications of twisted pair cable

a. Most common transmission media for both digital and analog signals.

b. Twisted pair cables are used in telephone lines to provide voice and data channels.

c. The line that connects subscribers to the central telephone office is most commonly UTP cable.

d. LAN (Local Area Network) also uses twisted pair cable.



RJ-45 Female RJ-45 Male

Figure 3.4: UTP RJ45 connector

Comparison of Cables

Factors	UTP	STP
Bandwidth capacity	1-155 mbps (typically 10 mbps)	1-155 mbps (typically 16 mbps)
Node Capacity per segment	2	3
Attenuation	High	High
Installation	Easy	Fairly easy
Electro Magnetic Interface (EMI)	Very high	High
Cost	Lowest	Moderate

iii. Fiber optics cable

This cable transmits signals in the form of light beam over a glass threaded wire.

The light signals are immune to outside interference and signals do not go beyond this cable.

Hence it proves to be excellent for high security use.

2

Apr. 2012 – *5M*
Write a short note on Fiber optic cables.

Apr. 2011 – *5M*
Explain Optical Fiber Cables.

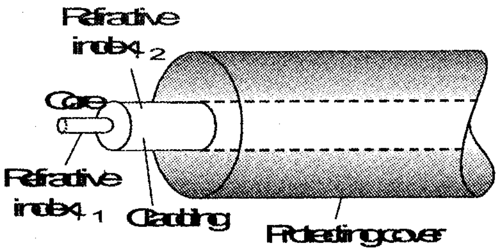


Figure 3.5: Fiber optic cable

Characteristics of fiber optics

a. High bandwidth therefore it can operate at higher data rates.

b. Reduces losses as the signal attenuation is low.

c. Distortion is reduced hence better quality is assured.

d. Small size and light weight.

e. Used for point to point communication.

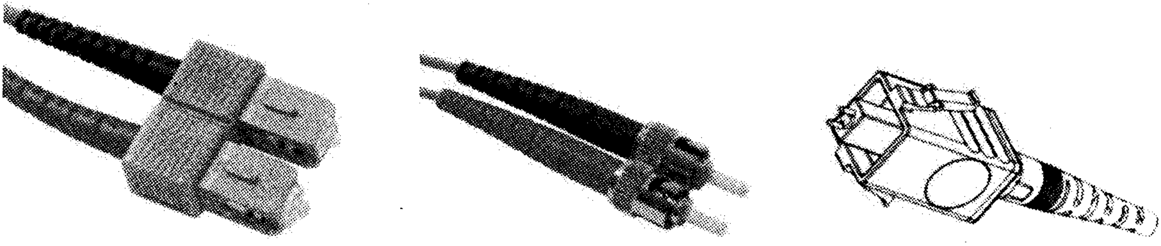
Fiber optics cable connectors

Fiber optic cables use three types of connectors. They are:

a. Subscriber Channel (SC) connector

b. Straight Tip (ST) connector

c. MT - RJ connector



SC connector **ST connector** **MT-RJ connector**

Figure 3.6: Fiber optic cable connector

Applications

a. Fiber optic cable is often found in backbone networks because its wide bandwidth is cost effective.

b. Some cable TV companies use a combination of optical fiber and coaxial cable.

c. Telephone companies also use optical fiber cable.

d. Local Area Networks (LANs) such as 100 Base FX network use fiber optic cable.

Advantages

a. *Higher bandwidth* than twisted pair and co-axial cable.

b. *Less signal attenuation* that means fiber optic transmission distance is significantly greater than that of other guided media.

c. *Noise resistance* it specifies that fiber optic transmission uses light rather than electricity.

d. *Light weight*

e. More security is provided.

f. Reliability is more than other and longer life span.

Disadvantages

a. Installation and maintenance need expertise.

b. Propagation of light is unidirectional.

c. Fiber optic is more expensive.

▶ Comparison of Wired Media

	Twisted pair	Co-axial	Optic fiber
i.	Transmission of signals takes place in the electrical form over the metallic conducting wires.	Transmission of signals takes place in the electrical form over the inner conductor of the cable.	Signal transmission takes place in an optical form over a glass fiber.
ii.	Noise immunity is low.	Higher noise immunity.	Highest noise immunity.
iii.	Affected due to external magnetic field.	less affected due to external magnetic field.	Not affected by the external magnetic field.
iv.	Short circuit between the two conductors is possible.	Short circuit between the two conductors is possible.	Short circuit is not possible.
v.	Cheapest	Moderately expensive.	Expensive.
vi.	Can support low data rates.	Moderately high data rates.	very high data rates.
vii.	Power loss due to conduction and radiation.	Power loss due to conduction	Power loss due to absorption, scattering, dispersion and bending.

2

Apr. 13, Oct. 10 – *5M*
Write differences between Co-axial Cable and Twisted Pair.

viii.	Low bandwidth	Moderately high bandwidth.	Very high bandwidth
ix.	Node capacity per segment is 2.	Node capacity per segment is 30 to 100.	Node capacity per segment is 2.
x.	Attenuation is very high.	Attenuation is low.	Attenuation is very low.
xi.	Installation is easy.	Installation is fairly easy.	Installation is difficult.
xii.	Electromagnetic Interference (EMI) can take place.	EMI is reduced due to shielding	EMI is not present.

2.2 Unguided Media / Wireless Transmission

3

Oct. 2012, 2010 – *5M*
Write a short note on Wireless Transmission.

Oct. 2010 – *5M*
Write short note on Unguided Medias.

Unguided media are natural parts of the Earth's environment that can be used as physical paths to carry electrical signals. The atmosphere and outer space are examples of unguided media that are commonly used to carry signals. These media can carry such electromagnetic signals as microwave, infrared light waves and radio waves.

Network signals are transmitted through all transmission media as a type of waveform. When transmitted through wire and cable, the signal is an electrical waveform. When transmitted through fibre-optic cable, the signal is a light wave: either visible or infrared light. When transmitted through Earth's atmosphere or outer space, the signal can take the form of waves in the radio spectrum, including VHF and microwaves, or it can be light waves, including infrared or visible light (e.g., lasers).

Typically, a wireless network uses infrared light or radio transmissions to distribute data. Infrared networks communicate by using beams of infrared light. They have a maximum range of 100 meters. Theoretically, they can transmit at 10 mbps, but 1-3 mbps is more typical. Narrow band radio networks can cover an area upto 5000 square meters at upto 4.8 Mbps. Their disadvantage is that they offer little security. Spread-spectrum radio networks use multiple frequencies. These multiple channels provide network security. They can transmit data upto 1 Mbps at a range of 800 feet indoors, though 300 Kbps is more typical.

Some common applications of wireless communication include the following:

i. Accessing the internet using a cellular phone

ii. Establishing a home or business internet connection over satellite.

viii.	Low bandwidth	Moderately high bandwidth.	Very high bandwidth
ix.	Node capacity per segment is 2.	Node capacity per segment is 30 to 100.	Node capacity per segment is 2.
x.	Attenuation is very high.	Attenuation is low.	Attenuation is very low.
xi.	Installation is easy.	Installation is fairly easy.	Installation is difficult.
xii.	Electromagnetic Interference (EMI) can take place.	EMI is reduced due to shielding	EMI is not present.

2.2 Unguided Media / Wireless Transmission

3

Oct. 2012, 2010 – *5M*
Write a short note on Wireless Transmission.

Oct. 2010 – *5M*
Write short note on Unguided Medias.

Unguided media are natural parts of the Earth's environment that can be used as physical paths to carry electrical signals. The atmosphere and outer space are examples of unguided media that are commonly used to carry signals. These media can carry such electromagnetic signals as microwave, infrared light waves and radio waves.

Network signals are transmitted through all transmission media as a type of waveform. When transmitted through wire and cable, the signal is an electrical waveform. When transmitted through fibre-optic cable, the signal is a light wave: either visible or infrared light. When transmitted through Earth's atmosphere or outer space, the signal can take the form of waves in the radio spectrum, including VHF and microwaves, or it can be light waves, including infrared or visible light (e.g., lasers).

Typically, a wireless network uses infrared light or radio transmissions to distribute data. Infrared networks communicate by using beams of infrared light. They have a maximum range of 100 meters. Theoretically, they can transmit at 10 mbps, but 1-3 mbps is more typical. Narrow band radio networks can cover an area upto 5000 square meters at upto 4.8 Mbps. Their disadvantage is that they offer little security. Spread-spectrum radio networks use multiple frequencies. These multiple channels provide network security. They can transmit data upto 1 Mbps at a range of 800 feet indoors, though 300 Kbps is more typical.

Some common applications of wireless communication include the following:

i. Accessing the internet using a cellular phone

ii. Establishing a home or business internet connection over satellite.

iii. Beaming data between two hand-held computing devices.

iv. Using a wireless keyboard and mouse for the PC.

▶ Advantages

i. Electromagnetic waves can travel longer distance.

ii. It is cost effective.

iii. Air, water or vacuum medium is used which is free.

▶ Disadvantages

i. No security, as signals can be tapped by anyone.

ii. Anybody can join the channel by broadcasting at the same frequency.

iii. Although the medium is free but connections to it are not free.

▶ Electromagnetic Spectrum for the Wireless Communication

The electromagnetic spectrum used for wireless communication is shown in *figure 3.7.*

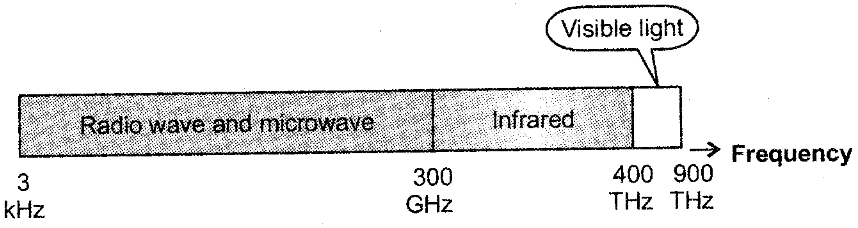
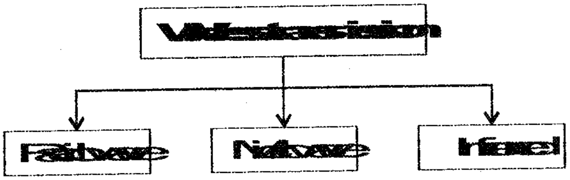


Figure 3.7: Wireless communication



i. ***Radio waves***

Radiowaves are widely used for both indoor and outdoor communication because they are easy to generate, can travel over long distances and can penetrate buildings easily.

Frequency range of radio waves is from 3 kHz to 1 GHz. This range covers AM and FM radio as well as Ultra High Frequency (UHF) and Very High Frequency (VHF).

The omini-directional (travel in all directions) characteristics of radio waves makes them useful for multicasting, in which there is one sender but many receivers. AM and FM Radio, television, mari-time radio, cordless phones and paging are examples of multicasting.

The range of electromagnetic spectrum between 10 KHz and 1GHz is called Radio Frequency (RF).

Radio waves include the following types:

a. Short wave used in AM radio

b. Very High Frequency (VHF) used in FM radio and TV

c. Ultra High Frequency (UHF) used in TV

Radio waves are omni directional. Various kinds of antennas are used to broadcast these signals as shown in *figure 3.8.*

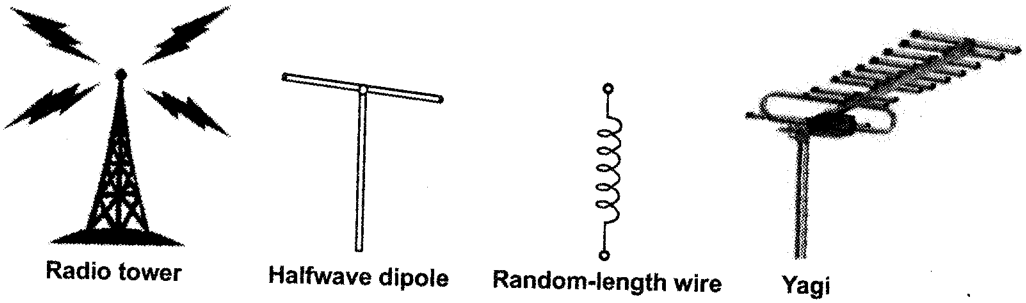


Figure 3.8: Various types of antenna

Important applications of radio transmission systems are:

1. Cellular communication
2. Wireless LAN
3. Point to point and point to multipoint radio system.
4. Satellite communication.

ii. *Micro waves*

The electromagnetic waves having frequencies between 1 GHz and 300 GHz are called microwaves.

Microwaves are unidirectional. Microwave propagation is a line of sight propagation. It can support high data rates.

At frequencies of 1 GHz and above, electromagnetic waves travel in straight lines and can be narrowly focused. Microwave is the upper part of the RF spectrum. Because of the larger bandwidth, microwave is used in many applications such as wireless PAN, wireless LAN, wireless MAN, satellite communication, radar, etc.

1
Apr. 2010 – *5M*
Explain Microwave as a Wireless Transmission.

A parabolic dish antenna can be used to focus the transmitted power into a narrow beam to give a high signal to noise ratio. As microwave travel in a straight line, the curvature of the earth limits the maximum distance over which microwave towers can transmit, so repeaters are needed to compensate for this limitation. At higher frequencies, transmitted waves do not easily pass through buildings. Some waves may be refracted by low lying atmospheric layers, and takes longer to arrive at destination than direct waves. The delayed waves may arrive out of phase with direct waves and cancel out signal. This effect is called as multipath fading. At higher frequencies expensive electronics are required, transmission is subject to interference from radar installations and microwave ovens. Obstacles like roads, railways and rivers are not a problem for microwave. However, weather and solar conditions may affect transmission.

Often used to communicate over long distance like cellular phones, garage door openers, and much more.

There are two types of microwave data communication systems:

a. **Terrestrial microwave transmission:** Communication is accomplished through line of sight parabolic dish antenna located on elevated sites. Long distance communication is possible by using a series of relay stations. The distance between the stations is dependent on the height above the ground. Used for voice and television transmission, private communications and telephone networks.

Attenuation can rise markedly in poor atmospheric condition *for example,* rain, but adversely affects the higher end of the frequency band, which is only used for short distance transmission. Natural noise severely affects transmission frequencies below 2 GHz. Quick to install and overcomes the problems of laying cables in congested locations or over difficult terrain.

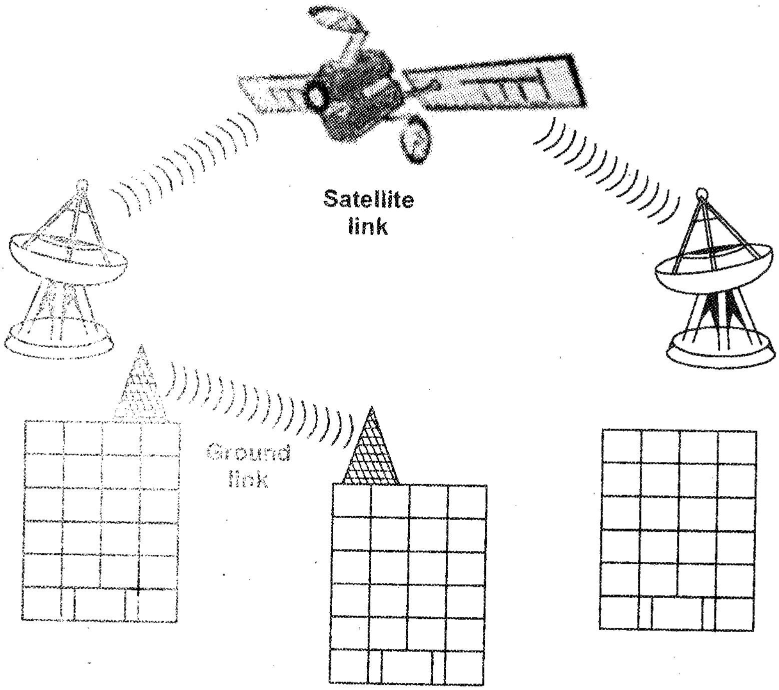


Figure 3.9: Terrestrial and satellite microwave links

b. **Satellite microwave transmission:** Overcomes the line of sight problems of terrestrial microwave and can be used for point to point or broadcast transmission. Uses an uplink and downlink frequency, a common frequency set is referred to as the 4/6 range which uses a downlink frequency of 4 GHz and an uplink frequency of 6 GHz.

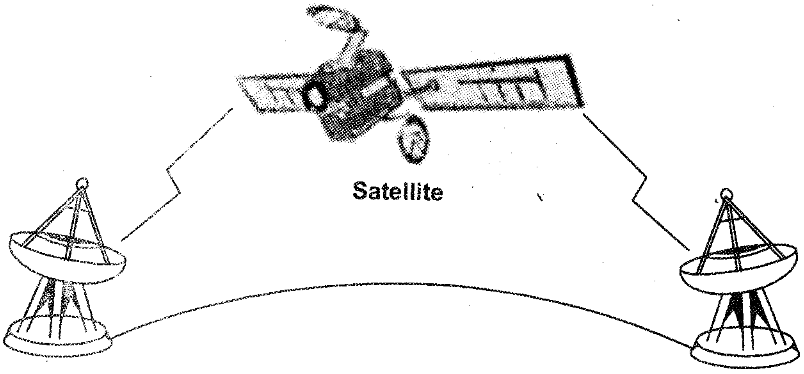


Figure 3.10: Point to point link via satellite microwave

iii. *Infrared waves*

Infrared (IR) light is a wavelength of energy that is invisible to the human eye. The most common source of this energy is heat; objects can have their relative temperatures measured by how much of this energy they give off. Lower wavelengths or near infrared closest to the visible light color red are not hot, and are often used to transmit data in electronics. A remote control, *for example*, may use a particular wavelength of near infrared to communicate with a receiver, sending pulses of light that transmit a signal to the device, telling it what to do.

2

Apr. 2013 – *5M*
Explain Infrared as wireless transmission.

Oct. 2011 – *5M*
What is wireless transmission? Explain Infrared as wireless transmission.

A form of energy, IR is part of the electromagnetic spectrum. This spectrum is comprised of radio waves; microwaves; infrared, visible, and ultraviolet light; X-rays and gamma rays. Each form of energy is ordered by wavelength; infrared falls between microwaves and visible light waves because its waves are shorter than microwaves but longer than those of visible light.

The prefix infra comes from the Latin word which means 'below'; the term means 'below red', indicating its position in the electromagnetic spectrum. Visible light has a range of wavelengths that are manifested in the seven colors of the rainbow; red has the longest wavelength and violet has the shortest. Infrared, with wavelengths longer than the color red, is invisible to the human eye.

Infrared waves acquire frequencies from 300 GHz - 400 THz (terahertz). Wave lengths from 1 mm to 770 nm can be used for short range communication.

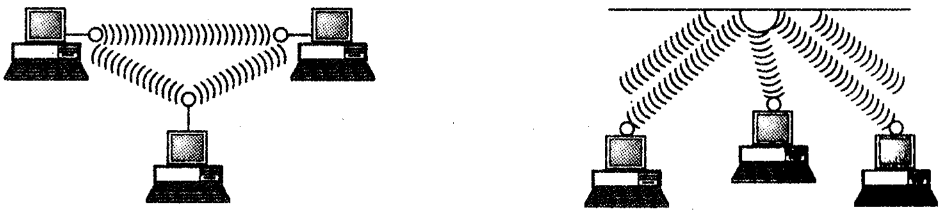
It has high frequencies which cannot penetrate walls. It means it can be easily contained within a room.

It can be used in development of very high speed wireless LANs in future.

There are two different ways of infrared waves:

a. Point to point infrared media

b. Broadcast infrared media



(a) Point-to-point infrared media **(b) Broadcast infrared media**

Figure 3.11

Differences of Bounded and Unbounded Media

	Bounded media	Unbounded media
i.	The signal energy is contained and bounded within a solid medium.	The signal energy propagates in the form of unbounded electromagnetic waves.
ii.	Used for point to point communication.	Used for broadcasting.
iii.	Twisted pair cable, co-axial cable, fiber optics cables are example of bounded media.	Radio and infrared light are the examples of unbounded media.
iv.	Attenuation depends exponentially on the distance.	Attenuation is proportional to the square of distance.

3. Propagation Methods

The unguided signals are the wireless media. It simply transports electromagnetic waves without using any physical conductor. Signals are normally broadcast through the air and thus are available to anyone who has the device capable of receiving them. Unguided signals can travel from source to the destination in several ways. These ways include ground propagation, sky propagation and line of sight propagation.

3

Apr. 13, 12, 10 – *5M*
Explain Propagation Methods.

In the *ground propagation*, the radio waves travel through the lowest portion of atmosphere, hugging the earth. These very low frequency signals emanate in all directions from transmitting antenna and follow the curvature of planet.

In *sky propagation*, the higher frequency radio waves radiate upward into the ionosphere, where they are reflected back to the earth.

In the *line of sight propagation*, very high frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by curvature of the earth. The line of sight propagation is tricky as radio transmissions cannot be completely focused.

The unguided signals can travel from the transmitter to receiver in many different ways.

The three most important methods are:

i. Ground wave propagation

ii. Sky wave propagation

iii. Space propagation or line-of-sight

3.1 Ground Wave Propagation

i. Radio waves in VLF band propagate in a ground, or surface wave. The wave is connected at one end to the surface of the earth and to the ionosphere at the other.

ii. The ionosphere is the region above the troposphere (where the air is) from about 50 to 250 miles above the earth. It is a collection of ions, which are atoms that have some of their electrons stripped off leaving two or more electrically charged objects.

iii. The ground waves travels between two limits, the earth and the ionosphere, which acts like dust.

Since the dust curves with the earth, the ground wave will follow. Therefore very long range propagation is possible using ground waves.

iv. It has low frequency. These low frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.

v. Distance depends on the amount of power in the signal. The greater the power, the greater the distance.

vi. The range of ground propagation is below 2 MHz.

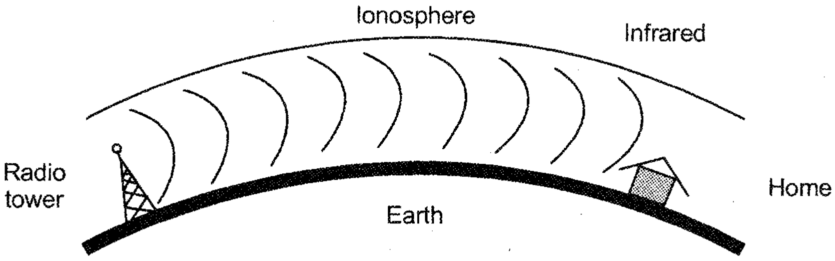


Figure 3.12: Ground waves

3.2 Sky Wave Propagation

i. Radio Waves in LF and MF ranges may also propagate as ground waves, but suffer significant losses, or are attenuated, particularly at higher frequencies. But as the ground wave mode fades out, a new mode develops: the sky wave.

1
Oct. 2011 - *5M*
Explain in detail sky wave propagation.

ii. Sky waves are reflections from the ionosphere.

While the wave is in the ionosphere, it is strongly bent, or refracted, ultimately back to the ground.

iii. From a long distance away this appears as a reflection.

iv. Long ranges are possible in this mode also upto hundreds of miles.

v. Sky waves in this frequency band are usually only possible at night, when the concentration of ions is not too great since the ionosphere also tends to attenuate the signal.

vi. However, at night, there are just enough ions to reflect the wave but not reduce its power too much.

vii. It has higher frequency radio waves which radiate upward into the ionosphere where they are reflected back to earth.

viii. This type of transmission allows for greater distance with lower output power.

ix. The range of this propagation is 2-30 MHz.

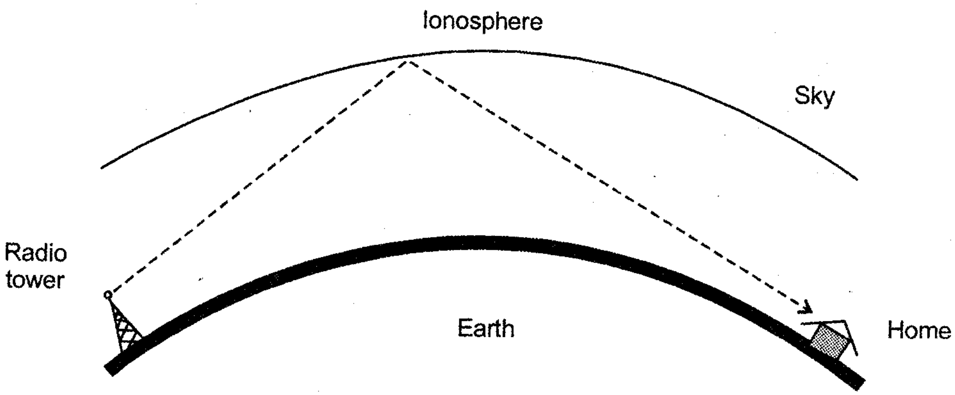


Figure 3.13: Sky waves

3.3 Space or Line-of-Sight Propagation

i. Line-of-sight propagation refers to electromagnetic radiation including light emissions traveling in straight line. The rays or waves are defracted, refracted, reflected or absorbed by atmosphere and abstractions with material and generally cannot travel over the horizon or behind obstacles.

ii. Especially radio signals, like all electromagnetic radiation including light emissions, travel in straight lines.

iii. At low frequencies (below approximately 2 MHz or so) these signals travel as ground waves, which follow the earth's curvature due to diffraction with the layers of atmosphere.

iv. It has very high frequency signals and are transmitted in straight lines directly from antenna to antenna. Antennas must be directional facing each other and either tall enough or close enough not to be affected by the curvature of the earth.

2

Oct. 2012 – *5M*
Write a short note on 'Line-of-Sight'.

Oct. 2010 – *5M*
Explain in detail 'Line-of-Sight'.

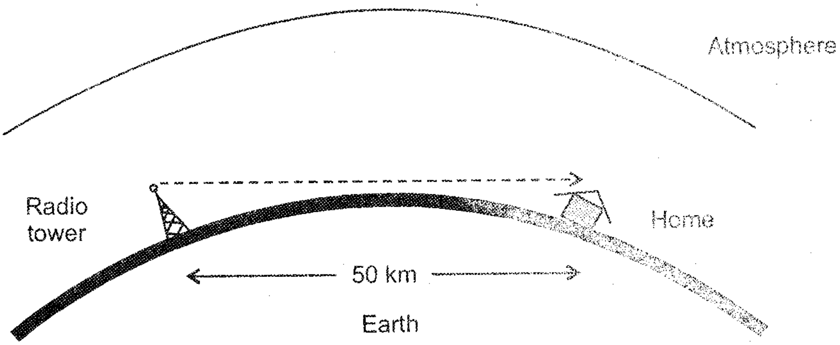


Figure 3.14: Line of sight propagation

PU Questions

5 Marks

1. Explain Infrared as wireless transmission. [Apr. 2013 – 5M]
2. Differentiate between coaxial cable and twisted pair cable. [Apr. 2013 – 5M]
3. Write a short note on Wireless Transmission. [Oct. 2012, 2010 – 5M]
4. Write a short note on Line-of-Sight. [Oct. 2012 – 5M]
5. Explain propagation methods. [Apr. 13, 12, 10 – 5M]
6. Write a short note on Fiber optic cables. [Apr. 2012 – 5M]
7. Explain Twisted Pair Cable in detail. [Apr. 2012, 2010 – 5M]
8. Explain in detail sky wave propagation. [Oct. 2011 – 5M]
9. Write a short note on coaxial cable. [Oct. 2011 – 5M]
10. What is wireless transmission? Explain infrared as wireless transmission. [Oct. 2011 – 5M]
11. Explain Optical Fiber Cables. [Apr. 2011 – 5M]
12. Explain in detail 'Line-of-Sight'. [Oct. 2010 – 5M]
13. Write differences between Co-axial Cable and Twisted Pair. [Oct. 2010 – 5M]
14. Write short note on Unguided Medias. [Oct. 2010 – 5M]
15. Explain Microwave as a Wireless Transmission. [Apr. 2010 – 5M]

VISION®

Chapter 4

WIRED AND WIRELESS LANS

1. Introduction

A **wired network** connects devices to the internet or other network using cables. The most common wired networks use cables connected to ethernet ports on the network router on one end and to a computer or other device on the cable's opposite end.

'Wi-Fi' is the universal standard for **wireless networks** and is the **wireless** equivalent of wired ethernet networks. In the office, Wi-Fi networks are adjuncts to the wired networks. It links two or more devices using some wireless distribution method and usually provides a connection through an access point to the wider internet. This gives users the ability to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

A wired network uses ethernet cable to connect the computers to the network router. It is less expensive, faster and more secure than wireless networks. Wireless LAN provides the flexibility to connect computers to the network using wireless network adapter devices.

2. IEEE Standards

The Institute of Electrical and Electronics Engineers is an organization of engineering professionals. It is probably best known for the work of its IEEE Standards Association, a standards body that defines specifications for many different technologies. *For example*, the IEEE Standards Association defines such wireless technologies as Bluetooth (IEEE 802.15.1) and WiFi (802.11).

The IEEE standards development process can be broken down into seven basic steps:

i. Securing Sponsorship

ii. Requesting Project Authorization

iii. Assembling a Working Group

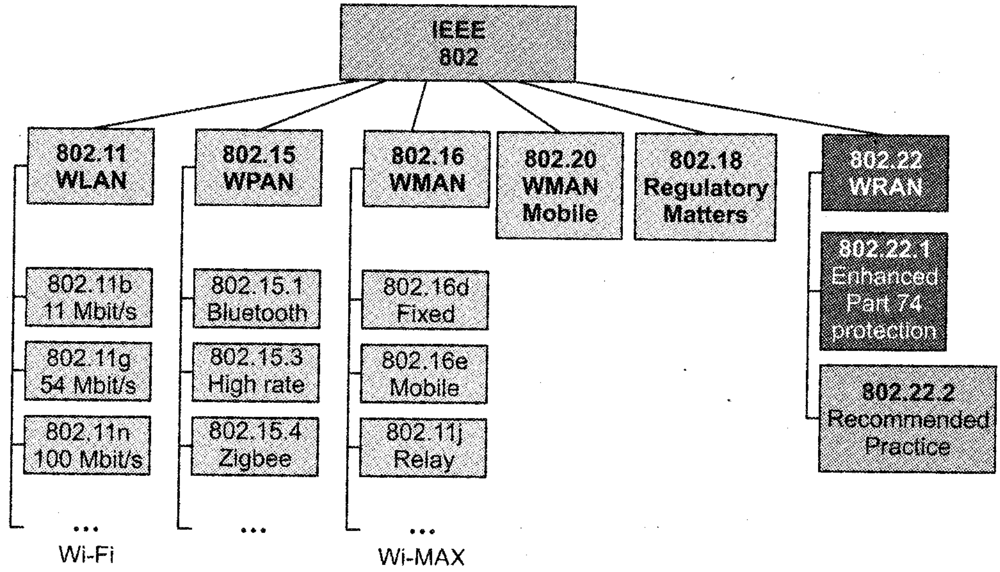
iv. Drafting the Standard

v. Balloting

vi. Review Committee

vii. Final Vote

A set of network standards developed by the IEEE include:



IEEE 802.1 Bridging (networking) and Network Management

IEEE 802.2 Logical link control (upper part of data link layer)

IEEE 802.3 Ethernet (CSMA/CD)

IEEE 802.4 Token bus (disbanded)

IEEE 802.5 Defines the MAC layer for a Token Ring (inactive)

IEEE 802.6 Metropolitan Area Networks (disbanded)

IEEE 802.7 Broadband LAN using Coaxial Cable (disbanded)

IEEE 802.8 Fiber Optic TAG (disbanded)

IEEE 802.9 Integrated Services LAN (disbanded)

IEEE 802.10 Interoperable LAN Security (disbanded)

IEEE 802.11 Wireless LAN & Mesh (Wi-Fi certification)

IEEE 802.12 demand priority (disbanded)

IEEE 802.13 Not Used

IEEE 802.14 Cable modems (disbanded)

IEEE 802.15 Wireless PAN

IEEE 802.15.1 (Bluetooth certification)

IEEE 802.15.4 (ZigBee certification)

IEEE 802.16 Broadband Wireless Access (WiMAX certification)

IEEE 802.16e (Mobile) Broadband Wireless Access

IEEE 802.17 Resilient packet ring

IEEE 802.18 Radio Regulatory TAG

IEEE 802.19 Coexistence TAG

IEEE 802.20 Mobile Broadband Wireless Access

IEEE 802.21 Media Independent Handoff

IEEE 802.22 Wireless Regional Area Network

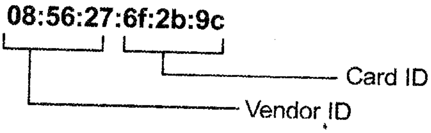
3. Standard Ethernet

The basic concept of ethernet networking is that packets are given destination addresses by senders, and those addresses are read and recognized by the appropriate receivers. Devices on the network check every packet, but fully process only those packets addressed either to themselves or to some group to which the device belongs.

It recognizes three types of addresses: physical addresses, logical addresses and symbolic names assigned to either of these.

i. **Physical addresses:** A physical address is the hardware-level address used by the ethernet interface to communicate on the network. Every device must have a unique physical address. This is often referred to as its MAC (Media Access Control) address. An Ethernet physical address is six bytes long and consists of six hexadecimal numbers, usually separated by colon characters (:).

For example



Typically, a hardware manufacturer obtains a block of physical address numbers from the IEEE and assigns a unique physical address to each card it builds. The vendor block of addresses is designated by the first three bytes of the six-byte physical ethernet address. In this way, ethernet physical addresses are generally distinct from each other, although some networks and protocols will override this built-in mechanism with one of their own.

ii. **Logical addresses:** A logical address is a network-layer address that is interpreted by a protocol handler. Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media. *Each type of protocol has a different kind of logical address: for example,*

- an IP address (IPv4) consists of four decimal numbers separated by period (.) characters, *for example:*

  130.57.64.11

- an AppleTalk address consists of two decimal numbers separated by a period (.), *for example*:

  2010.42

  368.12

Depending on the type of protocol in a packet (such as IP or AppleTalk), a packet may also specify source and destination logical address information, either as extensions to the physical addresses or as alternatives to them.

iii. **Symbolic names:** The strings of numbers typically used to designate physical and logical addresses are perfect for machines, but awkward for human beings to remember and use. Symbolic names stand for either physical or logical addresses. The domain names of the internet are an example of symbolic names. The relationship between the symbolic names and the logical addresses to which they refer is handled by DNS (Domain Name Services) in IP (Internet Protocol).

The standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Organization for Standardization (ISO) also approved it as an international standard under the designation ISO 8802. The relationship of the 802 Standard to the traditional OSI model is shown in *figure 4.1*. The IEEE has subdivided the data link layer into two sublayers:

a. Logical Link Control (LLC) and

b. Media Access Control (MAC)

IEEE has also created several physical layer standards for different LAN protocols.

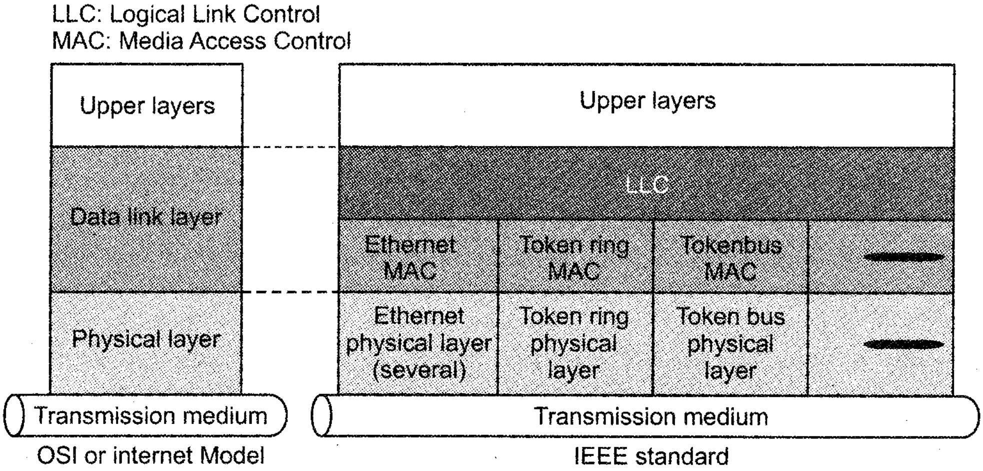


Figure 4.1: IEEE standard for LANs

▶ Data Link Layer

As we mentioned before, the data link layer in the IEEE standard is divided into two sublayers:

i. Logical Link Control (LLC) and

ii. Media Access Control (MAC)

i. **Logical Link Control (LLC):** In IEEE Project 802, flow control, error control and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MAC sublayer. The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer, which provides different protocols for different LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent. Following figure shows one single LLC protocol serving several MAC protocols.

Framing: LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC. The header contains a control field like the one in HDLC; this field is used for flow and error control. The two other header fields define the upper-layer protocol at the source and destination that uses LLC. These fields are called the destination service access point (DSAP) and the source service access point (SSAP).The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer. In other words, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer.

Need for LLC: The purpose of the LLC is to provide flow and error control for the upper-layer protocols that actually demand these services. For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols. However, most upper-layer protocols such as IP do not use the services of LLC.

ii. **Media Access Control (MAC):** The MAC sublayer has two primary responsibilities:

a. **Data encapsulation:** Includes frame assembly before transmission, frame parsing upon reception of a frame, data link layer MAC addressing, and error detection.

b. **Media Access Control:** Because Ethernet is a shared media and all devices can transmit at any time, media access is controlled by a method called Carrier Sense Multiple Access with Collision Detection (CSMA/CD) when operating in half-duplex mode.

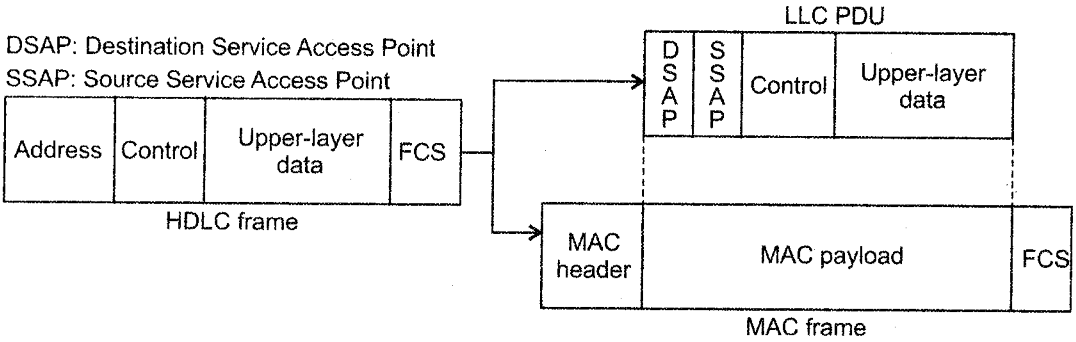


Figure 4.2: HDLC frame compared with LLC and MAC frames

At the physical layer, Ethernet specifies and implements encoding and decoding schemes that enable frame bits to be carried as signals across both unshielded twisted-pair (UTP) copper cables and optical fiber cables. In early implementations, Ethernet used coaxial cabling.

4. Fast Ethernet

Fast ethernet is a collective term for a number of ethernet standards that carry traffic at the nominal rate of 100 Mbit/s, against the original ethernet speed of 10 Mbit/s. Of the Fast ethernet standards 100BASE-TX is by far the most common and is supported by the vast majority of ethernet hardware currently produced.

Fast ethernet uses the same cabling and access method as 10Base-T. With certain exceptions, Fast ethernet is simply regular ethernet, just ten times faster. Whenever possible, the same numbers used in the design of 10Base-T were used in Fast Ethernet, just multiplied or divided by ten.

Fast ethernet supports a maximum data rate of 100 Mbps. It is so named because original ethernet technology supported only 10 Mbps. Fast Ethernet began to be widely deployed in the mid-1990s as the need for greater LAN performance became critical to universities and businesses.

Full motion video for video conferencing requires, typically, at least 25 Mb/sec. That means that a legacy ethernet, at 10 Mb/sec, can only deliver poor quality real-time video. With 100 Mb/sec, however, you can be watching a broadcast presentation in one window while you're in conference with three people in three other windows for a total of 100 megabits of bandwidth.

A key element of fast ethernet's success was its ability to coexist with existing network installations. Today, many network adapters support both traditional and fast ethernet. These so-called '10/100' adapters can usually sense the speed of the line automatically and adjust accordingly. Just as fast ethernet improved on traditional ethernet, gigabit ethernet improves on fast ethernet, offering rates upto 1000 Mbps instead of 100 Mbps.

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet can be summarized as follows:

i. Upgrade the data rate to 100 Mbps.

ii. Make it compatible with Standard Ethernet.

iii. Keep the same 48-bit address.

iv. Keep the same frame format.

v. Keep the same minimum and maximum frame lengths.

4.1 MAC Sublayer

A main consideration in the evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sublayer untouched. However, a decision was made to drop the bus topologies and keep only the star topology. For the star topology, there are two choices, half duplex and full duplex. In the half-duplex approach, the stations are connected via a hub; in the full-duplex approach, the connection is made via a switch with buffers at each port.

The access method is the same (CSMA/CD) for the half-duplex approach; for full duplex. Fast Ethernet, there is no need for CSMA/CD. However, the implementations keep CSMA/CD for backward compatibility with standard ethernet.

▶ Autonegotiation

A new feature added to Fast Ethernet is called autonegotiation.

It allows a station or a hub a range of capabilities. Autonegotiation allows two devices to negotiate the mode or data rate of operation. It was designed particularly for the following purposes:

i. To allow incompatible devices to connect to one another. *For example*, a device with a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity (but can work at a lower rate).

ii. To allow one device to have multiple capabilities.

iii. To allow a station to check a hub's capabilities.

4.2 Physical Layer

The physical layer in fast ethernet is more complicated than the one in etandard ethernet.

▶ Topology

Fast Ethernet is designed to connect two or more stations together. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center, as shown in *figure 4.3*.

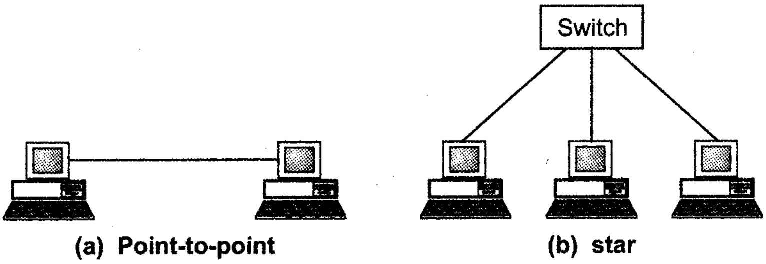


Figure 4.3: Fast ethernet topology

5. Giga Ethernet

Gigabit ethernet is part of the family of Ethernet computer networking and communication standards. The Gigabit ethernet standard supports a theoretical maximum data rate of 1 gigabit per second (Gbps) (1000 Mbps).

When first developed, some thought achieving gigabit speeds with ethernet would require using fiber optic or other special cables. However, today's Gigabit ethernet works using twisted pair copper cable (specifically, the CAT5e and CAT6 cabling standards) similar to older 100 Mbps Fast Ethernet (that works over CAT5 cables).

Gigabit ethernet allows connection between two devices in either a full-, or a half-duplex mode. In half-duplex mode, Gigabit ethernet uses the CSMA/CD access method, just like it's 10 and 100 Mb/s predecessors. In full-duplex mode, the MAC uses frame-based flow control as defined in the IEEE 802.3x standard.

The need for an even higher data rate resulted in the design of the Gigabit ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit ethernet design can be summarized as follows:

i. Upgrade the data rate to 1 Gbps.

ii. Make it compatible with standard or fast Ethernet.

iii. Use the same 48-bit address.

iv. Use the same frame format.

v. Keep the same minimum and maximum frame lengths.

vi. To support autonegotiation as defined in fast ethernet

5.1 MAC Sublayer

A main consideration in the evolution of ethernet was to keep the MAC sublayer untouched. However, to achieve a data rate 1 Gbps, this was no longer possible. Gigabit ethernet has two distinctive approaches for medium access: half-duplex and full-duplex. Almost all implementations of Gigabit ethernet follow the full-duplex approach. However, we briefly discuss the half-duplex approach to show that Gigabit Ethernet can be compatible with the previous generations.

▶ Full-Duplex Mode

In full-duplex mode, there is a central switch connected to all computers or other switches. In this mode, each switch has buffers for each input port in which data are stored until they are transmitted. There is no collision in this mode. This means that CSMA/CD is not used. Lack of collision implies that the maximum length of the cable is determined by the signal attenuation in the cable, not by the collision detection process.

▶ Half-Duplex Mode

Gigabit ethernet can also be used in half-duplex mode, although it is rare. In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. The half-duplex approach uses CSMA/CD. However, as we saw before, the maximum length of the network in this approach is totally dependent on the minimum frame size. Three methods have been defined: traditional, carrier extension and frame bursting.

i. **Traditional:** In the traditional approach, we keep the minimum length of the frame as in traditional ethernet (512 bits). However, because the length of a bit is 1/100 shorter in Gigabit ethernet than in 10 Mbps ethernet, the slot time for Gigabit ethernet is 512 bits × 1/1000 μs, which is equal to 0.512 μs. The reduced slot time means that collision is detected 100 times earlier. This means that the maximum length of the network is 25 m.

   This length may be suitable if all the stations are in one room, but it may not even be long enough to connect the computers in one single office.

ii. **Carrier extension:** To allow for a longer network, we increase the minimum frame length. The carrier extension approach defines the minimum length of a frame as 512 bytes (4096 bits). This means that the minimum length is 8 times longer. This method forces a station to add extension bits (padding) to any frame that is less than 4096 bits. In this way, the maximum length of the network can be increased 8 times to a length of 200 m. This allows a length of 100 m from the hub to the station.

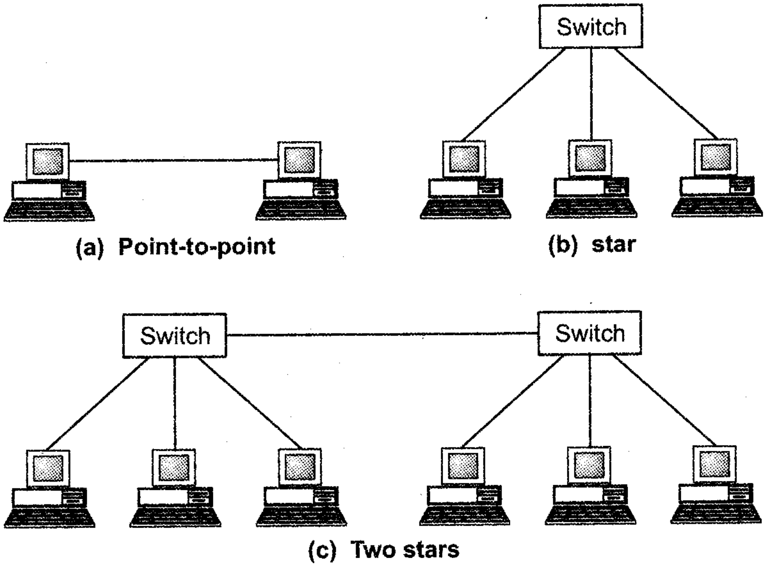
iii. **Frame bursting:** Carrier extension is very inefficient if we have a series of short frames to send; each frame carries redundant data. To improve efficiency, frame bursting was proposed. Instead of adding an extension to each frame, multiple frames are sent. However, to make these multiple frames look like one frame, padding is added between the frames (the same as that used for the carrier extension method) so that the channel is not idle. In other words, the method deceives other stations into thinking that a very large frame has been transmitted.

5.2 Physical Layer

The physical layer in Gigabit Ethernet is more complicated than that in Standard or Fast Ethernet. We briefly discuss some features of this layer.

▶ Topology

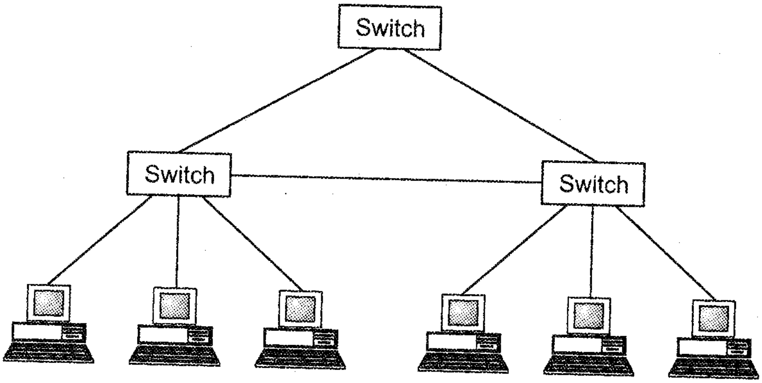
Gigabit ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center. Another possible configuration is to connect several star topologies or let a star topology be part of another as shown in *figure 4.4*.



(a) Point-to-point

(b) star

(c) Two stars



(d) Hierarchy of stars

Figure 4.4: Topologies of Gigabit ethernet

In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

6. Network Interface Cards (NIC)

Each PC or workstation, that is to be connected in a network has its own Network Interface Card (NIC).

The NIC fits inside the station and provides the station with a 6 byte physical address.

The ethernet address is 6 bytes (48 bits) and it is normally written in hexadecimal notation using hyphen to separate bytes from each other as shown below:

06 – 02 – 03 -04- 4c -2B

NIC is housed inside the computer on the motherboard, It provides physical connection between the network and the computer station.

The speed of NIC is important in determining the speed and efficiency of a network. It allows computer to be joined together in LAN. NIC is used to connect a computer to an ethernet network. The card (shown in the *figure 4.5* below) provides an interface to the media. This may be either using an external transceiver or through an internal integrated transceiver mounted on the network interface card PCB. The card usually also contains the protocol control firmware and ethernet controller needed to support the MAC (Media Access Control) data link protocol used by ethernet.

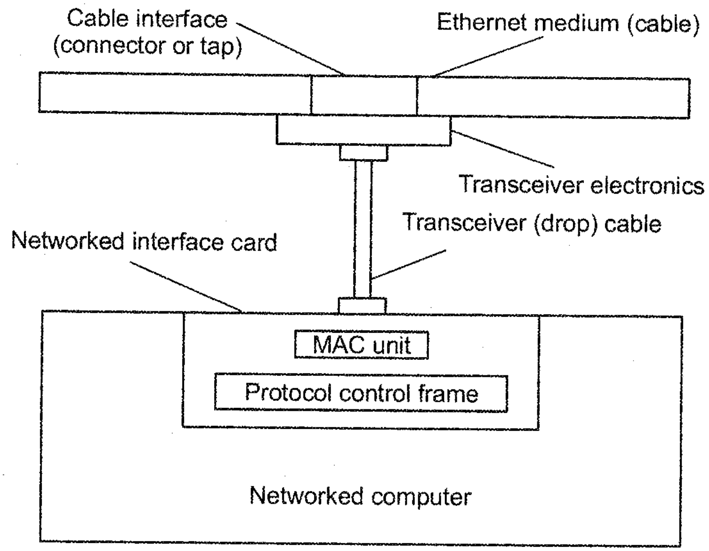


Figure 4.5: Network interface card for connection of a computer to an ethernet network

Network Interface Cards (NIC) are also called as, 'Network Adapters' NIC are installed in a computer that provides the connection point to a network.

Network Interface Cards (NIC) allows a network capable device access to a computer network such as the internet.

Every computer on a network communicates with another through this network adapter.

Network adapters perform all the functions required to communicate on a network. They convert data from the form stored in computer to the form transmitted or received on cable and provides a physical connection to the network.

Data stored in computer's memory is transmitted to NIC across system buses. This data is stored in buffer of NIC. NIC has got two buffers transmit and receive buffers. It checks data received for any error. It forms data frames inserting its own address and destination cards address.

NIC is responsible to prevent multiple systems on network from transmitting at the same time and losing data due to packet collision. It does this function using appropriate Media Access Control (MAC) mechanism. As it accepts parallel data from memory, it converts it to serial bits stream for transmission over network medium. Next function to convert serial bits of data to appropriate media is used for transfer over network.

6.1 Components of NIC

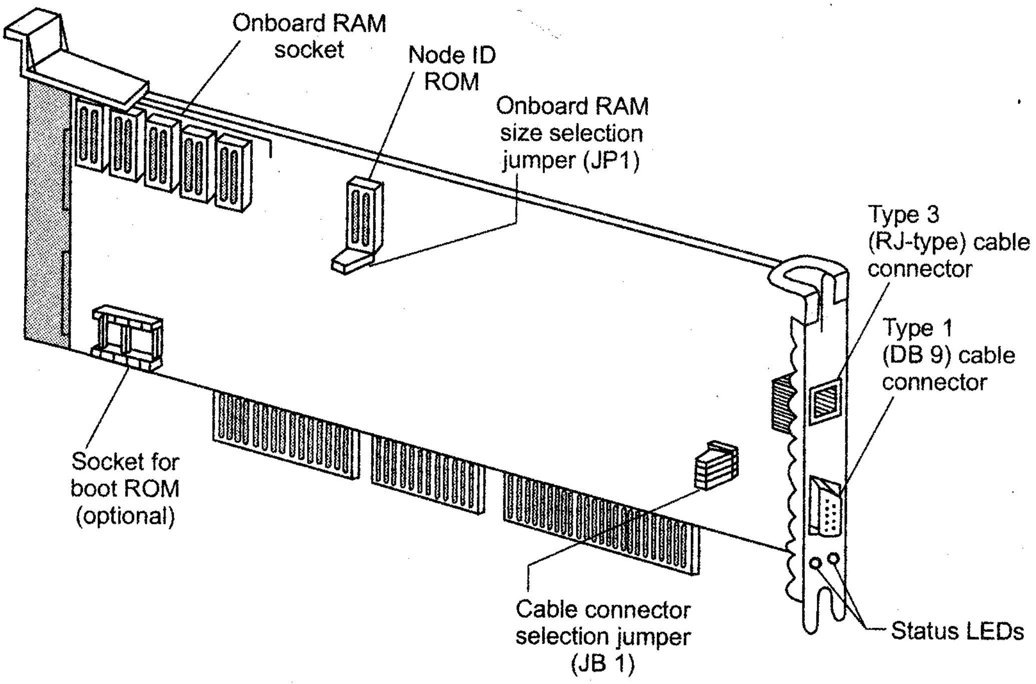

Onboard RAM socket
Node ID ROM
Onboard RAM size selection jumper (JP1)
Type 3 (RJ-type) cable connector
Type 1 (DB 9) cable connector
Socket for boot ROM (optional)
Cable connector selection jumper (JB 1)
Status LEDs

Figure 4.6: Network card

i. **Status LED's:** A network card usually has two indicator lights (LED's).

   a. The green LED shows that the card is receiving electricity.

   b. The orange (10 Mb/s) or red (100 Mb/s) LED indicates network activity (sending or receiving data).

ii. **Transceiver:** To prepare data to be sent the network card has a transceiver, which transforms parallel data into serial data.

iii. **MAC address:** Each card has a unique address, called MAC (Address, assigned by the cards Manufacturers which lets it be uniquely identified among all the network cards in the world. Network cards have settings which can be configured. Among them are hardware interrupts (IRQ), the I/O address and the memory address (DMA).

iv. **Socket:** To ensure that the computer and network are compatible, the card must be suitable for the computer's data bus architecture and have the appropriate type of socket for the cable. Each card is designed to work with a certain kind of cable. Some cards include multiple interface connectors (which can be configured using jumpers, DIP switches, or software). The most commonly used are RJ - 45 connectors.

v. **Connector:** To ensure that the computer and network are compatible the card must be compatible with the computer's internal structure (data bus architecture) and have a connector suitable for the kind of cabling used.

vi. **Internal expansion slots:** A NIC can only be installed in an internal expansion slot on the motherboard for which the card was designed.

vii. **External connectors and cables:** A wired NIC typically uses a RJ45 socket for network connections. The cabling used with an RJ45 connector is called 'twisted pair' or '10BaseT'. Older technologies include BNC connectors for use in coaxial 10Base2 networks and AUI connectors for use in thicknet or 10Base5 networks.

6.2 Functions of NIC

Following functions are performed by NIC for getting data to and from computer over network:

1

Apr. 2013 – *5M*
What is NIC? Explain components and functions of NIC.

1

Apr. 2012 – *5M*
Describe the functions of NIC.

i. **Data encapsulation:** NIC and its drivers are responsible for building the frame around the data generated by the network layer protocol. For encapsulating the frame, NIC attaches its own address to the frame.

ii. **Signal encoding and decoding:** NIC implements physical layer encoding scheme. NIC converts binary data generated by network layer into electrical signals. Such as voltages, light pulses or whatever other signal type the network medium uses. It also converts received electrical signals to binary data to be used by network layer.

iii. **Data buffering:** NIC has two buffers as send and receive. It temporarily stores data in buffers until a frame is complete and ready for processing.

iv. **Data transmission and reception:** The main function of NIC is to generate and transmit signals over network and receive incoming signals. NIC reads destination address of each incoming packet, if address is its own then it sends packet to network layer otherwise discards the packet.

v. **Serial/parallel conversions:** System buses of computers carries data in parallel format, i.e. computer communicates with NIC in parallel whereas network communications are serial i.e. NIC sends data over network cable in serial format. Therefore, NIC is responsible for conversion between the two types of transmission (parallel to serial for sending data and serial to parallel for receiving data).

vi. **Media Access Control (MAC):** The data link layer uses MAC to regulate the access to network medium. This MAC is implemented by NIC.

▶ What is the Role of a Network Card?

A network card is the physical interface between the computer and cable. It converts the data sent by the computer into a form which can be used by the network cable, transfers that data to another computer and controls the dataflow between the computer and cable. It also translates the data coming from the cable into bytes so that the computer's CPU can read it. This is why a network card is an expansion card inserted into an expansion slot.

Role of the Identifier

i. The card converts data and notifies the rest of the network of its address, so that it can be told apart from the other network cards.

ii. MAC addresses: Defined by IEEE (Institute of Electrical and Electronics Engineer), which assigns ranges of addresses to each manufacturer of network cards.

iii. They are inscribed on the cards chips, and as a result, each card has unique MAC address on the network.

▶ Network Card Functions

i. The computer and card must communicate so that data can travel between them. For this reason, the computer assigns part of its memory to cards that include DMA (Direct Memory Access).

ii. The interface card indicates that another computer is requesting data from that computer.

The computer's bus transfers the data from the computer memory to the network card.

iii. If the data is moving too fast for the adapter to process, they are placed in the card's buffer memory (RAM), where they are temporarily stored while the data is being sent and received.

6.3 Types of NIC

i. Ethernet (IEEE 802.3)

Ethernet is the most widely installed LAN technology, specified in a standard IEEE 802.3. It was originally developed by Xerox from an earlier specification called Alohanet and then developed further by Xerox, DEC and Intel.

An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Three data rates are currently defined for operation over optical fiber and twisted pair cables:

a. 10 Mbps: 10 Base - T Ethernet

b. 100 Mbps: Fast Ethernet

c. 1000 Mbps: Gigabit Ethernet

2

Oct. 2012 – *5M*
What is full form of NIC? List its types. Explain any one in detail.

Oct. 2011 – *5M*
What is NIC? Explain its types.

Ethernet has survived as the major LAN technology because its protocol has the following characteristics:

1. Is easy to understand, implement, manage and maintain.
2. Allows low-cost network implementations.
3. Provides extensive topological flexibility for network installation.
4. Guarantees successful interconnection and operation of standards compliant, products, regardless of manufacturer.

Ethernet features

a. It is the most popular physical layer LAN.

b. It is popular because it strikes a good balance between speed, cost and ease of installation.

c. It is currently the most popular network architecture. This baseband architecture uses a bus topology, usually transmits at 10 Mbps and relies on CSMA/CD to regulate traffic on the main cable segment.

d. The ethernet media is passive, which means it draws power from the computer and thus will not fail unless the media is physically cut or improperly terminated.

The following list summarizes ethernet features:

1. Traditional topology: Linear bus
2. Other topology: Star bus
3. Type of architecture: Baseband
4. Access method: CSMA / CD
5. Specifications: IEEE 802.3
6. Transfer speed: 10 Mbps or 100 Mbps
7. Cable types: Thicknet, thinnet, UTP.

Types of ethernet

There are four types of Ethernet:

1
Apr. 2012 – 5M
Explain Ethernet with reference to features and types.

a. **Traditional ethernet**

1. *Cable:* There are three types of cables used:
   - 10 Base 5 (thick Ethernet)
   - 10 Base 2 (thin Ethernet)
   - 10 Base T
2. *Transceiver:* A transceiver is a special device that is either clamped to the cable or is on the interface board (10 Base 2)
3. *Interface board:* It contains a controller chip that transmits frames to and receives frames from the transceiver.
4. *Repeater:* The maximum cable length allowed is 500 mtrs by 802.3
5. *Cable topologies*
6. *Encoding method*

b. **Switched ethernet**

As more stations are added to an ethernet LAN. The traffic will increase to deal with this increased load, switched ethernet can be used.

c. **Fast ethernet:** The basic idea of fast Ethernet was to keep all frame formats, interfaces and procedural rules the same, but reduce bit time from 100 nsec to 10 nsec.

d. **Gigabit ethernet:** It supports two modes of operation:

1. Full duplex mode
2. Half duplex mode

The full duplex mode is used when there is a central switch. All lines are buffered so computers can send frames whenever it wants to. On the line between a computer and the switch, the computer is the only sender and hence no contention is possible.

Types of ethernet cables

For many applications, readymade ethernet cables may be purchased, and knowledge of the construction of any ethernet cables is not required. However for other applications it is necessary to know the construction of ethernet cable. These cables may be used for different applications.

The Ethernet cables is as given below:

Specification	Cable type	Maximum length
10 Base T	Unshielded Twisted Pair	100 meters
10 Base 2	Thin Coaxial Cable	180 meters
10 Base 5	Thick Coaxial Cable	500 meters
10 Base F	Fiber Optic Cable	2000 meters
100 Base T	Unshielded Twisted Pair	100 meters
100 Base TX	Unshielded Twisted Pair	220 meters

Categories for Ethernet Cables

A variety of different cables are available for Ethernet and other telecommunications and networking applications. These cables are described by their different categories,

They are as given below:

Category 1: This is not recognized by the TIA / EIA. It is the form of wiring used for standard telephone wiring or ISDN.

Category 2: It is not recognized by the TIA / EIA. It is the form of wiring used for 4 Mbit/s token ring networks.

Category 3: It is defined by TIA / EIA. It is used for data networks employing frequencies upto 16 MHz. It was popular for use with 10 Mbps ethernet networks (100 Base-T).

Category 4: It is not recognized by TIA / EIA. It used on 16 Mbps token ring networks.

Category 5: It is not recognized by TIA / EIA. It is widely used for 100 Base-T and 1000 Base-T networks as it provides performance to allow data at 100 Mbps and slightly more for ethernet.

Category 6: It is defined by TIA / EIA. It provides more than double the performance of cat 5 cable allowing data at upto 250 Mbps to be passed.

Category 7: It is an informal number for ISO /IEC. It comprises four individual shielded pairs inside an overall shield. It is aimed at applications where transmission of frequencies upto 600 Mbps is required.

Ethernet network topologies and structures

LAN's take on many topological configurations, but regardless of their size of complexity, all will be a combination of only three basic interconnection structures or network building blocks.

The simplest structure is the point-to-point interconnection, shown in *figure 4.7.* Only two network units are involved and the connection may be DTE to DTE, DTE to DCE or DCE to DCE.

DTE (Data Terminal Equipment)

DCE (Data Communication Equipment)

The cable in point-to-point interconnections is known as a network link.

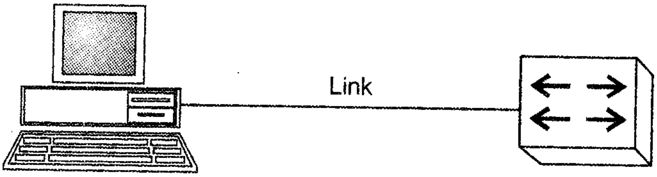


Figure 4.7: Example of point-to-point interconnection

Ethernet uses a protocol called CSMA/CD, this stands for Carrier Sense Multiple Access with Collision Detection.

To understand what this means lets separate it into three parts:

a. **Carrier sense:** When a device connected to an Ethernet network wants to send data it first checks to make sure it has a carrier on which to send its data.

b. **Multiple access:** This means that all machines on the network are free to use the network whenever they like so long as no one else is transmitting.

c. **Collision detection:** A means of ensuring that when two machines start to transmit data simultaneously, the resultant corrupted data is discarded and retransmissions are generated at differing time intervals.

Basic ethernet bus

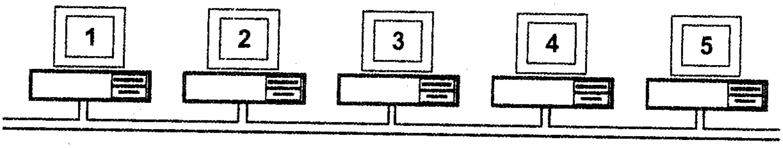


Figure 4.8: Basic ethernet bus

a. This is a coax based Ethernet network where all machines are daisy chained using RG58 coaxial cable (sometimes referred to as Thin Ethernet or Thin - net)

b. Machine 2 wants to send a message to machine 4, but first it 'Listens' to make sure no one else is using the network.

c. If it is all clear, it starts to transmit data on to the network. Each packet of the data contains the destination address, the senders address and the course the data is to be transmitted.

d. The signal moves down the cable and is received by every machine on the network but because it is only addressed to number 4, the other machines ignore 'd'.

e. Machine 4 then sends message back to number 2 acknowledging receipt of the data.

f. But what happens when two machines try to transmit at same time? A collision occurs, and each machine has to "back off" for a random period of time before re-trying.

Collision: The collision destroys both signals and each machine knows this has happened because they do not 'hear' their own transmission within a given period of time (this time period is a propagation delay and is equivalent to the time it takes for a signal to travel to the furthest part of the network and back again).

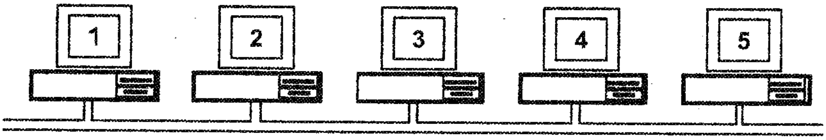
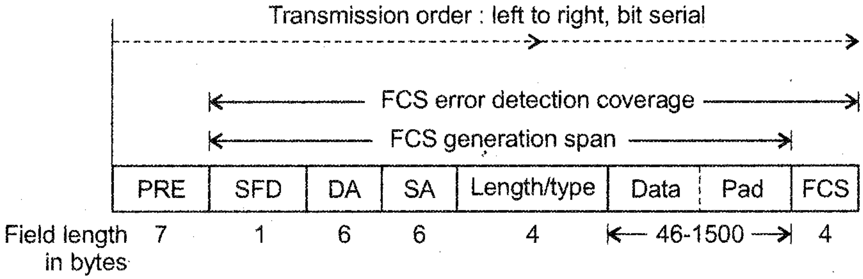


Figure 4.9: Collision

Both machines then wait for a random period of time before retyping. On small networks this all happens so quickly that it is virtually unnoticeable, however, as more and more machines are added, the network of collisions rises dramatically and eventually results in slow network response.

The basic ethernet frame format

The IEEE 802.3 standard defines data frame format that is required for all MAC implementations, plus several additional optional formats that are used to extend the protocol's basic capability. The basic data frame format contains the seven fields shown in *figure (4.10).*



PRE : Preamble

SFD : Start of Frame Delimiter

DA : Destination Address

SA : Source Address

FCS : Frame Check Sequence

Figure 4.10: Basic IEEE 802.3 MAC Frame format

a. **PRE (preamble):** Consists of 7 bytes. The PRE is an alternating pattern of ones and zeros that tells receiving stations that frame is coming and provides a means to synchronize the frame reception portions of receiving physical layers with the incoming bit stream.

b. **SFD (Start of Frame Delimiter):** Consists of 1 byte. SFD is an alternating pattern of 0's and 1's, ending with two consecutive 1-bits indicating that the next bit is the left most bit in the left most byte of the destination address.

c. **DA (Destination Address):** Consist of 6 bytes. DA field identifies which station (s) should receive the frame. The leftmost bit in DA field indicates whether the address is an individual address (indicated by 0) or a group address (indicated by 1). The second bit from the left indicates whether the DA is globally administered (indicated by 0) or locally administered (indicated by 1).

d. **SA (Source Address):** Consists of 6 bytes. The SA field identifies the sending station. The SA is always an individual address and the left most bit in the SA field is always 0.

e. **Length / type:** Consists of 4 bytes. This field indicates either the number of MAC client data bytes that are contained in the data field of the frame or the frame type ID if the frame is assembled using an optional format. If the length/type field value is less than or equal to 1500, the number of LLC bytes in the data field is equal to the length/type field value. If the length/type field value is greater than 1536, the frame is an optional type frame and the length/type field value identifies the particular type of frame being sent or received.

f. **Data:** Data is a sequence of n bytes of any value, where n is less than or equal to 1500. If the length of data field is less than 46, the data field must be extended by adding a filler (a pad) sufficient to bring the data field length to 46 bytes.

g. **FCS (Frame Check Sequence):** Consists of 4 byte. This sequence contains a 32 bit Cyclic Redundancy Check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames. The FCS is generated over DA, SA, length/type and data fields.

ii. ARCnet

The Attached Resource Computer Network (Arcnet) was developed by Datapoint Corporation in 1977. It is simple, inexpensive, flexible network architecture designed for workgroup-sized networks. The first ArcNet cards were shipped in 1983.

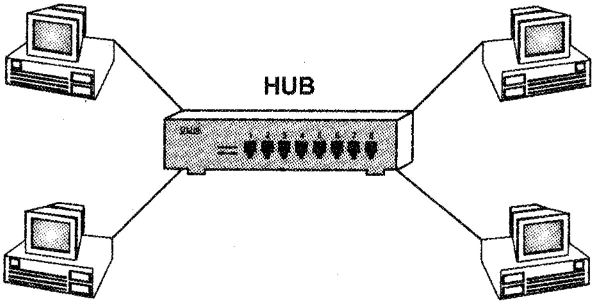


Figure 4.11: Simple star wired ArcNet network

ArcNet technology predates IEEE project 802 standards, but loosely maps to the 802.4 document. This specifies the standards for token passing bus networks using broadband cable. An ArcNet network can have a star bus or bus topology.

Working of ArcNet

ArcNet uses a token passing access method in a star bus topology passing data at 2.5 Mbps. A successor to the original ArcNet, ArcNet plus, supports data transmission rates of 20 Mbps. Because ArcNet is a token passing architecture, a computer in a ArcNet network must have the token in order to transmit data. The token moves from one computer to the next according to their numerical order regardless to how they are placed on the network. This means that the token moves from computer 1 to computer 2 in order even if computer 1 is at one end of the network and computer 2 is at the other end of the network.

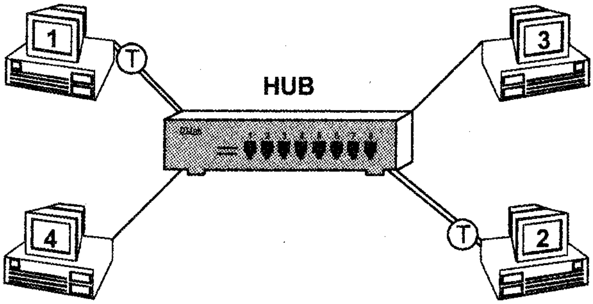


Figure 4.12: Token movement based on numerical order

The standard ArcNet packet contains:

a. Destination Address

b. Source address

c. Upto 508 bytes of data

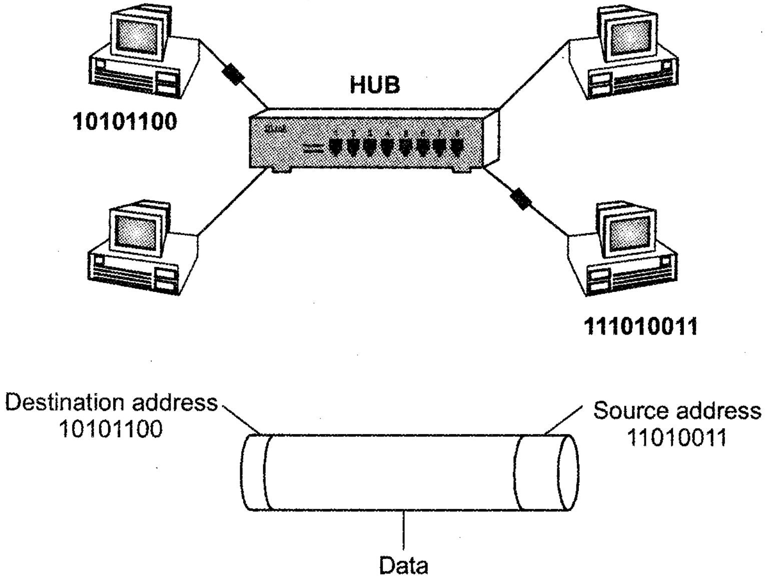


Figure 4.13: An ArcNet packet contains source and destination addresses

iii. Token Bus: IEEE 802.4

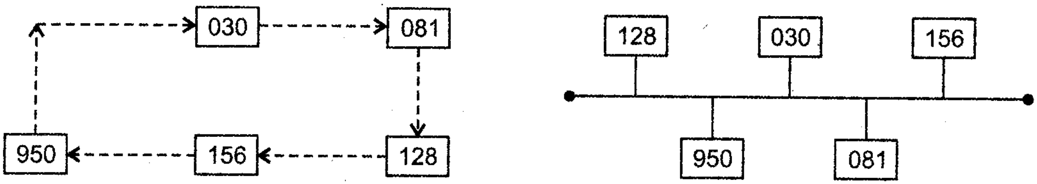
a. The IEEE 802.4 standard for media access control is known as Token bus.

b. Token bus is a Linear or tree shaped cable through which different stations are interconnected.

c. Logically the interconnected stations from a ring is as shown in the below *figure 4.14 (a).* The physical topology is as shown in the *figure 4.14 (b).*

d. Each station knows its own identification number on the identity of the stations preceding and following it.

e. The sequence number and the physical location of a station on the bus are not related to each other.



(a) Logical sequence of token passing

(b) Physical topology in token passing

Figure 4.14: Token bus

Look at the sequence of stations in the logical sequence of token passing as shown in *figure 4.14 (a).* It shows that the stations connected on a bus are arranged in a logical sequence.

Token

After initialization of a logical ring, the station bearing the highest number sends out the first frame. After doing so, it passes a permission to its neighboring station that now the neighboring station can send its frame. This permission is passed by sending a special control frame called 'Token'.

Media access control

The operation of tokes bus taken place as follows:

a. At any time, the station which holds the takes only can transmit its data frames on the bus. Every frame contains source and destination addresses.

b. All the other stations are ready to receive these data frames.

c. As soon as the transmission time of a station is over, it passes the token to the next station in the logical sequence. The transmission is then taken over by the next station.

d. In one cycle of operation, each station will get an opportunity to transmit once. The same station can get more number of chances to transmit in one cycle if more than one addresses are assigned to it.

Frame format

The frame format as specified by IEEE 802.4 is as shown in *figure.*

Number of Bytes →	1(min)	1	1	2-6	2-6		4	1
	Preamble	SD	FC	DA	SA	Data	FCS	ED

Preamble	:	Bit Synchronization
SD	:	Frame start Delimiter
FC	:	Frame Control (Type)
DA	:	Destination Address
SA	:	Source Address
DATA	:	Data field
FCS	:	Frame check sequence
ED	:	End delimiter

Figure 4.15: Format of IEEE 802.4 frame

a. **Preamble:** It is at least one octet long and used for bit synchronization.

b. **Start delimiter:** It is a unique one byte pattern which marks the beginning of a frame.

c. **Frame control:** It indicates the type of frame. It is one octet long and indicates if the frame is a data frame or control frame. Token is one of the control frames.

d. **Destination address:** It contains destination address and it is 2 to 6 bytes long.

e. **Frame check sequence:** This field contains a CRC code. It is 4 byte long and is used to check on DA, SA, FC and Data fields.

f. **End delimiter:** This is a one byte unique bit pattern which marks the end of the frame.

iv. Token Ring System [IEEE 802.5]

a. A token ring system is as shown in *figure 4.16.* It consists of a number of stations connected to the ring through a Ring Interface Unit (RIU).

b. RIU is a repeater, therefore it regenerates the received data frames and sends them to the next station after some delay.

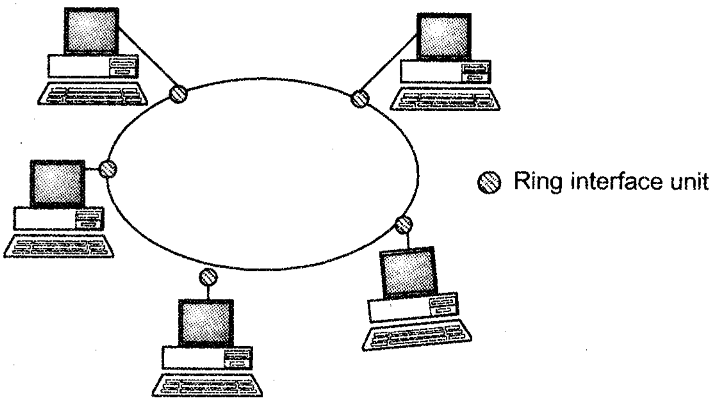


Figure 4.16: Token ring system

Media access control

a. In token bus system, the access to the medium (i.e. who will transmit) is controlled by the special control frame called token.

b. The token is passed from one station to the other round the ring. The sequence of token passing is dependent on the physical location of the stations connected to the ring.

c. A station which is in possession to hold the token only can transmit the frames. It may transmit one or more data frames but before the expiry of Token Holding Time (THT).

d. Typically this time is of 10 msec. After the THT, the token frame must be handed over to some other station.

Frame format

The IEEE 802.5 has standardized the formats for the token frame and data frame. They are as shown in the *figure 4.17.*

Token Frame

SD	AC	ED

Data Frame

SD	AC	FC	DA	SA	Data	FCS	ED	FS

SD: Start Delimiter

AC: Access Control

ED: End Delimiter

FC: Frame Control

DA: Destination Address

SA: Source Address

FCS: Frame Check Sequence

FS: Frame Status

P	P	P	T	M	R	R	R

Access Control (AC) Field

A	C	X	X	A	C	X	X

Frame status (FS) Field

Figure 4.17: Format of IEEE 802.5 frames

i. **Start delimiter:** This is one byte long containing a unique pattern which is used to mark the start of the token or data frames.

ii. **Access control:** This is also one octet long. It consists of the priority bits (p), token bits (T), monitoring bits (M) and reserved bits (R) as shown in above *figure.*

iii. **Frame control:** This is also one octet long used to indicate type of frame, data frame or control frame. It is also used to distinguish between different types of control frames.

iv. **Destination address:** It is 2 to 6 octets long indicating the destination address.

v. **Source address:** It is also 2 to 6 octet long indicating the source address.

vi. **Data field:** There is no limitation on the size of this field. So it can have 0 or more number of octets. The token holding time will decide the maximum size of the data field.

vii. **Frame check sequence:** This field is 4 byte long. It consists of a CRC code for error detection.

viii. **End delimiter:** This is one octet long field. It contains a unique bit pattern to mark the end of token or data frame.

ix. **Frame status:** This is one byte long. It consists of two address recognized bit (A), two frame copied bits (C) and preserved bits (X). Its shown in above *figure.*

▶ Comparison of 802.3, 802.4, 802.5 IEEE Standard

	Parameter	802.3 Ethernet	802.4 Token bus	802.5 Token ring
i.	Physical topology	Linear	Linear	Ring
ii.	Logical topology	None	Ring	Ring
iii.	Contention	Random Chance	Token	Token
iv.	Adding Stations	A new station can be added almost anywhere on the cable at anytime	Distributed algorithms are needed to add new stations.	Must be added between two specified stations.

v.	Performance	Stations often transmit immediately under light loads, but heavy traffic can reduce the effective data to nearly 0.	Stations must wait for the token even if no other station is transmitting. Under heavy load, token passing provides fair access to all stations.	Stations must wait for the token even if no other station is transmitting under heavy loads, token passing provides fair access to all stations.
vi.	Maximum delay before transmitting	None	Bounded, depending on distance spanned and number of stations.	Bounded, depending on distance spanned and number of stations. However if priorities are used, a low priority station may have no maximum delay.
vii.	Maintenance	No control on maintenance	Distributed algorithm provides Maintenance	A designated monitor station performs maintenance.
viii.	Cable used	Twisted pair, co-axial fiber optic.	Co-axial	Twisted pair is fiber optic
ix.	Cable length	50 m to 2000 m	200 m to 500 m	50 m to 1000m
x.	Frequency	10 to 100 Mbps	10 Mbps	4 to 100 Mbps.
xi.	Frame structure	1500 bytes	8191 bytes	5000 bytes

7. Wireless LAN

The wireless LAN's are becoming more and more popular because they can satisfy the requirements like mobility, relocation of user, ad-hoc networking and coverage of locations which are difficult to wire.

1

Apr. 2013 – *5M*
Write a short note on Wireless LAN Architecture.

Earlier the wireless LAN's were costly, could support only low data rates, a license was required. Hence there were limitations on the practical utility of wireless LAN's.

▶ Applications of Wireless LAN

i. LAN extension

ii. Cross building interconnection

iii. Nomadic access

iv. Ad-hoc networks.

▶ Wireless LAN: 802.11

1
Apr. 2013 – *5M*
Write a short note on Wireless Fiedelity.

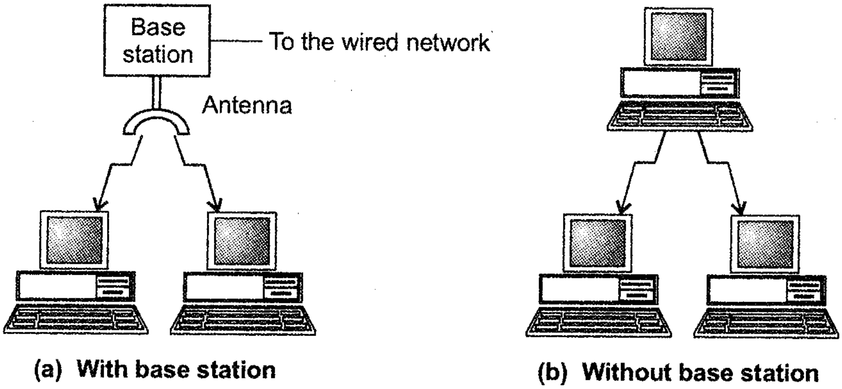
i. In wireless LAN, each computer and note book computer is equipped with a short range transmitter and receiver to allow communication between them.

ii. IEEE committee standardized the wireless LAN and the standard was 802.11.

iii. This standard had to work in two different modes:

a. In the presence of base station.

b. In the absence of base station.



(a) With base station

(b) Without base station

Figure 4.18: Wireless LAN

7.1 IEEE 802.11 Architecture

3
Apr. 12, Oct.12 – *5M*
Explain the architecture of IEEE 802.11 (wireless LAN).
Apr.2010 – *5M*
Explain Wireless LAN Architecture (IEEE 802.11).

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells, where each cell (called Basic Service set or BSS, in 802.11 nomenclature) is controlled by Base station (called Access point or AP).

Even though that a wireless LAN may be formed by a single cell, with a single Access Point (and as will be described later, it can also work without an Access Point), most installations will be formed by several cells, where the Access points are connected through some kind of backbone (called Distributed system or DS), typically Ethernet and in some cases wireless itself.

The whole interconnected wireless LAN including the different cells, their respective Access points and Distribution system is seen to the upper Layer of OSI Model as a single 802 network and is called in the standard as Extended Service Set (ESS).

The following fig shows a typical 802.11 LAN, with the components described previously:

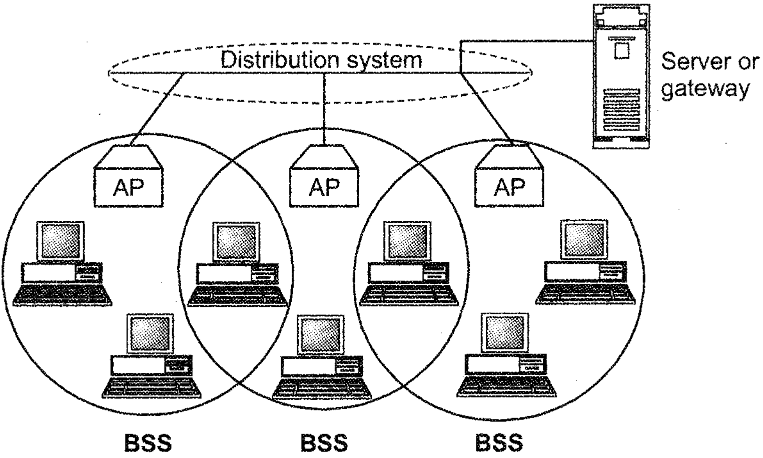


Figure 4.19: 802.11 LAN

The standard also defines the concept of portal a portal is a device that inter connects between an 802.11 and another 802 LAN.

7.2 Frame Types

There are three main types of frames:

i. **Data frame:** Data frame are used for data transmission.

ii. **Control frame:** Control frame are used to control access to the medium.

iii. **Management frame:** Management frame are the frames that are transmitted in the same way as data frames to exchange management information, but are not forwarded to the upper layer's.

Each of these types is as well subdivided into different subtypes, according to their specific function.

7.3 Frame Formats

All 802.11 frames are composed of the following components:

Preamble	PLCP Header	MAC data	CRC

▶ Preamble

1

Oct. 2011 – *5M*
Explain frame format for wireless LAN (IEEE 802.11).

This is physical dependent and includes:

i. **Synch:** An 80 bit sequence of alternating zeros and ones, which is used to select the appropriate antenna, and to reach steady-state frequency offset collection and synchronization with the received packet timing.

ii. **SFD:** A start frame delimiter which consist of a 16 bit binary pattern 0000 1100 1011 1101, which is used to define the frame timing.

▶ PLCP Header

The PLCP header is always transmitted at 1 Mbit/s and contains logical information that will be used by the PHY layer to decode the frame, and consists of:

i. **PLCP - PDU length word** which represents the number of bytes contained in the packet, this is useful for PHY to correctly detect the end of packet.

ii. **PLCP signaling field** which currently contains only the rate information, encoded in 0.5 MBPS increments from 1 Mbit/s to 4.5 Mbit/s.

iii. **Header error check field** which is a 16 Bit CRC error detection field.

7.4 MAC Sublayer

Figure 4.20 shows the general MAC frame format, part of the fields are only present on part of the frames as described later.

Octets:	2	2	6	6	6	2	6	0-2313	4
	Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Frame relay	CRC

MAC header

Figure 4.20: MAC header

i. **Frame control field:** The frame control field contains the following information:

	Protocol version	Type	Subtype	To DS	From DS	More frag.	Retry	Power mgt	More data	WEP	Order
Bits:	2	2	4	1	1	1	1	1	1	1	1

Figure 4.21

a. *Protocol version:* This field consists of 2 bit's which are invariant in size and placement across following versions of the 802.11 standard and will be used to recognize possible future versions. In the current version of the standard the value is fixed as 0.

b. *Type and subtype:* This 6 bits define the type and subtype of the frame.

c. *ToDS:* This bit is set to 1 when the frame is addressed to the AP for forwarding it to the Distribution system. The Bit is set to 0 in all other frames.

d. *From Ds:* This bit is set to 1 when the frame is coming from the Distribution system.

e. *More Fragments:* This bit is set to 1 when there are more fragments belonging to the same frame following this current fragment.

f. *Retry:* This bit indicates that this fragment is a retransmission of a previously transmitted fragment, this will be used by the receiver station to recognize duplicate transmissions of frames that may occur when an acknowledgment packet is lost.

g. *More data:* This bit indicates power management and it is used by the AP to indicate that there are more frames buffered to this station.

h. *Power management:* This bit indicates power management mode that the station will be in after the transmission of this frame. This is used by stations which are changing state either from power save to active or vice-versa.

i. *WEP:* This bit indicates that the frame body is encrypted according to the WEP algorithm.

j. *Order:* This bit indicates that this frame is being sent using the strictly – ordered service class.

ii. **Duration / ID:** This has two meanings

a. In power save poll message this is the station ID.

b. In all other frames this is the duration value used for NAV calculation.

iii. **Address fields:** A frame may contain upto 4 addresses depending on the TODs and from DS bits defined in the control field as follows:

Address 1: is always the recipient address. If TODs is set this is the address of the AP, if TODs is not set then this is the address of the end-station.

Address 2: is always the transmitter address. If from DS is set this is the address of the AP, if it is not set then it is the address of the station.

Address 3: is in most cases the remaining missing address, on a frame with 'from DS' is set to 1, then Address 3 is the original source address, if the frame has the TODs set then Address 3 is the destination address.

Address 4: is used on the special case where a wireless distribution system is used, and the frame is being transmitted from one access point to another, in this case both the TODs and 'from DS' bits are set, so both the original destination and the original source addresses are missing.

iv. **Sequence control:** The sequence control field is used to represent the order of different fragments belonging to the same frame and to recognize packet duplications, it consists of two subfields fragment number and sequence number which defines the frame and the number of the fragment in the frame.

v. **CRC:** The CRC is a 32 bit Cyclic Redundancy Check (CRC).

7.5 Addressing Mechanism

The local network addresses used in IEEE 802 networks and FDDI networks are called MAC addresses; they are based on the addressing scheme used in early ethernet implementations. A MAC address is a unique serial number. Once a MAC address has been assigned to a particular network interface (typically at time of manufacture), that device should be uniquely identifiable amongst all other network devices in the world. This guarantees that each device in a network will have a different MAC address (analogous to a street address). This makes it possible for data packets to be delivered to a destination within a subnetwork, i.e., hosts interconnected by some combination of repeaters, hubs, bridges and switches, but not by network layer routers. Thus, for example, when an IP packet reaches its destination (sub) network, the destination IP address (a layer 3 or network layer concept) is resolved with the Address Resolution Protocol for IPv4 or by Neighbor Discovery Protocol (IPv6) into the MAC address (a layer 2 concept) of the destination host.

Examples of physical networks are Ethernet networks and Wi-Fi networks, both of which are IEEE 802 networks and use IEEE 802 48-bit MAC addresses.

A MAC layer is not required in full-duplex point-to-point communication, but address fields are included in some point-to-point protocols for compatibility reasons.

7.6 Bluetooth Technology

Bluetooth is a set of specification for physical layer of wireless LAN using short distance radio frequency interface. It eliminates the need for cables between a laptop and a mobile cellular phone with a low cost short range radio link. This technology supports reliable data and voice communication in ad-hoc wireless networks. Printers, personal digital assistants, desktops, fax machines, keyboards and all other digital devices are part of the bluetooth technology.

2

Oct. 10, Apr. 10 – *5M*
Write short notes on Bluetooth.

▶ Evolution

The idea that resulted in the bluetooth wireless technology was born in 1994, when Ericsson Mobile communications decided to investigate the feasibility of a low – power, low cost radio interface between mobile phones and their accessories. The idea was that a small radio built into both the cellular telephone and the laptop would replace the cumbersome cable used today to connect the two devices. A year later, the engineering work began and the true potential of the technology showed possibilities to become a universal bridge to existing data networks, a peripheral interface and a mechanism to form small private ad-hoc groupings of connected devices away from fixed network infrastructures.

In February 1998, The Special Interest Group (SIG) was formed. The assignment of the SIG was to monitor the technical development of short range radio and to create an open global standard, thus preventing the technology from becoming the property of a single company. This work resulted in the release of the first bluetooth specification in July 1999.

Today, bluetooth is the implementation of a protocol defined by the IEEE 802.15 standard.

▶ Need for Bluetooth

The recent development in the field of networking and the mobility among people have increased the demand for a system that could easily connect devices for transfer of data and voice over short distances, without cables.

▶ Features of Bluetooth

i. **Inter-operability:** There should be inter operability between different devices from various manufacturers as long as they share the same profile.

ii. **Compliance:** The bluetooth qualification program guarantees global inter – operability between devices, regardless of the vendor and regardless of the country in which they are used. Hence, all bluetooth devices are globally compliant.

iii. **Usage Models:** bluetooth specification mainly addresses usage model, concerning the telecom and computing industries.

▶ Working of Bluetooth

Bluetooth is an open specification for short range wireless transmission of voice and data. It provides a simple, low cost seamless wireless connectivity between Personal Digital Assistants (PDAs), cellular phones, laptops and other portable handheld devices.

Bluetooth supports transmission of voice and data over 2.4 GHz radio frequencies, using a frequency-hopping scheme with a maximum of 1600 hops per second, resulting in a new frequency being used to transmit each packet. This scheme allows for smooth operation inspite of fading due to reflecting obstacles or excessive distance and inspite of noise due to Electro Magnetic Interference (EMI), such as that generated by microwave ovens. In addition, bluetooth uses short packets and fast acknowledgements to increase reliability and employs forward error correction to reduce the effects of random noise. Bluetooth also includes encryption and authentication mechanism. The entire Bluetooth technology is implemented in a single g-millimeter-by-g-millimeter chip. Bluetooth voice transmission can use upto three concurrent synchronous 64 kbps voice only channels or one channel that simultaneously supports both asynchronous data and synchronous voice transmission. The voice channels use the continuous variable slope delta modulation coding scheme.

▶ Bluetooth Architecture

Bluetooth communication occurs between a master radio and a slave radio. Bluetooth radios are symmetric in that the same device may operate as a master and also the slave. Each radio has a 48-bit unique device address (BD-ADDR) that is fixed.

Bluetooth defines two types of networks.

i. Piconet

ii. Scatternet

3

Apr. 13, 11 – *5M*
Explain Bluetooth Architecture.

Apr. 2012 – *5M*
Explain Bluetooth architecture with applications.

i. **Piconet architecture:** Generally, Bluetooth network is small so it is called as a, 'smallnet' or 'piconet'. A piconet can have upto 8 stations, one of which is called 'primary' or 'master' station and the other stations are called 'secondary' or 'slave' stations. All the secondary stations synchronize their clock and hopping sequence with primary station. Piconet can have only one primary station.

The communication between primary and secondary station may be either one-to-one or one-to-many. Piconet can have 7 maximum secondaries, an additional 8 secondaries can be in the parked state. A parked secondary station is synchronized with the primary but cannot participate in communication until it is moved from parked state. Only 8 stations of piconet can be activated that means they can take active participation in communication. All the 7 active nodes of piconet should be placed within 10 meter distance.

Piconet is just following the centralized TDM system. Master controls the clock and determines which device gets to communicate in which time slot. All communication is in between master and slave, direct slave-slave communication is not possible.

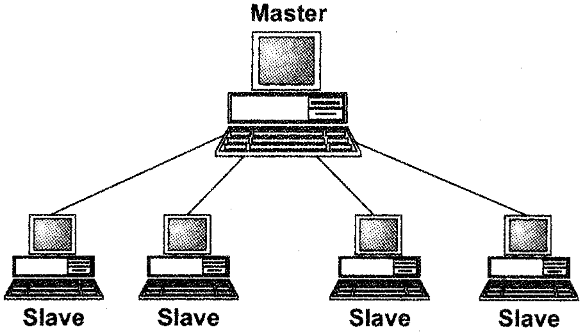


Figure 4.22: Piconet

ii. **Scatternet architecture or scatternet:** Interconnected collection of many piconets is called, 'scatternet'. There are two possible connection of scatternet.

a. A secondary station of one piconet can be a primary station of other piconet. This station can receive messages from the primary in the first piconet, and deliver them to secondaries in the second piconet.

b. One station can be member in two piconet that is called as a, 'Bridge slave' In each piconet there can be 7 active nodes. In all sactternet, there can be 255 parked nodes.

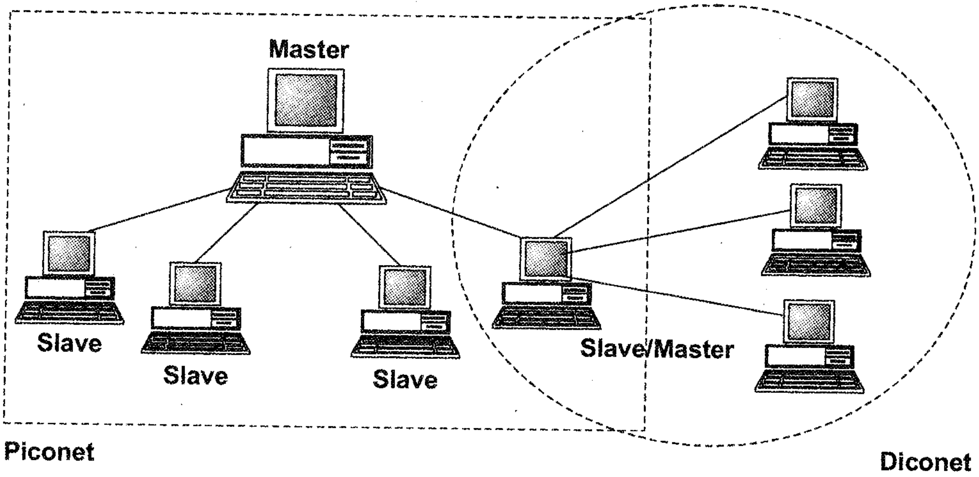


Figure 4.23: Scatternet

▶ Applications

i. **Data exchange:** This service enables a bluetooth user to synchronise his phone to his PC without taking his phone out of his pocket. Bluetooth allows synchronization to start when the phone is brought into the range of the PC.

ii. **LAN connection:** Due to non-requirement of line-of-sight, bluetooth is well suited to wirelessly connect a device to a wired LAN.

iii. **Dial-up networking:** By emulating EIA /T1A 232 connection between a portable computer and a mobile phone, dialup connection to the internet is possible. The mobile phone can be in movement, limited to the range without breaking the dial – up – connection.

iv. **Voice application:** A synchronous voice channel is a native feature of bluetooth specification. bluetooth has the ability to reserve bandwidth for carrying the digital voice data.

▶ Difference between Bluetooth and IEEE 802.11x

	Bluetooth	IEEE 802.11x
i.	Bluetooth hop frequency is 1,600 hops/ second.	IEEE 802.11x hop frequency is 2.5 hops/seconds.
ii.	Data transfer rate is 1 Mbps.	Data transfer rate is 11 Mbps.
iii.	Transmission range is 10 n.	Transmission range is 15-150 n indoor and 300m outdoor.
iv.	Bluetooth uses lower transmission power.	IEEE 802.11 uses more transmission power than bluetooth.
v.	It is used to connect devices that are in close proximity such as palm computing devices attached to smart phones, notebooks to printers.	It is a full LAN connectivity solution designed to provide full network service at ethernet data rate.
vi.	It is being a standard for short time network.	It is a standard for LAN and is for longer time network.
vii.	Bluetooth uses GFSK (Gaussian Frequency Shift Key) modulation technique.	It uses CCK (Complementary Code Keying) modulation technique.

PU Questions

5 Marks

[Apr. 2013 – *5M*] 1. What is NIC? Explain components and functions of NIC.

[Apr. 2013 – *5M*] 2. Write a short note on Wireless LAN Architecture.

[Apr. 2013 – *5M*] 3. Write a short note on Wireless Fiedelity.

[Apr. 2013, 2011 – *5M*] 4. Explain Bluetooth Architecture.

[Oct. 2012 – *5M*] 5. What is full form of NIC? List its types. Explain any one in detail.

[Oct. 12, Apr. 12 – *5M*] 6. Explain the architecture of IEEE 802.11 (wireless LAN).

[Apr. 2012 – *5M*] 7. Explain Ethernet with reference to features and types.

[Apr. 2012 – *5M*] 8. Explain Bluetooth architecture with applications.

[Apr. 2012 – *5M*] 9. Describe the functions of NIC.

[Oct. 2011 – *5M*] 10. Explain frame format for wireless LAN (IEEE 802.11).

[Oct. 2011 – *5M*] 11. What is NIC? Explain its types.

[Oct. 10, Apr. 10 – *5M*] 12. Write short notes on Bluetooth.

[Apr. 2010 – *5M*] 13. Explain Wireless LAN Architecture (IEEE 802.11).

Chapter 5

NETWORK CONNECTIVITY DEVICES

1. Categories of Connectivity Devices

1.1 Hub

i. A hub is a small, simple, inexpensive device that joins multiple computers together at a low level network protocol layer.

1

Oct. 2010 – ***1M***
Define Hubs.

ii. A hub is a physical layer device.

iii. Most hubs manufactured today support the ethernet standard.

iv. A hub is a small rectangular box as shown in *figure 5.1* often constructed mainly of plastic, that receives its power from an ordinary wall outlet. A hub joins multiple computers (or other network devices) together to form a single network segment.

v. On this network segment, all computers can communicate directly with each other.

vi. Ethernet hubs are by far the most the most common type, but hubs for other types of networks (such as USB) also exist.

vii. A hub includes a series of parts that each accept a network cable. Small hubs network four computers. They contain four or sometimes five parts. Larger hubs contain eight, 12, 16 and 24 parts.

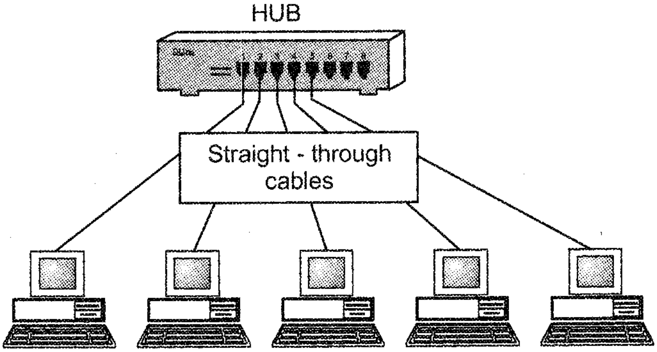


Figure 5.1: An illustration of hub in operation

▶ What Hub does?

A hub is a multiport repeater, therefore, hubs are a subset of repeaters. They receive data and then repeat it out at all ports. Hubs can be purchased in many different configurations with a fixed number of ports. Hubs are utilized in star physical topologies, hence have one PC per port.

▶ Working of hub

Hubs can support different media types-ethernet and can operate over unshielded twisted pair, thick and thin co-axial cable and fiber optic. This ability to support multiple media types enables the integration of network segments, having different cabling, with relative ease.

▶ Key Features of Hubs

i. Hub operates at physical layer in OSI model.

ii. At the physical layer, hubs can support little in the way of sophisticated networking.

iii. Hubs do not read any of the data passing through them and are not aware of a packet's source or destination.

iv. A hub simply receives incoming packets, possibly amplifies the electrical signal, and broadcasts these packets to all devices on the network (including the one that sent the packet).

▶ Types of Hubs

i. **Active hub:** An active hub is a powered distribution point with active devices which drive distant nodes upto 1 km away. It can be cascaded to connect 8 connections to which passive hubs: file servers or other active hubs can be connected. Maximum distance covered by an active hub is about 2000 feet. Active hubs require electrical power to run.

1 **Apr. 2013 – *5M***
Explain active and passive hub.

Active hub takes active participation in data communication within the network / LAN. They receive signal (data) from the input port and stores it for sometime before forwarding it, this feature allows the hub to monitor the data it is forwarding, some hubs come with a feature that helps in transmitting data that has high priority before the data that has lower priority. Some hubs help in synchronizing data communication and some active hubs come with a feature that rectify the data / signal before forwarding it in the network / LAN.

Active hubs also help in troubleshooting at certain level.

ii. **Passive hub:** As the name suggests it is a passive distribution point which does not use power or active devices in a network to connect upto 4 nodes within a very short distance. Maximum distance covered by a passive hub is about 300 feet. Passive hub do not require electrical power to run.

Passive hub works just as an interface between the topology and does not provide any additional feature. These types of hubs do not help in rectifying / enhancing the signals they pass on in the network. They do not help in enhancing the performance of network / LAN. It is very hard to get any help from the passive hubs while troubleshooting in case there is any fault in the hardware or the network.

A passive hub simply receives signals on input ports and broadcasts it on output ports without even rectifying it. They do not amplify the electrical signal of incoming packets before broadcasting them to the network.

iii. **Hybrid hub:** Advanced hubs that will accommodate several different types of cables are called as hybrid hubs. A hub based network can be expanded by connecting more than one hub. Hubs remain a very popular device for small networks because of their low cost. Hubs are versatile and offer several advantages over systems that do not use hubs. In the standard linear bus topology, a break in the cable will take the network down. With hubs, however, a break in any of the cables attached to the hub affects only that segment. The rest of the network keeps functioning as shown in *figure 5.2.*

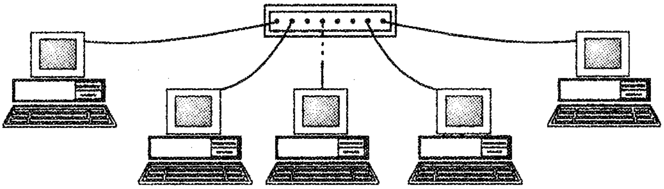


Figure 5.2: A break or unplugged cable takes down only the unplugged computer

1.2 Repeaters

1
Oct. 2010 – *1M*
Define Repeaters.

1
Apr. 2010 – *5M*
Write a short note on Repeaters.

A repeater is the simplest facility used for network interconnection, whose major function is to receive a network signal from one LAN terminal cable segment and to regenerate and retransmit the signal as it is in its original strength over one or more other cable segment. Basically repeater regenerates the strength of the signal before transmitting it.

Repeaters operate in the OSI model physical layer and are transparent to all the protocols operating in the layers above the physical layer.

A specific LAN implementation usually places a limit on the physical size of a single cable segment. The limit is based on the physical medium and transmission techniques used.

Repeaters allow a network to be constructed to exceed the size limit of a single, physical, cable segment. The number of repeaters that can be used in tandem is generally limited by a particular LAN implementation. Using a repeater between two or more LAN cables segment requires that the same physical layer protocol be used to send signal over all the cable segments.

Example of how this work

Two LAN cable segments in an ethernet LAN that use baseband transmission could be connected with a repeater. Different types of physical transmission medium can be connected using a properly designed repeater as long as they handle similar type of signal.

▶ Advantages

i. Simple to connect.

ii. Cost effective.

iii. Ability to strengthen signal.

▶ Disadvantages

i. Repeaters provide no method for isolating traffic generated on one cable segment from traffic generated by the other cable segment.

ii. When network uses a repeater to connect cable segment A to segment B whether or not there is a station in segment B, i.e., the destination of the signal.

▶ Working of Repeater

A repeater works at the OSI physical Layer to regenerate the network's signals and resends them out on other segments.

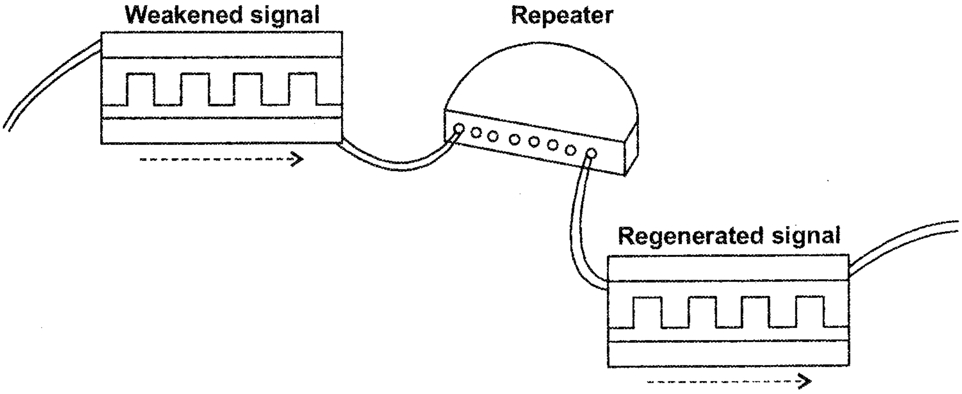


Figure 5.3: Repeaters regenerate weakened signals

i. A repeater takes a weak signal from one segment, regenerates it and passes it to the next segment. To pass data through the repeater in a usable fashion from one segment to the next, the packets and Logical Link Control (LLC) protocol must be the same on each segment.

ii. Repeaters do not translate or filter anything. For a repeater to work, both segments that the repeaters joins must have the same access method. The two most common access methods are CSMA/CD and token passing i.e., they cannot translate an ethernet packet into a Token Ring packet.

▶ A repeater

i. Connects two segments of similar or dissimilar media.

ii. Regenerates the signal to increase the distance transmitted.

iii. Functions in the physical layer of the OSI model.

iv. Passes all traffic in both directions.

1.3 Bridges

A Bridge is an electrical device which connects and passes packets between two network segments.

i. A bridge is a hardware device that connects LANs together.

ii. It can be used to connect LANs of the same type, such as two Token Ring segments or LANs with different types of media such as Ethernet and Token Ring.

iii. It operates at Data link layer of OSI reference model.

iv. It is a networking component used either to extend or to segment networks.

v. They can be used both to join dissimilar, media such as Unshielded Twisted Pair (UTP) cabling and fiber optic cabling, and to join different network architectures such as Token Ring and Ethernet.

A bridge can join segments or workgroup LANs. However, a bridge can also divide a network to isolate traffic or problems. For example, if the volume of traffic from one or two computers or a single department is flooding the network with data and slowing down the entire operation, a bridge could isolate those computers or that department.

▶ Bridge can be used to

i. Expand the distance of a segment.

ii. Provide for an increased number of computers on the network.

iii. Reduce traffic bottlenecks resulting from an excessive number of attached computers.

iv. Take an overloaded network and split it into two separate networks, reducing the amount of traffic on each segment, making each network more efficient.

v. Link unlike physical media such as twisted pair and co-axial Ethernet.

vi. Link unlike network segments such as Ethernet and Token Ring and forward packets between them.

▶ How Bridges Work?

Bridge work at data link layer of OSI model. Because they work at this layer, all information contained in the higher levels of OSI model is unavailable to them. Therefore, they do not distinguish,

i. Between one protocol and another.

ii. Bridges simply pass all protocols along the network. Because all protocols pass across bridges, it is up to the individual computer to determine which protocols they can recognize.

iii. The Data link layer has two sub layers, the logical link control sub layer and the media access control sub layer and are sometimes referred to as media access control layer bridges.

A Media Access Control Layer bridge

a. Listens to all traffic

b. Checks the source and destination addresses of each packets.

c. Builds a routing table as information becomes available.

d. Forwards packets in the following manner

- If destination is not listed in the routing table, the bridge forwards the packets to all segments or
- If the destination is listed in the routing table, the bridge forwards the packets to that segment (unless it is the same segment as the source).

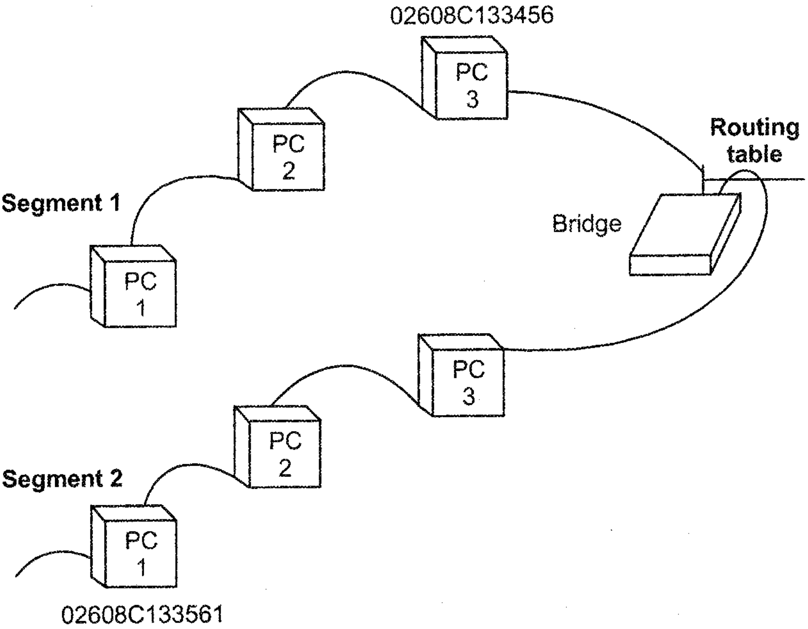


Figure 5.4: The routing table keeps track of addresses

A bridge works on the principle that each network node has its own address. A bridge forwards packets based on the address of the destination node.

Bridges actually have some degree of intelligence in that they know where to forward data. As traffic passes through the bridge, information about the computer addresses is stored in bridge's RAM. The bridge uses this RAM to build a routing table based on source addresses.

Initially, the bridge's routing table is empty. As nodes transmit packets, the source address is copied to the routing table. With this address information, the bridge learns which computers are on which segment of the network.

▶ Creating Routing Table

Bridges build their routing table based on the addresses of computers that have transmitted data on the network. Specifically, bridges use source addresses the address of the device that initiates the transmission to create a routing table.

When the bridge receives a packet, the source address is compared to the routing table. If the source address is not there, it is added to the table. The bridge then compares the destination address with the routing table data base.

i. If the destination address is in the routing table and is on the same segment and the source address, the packet is discarded. This filtering helps to reduce network traffic and isolate segments of the network.

ii. If the destination address is in the routing table and not in the same segment as the source address, the bridge forwards the packets out of the appropriate port to reach the destination address.

iii. If the destination address is not in the routing table, the bridge forwards the packet to all of its ports, except the one on which it originated.

In summary, if a bridge knows the location of the destination node, it forwards the packet to it. If it does not know the destination, it forwards the packet to all segments.

▶ Types of Bridges

There are 3 types of Bridges:

i. **Transparent bridge:** Derives its name from the fact that the devices on the network are unaware of its existence. A transparent bridge does nothing except block or forward data based on the MAC address.

There are two types of transparent bridge modes:

a. *Store-and-Forward:* Stores the entire frame and verifies the CRC before forwarding the frame. If a CRC error is detected, the frame is discarded.

b. *Cut-Through:* Forwards the frame just after it reads the destination MAC address without performing a CRC check.

2

Apr. 2012 – *5M*
What is bridge? What are its types? Explain any one.

Apr. 2010 – *5M*
What is Bridge? Explain its types.

The transparent spanning tree bridge: These bridges use a subnet of the full topology to create a loop free operation. The received frame is checked by the bridge. The destination address of arrived frame is checked with routing table in the database. Here more information is required for bridge so the bridge port is also stored in the database. This information is known as port state information and it helps in deciding that, a port can be used for this destination address or not. The port can be in a block state to fulfill the requirements of spanning tree operations or in a forwarding state. If the port is in forwarding state the frame is routed across the port.

The port can have different status such as; it may be in "disabled" state for the maintenance reason or may also be unavailable temporarily if databases are being changed in the bridge because of result of the change in the routed network.

To construct the spanning tree follow following spanning tree algorithm:

1. First of all select the root bridge. The root bridge is the bridge with the lowest serial number (this number is provided by the router manufacturer). All ports which are coming to the bridge or going out from the bridge are designated port. In our given example in figure the root bridge is 'A' and the ports coming from LAN 1 and LAN 2 are the designated ports.

2. Then select a root port for the non-root bridge. Root port for the non-root bridge is the port with the lowest path cost to the root bridge. In our example the incoming port to bridge 'B' is lowest cost path. Same logic applies for the other bridges.

3. Select a designated port on each segment. The designated port has the lowest cost to the root bridge. In our example the outgoing port from bridge 'B' is designated port which has the lowest cost to the root bridge. Same logic applies for the other bridges.

4. After spanning tree algorithm determine the lowest cost spanning tree, it enables all root ports and the designated ports, and disables all other ports.

5. The spanning tree algorithm continues to run during normal operation.

ii. **Source route bridge:** Used in token ring networks. The source route bridge derives its name from the fact that the entire path that the packet is to take through the network is embedded within the packets.

1
Apr. 2010 – *5M*
Write a short note on Source Routing Bridges.

iii. **Translational bridge:** Used to convert one networking data format top another, *for example*, from token ring to ethernet and vice versa.

Today, bridges are slowly but surely falling out of favour. Ethernet switches offer similar functionality. They can provide logical divisions or segments, in the network. In fact switches are sometimes referred to as multiport bridges because of the way they operate.

▶ Advantages

1
Oct. 2012 – *5M*
What is Bridge? What are its types? Explain advantages and disadvantages of Bridges.

i. Bridges have simple configuration modes.

ii. Bridges are simple to use and they are relatively inexpensive.

iii. It can prove to be an alternative to switches and help resulting in micro segmentation.

iv. Bridges help to lower the data load over the data link layer.

v. It appears to be translucent over the MAC layer.

vi. Bridges can be effectively programmed to disallow packets from meticulous networks.

vii. Bridges are more reliable if one wants to lower the bandwidth utilization.

▶ Disadvantages

i. All bridges are unable to read specific IP address; they are more concerned with the MAC addresses.

ii. Bridges cannot help to build a communication network between the networks of different architectures.

iii. Bridges transfer all types of broadcast messages, thus bridges are unable to limit the scope of these messages.

iv. Extremely large networks cannot rely on bridges; therefore the large networks as WAN which are IP address specific can not make use of it.

v. Bridges are expensive if we compare the prices of repeaters and hubs to it.

vi. Bridging is most suitable to be used for LAN network traffic data load. It is unable to handle more complex and variable data load such as occurring from WAN.

Bridges operates by sensing the source MAC addresses of the transmitting nodes on the network and automatically building an internal routing table. If the bridge knows which segment a packet is intended for, it forwards the packet directly to that segment. If the bridge doesn't recognize the packet's destination address, it forwards the packet to all connected segments except the one it originated on. And if the destination address is in the same segment as the source address, the bridge drops the packet. Bridges also forward broadcast packets to all segment except the originating one.

1.4 Routers

A router is a physical device that joins multiple networks together. In an environment consisting of several network segments with differing protocols and architectures, a bridge may not be adequate for ensuring for communication among all of the segments.

1

Oct. 2010 – ***1M***
Define Routers.

A network needs a device which not only knows the address of each segment but can also determine the best path for sending data and filtering broadcast traffic to the Local segment. Such a device is called a router.

Routers work at Network Layer of the OSI model. This means they can switch and route packets across multiple networks. They do this by exchanging protocol specific information between separate networks.

Routers read complex network addressing information in the packet and, because they function at a higher layer in the OSI local than bridges, they have access to additional information.

Routers can provide the following functions of a bridge:

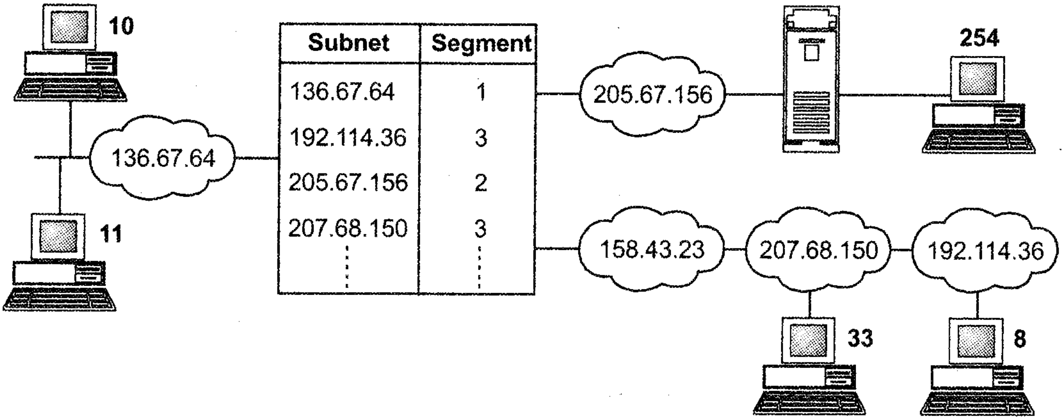
i. Filtering and isolating traffic

ii. Connecting network segment

Routers have access to more information in packets than bridges and uses information to improve packet deliveries. It is used in complex network situations because they provide better traffic management than bridges and do not pass broadcast traffic. Routers can share status and routing information with one another and use this information to bypass slow or malfunctioning connections.

▶ Working of Routers

In an heterogeneous environment, such as networks, a need of connection devices which would interconnect two different technologies is essential, the router is that device.



Subnet	Segment
136.67.64	1
192.114.36	3
205.67.156	2
207.68.150	3
⋮	⋮

Figure 5.5: Illustration of working of router

The router also serves as a routing switchboard. Routers connects two or more networks and forward data packets between them. When data arrives from one of the segments, the router decides, according to its routing table to which segment to forwards that data as shown in above *figure.* Even though each of the routers connections is to one physical network, that one network could connect to other networks through the use of other routers. This way, many networks can be interconnected.

To understand how routing occurs in such networks, refer to the below *figure* given below:

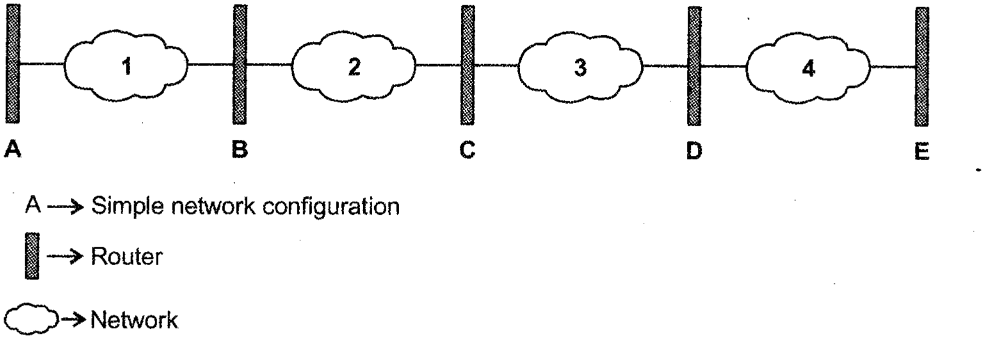


Figure 5.6: Computer network and router

Router is actually a special computer, which is dedicated to the task of interconnecting networks. It moves information from its source to its destination regardless of the middleware.

▶ Types of Routers

i. **Static routers:** must have their routing tables configured manually with all network address and paths in the internetwork. It requires an administrator to manually set up and configure the routing table and to specify each route. Always it is considered more secure because the administrator specifies each.

ii. **Dynamic routers**: automatically create their routing tables by listening to the network traffic. That is it automatically discovers the route and therefore has a minimal amount of set up and configuration. They are more sophisticated in that they examine information from other routers and make packet by packet decisions about how to send data across the network.

1.5 Switches

A switch is a small device that joins multiple computers together at a low level network protocol layer. Technically, switches operates at layer two (Data link Layer) of the OSI model.

Switches look nearly identical to hubs, but a switch generally contains more 'intelligence' than a hub. Unlike hubs, switches are capable of inspecting the data packets as they are received, determining the source and destination device of that packet, and forwarding that packet appropriately, by delivering messages only to the connected device that it was intended for. Switches conserve network bandwidth and offer generally better performance than hubs.

▶ Working of Switches

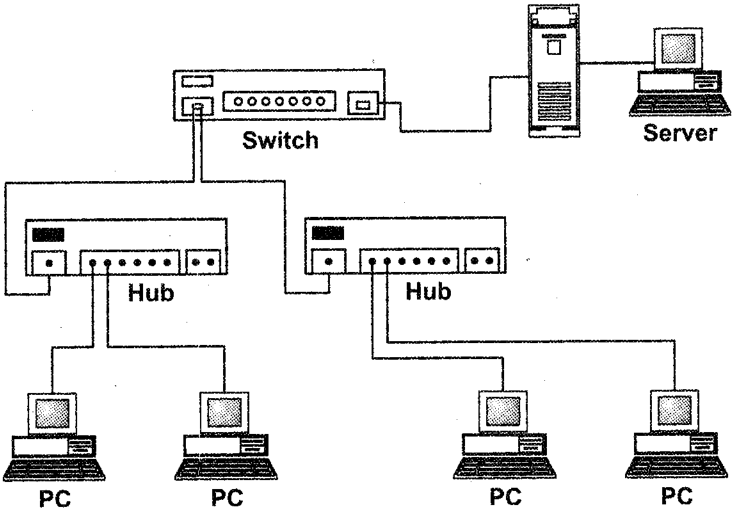


Figure 5.7: Illustration of working of switch

A switch is a networking component used to connect workgroup hubs to form a larger network or to connect computers that have high bandwidth needs as shown in *figure 5.7.*

The switches provide superior performance to hubs but are more expensive.

When a signal enters a port of the switch, the switch looks at the destination address of the frame and internally establishes a logical connection with the port connected to the destination node.

Other ports on the switch have no part in the connection. The result is that each port on the switch corresponds to an individual collision domain, and network congestion is avoided.

▶ Types of Switches

i. **Layer 2 switch:** Operates at data link Layer of OSI model and are based on bridging technologies. They establish logical connections between ports based on MAC addresses. Layer 2 switches are used for segmenting existing network into smaller collision domains to improve performance.

ii. **Layer 3 switch:** Operates at the network layer of the OSI model and are based on routing technologies. They establish logical connections between ports based on network addresses. These switches are used for connecting different networks into an internetwork. Layer 3 switches are sometimes called 'routing switching' or multilayer switches.

At present there are 3 basic architectures for data link switches:

i. **Cut through:** Where the frame is transmitted to its destination as soon as the switch has read the destination address in the frame. Cut through switches begin forwarding the frame as soon as the switch has read the destination address. It will forward the data before it has completed receiving the frame. These switches will function at wire speed, forwarding traffic as fast as it receives it. Nearly all cut through switches have no RAM buffer for storing frames.

ii. **Store and forward:** A switch performing store and forward will wait to forward a frame until it has received the entire frame. It is most often used in environments supporting receivable physical or data link protocols. Where the frame is copied into a buffer and the FCS is checked for errors before being retransmitted. Once, verified the packet is forwarded from the buffer to the appropriate destination device.

iii. **Hybrid switches:** These combine the best of both cut-through and store- and- forward by acting as a cut through switch while monitoring the traffic for errors. The switch reads only the first 64 bytes of the frame into buffer before forwarding it. If the number of errors on any given port reaches a pre-determined threshold, the hybrid switch will set the offending port to a store-and-forward mode to protect the rest of the network. The error threshold is normally configurable.

▶ Difference between Switch and Hub

	Switch	Hub
i.	A switch learns which devices are connected to its ports (by monitoring the packets it receives), and then forwards on packets to the appropriate port only.	Hub is multi-port repeater. This type of device simply passes on (repeats) all the information it receives, so that all devices connected to its ports receive that information.
ii.	Switch allows simultaneous communication across the switch, improving bandwidth.	Hubs pass on traffic to the network regardless of the intended destination; consume more bandwidth.
iii.	The switches divide the network into smaller, less congested sections.	The hubs extend the network by providing more ports
iv.	Switch divide the collision domain.	Hub can't divide the collision domain.
v.	Switches works on OSI Layer 2 and 3.	Hubs works on OSI Layer 1.
vi.	Switch is more intelligent device.	Hub is less intelligent device.
vii.	Switch is more costly solution.	Hub is less expensive.
viii.	When the network gets larger (about 50 users), you may need to use a switch to divide the groups of hubs, to cut down the amount of unnecessary traffic being generated.	In a small network (less than 30 users), a hub (or collection of hubs) can easily cope with the network traffic generated and is the ideal piece of equipment to use for connecting the users.

1

Apr. 2010 – *5M*
Compare Switch and Hub.

1.6 Gateways

A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes.

1

Oct. 2010 – *1M*
Define Gateways.

1
Apr. 2011 – *5M*
Explain Gateways.

2
Apr. 2012, 2010 – *5M*
Write short note on Gateways.

The computers that control traffic within the company's network or at the local Internet Service Provider (ISP) are gateway nodes.

In the network for an enterprise, a computer server acting as a gateway node is also acting as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

A network gateway is an internetworking system capable of joining together two networks that use different base protocols. A network gateway can be implemented completely in software, completely in hardware, or as a combination of both. Depending on the types of protocols they support, network gateways can operate at any level of the OSI model.

Because a network gateway, by definition, appears at the edge of a network, related capabilities like firewalls tend to be integrated with it. On home networks, a broadband router typically serves as the network gateway although ordinary computers can also be configured to perform equivalent functions.

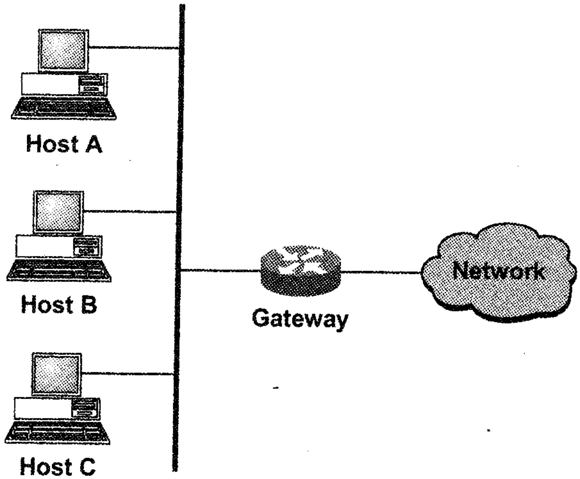


Figure 5.8: Gateway

Gateways make communication possible between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other environments data.

A gateway repackages information to match the requirements of the destination system. Gateway can change the format of a message so that it will conform to the application program at the receiving end of the transfer.

For Example, Electronic mail gateways, such as x. 400 gateway, receives message in one format, translates it and forwards in x. 400 format used by the receiver, and vice versa.

A gateway links two systems that do not use the same:

i. Communication protocols

ii. Data formatting structures

iii. Languages

iv. Architecture

▶ Working of Gateway

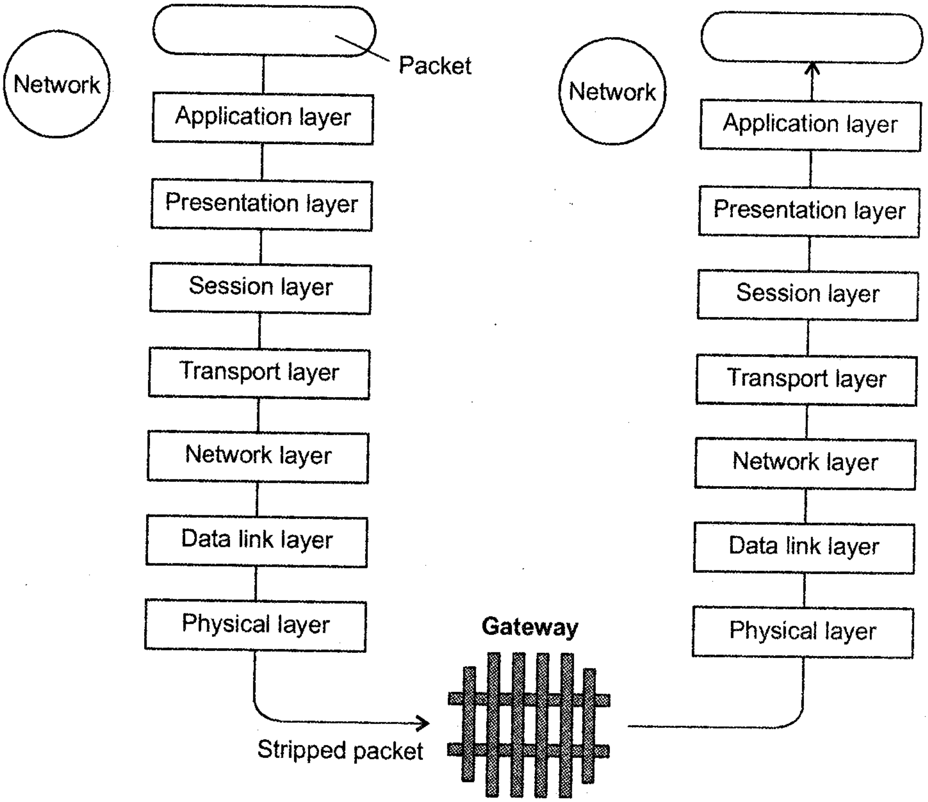


Figure 5.9: Gateway strips off an old protocol stack and adds a new protocol stack

i. Gateway are task specific, which means that, they are dedicated to a particular type of transfer.

They are often referred by their particular task name (Windows NT server to SNA gateways).

ii. The gateway takes the data from one environment, stripes off its old protocol stack and repackages it in the protocol stack from the destination network.

   a. Decapsulates incoming data through the network's complete protocol stack.

   b. Encapsulates the outgoing data in the complete protocol stack of the other.

2. Network Security Devices

1

Apr. 2010 – *5M*
Explain Network
Security Devices.

Network security basically means protecting data and system's resources from access by unauthorized users. Why is this necessary? Consider the following:

1. People outside the company might try to access network resource and data.

2. Upper management, middle management and other workers have different needs in terms of the information to which they have access. Network security can control the access given to various groups or individual users.

   For example, information about employee salaries are performance appraisals might be stored on a network; with access restricted only to a few users.

3. People might accidentally move or erase important information.

4. Former employees who are fired or other people might wish to harm your company in some way.

Individual computers in a network are free to decide who they want to communicate with, what information they want to allow access to and which services they will make available, called as 'host based security'. Internet is designed in this way. In actual individual computers are not good at defining and securely enforcing a consistent security policy. They run very complex, error prone software systems, which are very difficult to ensure security.

This situation may be adequate where individual users on a network have a similar level of trust, little chance or motive for a user to subvert host security, like a small company network where everyone with physical access is trusted.

Once network is connected to other networks where trust relationships simply don't exist in the same way, other mechanisms need to be put in place to provide adequate security by protecting resources on the trusted network from potential access by attackers on the un-trusted part of the network.

2.1 Firewall

A set of programs that monitor all communication passing into and out of a corporation's intranet.

Helps prevent, but doesn't eliminate, unauthorized access.

1

Oct. 2012 – *5M*
Write short note on Firewalls.

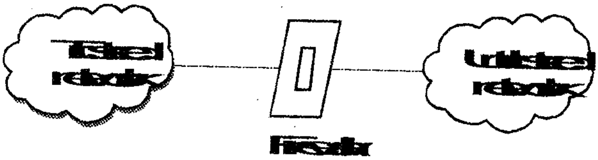


Figure 5.10

This is done by partially breaking connectivity at the network level so that nodes on the trusted and un-trusted parts of the network can no longer freely exchange information in an unfettered way. Device which dies this is called as 'firewall'.

A firewall disrupts free communication between trusted and un-trusted networks, attempting to manage the information flow and restrict dangerous free access.

There are different kinds of technique employed by a firewall in order to correctly identify a conversation and act on it.

The technique used by firewall have an impact on the accuracy with which it can identify traffic, level of sophistication of the checks it can implement, also complexity and cost.

Firewall is a piece of software or hardware that filters all networks traffic between a personal computer, home network or company network and the internet as shown in *figure 5.11.*

In addition to the danger of information leaking out, there is also a danger of information leaking in. In particular, viruses, worms and other digital pests can breach security, destroy valuable data and waste large amounts of administrator's time trying to clean up the mess they leave.

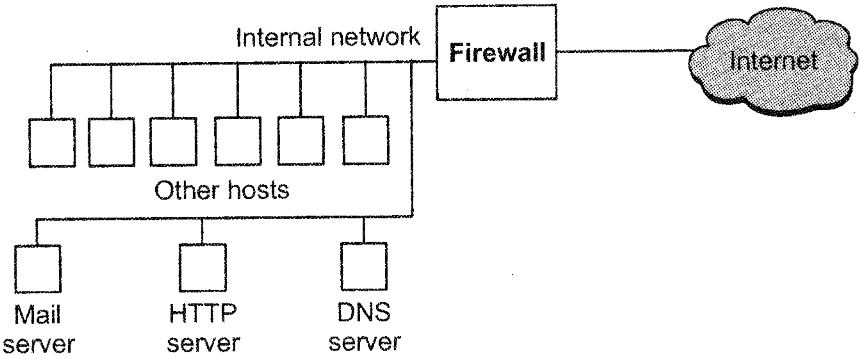


Figure 5.11: Basic firewall function

Firewalls are just a modern adaptation of that old medieval security standby: digging a deep moat around your castle. This design forced everyone entering or leaving the castle to pass over a single drawbridge, where they could be inspected by the I/O police. With networks, the same trick is possible: a company can have many LANs connected in arbitrary ways, but all traffic to or from the company is forced through an electronic drawbridge (firewall) as shown in *figure 5.12.*

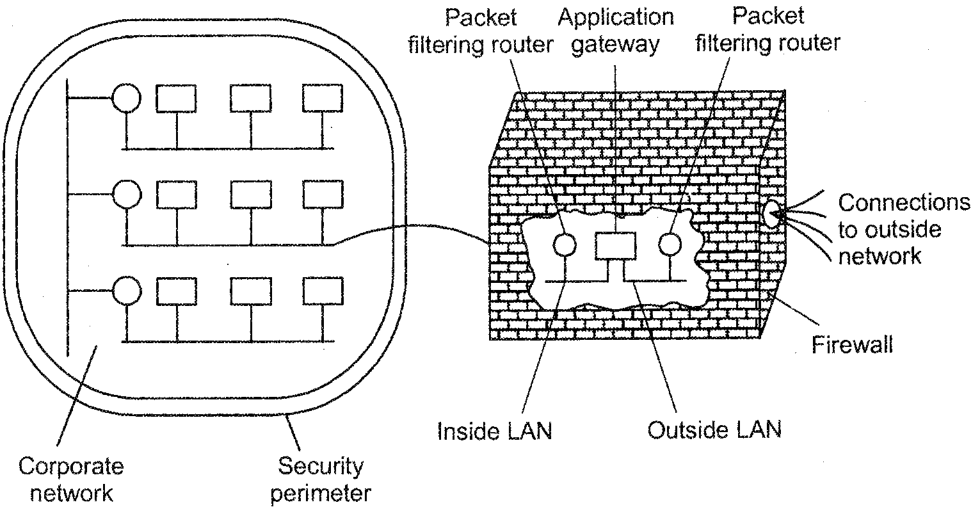


Figure 5.12: A firewall consisting of two packet filters and an application gateway

The firewall in this configuration has two components:

1. **Packet filtering:** It is a standard router equipped with some extra functionality. The extra functionality allows every incoming or outgoing packet to be inspected. Packet meeting some criterion are forwarded normally. Those that fail the test are dropped.

In the above *figure* the packet filter on the inside LAN checks outgoing packets and the one on the outside LAN checks incoming packets. Packets crossing the first hurdle go to the application gateway for further examination. The point of putting the two packet filters on different LANs is to the ensure that no packet gets in or out without having to pass through the application gateway: there is no path around it.

2. **Application gateway:** The gateway operates at the application level. A mail gateway, for e.g. can be set up to examine each message going in or coming out.

   For each one the gateway decides whether to transmit or discard the message based on header fields, message size or even the content.

   In principle, application firewalls can prevent all unwanted outside traffic from reaching protected machines.

▶ Limitations of Firewall

Information security professionals often find themselves working against misconceptions and popular opinions formed from incomplete data. Some of these opinions spring more from hope than fact, such as the misguided notion that simply deploying a firewall can solve all network-security problems. While firewall deserve a high spot on the agenda for organizations that have, or are creating, a connection between their network and others, firewall are not the whole answer. Many threats remains outside the scope of the firewalls capabilities.

Many of the hacking incidents reported by the media have very little to do with the internet itself. Social engineering, one of the most widely used hacking techniques, involves tricking someone into revealing something that compromises security, such as a network password. And phone lines intended for data, such as remote-maintenance lines and field office access lines, offer avenues of access to internal systems even without an internet connection.

Firewalls also do not address insider attacks, since they provide defense for external attacks only. Firewalls are not general-purpose access-control systems and do not control insiders' abuse of authorized access-perhaps the greatest risk of all. Information security surveys consistently report that more than half of all incidents are insider attacks, and many seasonal security professionals believe that insiders cause more security problems than the outsiders.

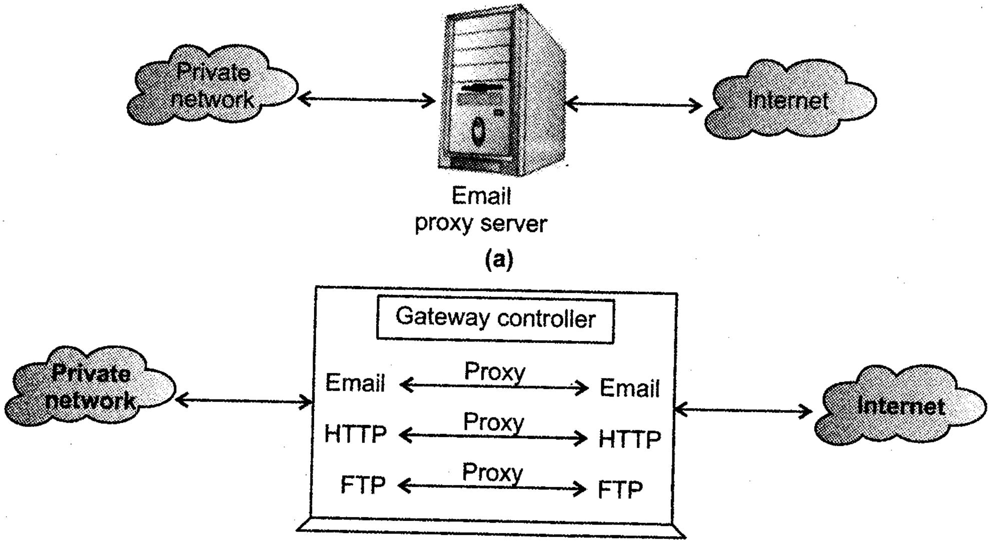
2.2 Proxy Server

Proxies are mostly used to control or monitor outbound traffic. Some application proxies cache the data requested. This lowers bandwidth requirements and decreases the access time for the next user while accessing the same data. It also gives unquestionable evidence of what was transferred. Proxy server functions as a middle man between the client and the server for a particular service (such as FTP, HTTP). A firewall might run individual proxy servers for each of the applications needed by the client system. It is an application that runs on a computer with registered IP address, while the clients use unregistered IP address, causing them to remain invisible from the internet.

2

Apr. 2013, 2011 – *5M*
Explain how Proxy Servers and Firewalls help in maintaining Network Security?

Client applications are configured to send their internet service requests to proxy server and then proxy server relays the request to the internet server, using its own registered IP address. On receiving a response from the Internet server, proxy server relays it back to the original client. So clients must be configured with address of proxy server, if he wants to use proxy server. A most common form of proxy server used is for the web. A firewall may use a single proxy server product for each application as shown in the *figure 5.13 (a)* or may use a single proxy server product for each application as shown in *figure 5.13 (b)*.



(a)

(b)

Figure 5.13

Drawback of proxy servers are:

i. That you need an individual server for every application.

ii. Each client should be configured to use it.

Types of proxy servers:

i. **Application proxy:** The best example is a person telneting to another computer and then telneting from there to the outside world. Only with an application proxy server, the process is automated. As you telnet to the outside world, the client sends you to the proxy first. The proxy then connects to the server requested (the outside world) and returns the data to you.

As the proxy servers are handling all the communications, they can log everything that you do. For HTTP (web) proxies, this would include URL that you see. For FTP proxies, this includes every file you download. They can even filter out 'inappropriate' words from the sites you visit or scan for viruses.

Application proxy servers can authenticate users. Before a connection to the outside network is made, the server can ask the user to login first. To a web user, this would make every site look that it required to login.

ii. **Socks proxy:** Socks are the cross platform mechanism that establishes secure communications between client and server computers. The socks proxy service supports socks version 4.3a and allows users transparent access to the internet by means of proxy server. The sock proxy service extends the redirection provided by the Winsock proxy service to non-windows platforms.

It uses TCP/IP and can be used for Telnet, FTP, Gopher, and HTTP. The socks proxy service does not support applications that rely on the UDP protocol.

Socks proxy clients establishes a connection to the proxy server computer and the socks proxy service relays information between the client and the internet server. Security is based on IP addresses, port numbers and destination hosts.

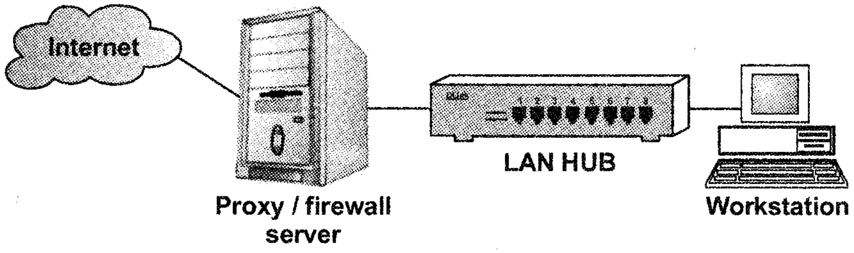


Figure 5.14

PU Questions

5 Marks

[Apr. 2013 – 5M] 1. Explain active and passive hub.

[Apr. 2013 – 5M] 2. Write a note on Source Routing Bridges.

[Apr. 2013, 2011 – 5M] 3. Explain how Proxy Servers and Firewalls help in maintaining Network Security?

[Oct. 2012 – 5M] 4. What is Bridge? What are its types? Explain advantages and disadvantages of Bridges.

[Oct. 2012 – 5M] 5. Write short note on Firewalls.

[Apr. 2012 – 5M] 6. What is bridge? What are its types? Explain any one.

[Apr. 2012, 2010 – 5M] 7. Write short note on Gateways.

[Oct. 2011 – 5M] 8. Explain bridge with its advantages and disadvantages.

[Oct. 2011 – 5M] 9. Write a short note on Repeaters.

[Apr. 2011 – 5M] 10. Explain Gateways.

[Apr. 2011 – 5M] 11. Write a short note Hubs.

[Oct. 2010 – 5M] 12. Define Firewall. What are several types of Firewall Techniques available?

[Oct. 2010 – 5M] 13. Define

i. Hubs ii. Repeaters iii. Routers
iv. Bridges v. Gateways

[Apr. 2010 – 5M] 14. Explain Network Security Devices.

[Apr. 2010 – 5M] 15. Compare Switch and Hub.

[Apr. 2010 – 5M] 16. What is Bridge? Explain its types.

Chapter 6

INTERNET BASICS

1. Concept of Intranet and Extranet

1.1 Intranet

An intranet is a private network that uses Internet protocols to securely share any part of an organization's information or operational systems within that organization. The term is used in contrast to internet - a network between organizations and instead refers to a network within an organization. Sometimes the term refers only to the organization's internal website, but may be a more extensive part of the organization's information technology infrastructure.

1

Oct. 2010 – *5M*
Explain Intranet and Extranet.

▶ Characteristics of Intranet

i. An intranet is built from the same concepts and technologies used for the internet, such as client-server computing and the Internet Protocol Suite (TCP/IP). Any of the well known internet protocols may be found in an intranet, such as HTTP (web services), SMTP (e-mail), and

FTP (file transfer). Internet technologies are often deployed to provide modern interfaces to legacy information systems hosting corporate data.

ii. An intranet can be understood as a private version of the internet, or as a private extension of the internet confined to an organization by a firewall. The first intranet websites and home pages began to appear in organizations in 1990-91. Although not officially noted, the term intranet first became common-place with early adopters, such as universities and technology corporations, in 1992.

iii. Intranets are also contrasted with extranets; the former are generally restricted to employees of the organization, while the latter may also be accessed by customers, suppliers, or other approved parties. Extranets extend a private network onto the internet with special provisions for access, authorization, and authentication.

iv. An organization's intranet does not necessarily have to provide access to the internet, when such access is provided it is usually through a network gateway with a firewall, shielding the intranet from unauthorized external access. The gateway often also implements user authentication, encryption of messages, and often Virtual Private Network (VPN) connectivity for off- site employees to access company information, computing resources and internal communications.

▶ Uses of Intranet

i. Increasingly, intranets are being used to deliver tools and applications, *for example*, collaboration (to facilitate working in groups and teleconferencing) or sophisticated corporate directories, sales and customer relationship management tools, project management etc., to advance productivity.

ii. Intranets are also being used as corporate culture-change platforms. *For example,* large number of employees discussing key issues in an intranet forum application could lead to new ideas in management, productivity, quality and other corporate issues.

iii. In large intranets, website traffic is often similar to public website traffic and can be better understood by using web metrics software to track overall activity. User surveys also improve intranet website effectiveness, larger businesses allow users within their intranet to access public internet through firewall servers. They have the ability to screen messages coming and going thus keeping security intact.

iv. When part of an intranet is made accessible to customers and others outside the business, that part becomes part of an extranet. Businesses can send private messages through the public network, using special encryption/ decryption and other security safeguards to connect one part of their intranet to another.

v. Intranet user-experience, editorial and technology teams work together to produce inhouse sites. Most commonly, intranets are managed by the communications HR or CIO departments of large organizations, or a combination of these.

▶ Benefits of Intranets

i. **Workforce productivity:** Intranets also help users to locate and view information faster and use applications relevant to their roles and responsibilities. With the help of a web browser interface, users can access data held in any database, the organization wants to make available, anytime and subject to security provisions – from anywhere within the company workstations, increasing employees ability to perform their jobs faster, more accurately, and with confidence that they have the right information. It also helps to improve the services provided to the users.

ii. **Time:** With intranets, organizations can make more information available to employees on a 'pull' basis (i.e. employees can link to relevant information at a time which suits them) rather than being deluged indiscriminately by emails.

iii. **Communication:** Intranets serve as powerful tools for communication within an organization, vertically and horizontally. From a communications standpoint, intranets are useful to communicate strategic initiatives that have a global reach throughout the organization. The type of information that can easily be conveyed is the purpose of the initiative and what the initiative is aiming to achieve, who is driving the initiative, results achieved to date, and who to speak to for more information. By providing this information on the intranet, staff have the opportunity to keep up-to-date with the strategic focus of the organization. Some examples of communication would be chat, email, and /or blogs. A great real world example of where an intranet helped a company communicate is when Nestle had a number of food processing plants in Scandinavia. Their central support system had to deal with a number of queries every day (Mc Govern, Gerry). When Nestle decided to invest in an intranet, they quickly realized the savings. McGovern says the savings from the reduction in query calls was substantially greater than the investment in the intranet.

iv. **Web publishing** allows 'cumbersome' corporate knowledge to be maintained and easily accessed throughout the company using hypermedia and Web technologies. *Examples*: employee manuals, benefits documents, company policies, business standards news feeds, and even training, can be accessed using common internet standards, acrobat files, flash files, CGI applications. Because each business unit can update the online copy of a document, the most recent version is always available to employees using the intranet.

v. **Business operations and management:** Intranets are also being used as a platform for developing and deploying applications to support business operations and decisions across the internet worked enterprise.

vi. **Cost effective:** Users can view information and data via web-browser rather than maintaining physical documents such as procedure manuals, internal phone list and requisition forms. This can potentially save the business money on printing, duplicating documents, and the environment as well as document maintenance overhead. 'PeopleSoft, a large software company, has derived significant cost savings by shifting HR processes to the intranet' Gerry McGovern goes on to say the manual cost of enrolling in benefits was found to be USD 109.48 per enrollment. 'Shifting this process to the intranet reduced the cost per enrollment to $21.79; a saving of 80 percent'. PeopleSoft also saved some money when they received requests for mailing address change. For an individual to request a change to their mailing address, the manual cost was USD17.77. The intranet reduced this cost to USD4.87, a saving of 73 percent.' PeopleSoft was just one of the many companies that saved money by using an intranet. Another company that saved a lot of money on expense reports was Cisco. 'In 1996, Cisco processed 54,000 reports and the amount of dollars processed was USD19 million'.

vii. **Promote common corporate culture:** Every user is viewing the same information within the Intranet.

viii. **Enhance Collaboration:** With information easily accessible by all authorized users, teamwork is enabled.

ix. **Cross-platform Capability:** Standards- compliant web browsers are available for Windows, Mac and UNIX.

x. **Built for one Audience:** Many companies dictate computer specifications which, in turn, may allow Intranet developers to write applications that only have to work on one browser (no cross-browser compatibility issues).

xi. **Knowledge of your Audience:** Being able to specifically address your 'viewer' is a great advantage. Since Intranets are user specific (requiring database/network authentication prior to access), you know exactly who you are interfacing with. So, you can personalize your Intranet based on role (job title, department) or individual ('Congratulations Jane, on your 3rd year with our company!').

xii. **Immediate Updates:** When dealing with the public in any capacity, laws / specifications / parameters can change. With an intranet providing your audience with 'live' changes, they are never out of date, which can limit a company's liability.

xiii. **Supports a distributed computing architecture:** The intranet can also be linked to a company's management information system, *for example,* a time keeping system.

1.2 Extranet

An extranet is a private network that uses internet protocols, network connectivity and possibly the public telecommunication system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other business. An extranet can be viewed as part of a company's intranet that is extended to users outside the company, usually via the internet. It has also been described as a 'state of mind' in which the internet is perceived as a way to do business with a selected set of other companies (Business-to-Business, B2B), in isolation from all other internet users. In contrast, Business-to-Consumer (B2C) models involve known servers of one or more companies, communicating with previously unknown consumer users.

An extranet can be understood as an intranet mapped onto the public internet or some other transmission system not accessible to the general public, but managed by more than one company's administrator(s). *For example,* military networks of different security levels may map onto a common military radio transmission system that never connects to the Internet. Any private network mapped onto a public one is a Virtual Private Network (VPN), often using special security protocols.

For decades, institutions have been interconnecting to each other to create private networks for sharing information. One of the differences that characterizes an extranet, however, its interconnections are over a shared network rather than through dedicated physical lines. With respect to Internet Protocol networks, RFC 4364 states “if all the sites in a VPN are owned by different enterprises, the VPN is a corporate intranet. If the various sites in a VPN are owned by the same enterprise, the VPN is an extranet. A site can be in more than one VPN; *for Example*, in an intranet and several extranets. We regard both intranets and extranets as VPNs. In general, when we use the term VPN we will not be distinguishing between intranets and extranets. Even if this argument is valid, the term 'extranet' is still applied and can be used to eliminate the use of the above description.

In the quote above from RFC 4364, the term 'site' refers to a distinct networked environment. Two sites connected to each other across the public internet backbone comprise a VPN. The term 'site' does not mean 'website'. Thus, a small company in a single building can have an 'intranet', but to have a VPN, they would need to provide tunneled access to that network for geographically distributed employees.

For smaller, geographically united organizations, 'extranet' is a useful term to describe selective access to intranet systems granted to suppliers, customers, or other companies. Such access does not involve tunneling, but rather simply an authentication mechanism to a web server. In this sense, an 'extranet' designates the 'private part' of a website, where 'registered users' can navigate, enabled by authentication mechanisms on a 'login page'.

An extranet requires network security. These can include firewalls, serve management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages and the use of Virtual Private Networks (VPNs) that tunnel through the public network.

Many technical specifications describe methods of implementing extranets but often never explicitly define an extranet. RFC 3547 presents requirements for remote access to extranets. RFC 2709 discusses extranet implementation using IPsec advanced Network Address Translation (NAT).

▶ Advantages

i. Exchange large volumes of data using Electronic Data Interchange (EDI).

ii. Work is done quickly as compared to past manual systems.

iii. Improve company efficiency and output by automating procedures.

iv. Automation decreases scope of mistakes.

v. Information can be modified, updated and changed immediately. Instant access to the most advanced information.

vi. Improve relationships with main or potential customers by giving them correct, precise and efficient information.

vii. Access services provided by one company to a group of other companies.

▶ Disadvantages

i. Expensive to implement and maintain within an organization.

ii. Security of an extranet can be a concern when hosting valuable or proprietary information. System access must be carefully controlled to secure sensitive data.

iii. Protection problem when dealing with precious information system access should be controlled and checked properly to protect the system and information going into the correct hand.

iv. Decrease personal face-to-face contact with clients and business partners.

2. Internet Information Server (IIS)

Internet Information Server (IIS) is a Microsoft's web server that runs on Windows NT platforms. A powerful web server, Internet Information Services (IIS) 6.0 provides a highly reliable, manageable and scalable web application infrastructure for all versions of windows server 2003.

IIS helps organizations increase website and application availability while lowering system administration costs. It is a set of internet based services for servers created by Microsoft for use with Microsoft windows.

1
Oct. 2012 – *5M*
Write short note on Internet Information Server (IIS).

▶ Features of IIS

i. **File publication:** To publish existing files from file servers.

ii. **Support of common internet standards:** To support Common Gateway Interface (CGI) and PERL, which are common languages for developing web applications?

iii. **Network management:** To monitor and record network activity and provide client with access to valuable network resources like HTML pages, shared files and printers, databases and legacy systems.

iv. **Security:** To provide clients with secure access to internet and intranet resources.

v. **Back office applications:** To support integration with back office applications like Microsoft SQL Server and Microsoft SNA Server. Back office support provides businesses with the ability to deliver commercial solutions on the web to customers.

▶ Benefits of IIS

Benefits of IIS are:

IIS (Internet Information Server) is a group of internet servers (including a web or hypertext Transfer protocol server and a file transfer protocol server) with additional capabilities for Microsoft's Windows NT and Windows 2000 Server operating systems. IIS is Microsoft's entry to compete in the Internet server market that is also addressed by Apache, Sun Microsystems, O'Reilly and others. With IIS, Microsoft includes a set of programs for building and administering web sites, a search engine, and support for writing web-based applications that access databases. Microsoft points out that IIS is tightly integrated with the Windows NT and 2000 Servers in a number of ways, resulting in faster web page serving.

2
Oct. 11, Apr. 10 – *5M*
What is Internet Information Server (IIS)? Explain with benefits.

▶ IIS Benefits

i. **Reliability:** IIS uses a new request-processing architecture and application isolation environment that enables individual Web applications to function within a self-contained worker process.

ii. **Scalability:** IIS introduces a new kernel-mode driver for Hypertext Transfer Protocol (HTTP) parsing and caching that is specifically tuned to increase web server throughput and scalability of multiprocessor computers.

iii. **Security:** IIS includes a variety of security features and technologies to help ensure the integrity of the Web and File Transfer Protocol (FTP) site content, as well as the data that is transmitted through the sites. These security features and technologies include Advanced Digest authentication, improved access control, Secure Sockets Layer (SSL) encryption, centralized certificate storage, and detailed auditing capabilities.

iv. **Manageability:** To meet the needs of a diverse set of organizations, IIS provides a variety of manageability and administration tools.

Main types of services IIS supports is

a. HTTP

b. FTP

c. GOHPER

IIS allows different application to be build using

a. HTTP

b. ASP

c. ISAPI

d. Internet Database Connector

3

Apr. 2013, 2012 – *5M*
Explain in details: Web server.

Apr. 2010 – *5M*
Explain working of Web Server.

3. Web Server

A web server is a piece of software that enables a website to be viewed using HTTP. HTTP (Hypertext Transfer Protocol) is the key protocol for the transfer of data on the web. You know when you're using HTTP because the website URL begins with http:// '(*example* http:// www.quackit.com)

You might be thinking 'I always thought a web server was a special, high-powered computer'. Well, you'd be right too. Some high powered computers are referred to as web servers as they have been built with web hosting in mind. But in most cases, when someone refers to a web server, they are referring to a piece of software that you install on a computer.

At the most basic level possible, the following diagram shows the steps that brought the page to your screen:

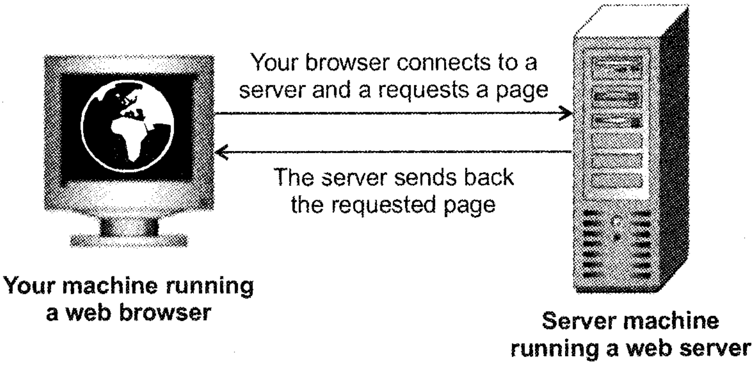
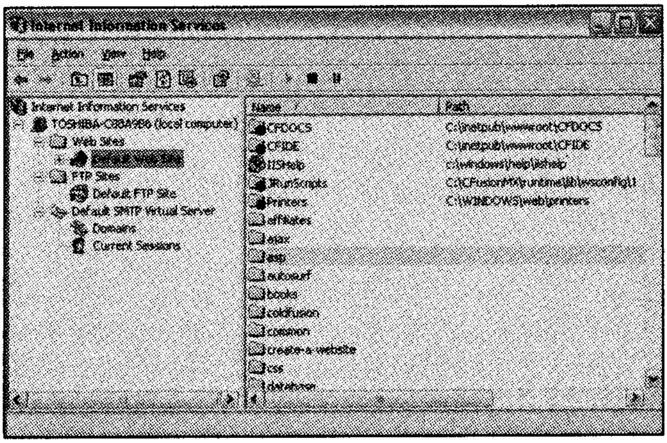

Your browser connects to a server and a requests a page
The server sends back the requested page
Your machine running a web browser
Server machine running a web server

Figure 6.1: Web server

Your browser formed a connection to web server, requested a page and received it.

▶ What does a Web Server look like?

It depends on which web server you choose to install. Here's an example of Microsoft's internet Information Services (IIS) 5.1.



- Internet Information Services
  - TOSHIBA-C8BA986 (local computer)
    - Web Sites
      - Default Web Site
    - FTP Sites
      - Default FTP Site
    - Default SMTP Virtual Server
      - Domains
      - Current Sessions

Name	Path
CFDOCS	C:\inetpub\wwwroot\CFDOCS
CFIDE	C:\inetpub\wwwroot\CFIDE
IISHelp	c:\windows\help\iishelp
JRunScripts	C:\CFusionMX\runtime\lib\wsconfig\1
Printers	C:\WINDOWS\web\printers
affiliates	
ajax	
asp	
autosurf	
books	
coldfusion	
common	
create-a-website	
css	
database	

Figure 6.2: Internet information services

The left pane represents the various website, FTP sites, and SMTP virtual servers. When an item in the left pane is selected, the contents are displayed in the pane on the right hand side.

In the above screen shot, there is one website (called 'Default Web Site'), one FTP site (called 'Default FTP Site') and one SMTP virtual server (called 'Default SMTP virtual server').

You can right click on an item to display its properties. *For example*, you can right click on 'Default Web Site' to display (and configure) the properties of that website.

▶ Features

There is a common set of features that you'll find on most web servers. Because web servers are built specifically to host websites, their features are typically focused around setting up and maintaining a website's hosting environment.

Features are as follows:

i. Create one or more website.

ii. Configure log file settings, including where the log files are saved, what data to include on the log files etc.

iii. Configure websites/directly. *For example*, which user accounts are/aren't allowed to view the websites, which IP addresses are/aren't allowed to view the website etc.

iv. Create an FTP site. An FTP site allows users to transfer files to and from the site.

v. Create virtual directories and map them to physical directories.

vi. Configure/nominate custom error pages. This allows you to build and display user friendly error messages on your website. *For example,* you can specify which page is displayed when a user tries to access a page that doesn't exist (i.e., a '404 error').

vii. Specify default documents. Default documents are displayed when no file name is specified. For *example,* if you open 'http:// Local host', which file should be displayed? This is typically 'index.html' or similar but it doesn't need to be. You could nominate 'index.cfm' if your website is using cold fusion. You could also nominate.

▶ How Web Servers Work?

Whenever you view a webpage on the internet, you are requesting that page from a web server, when you type a URL into your browser.

For example, 'http://www.quackit.com/htmt/tutorial/index.cfm'), your browser requests the page from the web server and the web server sends the page back:

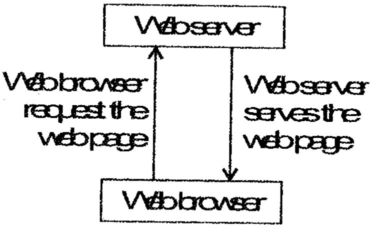


Figure 6.3: Working of web server

The above diagram is a simplistic version of what occurs. Here's a more detailed version:

i. Your web browser first needs to know which IP address the website www.quackit.com resolves to. If it doesn't already have this information stored in its cache, it requests the information from one or more DNS servers (via internet). The DNS server tells the browser which IP address the website is located at. Note that the IP address was assigned when the website was first created on the web server.

ii. Now the web browser knows which IP address the website is located at, it can request the full URL from the web server.

iii. The web server responds by sending back, the requested page. If the page doesn't exist, it will send back the appropriate error message.

iv. Your web browser receives the page and renders it as required.

▶ Advantages

i. Your local website behaves more like the live one.

ii. You can use server-side scripting languages.

iii. Allows you to standardize your coding.

iv. Increases knowledge.

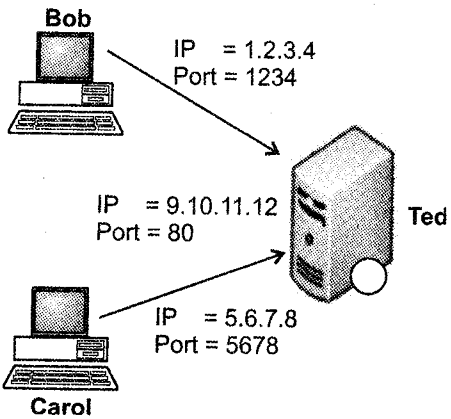


Figure 6.4

1

Apr. 2011 – *5M*
Write a short note on WWW.

4. WWW (World Wide Web)

The World Wide Web is a system of internet servers that supports hypertext to access several Internet protocols on a single interface. The World Wide Web is often abbreviated as the web or WWW.

The WWW was developed in 1989 by Tim Berners-Lee of the European Particle Physics lab (CERN) in Switzerland. The purpose of the web was to use networked hypertext to facilitate communication among its members, who was soon spread beyond CERN, and a rapid growth in the number of both developers and users ensued. The use of the web has reached global proportions and has become a defining element of human culture in an amazingly short period of time.

In order for the web to be accessible to anyone, certain agreed upon standards must be followed in the creation and delivery of its content. An organization leading the efforts to standardize, the web is the World Wide Web (W3C) consortium. Take a look at the W3C consortium web site to get an idea of its activities. A lot of the material is technical because, after all, the web is a technical phenomenon.

The WWW is an information space in which the items of interest, referred to as resources, are identified by global identifiers called Uniform Resource Identifiers (URI).

Examples such as the following travel scenario are used throughout this document to illustrate typical behavior of web agents-people or software acting on this information space. A user agent acts on behalf of a user. Software agents include servers, proxies, spiders, browsers and multimedia players.

The World Wide Web (WWW) is a global hypertext system that was initially developed in 1989 by *Tim Berners Lee.*

The www is a repository of information linked together from points all over the world. It has a unique combination of portability, flexibility and user-friendly features that distinguish it from other services provided by the internet.

4.1 WWW Architecture

WWW is a distributed client/server service, in which a client using a browser can access a service using a server. However, a server provided is distributed over many different locations called sites.

Each and every site holds one or more web documents, referred to as web pages. Web page contains a link to other web pages in the same site or at other sites. The web pages can be retrieved and viewed by using browsers. The client needs to see some information that it knows belongs to site A. It sends a request through its browser, a program that is designed to fetch web documents. The request among other information, includes the address of the site and the web page, called URL (Uniform Resource Locator). The server at site A finds the document and sends to the client. When the user views the document, he finds some references to other documents such as web page at site B. The reference has the URL for the new site. The user is also interested in seeing this web document. The client sends another request to the new site, and the new page is retrieved.

3

Oct. 2012, 2010 – *5M*
Explain www Architecture.

Oct. 2011 – *5M*
What is WWW? Explain its architecture.

WWW architecture includes: server, client (browser), URL and cookies.

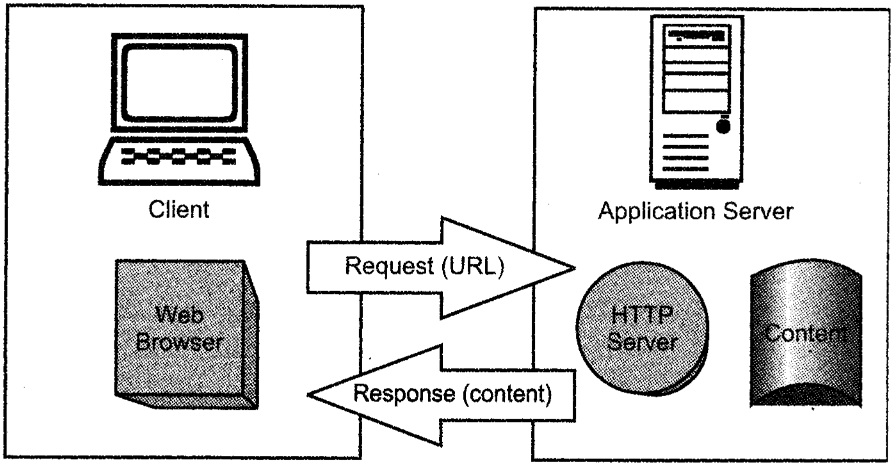


Figure 6.5: Architecture of WWW

i. **Server:** The web page is stored at the server. Each and every time a client request arrives, the corresponding web document is sent to the client. Servers normally stores requested files/information in a cache memory. A server can also become more efficient through multiprocessing or multithreading. In such a condition, a server can answer more than one request at a time.

ii. **Client (browser):** Each and every browser usually consists of the following parts:

  a. Controller

  b. Client protocol

  c. Interpreter

  The controller receives input from the keyboard or any input device and uses the client programs to access the document. When the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of as HTTP or FTP. The interpreter can be Java, HTML or javascript depending on the type of web document.

iii. **Uniform Resource Locator (URL):** A client that wants to access web page needs the address of the web page. To facilitate the access of documents distributed throughout the world, HTTP uses locators. The URL is a standard for specifying any kind of information on the internet. It defines 4 things protocol, host computer, port and path.

iv. **Cookies:** The www was originally developed as a stateless entity. A client sends a request and then a server responds. Their relationship is over. The original design of www, retrieving publicly available web documents, exactly fits this purpose. Some functions of web are given below:

  a. Some websites need to allow registered clients only.

  b. Some websites are just advertising.

For these purposes, the cookie mechanism was devised.

▶ How WWW Works?

The Web consists of all client and server applications that communicate over the internet using the client/server protocol Hypertext Transfer Protocol (HTTP), as well as the resources that reside on those servers and are accessed by those clients. These resources are generally referred to as 'Web Sites' and consist mainly of text files formatted in Hypertext Markup Language (HTML) and associated image, sound, multimedia, script and other files. Each HTML file is called as Web page and pages in a site are generally linked in a hierarchical fashion, starting with the home or top page, using anchor tags. Web sites are stored on web servers, which run software that handles the server side of HTTP, such a Internet Information Services (IIS) for Microsoft windows 2000. Users access web sites on the internet by using client software, typically called a web browser (such as Microsoft Internet Explorer).

4.2 Web Documents

The documents in the WWW can be grouped into three broad categories:

The category is based on the time at which the contents of the document are determined.

1
Apr. 2012 – *5M*
Explain the following terms:
a. Web server
b. Web documents

i. **Static documents:** Static document are fixed content documents that are created and stored in a server. The client can get only a copy of the document. In other words, the contents of the file are determined when the file is created, not when it is used. Of course, the contents in the server can be changed, but the user cannot change them. When a client accesses the document, a copy of the document is sent. The user can then use a browsing program to display the document.

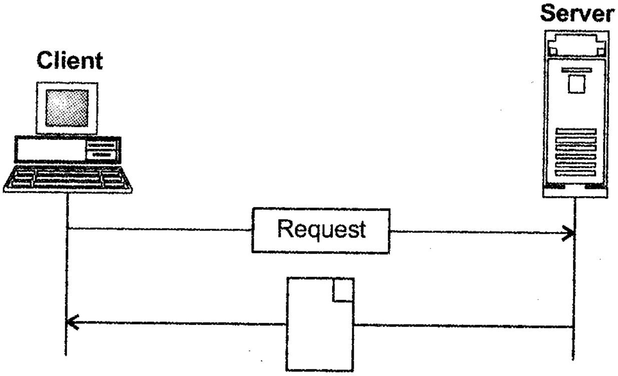


Figure 6.6: Static documents

ii. **Dynamic documents:** A dynamic document is created by web server whenever a browser requests the document. When a request arrives, the web server runs an application program or a script that creates dynamic document. The server returns the output of the program or script as a response to the browser that requested the document. Because a fresh document is created for each request, the contents of this document can vary from one request to another.

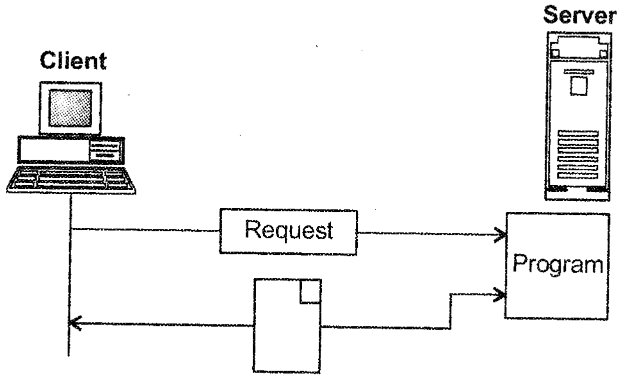


Figure 6.7: Dynamic HTML, document

iii. **Active documents:** For many applications, we need a program or a script to be run at the client site. These are called as active documents. *For example*, Java applets, JavaScript.

5. Search Engines

4
Apr. 11, Oct. 10 – *5M*
Write a short note on Search Engines.
Apr. 2013, 2012 – *5M*
Explain in details: Search engines.

A search engine is a tool that searches the information available on the internet.

Enormous amount of information is at your fingertips with the click of mouse with the millions of web sites on the Internet.

Search technique discusses how to classify, categorizing and indexing the required sources for easy retrieval by the users.

Selection of the correct search engine depends upon the information for what you are looking for, best search result includes only relevant information, search tips to locate the information more quickly.

▶ Types of Search Engine

There are five types of search engine:

i. **Directory:** Directory is the indexed listing of specified categories of web pages. They are scrolled during the search and updated after review.

ii. **Search engine crawl:** This type of search engines crawl the web site searching for the web pages automatically. They have spiders to index the web pages and to do the revisits to the sites. Search engine makes just the queries to its database and detects the web pages that contain the information specified by the user.

iii. **Meta search engine:** This is the program that search with the number of search engines at a time. It provides best results than the others. It gives too many matches that overwhelm the user.

iv. **Free text query engine:** It accepts the query in the form of text question. It gives specific results with the defined level of comfort. Many times it gives question and answer approach to find the desired results.

v. **Hybrid search engine:** This type has search engines with a related directory. Hence it is called 'Hybrid Search Engine'.

▶ Working of Search Engine

Working of the search engine depends upon the type of search criteria for indexing pages and returning results. Size of the index, review of web pages, links with the priorities, Meta tags, importance of pages are the categories for getting the different search approaches of the search engines. Hence, we get different results on the different engines. Frequency, with which the word appears on the page, locations of the searched word are also considered during the search.

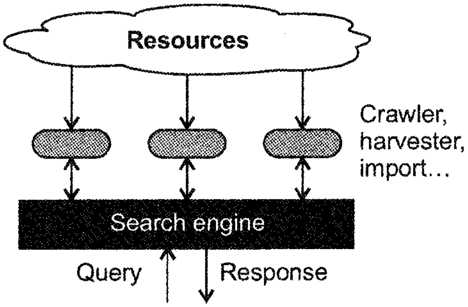


Figure 6.8: Search engine

6. Internet Service Providers (ISP)

To take an internet connection, firstly we need to approach an Internet Service Provider (ISP), who gives us an internet connection. Depending upon users need the type of connection to be taken is decided. Also depending upon users need, you need to decide which service provider to choose. As in case of any other service providers like mobile service providers (like Airtel, idea Reliance), each provider has its own services and facilities that they offer to their customers.

Each mobile service provider offer different services like one may provide Re. 1 per local call from mobile to mobile whereas one may provide a free local call between two similar mobiles. Each mobiles coverage area is also different i.e. how much large area they can cover. Few may offer free talk time in late night etc. also charges of each mobile service providers are different. Few providers have better quality service. Here user will decide which provider to choose depending on how much usage of mobile talk he needs and which one is affordable to him.

Exactly the same idea applies here when one needs to take an internet connection. First of all ISP form a pyramid of service providers, from large backbone network at the top of pyramid, providing internet services to all other ISPs at lower level than it. Each of these ISP, then in turn, also provides service to other ISPs at low level than them. Once again, it turns, these ISPs provide service to other ISPs at low level than them or provide service to individual home user or to corporate office site.

From top level towards bottom each ISP sells bandwidth to low level ISP or directly to user. At the top level, there are large backbone networks that are connected to regional networks and they sell Internet bandwidth to regional ISPs, which in turn split the band width into smaller units and resell it to other ISPs or end users, as shown in *figure 6.9.*

Providers at higher level in pyramid use high bandwidth connections to the backbone. These high bandwidth connections are called 'fat data pipes', and they can handle all traffic generated by their client ISPs. In turn, the client ISPs use comparatively smaller bandwidth connections.

For example, a local ISP that provides only dial-up connection may have a T_1 connection running at 1.544 mbps to its own provider, which in turn, it sub divides into a number of 56 kbps connection to its provider, which can support 25-30 user connections at 56 kbps speed and ISP might sell it to 50 or more users. In this case, it may happen that few users are unable to connect, if all lines are in use.

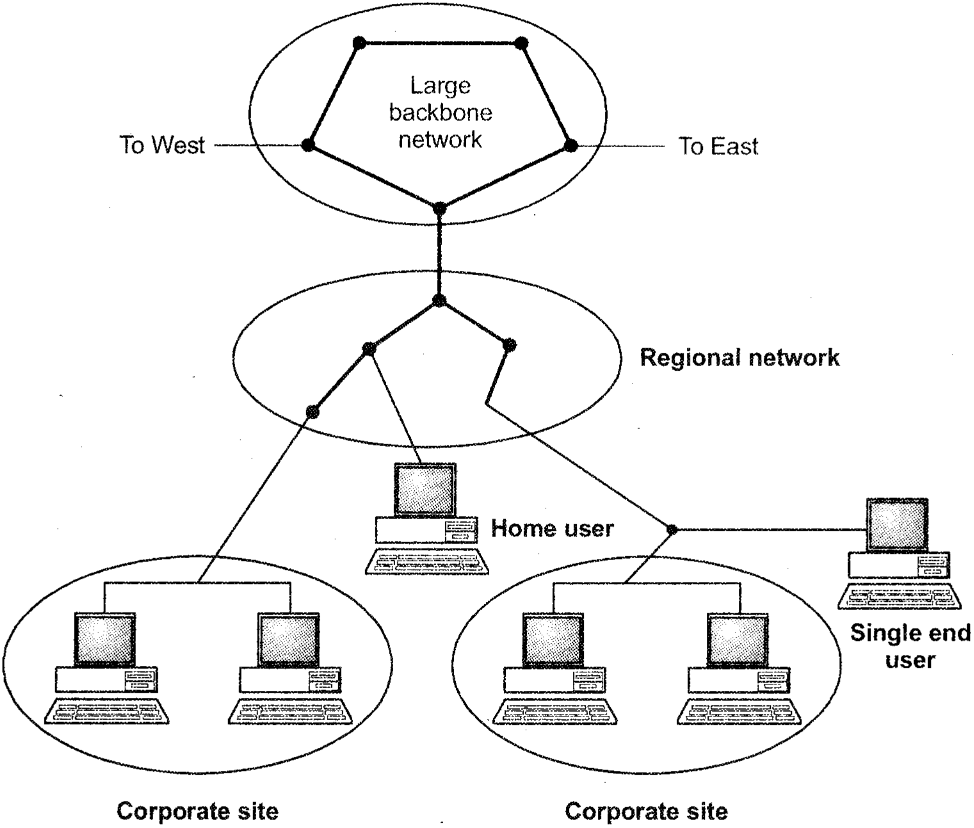


Figure 6.9: Pyramid structure of ISP

▶ How ISPs connect to the Internet?

Just as their customers pay them for internet access, ISPs themselves pay upstream ISPs for internet access. In the simplest case, a single connection is established to an upstream ISP using one of the technologies, and the ISP uses this connection to send or receive any data to or from parts of the internet beyond its own network; in turn, the upstream ISP uses its own upstream connection, or connections to its other customers to allow the data to travel from source to destination.

7. HTTP

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e., internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extension of its request methods, error codes and headers. It provides a standard for Web browsers and servers to communicate.

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.

7.1 HTTP Transaction

A request sent from the browser to,the server and the corresponding response from the server to the browser, both sent using HTTP. This round-trip communication path allows the browser to request a resource (URL) and receive a response from the server. It may include content sent by the browser (data entered in form fields, uploaded files) and content returned from the server (web page, image, etc).

An HTTP client can have multiple concurrent sessions, and each session can have multiple transactions.

A transaction represents an interaction between an HTTP client and an HTTP origin server. An HTTP transaction is a two-way communication between the client and the server: a client requests and a server responds. In a basic HTTP transaction, the client sends a request to the server, and the server processes the request and sends a response back to the client.

Figure 6.10 describes the general HTTP client structure for sessions and transactions.

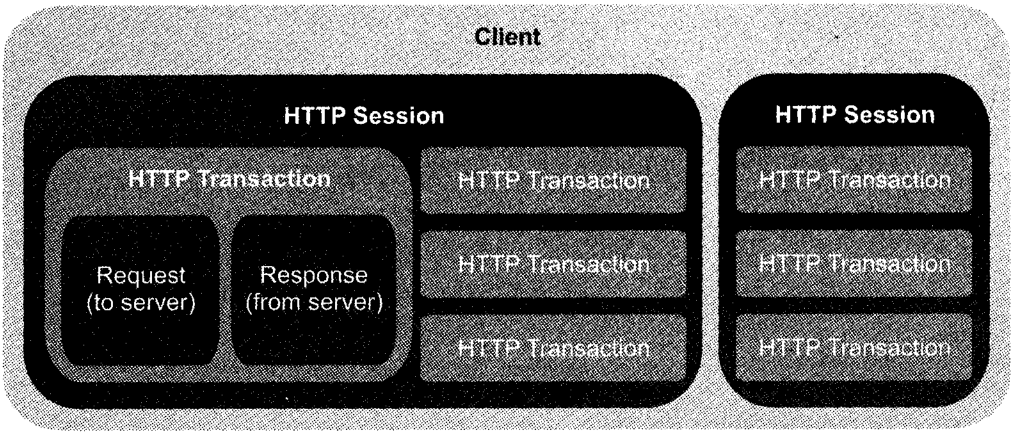


Figure 6.10: HTTP sessions and transactions

An HTTP transaction is implemented using the Osp::Net::Http::HttpTransaction class. The request and response portions of a transaction are composed of a header and an optional body. The header is a collection of header fields defined by and accessed through the Osp::Net::Http::HttpHeader class. Header fields can be created, read, modified, and removed through this class, and each field can have multiple values.

The request portion of the transaction specifies an HTTP method that describes the type of operation that the client wishes to invoke on the origin server. It also states the URI, which specifies the resources held on the server where the HTTP method is to be invoked. The response portion of a transaction contains an HTTP status code and a message, which indicates the success of the method or the state of the resources following the method.

The transaction can be submitted using one of the following modes:

i. **Non-chunked mode (default):** To send an HTTP request in non-chunked mode, add a header field Content-Length: body-length to a request header.

ii. **Chunked mode:** *To send an HTTP request in chunked mode:*

   a. Add a header field Transfer-encoding: chunked to a request header.

   b. Use the HttpTransaction::EnableTransactionReadyToWrite() method.

   c. Implement the OnTransactionReadyToWrite() event handler to send the chunks. An empty chunk is considered as the last chunk.

▶ Simple HTTP Transaction

A simple HTTP transaction is one where the client makes a single request for HTTP content.

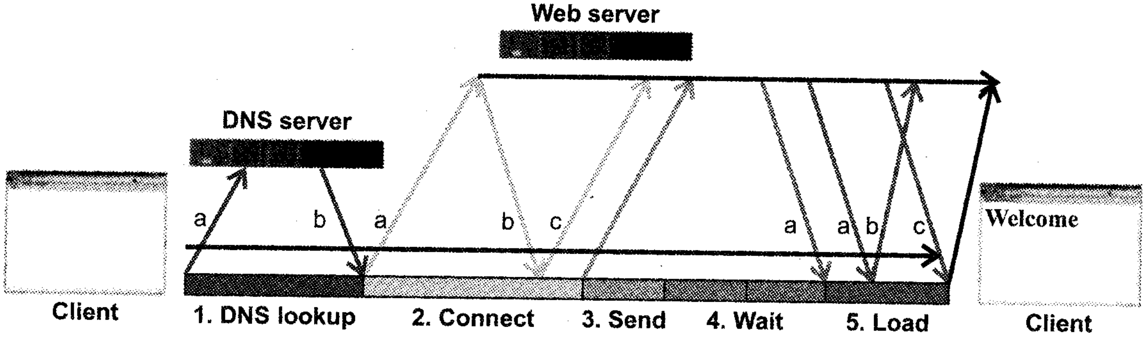


Figure 6.11

i. **DNS lookup**: The client tries to resolve the domain name for the request.

   a. Client sends DNS Query to local ISP DNS server.

   b. DNS server responds with the IP address for hostname.com

ii. **Connect**: Client establishes TCP connection with the IP address of hostname.com

   a. Client sends SYN packet.

   b. Web server sends SYN-ACK packet.

   c. Client answers with ACK packet, concluding the three-way TCP connection establishment.

iii. **Send**: Client sends the HTTP request to the web server.

iv. **Wait**: Client waits for the server to respond to the request.

   Web server processes the request, finds the resource, and sends the response to the client. Client receives the first byte of the first packet from the web server, which contains the HTTP response headers and content.

v. **Load**: Client loads the content of the response.

   a. Web server sends second TCP segment with the PSH flag set.

   b. Client sends ACK. (Client sends ACK every two segments it receives from the host)

   c. Web server sends third TCP segment with HTTP_Continue.

vi. **Close**: Client sends a FIN packet to close the TCP connection.

7.2 Persistent HTTP connections

The server must support this first of all, I cannot think of a server which is not supporting this at the moment. The header used to announce we want a persistent connection is:

Connection: Keep-Alive

The response from the server must contain the same header if the server supports keep-alive mode (persistent HTTP connections), and also, if we're using the HTTP v1.1, the server may also return information on how many HTTP requests may be sent via that same opened TCP stream, and what's the timeout period until the TCP stream closes if nothing is sent over the wire to the remote server.

▶ Advantages

i. **Faster content delivery:** Less round-trip time, everything is served via the same TCP stream which obviously saves a lots of time. When adding HTTP pipelining support to this, things are even faster. This is also extremely beneficial when it comes to secure delivery using the SSL protocol, which require extra round.

ii. **Less CPU usage:** We're involving a less amount of low level OS routine calls.

iii. **Reduced network congestion:** Less packets on the line, and more control for TCP to handle the congestion in a single stream.

▶ Disadvantages

i. **Possible scalability issues:** In case of a traffic burst, all the 'slots' on the web server (the connections pool) are kept busy by few users, while everybody else waits for a server response. This also happens with non-persistent connections as well, however the time to serve a different HTTP request is lower than with persistent connection, because there's no time-out period.

ii. **No simplicity friendliness:** A server serving simple one time files has no reason to serve HTTP content via persistent connection, because the one-time required content can be served using one HTTP request and the client will be gone.

Persistent connections allow the browser / HTTP client to utilize the same connection for different object requests to the same hostname. The HTTP 1.1 protocol supports persistent connections natively and does not require any specific HTTP header information. For HTTP 1.0, persistent connections are controlled via the Keep-Alive HTTP header.

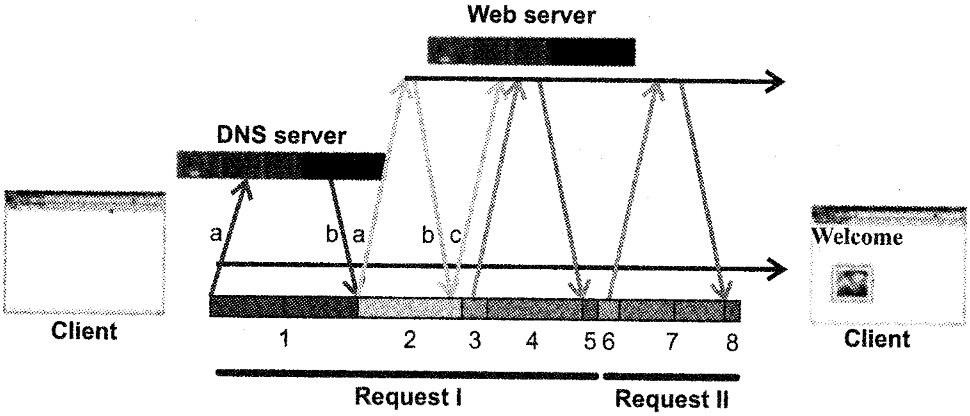


Figure 6.12

a. **DNS Lookup**: Client tries to resolve the domain name.
   1. Client sends DNS query to local ISP DNS server.
   2. DNS server responds with the IP address to hostname.com
b. **Connect**: Client establishes TCP Connection (1) with the IP address of hostname.com
   1. Client sends SYN packet.
   2. Web server sends SYN-ACK packet
   3. Client sends ACK packet, concluding three way TCP connection establishment
c. **Send**: Client sends the HTTP request to the web server.
d. **Wait**: Client waits for the server to respond to the request.
e. **Load**: Client loads the content of the response.
f. **Send**: Client sends the HTTP request to the web server
g. **Wait**: Client waits for the server to respond to the request.
h. **Load**: Client loads the content of the response.

7.3 Non-persistent HTTP Connection

As the browser receives the Web page, it displays the page to the user. Two different browsers may interpret a Web page in somewhat different ways. HTTP has nothing to do with how a Web page is interpreted by a client. The HTTP specifications define only the communication protocol between the client HTTP program and the server HTTP program.

We define the **round-trip time (RTT),** which is the time it takes for a small packet to travel from one client to server and then back to the client. The RTT includes packet-propagation delays, packet-queuing delays in intermediate routers and switches, and packet-processing delays.

▶ Advantages

i. **Possibly more scalable:** Depending on the design of the application and the usage patterns (like mentioned in the disadvantages for persistent HTTP connections), more clients can be served if they require content from the server sporadically.

ii. **Simple server architecture:** The server may be a bit faster if it doesn't require the implementation of the persistent HTTP connections and the pipelining support.

▶ Disadvantages

i. **Possibly less scalable:** Depending on the type of traffic the server gets, serving individual HTTP requests on their own TCP stream may quickly starve the server's resources.

ii. **More CPU usage:** There are low level operating system routines involved in opening a new TCP stream for each request. This puts the web server under more work.

PU Questions

5 Marks

[Apr. 2013 – *5M*] 1. Explain intranet and extranet in detail.

[Apr. 2013 – *5M*] 2. Explain in details:

i. Web Servers ii. Search engines

[Oct. 2012 – *5M*] 3. Write short note on Internet Information Server (IIS).

[Oct. 2012 – *5M*] 4. Explain the architecture of www.

[Apr. 2012 – *5M*] 5. Write a note on ISP.

[Apr. 2012 – *5M*] 6. Explain the following terms:

i. Web Server ii. Web Documents

[Oct. 2011 – *5M*] 7. What is WWW? Explain its architecture.

[Oct. 2011 – *5M*] 8. What is Internet Information Server? Explain with benefits.

[Apr. 11, Oct. 10 – *5M*] 9. Write a short note on Search Engines.

[Apr. 2011 – *5M*] 10. Write a short note on WWW.

[Oct. 2010 – *5M*] 11. Explain www Architecture.

[Oct. 2010 – *5M*] 12. Explain Intranet and Extranet.

[Apr. 2010 – *5M*] 13. Explain working of Web Server.

[Apr. 2010 – *5M*] 14. What is Internet Information Server (IIS)? Explain with benefits.

VISION

Suggestive Readings:

1. Computer Networks (3rd & 4th Edition), Andrew S. Tannenbaum, PHI / Pearson’s Publications.
2. Behrouz A Forouzan, “Data Communications and Networking”, McGraw Hill.
3. Computer Networks (2nd edition), Uyless Black, PHI Publication
4. Computer Network, ED Tittle, Tata MacGraw Hills Publications
5. Computer Networks : Andrew Tanenbaum
6. Computer Networks : A Top Down Approach by Behrouz forouzan mosharraf
7. Networking Essentials : Emmett Dulaney
8. Andrew S. Tanenbaum, Computer Networks, Prentice Hall
9. Behrouz A. Forouzan and Sophia Chung Fegan, Data Communications and Networking, McGraw-Hill Companies
10. Burton, Bill, Remote Access for Cisco Networks, McGraw-Hill, Osborne Media
11. Dale Tesch/Greg Abelar, Security Threat Mitigation and Response: Understanding CS-MARS, Cisco Press, Sep. 26, 2006.
12. Gary Halleen/Greg Kellogg, Security Monitoring with Cisco Security MARS, Cisco Press, Jul. 6, 2007.
13. Web Tutorials on HTML and Front Page