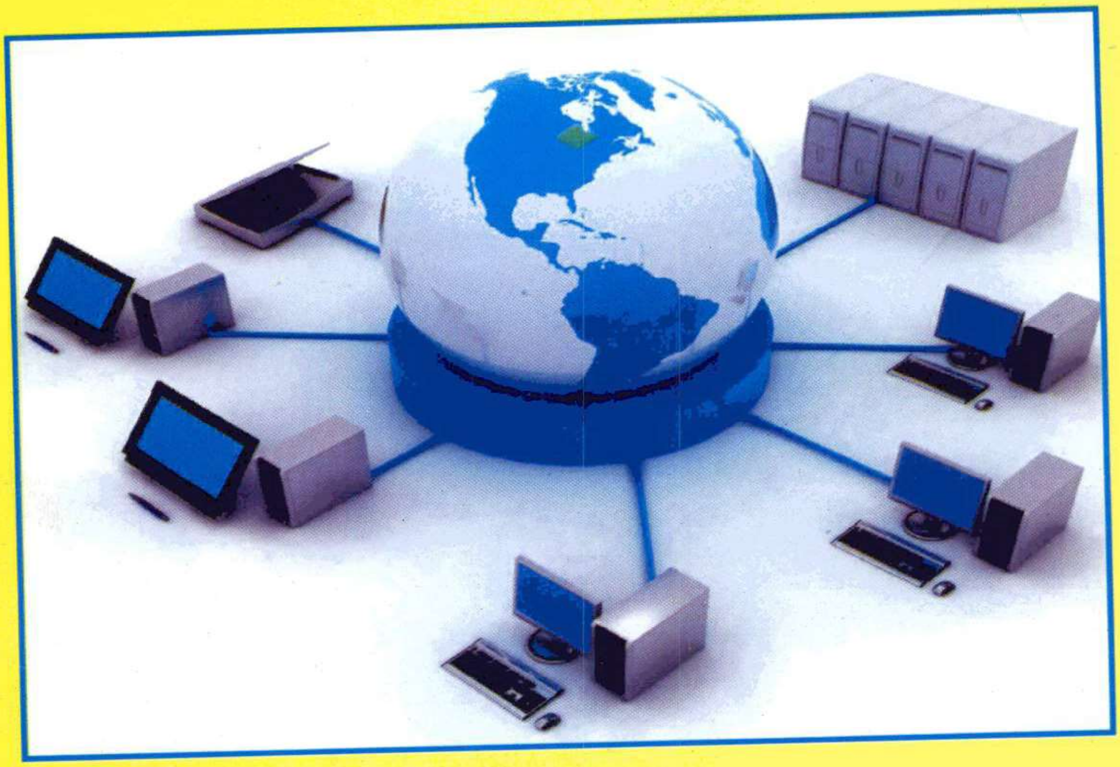
ಕರ್ನಾಟಕ ರಾಜ್ಯ ಮುಕ್ತ ವಿಶ್ವವಿದ್ಯಾನಿಲಯ
ಮಾನಸಗಂಗೋತ್ರಿ, ಮೈಸೂರು – 570 006

KARNATAKA STATE OPEN UNIVERSITY
Manasagangotri Mysore - 570 006

# M.Sc. Computer Science

## Second Semester



# COMPUTER NETWORKS

Course: 10

Module : 1 - 6

MSCS-510 COMPUTER NETWORKS

ಉನ್ನತ ಶಿಕ್ಷಣಕ್ಕಾಗಿ ಇರುವ ಅವಕಾಶಗಳನ್ನು ಹೆಚ್ಚಿಸುವುದಕ್ಕೆ ಮತ್ತು ಶಿಕ್ಷಣವನ್ನು ಪ್ರಜಾತಂತ್ರೀಕರಿಸುವುದಕ್ಕೆ ಮುಕ್ತ ವಿಶ್ವವಿದ್ಯಾನಿಲಯ ವ್ಯವಸ್ಥೆಯನ್ನು ಆರಂಭಿಸಲಾಗಿದೆ.

ರಾಷ್ಟ್ರೀಯ ಶಿಕ್ಷಣ ನೀತಿ 1986

*The Open University System has been initiated in order to augment opportunities for higher education and as instrument of democrating education.*

*National Educational Policy 1986*

---

## ವಿಶ್ವ ಮಾನವ ಸಂದೇಶ

ಪ್ರತಿಯೊಂದು ಮಗುವು ಹುಟ್ಟುತ್ತಲೇ – ವಿಶ್ವಮಾನವ, ಬೆಳೆಯುತ್ತಾ ನಾವು ಅದನ್ನು 'ಅಲ್ಪ ಮಾನವ'ನನ್ನಾಗಿ ಮಾಡುತ್ತೇವೆ. ಮತ್ತೆ ಅದನ್ನು 'ವಿಶ್ವಮಾನವ'ನನ್ನಾಗಿ ಮಾಡುವುದೇ ವಿದ್ಯೆಯ ಕರ್ತವ್ಯವಾಗಬೇಕು.

ಮನುಜ ಮತ, ವಿಶ್ವ ಪಥ, ಸರ್ವೋದಯ, ಸಮನ್ವಯ, ಪೂರ್ಣದೃಷ್ಟಿ ಈ ಪಂಚಮಂತ್ರ ಇನ್ನು ಮುಂದಿನ ದೃಷ್ಟಿಯಾಗಬೇಕಾಗಿದೆ. ಅಂದರೆ, ನಮಗೆ ಇನ್ನು ಬೇಕಾದುದು ಆ ಮತ ಈ ಮತ ಅಲ್ಲ; ಮನುಜ ಮತ. ಆ ಪಥ ಈ ಪಥ ಅಲ್ಲ ; ವಿಶ್ವ ಪಥ. ಆ ಒಬ್ಬರ ಉದಯ ಮಾತ್ರವಲ್ಲ; ಸರ್ವರ ಸರ್ವಸ್ತರದ ಉದಯ. ಪರಸ್ಪರ ವಿಮುಖವಾಗಿ ಸಿಡಿದು ಹೋಗುವುದಲ್ಲ; ಸಮನ್ವಯಗೊಳ್ಳುವುದು. ಸಂಕುಚಿತ ಮತದ ಆಂಶಿಕ ದೃಷ್ಟಿ ಅಲ್ಲ; ಭೌತಿಕ ಪಾರಮಾರ್ಥಿಕ ಎಂಬ ಭಿನ್ನದೃಷ್ಟಿ ಅಲ್ಲ; ಎಲ್ಲವನ್ನು ಭಗವದ್ ದೃಷ್ಟಿಯಿಂದ ಕಾಣುವ ಪೂರ್ಣ ದೃಷ್ಟಿ.

ಕುವೆಂಪು

---

## *Gospel of Universal Man*

Every Child, at birth, is the universal man. But, as it grows, we trun it into "a petty man". It should be the function of education to turn it again into the enlightened "universal man".

The Religion of Humanity, the Universal Path, the Welfare of All, Reconciliation, the Integral Vision - these ***five mantras*** should become view of the Future. In other words, what we want henceforth is not this religion or that religion, but the Religion of Humanity; not this path or that path, but the Universal Path; not the well-being of this individual or that individual, but the Welfare of All; not turning away and breaking off from one another, but reconciling and uniting in concord and harmony; and above all, not the partial view of a narrow creed, not the dual outlook of the material and the spiritual, but the Integral Vision of seeing all things with the eye of the Divine.

*Kuvempu*

# SECOND SEMSTER M. Sc COMPUTER SCIENCE

## Module 1

## MODULE 2

## MODULE 3

## MODULE 4

## MODULE 5

## MODULE 6

**Course Design and Editorial Committee**

**Prof. K.S.Rangappa**
Vice-Chancellor & Chairperson
Karanataka State Open University
Manasagangotri, Mysore – 570 006

**Prof. Jagadeesha**
Dean (Academic) & Convenor
Karnataka State Open University
Manasagangotri, Mysore– 570 006

**Head of the Department - Incharge**

**Prof. Jagadeesha**
Chairman, DOS in Commerce
and Management,
Karnataka State Open University ,
Manasagangothri ,
**Mysore-570 006**

**Course Co-Ordinator**

**Smt. Sumati. R. Gowda**
***BE(CS & E)., MSc(IT)., MPhil (CS).,***
Lecturer, DOS in Computer Science,
Karnataka State Open University ,
Manasagangothri,
**Mysore-570 006**

**Course Writers** **Module 1 - 6** **Units 1-24**

**Dr. Hemanth Kumar** **Module-1 to 3**
Professor and Chairman,
Department of Studies in Computer Science
University of Mysore
Manasagangotri, Mysore – 570 006

**Dr. K. Raghuveer** **Module-4 to 6**
Professor and HOD,
Department of IS & E
NIE, Mysore
Manasagangotri, Mysore – 570 006

**Publisher**

Registrar
Karnataka State Open University,
Manasagangotri, Mysore - 6.

**Developed by Academic Section, KSOU, Mysore**
Karnataka State Open University, 2010

Further information on the Karnataka State Open University Programmes may obtained from the University's office at Manasagangotri, Mysore-6

Printed and Published on behalf of Karnataka State Open University. Mysore-6 by **Registrar (Administration)**

# Preface

This book covers fundamental concepts computer networks, with their application to modeling and analysis of computer systems and communication networks. The aim of the book is to provide the reader with state-of-the-art analytical and computational tools to evaluate the performance and operating characteristics of today's computer systems and communication networks. The organization of book is as follows, it consists of total 6 modules and each module is divided in four units. Module 1 reveals the necessity of network hardware as well as network software; which mainly focuses on the today's requirement and advantages computer networks. Unit 1 covers the different network categories such as local area network, Wide area network and internetworks and their design issues. Next part of the unit is mainly focuses on the network software at different level of OSI reference model. Topologies are also important when the concept of networks appears hence in this book it has been clearly discussed about the different topologies. In unit 2 OSI reference model, TCP/IP model are discussed in detail with comparison with one another. Unit 3 gives an idea about how these models or topologies can be achieved easily by giving example such as novel netware, ernet, ATM and Ethernet systems. Module 3 and 4 explains about the different layer design issues and working principles of different protocols at different levels including dta link layer, medium access layer, physical layer etc. Different protocol principle and their design issues and working property are discussed in details with suitable example and many programming aspects about some important protocols are also considered in this book. Remaining part of the book will provide idea about the network traffic and network security. Different routing algorithm and error detection and correction policies with suitable examples are covered. Apart from this book also consists of flow charts, block diagrams and block of codes and figure which are visual friendly and readers can easily understand the concepts with the help of figures. The many mathematical calculations are solved and it has been showed step by step with useful information. Each unit has keywords part so the reader can get important issues related to respective unit.

# UNIT-1: Network hardware, Network software

## Structure

## 1.0 OBJECTIVES

After studying this unit you will be able to:

- Explain the sharing of resources such as information or processors.
- Elucidate the Different uses of Computer Network
- Discuss Different Types of Network Hardware and Software
- State Functions of Network Components

## 1.1 Introduction

Traditional definition of "network" is a group of computers connected together to share resources such as programs, files, printer, and storage disk. However modern network also includes connections to portable/mobile devices (such as tablet PC, notebook, PDA, digital camera, portable MP3 player, and mobile phone), home entertainment devices (such as TV, video player/recorder, stereo, and radio), home appliances (such as refrigerator and washing machine), and monitoring or sensor devices. Wearable things (such as wristwatch, clothing) and perhaps living objects like human, pet, and tree will be network-able in the not-so-distant future.

Network design is not a hard-to-grasp science, yet it had been only the job of IT professionals or network specialists before because it was only about big company networks with complex wiring and many computers. Nowadays network design comes down to consumer realm because of the growing popularity of wireless ad-hoc networks using IrDA and Bluetooth and the prevailing home networking technologies such as Ethernet, Wi-Fi, HomePNA, and HomePlug. New technologies such as ZigBee and WiMedia (UWB) will give even more connectivity choices for consumer networks.

## 1.2 Advantages of Computer Networks

These purposes must be fulfilled by various advantages of networks.

**1. Resource Sharing**

Resource sharing means the goal is to make all programs, data and equipment available to anyone on the network without regard to the physical location of the resource and the user.

Example: Suppose a user happens to be 1000 km away from his data should not prevent him from using the data as though they were local. Also load sharing is another aspect of resource sharing.

**2. High Reliability**

Network provides high reliability by having alternative sources of supply.

Example: Suppose all files could be replicated on two or three machines, so if one of them is unavailable (due to a hardware failure), the other copies could be used. For military, banking, air traffic control, and other applications, the ability to continue operating the face of hardware problems is of great importance.

**3. Low Cost/Saving Money**

Small computers have a much better price/performance ratio than large one. Mainframes are roughly a factor of fourty faster than the fastest single chip microprocessors, but they cost a thousand times more. This imbalance has caused many system designers to build systems consisting of powerful personal computers, as per user, with data kept on one or more shared file server machines.

**4. Communications**

Another goal of setting up a computer network has little to do with technology at all. A computer network can provide a powerful communication medium among widely separated people. Using a network, it is easy for two or more people who live far apart to write a report together. i.e. when one author makes a change to the document, which is kept online, the others can see the change immediately, instead of waiting several days for a letter.

## 1.3 Uses of Computer Networks

1. Access to remote programs: A company that has produced a model simulating the world economy may allow its clients to log in over the network and run the program to see how various projected inflation rates, interest rates, and currency fluctuations might affect their business. This approach is often preferable to selling the program outright, especially if the model is constantly being adjusted or requires an extremely large mainframe computer to run.

2. Access to remote data bases: It may soon be easy for the average person sitting at home to make reservations for aeroplanes, trains, buses, boats, hotels, restaurants, theatres and so on, anywhere in the world with instant confirmation. Home banking and the automated newspaper also fall in this category.

3. Value-added communication facilities: High-quality communication facilities tend to reduce the need for physical proximity. Everyone in the world, have an ability to send and receive

electronic mail. These mails are also be able to contain digitized voice, still pictures and possibly even moving television and video images.
4. using for entertainment purpose.
5. Accessing the information systems like World Wide Web, this contains almost any information.

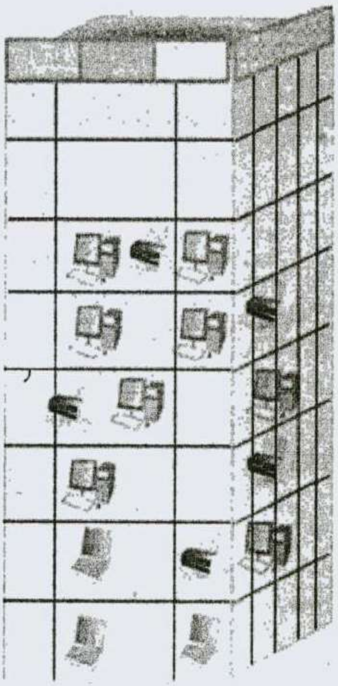
## 1.4 Categories of Network Hardware

Today when we speak of networks, we are generally referring to three primary categories based on its size, its ownership, the distance it covers and its physical architecture.

- ➢ Local-Area Networks.
- ➢ Metropolitan-Area Networks.
- ➢ Wide-Area Networks.
- ➢ Internetworks

a. **Local Area Network**

LAN (Local Area Network) is a network that connects computers, peripherals and other devices within a building (e.g. office, home) or in a limited area. Typical LAN coverage is about 50 to 300 meters. LAN is also known as campus network. Most LANs today are implemented using Ethernet. Wireless LAN using Wi-Fi technology also grows in popularity as an alternative to Ethernet.



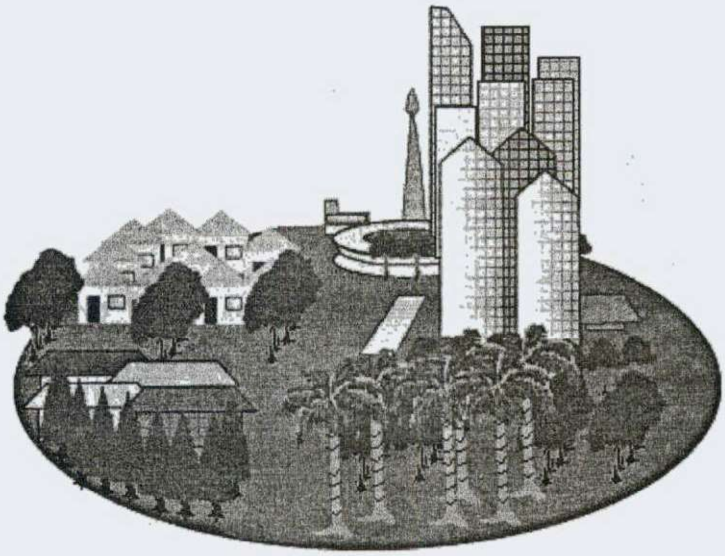
**LAN.** Computers and printers in an office network.

- The main reason for designing a LAN is to share resources such as disks, printers, programs and data.
- It also enables the exchange of information.
- LAN having data rate of 4 Mbps to hundreds of Mbps.

- LANs typically can use the star, bus or a ring topology.
- Example Ethernet LANs, Token Bus LANs, Token Ring LANs, FDDI.

### b. Metropolitan Area Networks.

MAN (Metropolitan Area Network) is a city wide network. The coverage limitation is not strict, but real implementation may have range of up to 50 km in urban, suburban, or rural area. MAN is built to interconnect LANs, provide access to special contents and high speed Internet access. MAN is implemented using technologies such as ADSL or VDSL, HFC (CATV), FTTN or FTTH/FTTP.

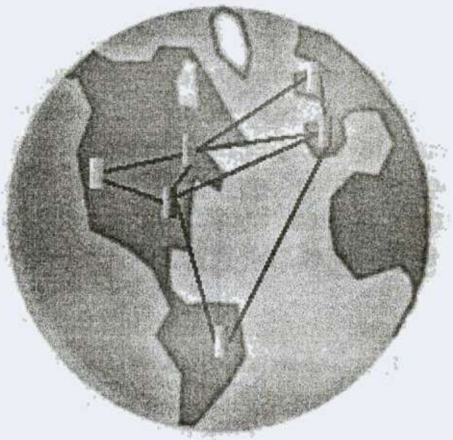


**MAN.** A network that covers a city.

- It may be a single network such as a cable television network, or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device.
- A MAN may be wholly owned and operated by a private company, or it may be a service provided by a public company, such as local telephone company.
- Many telephone companies provide a popular MAN device called switched Multimegait Data Services.
- A MAN has a larger geographical scope compared to a LAN and can range from 10 km to a few hundreds km in length.
- A typical LAN operates at a speed of 1.5 to 150 Mbps.

### c. Wide Area Network

WAN (Wide Area Network) is a network that spans larger geographical area. PSTN (fixed telephone network) and PLMN (mobile cellular telephone network such as GSM, CDMA, and 3G) are examples of WAN. The largest WAN is the Internet that has worldwide coverage.

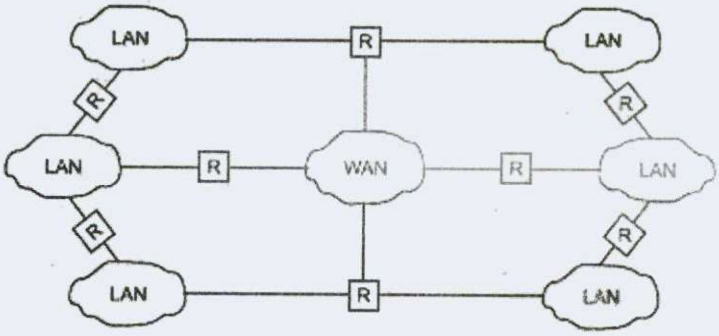


**WAN.** Regional, national or international network

- A WAN speed ranges from 1.5 Mbps to 100 Gbps.
- WANs may utilize public, leased or private communication devices, usually in combinations, and can therefore span an unlimited number of miles.
- A good example of such a network is internet, which has a connection to similar networks in other countries.

**d. Internetworks**

When two or more networks are connected, they become an internetwork, or internet



**Internetwork (internet)**

The boxes labeled R represent routers.

- Individual networks are joined into internetworks by the use of internetworking devices.
- These devices, which include routers and gateways.
- The term internet (lower case i) should not be confused with the internet (upper case I). The first is a generic term used to mean an interconnection of networks. The second is the name of a specific worldwide network.

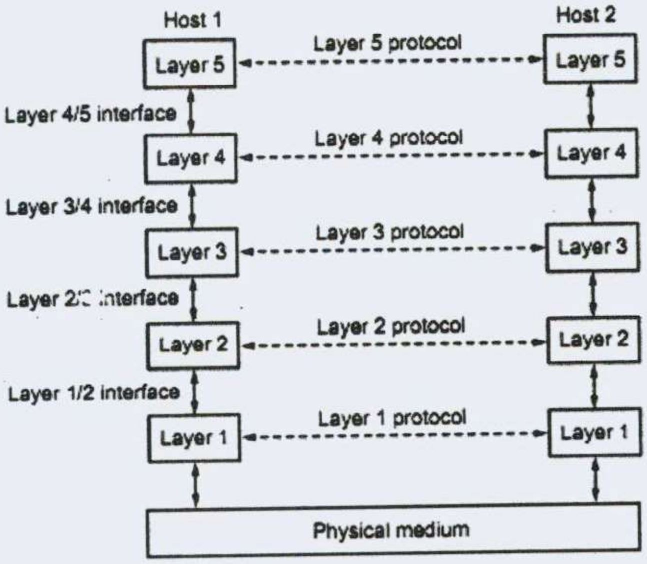
## 1.5 Network Software

The first computer networks were designed with the hardware as the main concern and the software as an afterthought. This strategy no longer works. Network software is now highly structured. In the following sections we examine the software structuring technique in some detail.

## Protocol Hierarchies

To reduce their 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, the contents 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 layers, 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.

This concept is actually a familiar one and used throughout computer science, where it is variously known as information hiding, abstract data types, data encapsulation, and object-oriented programming. The fundamental idea is that a particular piece of software (or 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 this conversation are collectively known as the layer n protocol. Basically, a protocol is an agreement between the communicating parties on how communication is to proceed. As an analogy, when a woman is introduced to a man, she may choose to stick out her hand. He, in turn, may decide either to shake it or kiss it, depending, for example, on whether she is an American lawyer at a business meeting or a European princess at a formal ball. Violating the protocol will make communication more difficult, if not completely impossible.



Layers, protocols, and interfaces.

A five-layer network is illustrated in above figure. 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.

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. Below layer 1 is the physical medium through which actual communication occurs. In Figure, virtual communication is shown by dotted lines and physical communication by solid lines.

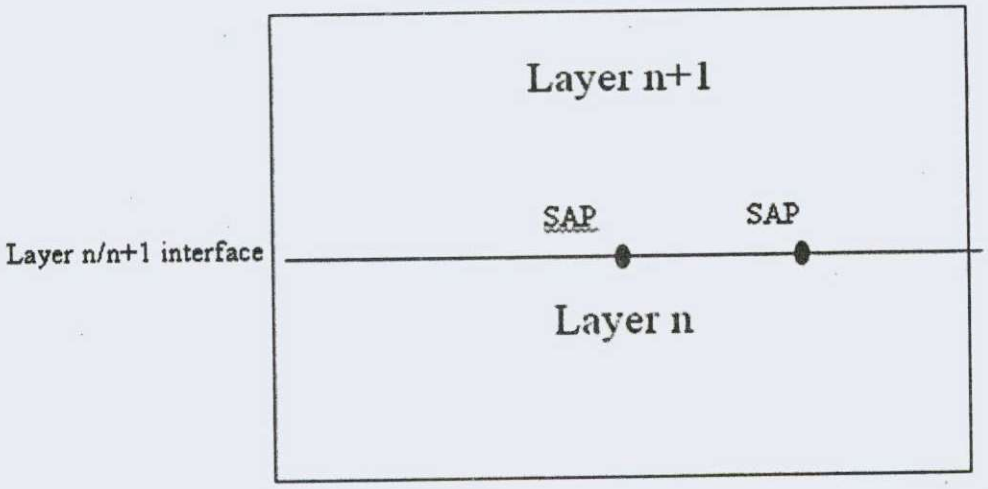
**Design Issues for the Layers**

Some of the key design issues that occur in computer networks are present in several layers. Below, we will briefly mention some of the more important ones. Every layer needs a mechanism for identifying senders and receivers.

1. Every layer needs mechanism for identifying senders and receivers. Since a network normally has many computers, a means is needed for a process on one machine to specify with whom it want to talk. Example, network layer uses IP address for identifying sender and receiver.
2. The rules for data transfer must be specified. In some system data only traveled in one direction (simplex communication), ir others they can travel in either directions but not simultaneously (half-duplex communication), or they can travel in both directions at the same time (full-duplex communication).
3. Error control is an important issue because physical communication circuits are not perfect Thus, ends of the connection must agree with a certain error-detecting or error correcting code.
4. Not all communication channels preserve the order messages sent to them. To deal with possible loss of sequencing, the protocol must make explicit provision for receiver to allow the pieces of data to put back together properly.
5. An issue that occurs at every level is how to keep a fast sender form swamping a slow receiver with data. One possible solution is by limiting the sender to an agreed upon transmission rate.
6. The inability of all processes to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting and then reassembling messages. This is called fragmentation.
7. When there are multiple paths between source and destination, a route must be chosen. Sometimes this decision must be split over two or more layers.

## 1.6 Interfaces and services

The function of each layer is to provide service to the layer above it. The active element in each layer is often called “entities" which could be software entity or hardware entity. Entities in the same layer on different machines are called peer entities. The entity on layer n implement a service used by layer n+1. In this case layer n called "service provider" and layer n+1 is called "service user". Layer n may use the service of layer n-1 in order to provide its services. Services are available at SAPs (Service Access Points). The layer n SAPs are placed where layer n+1 can access the service offered. Each SAP has an address that uniquely identifies it.



**Relation between layers at an interface**

Layers can offers two different types of services to the layers a above them: connection-oriented and connection less.

- Connection oriented service: is implemented by service user first establish a connection, use the connection and then release the connection. Thus sender pushes objects (bits) in at one end, and the receiver takes them out in the same order at other end (for example to a connection- oriented networks is the telephone system).

- Connection less service: in which each message carries the full destination address and each one is routed in the system independent of all the others. Hence, there is a possibility that the first one sent can be delayed so that the second one arrives first. This is impossible with a connection oriented service. In connection less there is no need to establish connection first as the provider and destination always on line. (For example to a connection less networks is ISDN network "Integrated Service Digital Network").

## 1.7 NETWORK TOPOLOGIES

The term "TOPOLOGY" refers to the way in which the end points or stations/computer systems, attached to the networks, are interconnected. We have seen that a topology is essentially a stable geometric arrangement of computers in a network. If you want to select a topology for doing networking. You have attention to the following points.

- Application S/W and protocols.
- Types of data communicating devices.
- Geographic scope of the network.
- Cost.
- Reliability.

Depending on the requirement there are different Topologies to construct a network.
(1) Mesh topology.

(2) Star topology.
(3) Tree topology.
(4) Bus topology.
(5) Ring topology.

- Ring and mesh topologies are felt convenient for peer to peer transmission.
- Star and tree are more convenient for client server.
- Bus topology is equally convenient for either of them.

### Mesh Topology

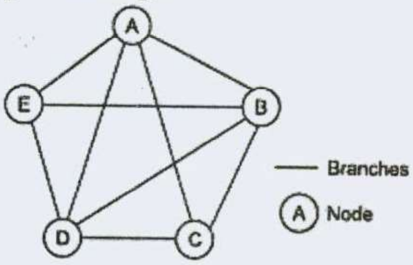
In mesh topology each and every computer is connected to each other with direct point to point link. A fully connected mesh network therefore has **n (n–1/2)** physical channels to link **n** devices. To accommodate these, every device on the network must have **(n–1)** input/output parts.

**Advantages**

- Use of dedicated links eliminates the traffic problems.
- It is robust, i.e. if one link becomes unusable it does not incapacitate the entire system.
- Privacy is maintained since the message travels along the dedicated lines.
- Point-to-point link makes fault identification and fault isolation easy.

**Disadvantages**

- The amount of cabling required is high.
- The number if I/O ports required is high.



Mesh topology

### Star Topology

In a star topology, cables run from every computer to a centrally located device called a HUB. Star topology networks require a central point of connection between media segment. These central points are referred to as Hubs. Hubs are special repeaters that overcome the electromechanical limitations of a media. Each computer on a star network communicates with a central hub that resends the message either to all the computers. (In a broadcast network) or only the destination computer. (In a switched network).

Ethernet 10 base T is a popular network based on the star topology.

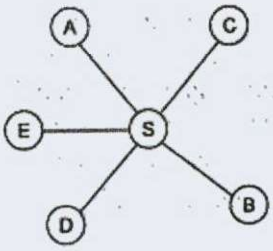
**Advantages**

- Easy to modify and to add new computers without disturbing the rest of the network.

- Less expensive than mesh topology.
- Each device needs only one link and one port.
- Easy to install and configure.
- Easy to diagnose network faults.
- Single computer failure does not affect the network.
- Ordinary telephone cables can be used.

### Disadvantages

- More cabling is required as compare to others.
- Failure of the central hub brings the entire network down.



Star topology

### Bus Topology

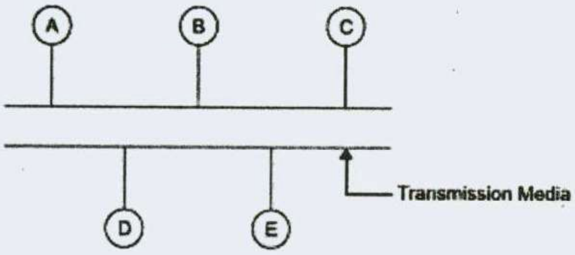
- A bus topology is multipoint.
- One long cable acts as a backbone to link all the devices in the network.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a line running between the device and main cable.
- A tap is connector that splices into the main cable. There is a limit on the number of Taps used and distance between the taps.

### Advantages

- Simple, reliable and easy to use.
- Easy to installation and cheaper than when compared with others.
- Less cabling.

### Disadvantages

- Can be used in relatively small networks.
- All computers share the same bus.
- Reconfiguration is difficult.
- Fault identifications is difficult.
- Adding new nodes is difficult.
- A fault on the cable stops all transmission.



Bus topology

### Ring Topology

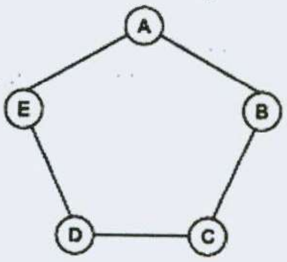
In ring topology, each device has a dedicated point-to-point line configuration only with two devices on either side of it. A signal is passed along the ring in one direction, from device to device until it reaches its destination. Each device in the ring has a repeater. When the devices receive the signal intended for the other node, it just regenerates the bits and passes them along. Ring network passes a token. A token is a short message with the electronic address of the receiver. Each network interface card is given a unique electronic address, which is used to identify the computer on the network.

### Advantages

- Easy to install and reconfigure.
- Adding/deleting the new device is easy as only two connections have to be adjusted.
- Fault isolation is simplified.
- No terminators required.

### Disadvantages

- A break in the ring can stop the transmission the entire network.
- Difficult to troubleshoot.
- Adding/removing computer distrupts the entire network.
- Expensive when compared with other topologies.
- When one computer fails overall network distrupts.

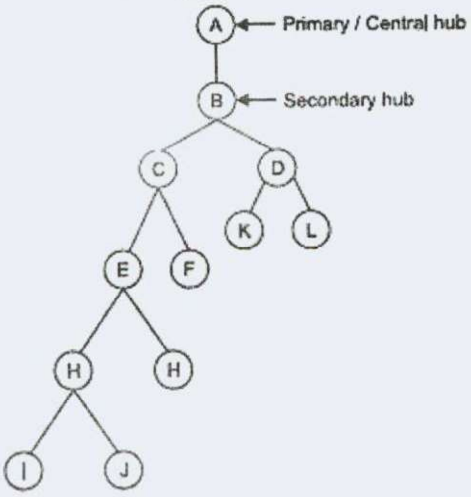


Ring topology

### Tree Topology

It is similar to the star network, but the nodes are connected to the secondary hub that in turn is connected to the central hub. The central hub is the active hub. The active hub contains the repeater, which regenerates the bits pattern it receives before sending them out. The secondary hub can be either active or passive. A passive hub provides a simple physical connection between the attached devices.

Advantages and Disadvantages of the tree are same as that of the star network. Also, the addition of the secondary hub allows more devices to be attached to the central hub. It also allow the network to isolate priorities communication from different computers. The tree topology structure is shown in the figure



Tree topology

## 1.8 Summary

This unit introduces internetworking concept and its application in the modern era internet and communication, later it describes the key elements such as LAN, WAN, MAN and also the about network software finally in summary we have included the network component and there functions.

The following table explains network components along with their functions

| Network Component | Functions |
|---|---|
| Network Adapter | Converts a computer message into electrical/optical signals for transmission across a network. |
| Modem (Modulator demodulator) | Puts a message (baseband signal) on a carrier for efficient transmission; takes the baseband signal from the carrier. |
| Repeater (Regenerator) | Receives signal, amplifies it, and then retransmits it. |
| Bridge | Connects networks with different Layer 2 protocols; divides a network into several segments to filter traffic. |
| Hub | Connects computers in a network; receives a packet from a sending computer and transmits it to all other computers. |
| Switch | Connects computers in a network; receives a packet |

|  |  |
|---|---|
|  | from a sending computer and transmits it only to its destination. |
| Access Point | Connects computers in a wireless network; connects the wireless network to wired networks; connects it to the Internet. |
| Router | Forwards a packet to its destination by examining the packet destination network address. |
| Gateway | Connects a home network to the Internet; hides all computers in the home network from the Internet. |

## 1.9 Keywords

Network, Internet, LAN, MAN, WAN, Layers

## 1.10 Exercises

1. What is computer network? Give its advantages and applications
2. Discuss different types of network hardware with their uses
3. Distinguish between LAN MAN and WAN with an examples
4. Explain various issues in design of layers

## 1.11 References

1. Data Communications and Networking – Behrouz A. Forouzan, 4th Edition, Tata McGraw-Hill, 2006.
2. Communication Networks: Fundamental Concepts and Key Architectures - Alberto Leon, Garcia and Indra Widjaja, 3rd Edition, Tata McGraw- Hill, 2004.
3. Data and Computer Communication, William Stallings, 8th Edition, Pearson Education, 2007.

# UNIT-2: Reference Models: OSI and TCP

## Structure

## 2 .0 OBJECTIVES

After studying this unit you will be able to

- Explain the OSI Reference Model Overview
- Understand TCP/IP origin and history
- Discuss the OSI reference models functions
- Understand data encapsulation and how it relates to four layer of TCP/IP protocols
- State the Applications of each layer in the model

## 2.1 Introduction

To varying extents, architectures for computer networking have used conceptual models, into which their mechanisms are mapped, the scope of mechanisms defined, and possible gaps in coverage. The best-known of these, the Open Systems Interconnection Reference Model (OSIRM), developed by the International Organization for Standardization (ISO) is indeed best known, but is, in practical networks, relegated to historical significance. In contrast, the Internet Protocol Suite, which is far less abstract, and not routinely called a reference model,

Two major approaches:

1. The seven-layer OSI/ISO model – Open Systems Interconnection, currently maintained by the International Organization for Standards.
2. The five-layer TCP/IP model – Transmission Control Protocol/Internet Protocol.

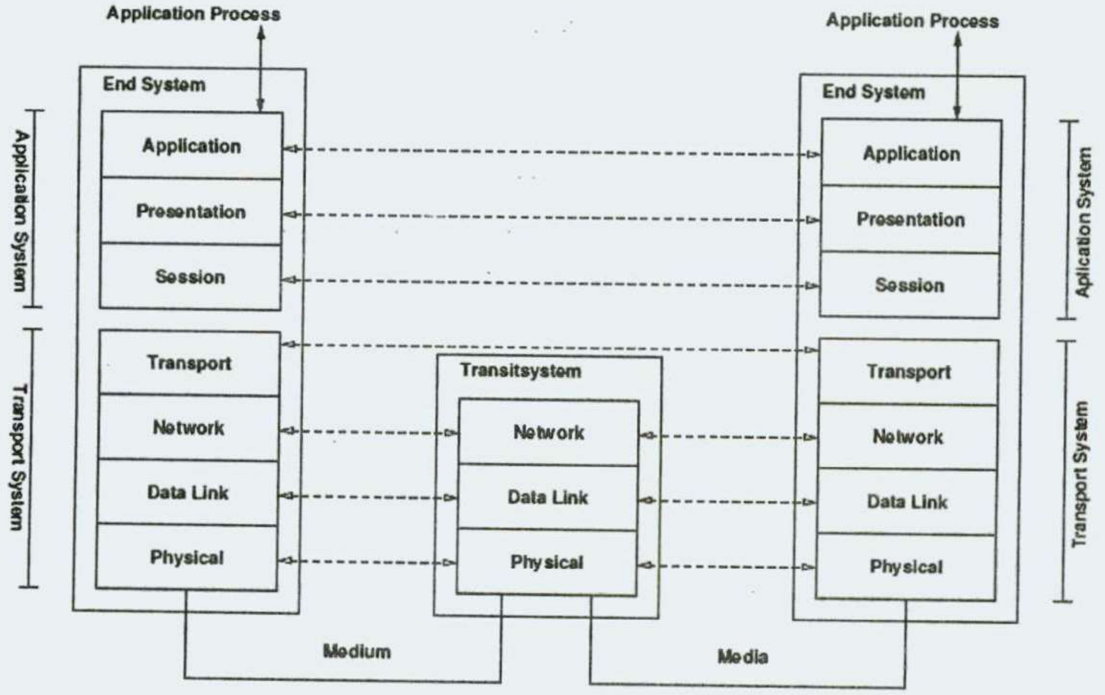
## 2.2 The OSI Reference Model

The International Organization of Standardization (ISO) defined procedures for computer communications which was called Open System Interconnection (OSI) Reference Model or OSI Model for short. The OSI Model describes how data flows from one computer to another computer in a network.

The OSI Model is defined as a protocol stack that consists of seven logical layers. Each layer has specific functions and handles a unique data format. When two computers communicate, data flows from the user-to-network interface (application) at the sending computer down through the protocol stack to the connecting physical medium (i.e. cable, radio, or infrared) and up through the protocol stack to the network-to-user interface (application) at the receiving computer. When data flows from an upper layer to a lower layer, it is converted to the lower layer data format and a lower layer header is added to it. This process is called encapsulation. Conversely, when data flows from a lower layer to an upper layer, it is converted to the upper layer data format and the lower layer header is discarded.

The 'standard' layered model used for illustrative purposes only is the OSI Model It consists of seven layers:

- Application Layer (Provide end-user services, like e-mail)
- Presentation Layer (Data compression, and other data conversion)
- Session Layer (Authentication/Authorization)
- Transport Layer (Guarantee end-to-end data transfer—from machine to machine)
- Network Layer (Routing, accounting).
- Data Link Layer (Transmit/receive packets, resolve hardware addresses)
- Physical Layer (Physical cable, medium, air)



ISO/OSI reference model

**Application Layer**

Layer 7, the highest layer: This layer interfaces directly to and performs common application services for the application processes. The common application services provide semantic conversion between associated application processes. Examples of common application services include the virtual file, virtual terminal (for example, Telnet), and ”Job transfer and Manipulation protocol”.

**Presentation Layer**

Layer 6: The Presentation layer relieves the Application layer of concern regarding syntactical differences in data representation within the end-user systems. MIME encoding, encryption and similar manipulation of the presentation of data is done at this layer. An example of a presentation service would be the conversion of an EBCDIC-coded text file to an ASCII-coded file.

**Session Layer**

Layer 5: The Session layer provides the mechanism for managing the dialogue between end-user application processes. It provides for either duplex or half-duplex operation and establishes checkpointing, adjournment, termination, and restart procedures. This layer is responsible for setting up and tearing down TCP/IP sessions.

**Transport Layer**

Layer 4: The purpose of the Transport layer is to provide transparent transfer of data between end users, thus relieving the upper layers from any concern with providing reliable and cost-effective data transfer. The transport layer controls the reliability of a given link. Some protocols are stateful and connection oriented. This means that the transport layer can keep track of the packets and retransmit those that fail. The best known example of a layer 4 protocol is TCP.

**Network Layer**

Layer 3: The Network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the Transport layer. The Network layer performs network routing, flow control, segmentation/desegmentation, and error control functions. The router operates at this layer – sending data throughout the extended network and making the Internet possible, although there are layer 3 (or IP) switches.

**Data Link Layer**

Layer 2: The Data link layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical layer. The addressing scheme is physical which means that the addresses (MAC) are hard-coded into the network cards at the time of manufacture. The addressing scheme is flat. Note: The best known example of this is Ethernet

**Physical Layer**

Layer 1: The physical layer defines all electrical and physical specifications for devices. This includes the layout of pins, voltages, and cable specifications. Hubs and repeaters are physical-layer devices. The major functions and services performed by the physical layer are:

- Establishment and termination of a connection to a communications medium.
- Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.

- Modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel.

Even though most computer network technologies do not follow strictly to the OSI Model in that they combine several OSI layers functions in one protocol, the OSI Model is still used as a reference and a guideline in network design. Understanding the OSI Model will help you understand how a network works. The OSI Model protocol stack is explained in the following table:

| Layer | Layer Name | Functions | Examples |
|---|---|---|---|
| Layer 7 | Application Layer | application support | HTTP, FTP, Telnet, SMTP, SNMP,POP3, IMAP4 |
| Layer 6 | Presentation Layer | data format conversion, data compression, and encryption | |
| Layer 5 | Session Layer | user identification; establishing, maintaining, and terminating a session | SIP |
| Layer 4 | Transport Layer | end-to-end transport | TCP, UDP, RTP, RTCP |
| Layer 3 | Network Layer | addressing, routing | IP, IPSec, IPX, NetBEUI, AppleTalk, ICMP |
| Layer 2 | Data Link Layer | medium access control, error detection, retransmission | Ethernet, Wi- Fi, HomePNA, HomePlug, PPP, PPTP, L2TP, ATM,Frame Relay, Token Ring, FDDI |
| Layer 1 | Physical Layer | electrical/optical signaling, cabling, connector pin assignment | RF, UTP, STP, coax, fiber optic, connectors, signaling, voltages |

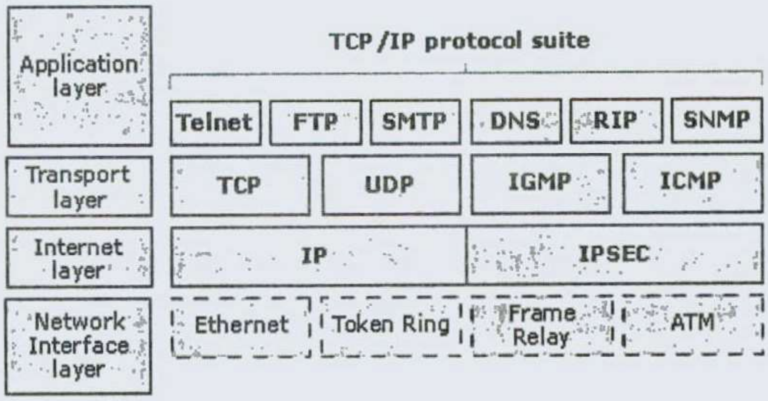
Use to its complex functions, the Data Link Layer is divided into two sublayers, that is Media Access Control (MAC) sublayer and Logical Link Control (LLC) sublayer. MAC sublayer is the lower part, closer to the Physical Layer. MAC sublayer controls access to the physical medium. LLC sublayer is the upper part that interfaces with the Network Layer.

Session Layer, Presentation Layer, and Application Layer are often referred to as Upper Layers. These layers basically handle user connection and data formatting. In most network technologies, such as TCP/IP, the differences between the three layers are blurred and their functions are often handled by one protocol.

Physical Layer, Data Link Layer, Network Layer, and Transport Layer are referred to as Lower Layers. The lower layers generally concern with how data is transported across the network.

## 2.3 The TCP/IP model

TCP/IP is based on a four-layer reference model. All protocols that belong to the TCP/IP protocol suite are located in the top three layers of this model.



As shown in the following illustration, each layer of the TCP/IP model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) reference model proposed by the International Standards Organization (ISO).

The TCP/IP can be thought of consisting of four layers:

- Application Layer (End-user application programs)
- Transport Layer (Communication among programs on a network)
- Network Layer (Communication, addressing, and routing)
- Link Layer (Network hardware and device level)

The TCP/IP does most of the things the OSI model does, except it does it in four layers, and is actually a lot more robust and real than the OSI idea. TCP/IP is setup in such a way that it doesn't really matter which network is used underneath. The Link Layer can use physical wire, wireless, serial lines, etc.

**Note**

The OSI reference model is not specific to TCP/IP. It was developed by the ISO in the late 1970s as a framework for describing all functions required of an open interconnected network. It is a widely known and accepted reference model in the data communications field and is used here only for comparison purposes.

| Layer | Description | Protocols |
|---|---|---|
| Application | Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network. | HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, other application protocols |
| Transport | Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data. | TCP, UDP, RTP |
| Internet | Packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams. | IP, ICMP, ARP, RARP |
| Network interface | Specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire. | Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35 |

## 2.4 A Comparison of the OSI and TCP Reference Models

**Similarities**

- These two, layers are based on the concept of a stack of independent protocols.
- The functionality of the layers is roughly similar.

**Examples**

- In both models the layers up through and including the transport layer are there to provide an end-to-end network independent transport services to processes wishing to communicate. These layers form the transport provider.
- In both models, the layers above transport are application oriented users of the transport service.

Despite these fundamental similarities, the two models also have many differences. In this section we will focus on the key differences between the two reference models. It is important to note that we are comparing the reference models here, not the corresponding protocol stacks. The protocols themselves will be discussed later.

Three concepts are central to the OSI model.

1. Services
2. Interfaces
3. Protocols

The OSI model originally clearly distinguishes between service, interface, and protocol. The service definition tells what the layer does, not how entities above it access it or how the layer works. A layer's interface tells the processes above it how to access it. It specifies what the parameters are and what results to expect. The peer protocols used in a layer are the layer's own business.

The TCP/IP model did not originally clearly distingish between service, interface and protocol, although people have tried to retrofit it after the fact to make it more OSI-like.
As a consequence, the protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes.
The OSI reference model was devised before the protocols were invented. This ordering means that the model was not biased toward one particular set of protocols, which made it quite general.

With the TCP/IP the reverse was true: the protocols came first, and the model was really just a description of the existing protocols. There was no problem with the protocols fitting the model. They fit perfectly. The only trouble was that the model did not fit any other protocol stacks.
The OSI model has seven layers and the TCP/IP has four layers. Both have network, transport and application layers, but the other layers are different.
Another difference is in the area of connectionless versus connection oriented communication. The OSI model support both connectionless and connection oriented communication the network layer, but only connection oriented communication in the transport layer, where it counts.
The TCP/IP model has only one mode in the network layer. (Connectionless) but supports both modes in the transport layer, giving the users a choice. This choice especially important for simple request-response protocols.

## 2.5 Unit Summary

The OSI Reference Model is the basis for communicating over a network, whether it is a local area network, a wide area network, or the internetwork. The OSI model, as it called for short, defines the rules, mechanisms, formats, and protocols used to guide how data flows from one device to another.

The functions of each layer both in OSI and TCP/IP has been discussed and also the similarities and differences are noted.

## 2.6 Keywords

OSI, TCP/IP, MAC, FTP

## 2.7 Exercise

1) Explain the communication procedure between the layers. What different units exist in this communication?
2) Explain various issues in designing of layers in layered reference models and explain term protocol.
3) Explain OSI reference model.
4) Draw TCP/IP model and explain function of each layer.
5) Compare OSI and TCP/IP reference model.

## 2.8 Reference

1. Data and Computer Communication, William Stallings, 8th Edition, Pearson Education, 2007.
2. Computer Networks: A Systems Approach - Larry L. Peterson and Bruce S. David, 4th Edition, Elsevier, 2007.
3. Introduction to Data Communications and Networking – Wayne Tomasi, Pearson Education, 2005.
4. Computer and Communication Networks – Nader F. Mir, Pearson Education, 2007.

# UNIT-3: Example Networks: Arpanet, X.25, Frame Relay, ATM, Ethernet

## Structure

## 3 .0 OBJECTIVES

After studying this unit you will be able to

- Explain Novell Netware predates OSI and is not based on it
- Elucidate Applications of X.25
- State the Structure of Frame Relay

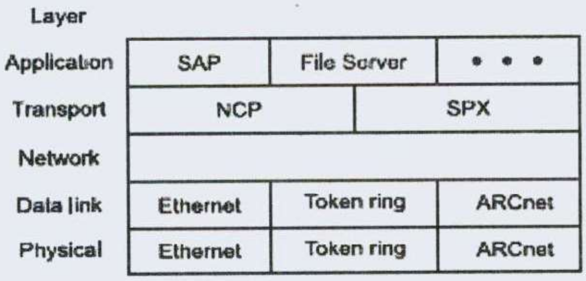
## 3.1 Introduction

The subject of computer networking covers many different kinds of networks, large and small, well known and less well known. They have different goals, scales, and technologies. In the following sections, we will look at some examples, to get an idea of the variety one finds in the area of computer networking. We will start with the Internet, probably the best known network, and look at its history, evolution, and technology. Then we will consider ATM, which is often used within the core of large (telephone) networks.

In the following sections we will look at a few examples. These are the popular commercial LAN networking package, Novell Netware, the Worldwide Internet (including its predecessors, the ARPANET).

## 3.2 Novell Netware

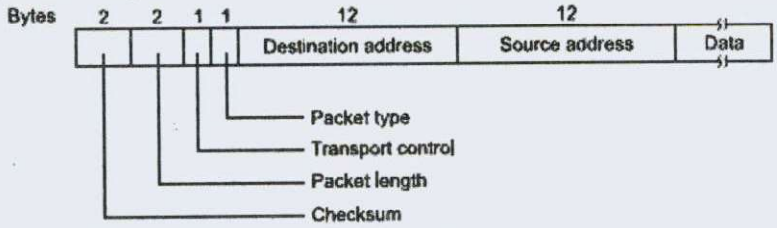
The most popular network system in the PC world is Novel Netware. It was designed to be used by companies downsizing from a mainframe to a network of PCs. In such systems, each user has a desktop PC functioning as a client. In addition, some number of powerful PCs operates as server providing file services, database services, and other services to a collection of clients. In other words, Novell Netware is based on the client-server model. Netware uses a proprietary protocol stack illustrated in figure. It is based on the old Xerox Network System, XNSTM but with various modifications. Novell Netware predates OSI and is not based on it. If anything, it looks more like TCP/IP than like OSI.



| Layer | | | |
|---|---|---|---|
| Application | SAP | File Server | • • • |
| Transport | NCP | SPX | |
| Network | | | |
| Data link | Ethernet | Token ring | ARCnet |
| Physical | Ethernet | Token ring | ARCnet |

The Novell Netware reference model.

The physical and data link layers can be chosen from among various industry standards, including Ethernet, IBM token ring, and ARCnet. The network layer runs an unreliable connectionless internetwork protocol called IPX. It passes packet transparently from source to destination, even if the source and destination are on different networks. IPX is functionally similar to IP, except that it uses 10-byte addresses instead of 4-byte addresses. Above IPX comes a connection-oriented transport protocol called NCP (Network Core Protocol). NCP also provides various other services besides user data transport and is really the heart of Netware. A second protocol, SPX is also available, but provides only transport. TCP is another option. Applications can choose any of them. The file system uses NCP and Lotus Notes® uses SPX, for example. The session and presentation layer do not exist. Various application protocols are present in the application layer.



A Novell Netware IPX packet.

As in TCP/IP, the key to the entire architecture is the internet datagram packet on top of which everything else is built. The format of an IPX packet is shown in above figure. The checksum field is rarely used. Since the underlying data link layer also provides a checksum. The packet length field tells how long the entire packet is, header plus data. The Transport Control field counts how many networks the packet has transferred. When this exceeds a maximum, the packet is discarded. The Packet type field is used to mark various control packets. The two addresses each contain a 32-bit network number, a 48-bit machine number (the 802 LAN address), and 16-bit local address (socket) on that machine. Finally, we have the data, which occupy the rest of the packet, with the maximum size being determined by the underlying network.

About once a minute, each server broadcasts a packet giving its address and telling what services it offers. These broadcasts use, the SAP (Service Advertising Protocol) Protocol. The packets are seen and collected by special agent processes running on the router machines. The agents use the information contained in them to construct database of which servers are running where.

When a client machine is booted, it broadcasts a request asking where the nearest server is. The agent on the local router machine sees this request, looks in its database of servers and matches up the request with the best server. The choice of server to use is then sent back to the client. The client can now establish on NCP connection with the server. Using this connection, the client and server negotiate the maximum packet size. From this point on, the client can access the file system and other services using this connection. It can also query the server's database to look for other (more distant) servers.

## 3.3 The ARPANET

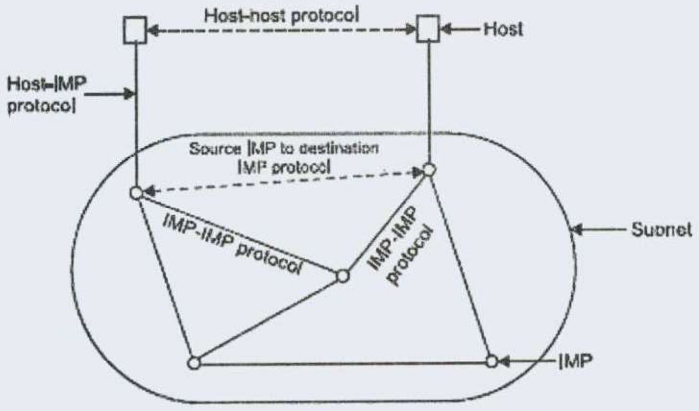
Let us now switch gears from LANs and WANs. In the mid-1960s, at the height of the cold war, the DOD wanted and control network that could service a nuclear war. Traditional Circuit-Switches telephone networks were considered too vulnerable since the loss of one line or switch would certainly terminate all conversations using them and might even partition the network. To solve this problem, DOD turned to its research arm, ARPA (later DARPA, now ARPA again), the (Periodically Defense) Advanced Research Project Agency.

ARPA was created in response to the Soviet Union's launching Sputnik in 1957 and had the mission of advancing technology that might be useful to the military. ARPA had no scientists or laboratories, in fact, it had nothing more than an office and a small (by Pentagon standard) budget. It did its work by issuing grants and contracts to universities and companies whose ideas looked promising to it.

Several early grants went to universities for investigating the then-radical idea of packet switching, something that had been suggested by Paul Baran in a series of RAND Corporation reports published in the early 1960s. After some discussions with various experts, ARPA decided that the network the DOD needed should be a packet-switched network, consisting of a subnet and host computers.

The subnet would consists of minicomputers called IMPs (Interface Message Processors) connected by transmission lines. For high reliability, each IMP would be connected to at least two other IMP. The subnet was to be a datagram subnet, so if some lines and IMPs were destroyed, messages could be automatically rerouted along alternative paths. Each node of the network was to consist of an IMP and a host, in the same room, connected by a short wire. A host could send message of up to 8063 bits to its IMP, which would then break these up into packets of at most 1008 bits and forward them independently towards the destination. Each packet was the first electronic store-and-forward packet switching network. (received in its entirety before being forwarded, so the subject was).

ARPA then put out a tender for building the subnet. Twelve companies bid for it. After evaluating all the proposals, ARPA selected BBN, a consulting firm in Cambridge, Massachusetts, and in December 1968, awarded it a contract to build the subnet and write the subnet software. BBN chose to use specially modified Honeywell DDP-316 minicomputers with 12k 16-bit words of core memory as the IMPs. The IMPs did not have disks, since moving parts were considered unreliable. The IMPs were interconnected by 56-kbps lines leased from telephone companies. The software was split into two parts : subnet and host. The subnet software consisted of the IMP end of the host-IMP connection, the IMP-IMP protocol, and a source IMP to destination IMP protocol designed to improve reliability. The original ARPANET design is shown in Figure.



**The original ARPANET design.**

Outside the subnet, software was also needed namely, the host end of the host-IMP connection, the host-host protocol, and the application software. It soon became clear that BBN felt that when it have accepted a message on a host-IMP wire and placed it on the host- IMP wire at the destinations, its job was done.

## 3.4 X.25

X.25 is a standard suite of protocols used for packet switching across computer networks. The X.25 protocols works at the physical, data link, and network layers (Layers 1 to 3) of the OSI model. Each X.25 packets contains up to 128 bytes of data. The X.25 network handles packet assembly at the source device, delivery, and then disassembly at the destination. X.25 packet delivery technology includes not only switching and network-layer routing, but also error checking and re-transmission logic should delivery failures occur. X.25 supports multiple simultaneous conversations by multiplexing packets and using virtual communication channels.

X.25 was originally designed more than 25 years ago to carry voice over analog telephone lines (dialup networks). Typical applications of X.25 today include automatic teller machine networks and credit card verification networks. X.25 also supports a variety of mainframe terminal/server applications.

With the widespread acceptance of Internet Protocol (IP) as a standard for corporate networks, many X.25 applications are now being migrated to cheaper solutions using IP as the network layer protocol and replacing the lower layers of X.25 with Ethernet or ATM hardware.

## 3.5 Frame Relay

Frame Relay is a protocol standard for LAN internetworking which provides a fast and efficient method of transmitting information from a user device to LAN bridges and routers.

The Frame Relay protocol uses a frame structured similar to that of LAPD, except that the frame header is replaced by a 2-byte Frame Relay header field. The Frame Relay header contains the user-specified DLCI field, which is the destination address of the frame. It also contains congestion and status signals which the network sends to the user.

**Virtual Circuits**

The Frame Relay frame is transmitted to its destination by way of virtual circuits (logical paths from an originating point in the network) to a destination point. Virtual circuits may be permanent (PVCs) or switched (SVCs). PVCs are set up administratively by the network manager for a dedicated point-to-point connection; SVCs are set up on a call-by-call basis.

Advantages of Frame Relay

Frame Relay offers an attractive alternative to both dedicated lines and X.25 networks for connecting LANs to bridges and routers. The success of the Frame Relay protocol is based on the following two underlying factors:

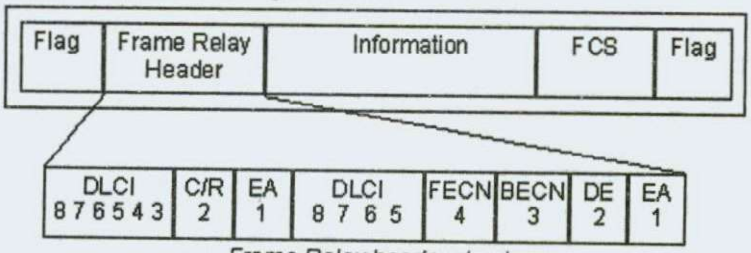
- Because virtual circuits consume bandwidth only when they transport data, many virtual circuits can exist simultaneously across a given transmission line. In addition, each device can use more of the bandwidth as necessary, and thus operate at higher speeds.
- The improved reliability of communication lines and increased error-handling sophistication at end stations allows the Frame Relay protocol to discard erroneous frames and thus eliminate time-consuming error-handling processing.

These two factors make Frame Relay a desirable choice for data transmission; however, they also necessitate testing to determine that the system works properly and that data is not lost.

**Frame Relay Structure**

Standards for the Frame Relay protocol have been developed by ANSI and CCITT simultaneously. The separate LMI specification has basically been incorporated into the ANSI specification. The following discussion of the protocol structure includes the major points from these specifications.

The Frame Relay frame structure is based on the LAPD protocol. In the Frame Relay structure, the frame header is altered slightly to contain the Data Link Connection Identifier (DLCI) and congestion bits, in place of the normal address and control fields. This new Frame Relay header is 2 bytes in length and has the following format:



*Frame Relay header structure*

**DLCI:** 10-bit DLCI field represents the address of the frame and corresponds to a PVC.

**C/R:** Designates whether the frame is a command or response.

**EA:** Extended Address field signifies up to two additional bytes in the Frame Relay header, thus greatly expanding the number of possible addresses.

**FECN:** Forward Explicit Congestion Notification (see ECN below).

**BECN:** Backward Explicit Congestion Notification (see ECN below).

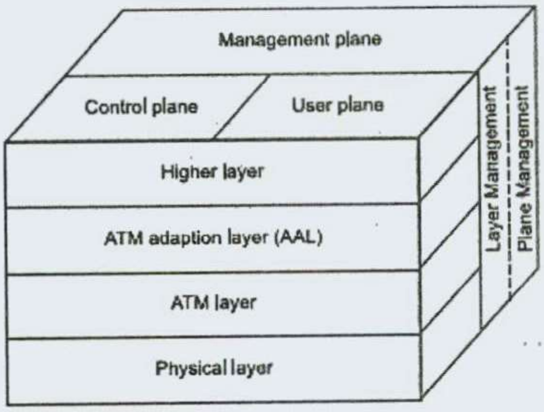
**DE:** Discard Eligibility (see DE below).

**Information:** The Information field may include other protocols within it, such as an X.25, IP or SDLC (SNA) packet.

## 3.6 ATM

Asynchronous transfer mode (ATM), also known as cell relay, is in some ways similar to packet switching using X.25 and frame relay. Like packet switching and frame relay, ATM involves the transfer of data in discrete chunks. Also, like packet switching and frame relay, ATM allows multiple logical connections to be multiplexed over a single physical interface. In the case of ATM, the information flow on each logical connection is organized into fixed-size packets, called cells.

ATM is a streamlined protocol with minimal error and flow control capabilities, this reduces the overhead of processing ATM cells and reduces the number of overhead bits required with each cell, thus enabling ATM to operate at high data rates. Further, the use of fixed-size cells simplifies the processing required at each ATM node, again supporting the use of ATM at high data rates.



ATM Protocol reference model.

The standards issued for ATM by ITU-T are based on the protocol architecture shown in the above figure, which illustrate the basic architecture for an interface between user and network. The physical layer involves the specification of a transmission medium and a signal encoding scheme. The data rates specified at the physical layer include 155.52 Mbps and 622.08 Mbps. Other data rates, both higher and lower, are possible.

Two layers of the protocol architecture related to ATM functions. There is an ATM layer common to all services that provide packet transfer capabilities, and an ATM adaptation layer (AAL) that is service dependent. The ATM layer defines the transmission of data in fixed-size cells and also defines the use of logical connections. The use of ATM creates the need for an adaptation layer to support information transfer protocols not based on ATM. The AAL maps higher-layer information into ATM cells to be transported over an ATM network, then collects information from ATM cells for delivery to higher layers.

The protocol reference model makes reference to three separate planes.

- User Plane: Provides for user information transfer along with associated controls. (e.g. flow control, error control).
- Control Plane: Performs call control and connection control functions.

- Management Plane: Includes plane management, which performs management functions related to a system as a whole and provides coordination between all the planes, and layer management, which perform management functions relating to resources and parameters residing in its protocol entities.

## 3.7 Ethernet

Ethernet is the most widely-installed local area network ( LAN) technology. Specified in a standard, IEEE 802.3, Ethernet was originally developed by Xerox from an earlier specification called Alohanet (for the Palo Alto Research Center Aloha network) and then developed further by Xerox, DEC, and Intel. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Ethernet is also used in wireless LANs. The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps. Devices are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.

Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems, supporting workstations with 10BASE-T cards. Gigabit Ethernet provides an even higher level of backbone support at 1000 megabits per second (1 gigabit or 1 billion bits per second). 10-Gigabit Ethernet provides up to 10 billion bits per second.
Ethernet was named by Robert Metcalfe, one of its developers, for the passive substance called "luminiferous (light-transmitting) ether" that was once thought to pervade the universe, carrying light throughout. Ethernet was so- named to describe the way that cabling, also a passive medium, could similarly carry data everywhere throughout the network

## 3.8 Unit Summary

The main proponents of the connectionless subnets come from the ARPANET/Internet community. Remember that original desire infunding and building the ARPANET was to have a network that would continue functioning even after multiple direct hits by nuclear weapons wiped out numerous routers and transmission lines. Thus, fault tolerance was high on their priority list; billing customers was not. This approach led to a connectionless design in which every packet is routed independently of every other packet. As a consequence, if some routers go down during a session, no harm is done as long as the system can reconfigure itself dynamically so that subsequent packets can find some route to the destination, even if it is different from that which previous packets used.
Frame Relay provides some basic quality of service and congestion-avoidance features, but these are rather lightweight compared to X.25 and ATM. The Frame Relay packet format provides a good example of a packet used for virtual circuit switching.

## 3.9 Keywords

Arpanet, X.25, Frame Relay, ATM, Ethernet

## 3.10 Exercise

1. Explain with neat diagram ATM protocol reference model with its planes
2. Discuss the Frame relay protocol structure
3. What is ARPANET? How does it works

## 3.11 Reference

1. Computer and Communication Networks – Nader F. Mir, Pearson Education, 2007.
2. Communication Networks: Fundamental Concepts and Key Architectures - Alberto Leon, Garcia and Indra Widjaja, 3rd Edition, Tata McGraw- Hill, 2004.
3. Introduction to Data Communications and Networking – Wayne Tomasi, Pearson Education, 2005.

# UNIT-4: Network Standardization

## Structure

## 4.0 OBJECTIVES

After studying this unit you will be able to

- Explain The standards allow the computers to communicate with each others.
- Elucidate the Increases the market for the products that adhere to the standards.
- Facilitate the users by providing standardized communications.

## 4.1 Introduction

Computer networking is a great way of connecting the computers and sharing data with each other. There are many vendors that produce different hardware devices and software applications and without coordination among them there can be chaos, unmanaged communication and disturbance can be faced by the users. There should be some rules and regulations that all the vendors should adopt and produce the devices based on those communication standards.

The network standards are the open standards that are administered the standards organizations. ISO is a voluntary organization that was founded in 1946. ISO makes the standards for the network communications and other computing and mobile technologies. There is another organization known Institute of Electrical and Electronics Engineers (IEEE). IEEE mostly makes the standards for the electrical interfaces.

## 4.2 IEEE 802 Standards

Immediately after somebody invented networking by connecting two computers together to share files and send secret messages, it was apparent that it was a good thing. As local area networks (LANs) began to spread, it was obvious that if networks hoped to grow large or began to communicate with one another, some standards would be needed. To this end, the Institute for Electric and Electronic Engineering (IEEE), a well–known and highly respected organization, started a project in February, 1980, to create a set of standards for LAN architectures, cabling, and data transmission formats. The date that this project started is important because it formed the name of the project (the 802 project) and the resulting standards developed (IEEE 802) by it. The 802 projects goal was to define the Data Link layer, including the logical link control (LLC) and media access control (MAC) sub layers (these are each discussed more fully later in this chapter) and beyond. To date, the 802 project and its 12–plus subcommittees have produced a variety of networking standards. Those defining the Data Link layer are listed in Table below. The 802–dot number of each standard represents the number of the subcommittee assigned to develop and define each area. For example, the 802.3 standard is assigned to the 802.3 subcommittee.

| Subcommittee | Subject | Description |
|---|---|---|
| 802.1 | Internetworking/ LAN Protocols | Defines routing, bridging, and internetwork communications |
| 802.2 | Logical Link Control (LLC) | Allows Network layer protocols to link to Physical layer and MAC sublayer rotocols |
| 802.3 | Ethernet | The Ethernet standard; defines CSMA/CD |
| 802.5 | Token Ring | Defines logical ring topology, media, and interfaces |
| 802.12 | High–speed networks | Defines 100 Mbps technologies |

**Ethernet and the mighty 802.3**

The IEEE 802.3 is the standard that defines the Ethernet, by far the networking standard of choice. The 802.3 standard defines the bus topology, the network media (10BaseX), and the functions of an Ethernet network, as well as defining the tools used on the MAC sublayer of the Data Link layer; primary of these in the Ethernet world is the CSMA/CD access method.

**The sublayers of the Data Link layer**

Remember The Data Link layer is divided into two sublayers by the 802 standards: the Logical Link Control (LLC) and Media Access Control (MAC) sublayers. The LLC sublayer is defined in 802.1 and 802.2. The MAC sublayer is defined in the 802.1, 802.3, 802.5, and 802.12. Be sure you know the general subject of each of these standards.

**Connecting on the LLC sublayer**

The LLC (Logical Link Control) layer creates connections between networked devices. If you want to send data from your workstation client to a server on the same network segment, its the LLC that creates and manages the connection required to transmit your data.

Remember conceptually, the LLC sublayer sits on top of the MAC sublayer. Its defined by the 802.2 standard to be topology independent. The LLC functions include

- Managing frames to upper and lower layers
- Error control
- Flow control

The LLC works with the transport layer by providing connection–oriented and connectionless services. It manages and creates the communication link.

The LLC sublayer transfers data in two ways:

**Connectionless services:** Messages are not acknowledged by the receiving device, which speeds up the processing. Although it sounds unreliable, this type of transfer is commonly used at this level because the upper OSI layers implement their own error–checking and control.

**Connection–oriented services:** Because each message is acknowledged, this service is much slower than connectionless services, but its much more reliable.

### Going with the flow control

Remember another communications control defined on the LLC sublayer is flow control. Flow control meters the flow of data between network devices that may not be running at the same speeds. Please don't think that flow control occurs on the Data Link layer. The Transport layer of the OSI model actually manages the mechanisms used to control the flow of data between two hosts. The Data Link layer defines the data values used in the flow control signaling between two transmitting hosts.

In situations where one communicating device is sending information at either a faster or a slower rate than the other device, some form of control is necessary to meter the flow of data between the devices to avoid a loss of data. Flow control prevents the slower device from being swamped, and, more importantly, prevents data from being lost or garbled. It works by pausing the faster device to enable the slower device to catch up.

Remember there are two types of flow control implemented in data communications software and hardware. Software flow control, common to networking, involves a process called XON/XOFF, which roughly stands for transmission on/transmission off. This process involves the sending device continuing to send data until the receiving device signals (by sending a control character) that transmissions need to stop until the receiving device can catch up. When the receiving device is ready to go, it sends another control signal for the sending device to begin the data flow again.

Hardware flow control, also called RTS/CTS (Ready to Send/Clear to Send), uses two wires in a cable, one for RTS and one for CTS. The sending device uses the RTS signal to indicate when its ready to send. The receiving device uses the CTS to indicate its ready to receive. When either is turned off, the flow is interrupted.

### Detecting errors in the flow

Remember another function of the Data Link layer is error detection. Error detection is the process of detecting whether errors occurred during the transmission of the bits across the wire. The Data Link layer uses a calculated value called the CRC (Cyclic Redundancy Check) thats placed into the Data Link trailer that's added to the message frame before its sent to the Physical layer. The receiving computer recalculates the CRC and compares it to the one sent with the data. If the two values are equal, its assumed that the data arrived without errors. Otherwise, the message frame may need to be retransmitted under control of an upper layer. Although the Data Link layer implements error detection, it does not include a function to perform error recovery. This is left for the upper layers to deal with, primarily on the Transport layer.

## 4.3 Communicating on the MAC sublayer

The MAC sublayer of the Data Link layer provides a range of network services, including controlling which network device has access to the network and providing for physical addressing.

Remember The MAC sublayer carries the physical address of each device on the network. This address is more commonly called a devices MAC address. The MAC address is a 48–bit address that's encoded on each network device by its manufacturer. This works on the same principle that each domicile on your street has a unique address assigned to it by the Postal Service. It's the MAC address that the Physical layer uses to move data between nodes of the network.

A MAC address is made up of two parts: the manufacturers ID number and a unique serialized number assigned to the device by its manufacturer. The 48–bits (6 bytes) of the MAC address are divided evenly between these two numbers. The first three bytes of the MAC address contain a hexadecimal manufacturer code that has been assigned by the IEEE. For example, Ciscos IEEE MAC ID is 00 00 0C (each byte holds two half–byte hexadecimal values), Intel's is 00 55 00, and IBMs is 08 00 5A. The remaining three bytes contain a hexadecimal number assigned by the manufacturer that's unique to each piece of equipment.

Just as you need to know someone's telephone number to call them, computers must know each other's addresses to communicate. Depending on the protocol in use, various addressing schemes are used. For the exam, you should be aware of TCP/IP and IPX addressing schemes.

In a workstation, the MAC address is usually burned into the NIC card. On a router, each port has its own MAC physical address. Theoretically, no two devices ever have the same MAC address. Although, we have heard of instances where this has occurred in a network with very unpleasant circumstances resulting.

Hardware (MAC) addresses are used to get data from one local device to another. However, not all network operating systems (NOS) use the physical address to reference network nodes. This sets up the conflict between the network (logical) address and the MAC (physical) addresses.

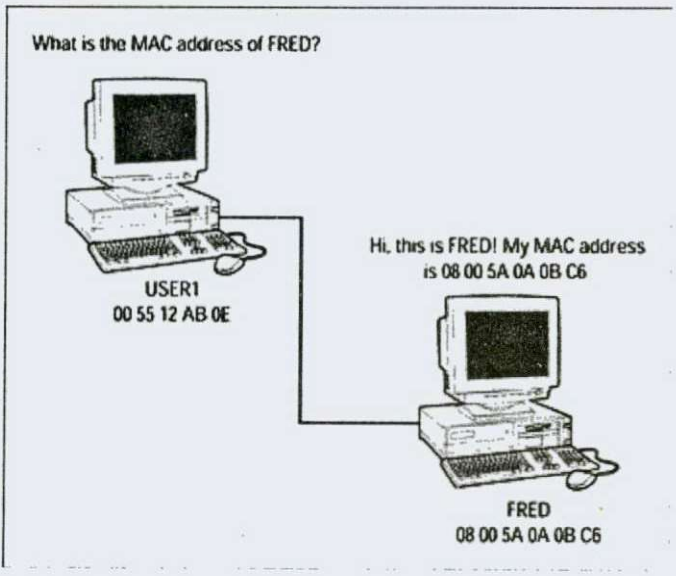
Network operating systems assign a logical network name to each networked device, such as ACCTG_SERVER, NT1, or FRED, to make it easy for its human users to reference its resources. On the other hand, references on the network itself, that is those on Layer 1 (Physical layer), use the physical addresses provided by the Data Link layer to reference the actual devices on the network. When you request services from the file server FRED, a service like DNS (Domain Naming System) or WINS (Windows Internet Name Service) is used to translate or resolve the node name FRED into its logical address, which is typically an IP address. In some cases, a HOSTS or LMHOSTS file may be used instead to resolve the node name to its logical address. The Data Link layer activities then resolve the logical address into its corresponding MAC address. To resolve between these two addresses involves a process called (what else?) address resolution, which associates logical network addresses to physical MAC addresses, and vice versa.

Remember the protocol for this service is ARP (Address Resolution Protocol). ARP maintains a small database in memory, called the ARP cache that cross–references physical and logical addresses. When a device wants to communicate with a local device, it checks its ARP cache to determine whether it has that devices MAC address. If it doesn't, it sends out an ARP broadcast request, as shown in Figure, to all devices on the local network. Each device examines the message to see whether the request is intended for it. If it is, the device responds with its MAC address, which is stored in the sending devices, ARP cache. In the example shown in Figure, USER1 wants to communicate with FRED, a file server. However, USER1 doesn't have a MAC address in its ARP cache for FRED, so it sends out a broadcast message that asks FRED to respond with its MAC address, which FRED does.

When a workstation or server needs to communicate with a device remote to the local network, essentially the same process takes place with the exception that a router through which the remote device is accessed will likely respond with its MAC address and not that of the device itself.

**Controlling access to the network**

The primary media access control mechanism defined in 802.3 for use in the Data Link layer is CSMA/CD (Carrier Sense Multiple Access/Collision Detection) access method. CSMA/CD is the method used in Ethernet networks for controlling access to the physical media by network nodes. As its name infers, CSMA/CD (say it ten times fast to lock it away in your brain!) tries to keep network devices from interfering with each others communications by detecting access attempts by multiple devices. When sneaky devices avoid detection, and they do, CSMA/CD detects and deals with the collision that undoubtedly occurs.


What is the MAC address of FRED?
Hi, this is FRED! My MAC address is 08 00 5A 0A 0B C6
USER1
00 55 12 AB 0E
FRED
08 00 5A 0A 0B C6

**Avoiding collisions**

To avoid collisions, CSMA/CD devices listenor sense signals on the network backbone before sending a message over the network. If the network is quiet, meaning its not in use, the device can send a message. Otherwise, the device waits until the network isnt in use. However, if between the times a device decides the network is available and the time it actually transmits its message, another device sends a message, the two messages may collide on the network. When this happens, the device that detected the collision sends out an alert to all network devices that a collision has occurred. All devices quit transmitting for a random amount of time to clear the line.

Remember The CSMA/CD process can be described as follows:

1. Listen to see whether the wire is being used.
2. If the wire is busy, wait.
3. If the wire is quiet, send.
4. If a collision occurs while sending, stop, wait a specific amount of time, and send again.

When a collision is detected by a sending device, it sends out a jamming signal that lasts long enough for all nodes to recognize it and stop broadcasting. Then each device waits a random amount of time to begin the CSMA/CD process again. This amount of time is determined by a back–off algorithm that calculates the amount of time the device should wait before resuming its attempts to transmit.

**Working on a busy intersection**

A collision domain is a network segment in which all devices share the same bandwidth. The more devices you have on a segment, the more likely that youll experience collisions. With too many devices on a segment network, performance is considerably less than optimal. Increasing bandwidth is one way to deal with the problem, but a better way to deal with this problem is by using the available bandwidth more efficiently.

**Segmenting a Network for Fun and Profit**

Dividing a network into smaller parts, known as segments, decreases congestion and chances of message collision on each new segment. Yes, each new segment forms a new collision domain, but that doesn't mean it becomes a problem very quickly (not if the network is segmented properly). Devices within a segment share the same bandwidth. Data passed outside a segment contends with the next higher segment on the network or perhaps enters the network backbone, both of which are collision domains themselves.

Instant Answer Dividing up a LAN into smaller collision domains (segments) is called segmentation. Count on seeing this concept on the exam.When you segment a network, you increase the number of smaller collision domains.

**Reaping the benefits of segmentation**

Time–Saver For the exam, you need to recognize the following as the general benefits of LAN segmentation:

- Increased bandwidth per user
- Keeping local traffic local
- Reduced broadcasts
- Decreased collisions

**Bridging the difference**

Remember a Bridge, which is a Layer 2 device, is used to break larger network segments into smaller network segments. It works much like a repeater (see Chapter 3), but because a bridge works solely with Layer 2 protocols and and Layer 2 MAC sublayer addresses, it operates at the Data Link layer.

## 4.4 The MAC Bridge

No, McDonalds is not in the networking business now. Bridges are commonly referred to as MAC layer bridges because they operate on the MAC sublayer of the Data Link layer. As I discussed earlier in this chapter (see Communicating on the MAC sublayer), each network device has a unique identification number (MAC address) that identifies it on the MAC layer. A bridge uses the MAC address to perform its tasks, including:

- Monitoring network traffic
- Identifying the destination and source addresses of a message
- Creating a routing table that identifies MAC addresses to the network segment on which they relocated

- Sending messages to only the network segment on which its destination MAC address is located

**The bridge routing table**

A bridge builds up its routing table by cataloging the network nodes that send out messages. A bridge examines the MAC address of a messages source or sending node. If this address is new to the bridge, it adds it to the routing table along with the network segment from which it originated. The bridges routing

Table is stored in its RAM and just like a PCs RAM, it is dynamic when the power goes off, it goes away. When the power is restored, the bridge rebuilds the table. Because most network nodes send and receive packets continuously, it doesn't take long to completely rebuild the routing table.

**Bridging over troubled waters**

Remember the two devices you need to be concerned with for the exam are bridge and switch. Switches and LAN switching is a major portion of the exam. I cover them in depth in Chapter 16. Bridges, on the other hand, dont play as large a role on the exam, but theyre important Layer 2 devices. Its important that you know that a bridge is the primary networking device used to create new segments on a LAN.

One problem that can arise on a bridged and switched network is caused by the lack of a time to live value (such as that used in Layer 3 protocols) assigned to Layer 2 messages. Because a Data Link frame can effectively live forever, its possible that a packet addressed to an unknown MAC address may bounce around the network indefinitely. This condition can be avoided by allowing only a single path to be active between two segments at a time by using the Spanning Tree Protocol.

**Spanning the tree protocols**

The Spanning Tree protocol designates each interface on a bridge to be either in Forwarding or Blocking State. When an interface is in Blocking State, only special packets reporting the status of other bridges on the network are allowed through. All other packets are blocked. As you can probably guess, an interface in Forwarding State allows all packets to be received and forwarded. The state of a bridges interfaces are affected whenever a path on the network goes down and the bridges negotiate a new path, changing interface states from Blocking to Forwarding, as needed.

Instant Answer The normal forwarding mode for a bridge is called store and forward. A store and forward bridge receives (stores) and examines an entire frame before forwarding it to the appropriate interface. The time it takes to examine each frame increases the latency (delay) in the network. Latency is the delay introduced by network devices, such as a bridge, switch, or router, as they process packets. Store and forward bridges create a variable amount of latency because they read in the entire frame, which are variable in length, before examining the frame and passing it on.

## 4.5 Unit Summary

The broadband wireless access industry, which provides high-rate network connections to stationary sites, has matured to the point at which it now has a standard for second - generation wireless metropolitan area networks. PC users may connect to the Internet via a physical cable connection, or they can connect wirelessly, without the need for cables or lines.

Such wireless connections require certain standards or regulations in order to be properly established. The IEEE Standard of Information technology set these protocols.

## 4.6 Keywords

CSMA/CD, Ethernet, Token Ring, LLC, Bridge

## 4.7 Exercise

1. Explain 802 standard.
2. What are different types of cabling for 802.3.
3. Explain MAC sublayer and protocol of 802.3.
4. Explain frame format of 802.3.
5. Explain token bus MAC sublayer protocol.

## 4.8 Reference

1. Data Communications and Networking, 4Fd (McGraw-Hill Forouzan Networking) Behrouz A. Forouzan
2. Communication Networks: Fundamental Concepts and Key Architectures - Alberto Leon, Garcia and Indra Widjaja, 3rd Edition, Tata McGraw- Hill, 2004.
3. Computer and Communication Networks – Nader F. Mir, Pearson Education, 2007.

# UNIT-5: ANALOG AND DIGITAL SIGNALS

## Structure

## 5.0 OBJECTIVES

After studying this unit you will be able to

- Explain the Digital signals use a stream of digital data
- Elucidate Few of the information bearing signals
- Explain the Difference between analog and digital signals
- State the Attenuation Signals loose power in time.

## 5.1 Introduction

An analog or analogue signal is any continuous signal for which the time varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal. Any information may be conveyed by an analog signal; often such a signal is a measured response to changes in physical phenomena, such as sound, light, temperature, position, or pressure, and is achieved using a transducer.

In computer architecture and other digital systems, a waveform that switches between two voltage levels representing the two states of a Boolean value (0 and 1) is referred to as a digital signal

### ANALOG TRANSMISSION

Analog transmission is a transmission method of conveying voice, data, image, signal or video information using a continuous signal which varies in amplitude, phase, or some other property in proportion to that of a variable. It could be the transfer of an analog source signal using an analog modulation method such as FM or AM, or no modulation at all.

## 5.2 DIGITAL TO ANALOG CONVERSION

### 1. AMPLITUDE SHIFT KEYING

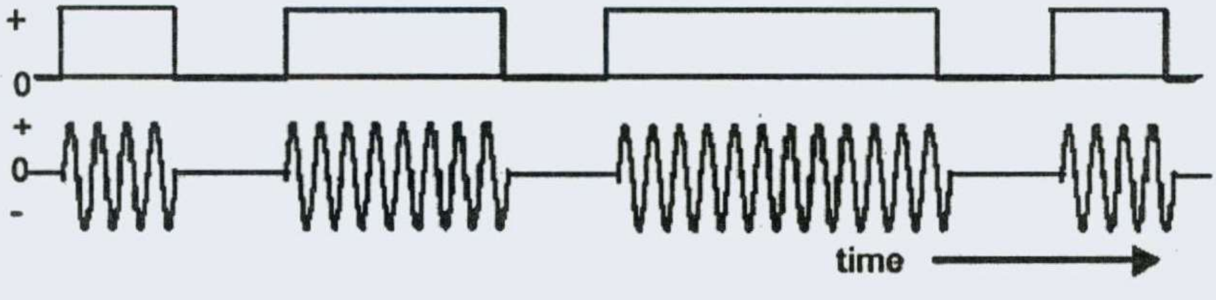
Amplitude Shift Keying (ASK) is the digital modulation technique. In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes. In ASK, the amplitude of the carrier assumes one of the two amplitudes dependent on the logic states of the input bit stream. This modulated signal can be expressed

$$x_c(t) = \begin{cases} 0 & \text{symbol "0"} \\ A\cos\omega_c t & \text{symbol "1"} \end{cases}$$

as:

**Note that the modulated signal is still an on-off signal.**

Amplitude shift keying (ASK) in the context of digital signal communications is a modulation process, which imparts to a sinusoid two or more discrete amplitude levels. These are related to the number of levels adopted by the digital message. For a binary message sequence there are two levels, one of which is typically zero. Thus the modulated waveform consists of bursts of a sinusoid. Figure 1 illustrates a binary ASK signal (lower), together with the binary sequence which initiated it (upper). Neither signal has been band limited.



**ASK signal (below) and the message (above)**

There are sharp discontinuities shown at the transition points. These result in the signal having an unnecessarily wide bandwidth. Band limiting is generally introduced before transmission, in which case these discontinuities would be 'rounded off'. The band limiting may be applied to the digital message, or the modulated signal itself. The data rate is often made a sub-multiple of the carrier frequency. This has been done in the waveform of Fig.

One of the disadvantages of ASK, compared with FSK and PSK, for example, is that it has not got a constant envelope. This makes its processing (eg, power amplification) more difficult, since linearity becomes an important factor. However, it does make for ease of demodulation with an envelope detector.With bandlimiting of the transmitted ASK neither of these demodulation methods (envelope detection or synchronous demodulation) would recover the original binary sequence; instead, their outputs would be a bandlimited side. Thus further processing by some sort of decision-making circuitry for example – would be necessary.

**Thus ASK demodulation is a two-stage process:**

- recovery of the bandlimited bit stream
- regeneration of the binary bit stream.

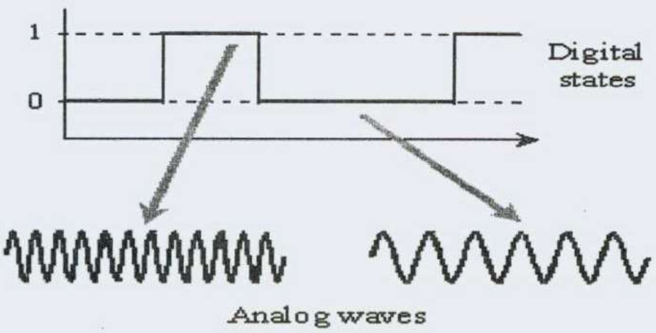
**Application of ASK:**

- Amplitude-shift keying is used extensively for commercial terrestrial
- It is usefulness for satellite applications is limited.
- Space systems typically employ saturated power amplifiers.

When an amplitude-shifted keying signal is passed through such a nonlinear amplifier, sidelobes can grow large enough to interfere with the adjacent signals. As a result, the amount of bandwidth or power needed for signal transmission increases.

## 2. FREQUENCY SHIFT KEYING

Frequency-shift keying (FSK) is a method of transmitting digital signals. The twobinary states, logic 0 (low) and 1 (high), are each represented by an analog wave form. Logic 0 is represented by a wave at a specific frequency, and logic 1 is represented by a wave at a different frequency. A modem converts the binary data from a computer to FSK for transmission over telephone lines, cables, optical fiber, or wireless media. The modem also converts incoming FSK signals to digital low and high states, which the computer can "understand."

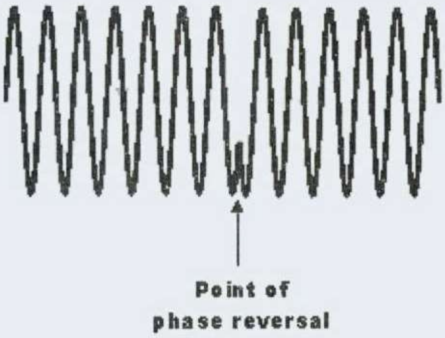


The FSK mode was introduced for use with mechanical teleprinters in the mid-1900s. The standard speed of those machines was 45 baud, equivalent to about 45 bits per second. When personal computers became common and networks came into being, this signaling speed was tedious. Transmission of large text documents and programs took hours; image transfer was unknown. During the 1970s, engineers began to develop modems that ran at faster speeds, and the quest for ever-greater bandwidth has continued ever since. Today, a standard telephone modem operates at thousands of bits per second. Cable and wireless modems work at more than 1,000,000 bps (one megabit per second or 1 Mbps), and optical fiber modems function at many Mbps.

### 3. PHASE SHIFT KEYING

Phase shift keying, PSK, is widely used these days within a whole raft of radio communications systems. It is particularly well suited to the growing area of data communications. PSK, phase shift keying enables data to be carried on a radio communications signal in a more efficient manner than Frequency Shift Keying, FSK, and some other forms of modulation.

Phase Shift Keying, PSK, basics like any form of shift keying; there are defined states or points that are used for signalling the data bits. The basic form of binary phase shift keying is known as Binary Phase Shift Keying (BPSK) or it is occasionally called Phase Reversal Keying (PRK). A digital signal alternating between +1 and -1 (or 1 and 0) will create phase reversals, i.e. 180 degree phase shifts as the data shifts state.



**Binary phase shift keying, BPSK**

The problem with phase shift keying is that the receiver cannot know the exact phase of the transmitted signal to determine whether it is in a mark or space condition. This would not be possible even if the transmitter and receiver clocks were accurately linked because the path length would determine the exact phase of the received signal. To overcome this problem PSK systems use a differential method for encoding the data onto the carrier. This is accomplished, for example, by making a change in phase equal to a one, and no phase change equal to a zero. Further improvements can be made upon this basic system and a number of other types of phase shift keying have been developed. One simple improvement can be made by making a change in phase by 90 degrees in one direction for a one, and 90 degrees the other way for a zero. This retains the 180 degree phase reversal between one and zero states, but gives a distinct change for a zero. In a basic system not using this process it may be possible to loose synchronisation if a long series of zeros are sent. This is because the phase will not change state for this occurrence.

There are many variations on the basic idea of phase shift keying. Each one has its own advantages and disadvantages enabling system designers to choose the one most applicable for any given circumstances. Other common forms include QPSK (Quadrature phase shift keying) where four phase states are used, each at 90 degrees to the other, 8-PSK where there are eight states and so forth.

## 5.3 ANALOG TO ANALOG CONVERSION

### 1. AMPLITUDE MODULATION

Amplitude modulation (AM) is a method of impressing data onto an alternating-current (AC) carrier waveform.The highest frequency of the modulating data is normally less than 10 percent of the carrier frequency.The instantaneous amplitude(overall signal power) varies depending on the instantaneous amplitude of the modulating data.

In AM, the carrier itself does not fluctuate in amplitude. Instead,the modulating data appears in the form of signal components at frequencies slightly higher and lower than that of the carrier. These components are called***sidebands***.The lower sideband (LSB) appears at frequencies below the carrier frequency; the upper sideband (USB) appears at frequencies above the carrier frequency.The LSB and USB are essentially "mirror images" of each other in a graph of signal amplitude versus frequency, as shown in the illustration.The sideband power accounts for the variations in the overall amplitude of the signal.

When a carrier is amplitude-modulated with a pure sine wave, up to 1/3 (33percent) of the overall signal power is contained in the sidebands.The other 2/3 of the signal power is contained in the carrier, which does not contribute to the transfer of data.With a complex modulating signal such as voice, video, or music, the sidebands generally contain 20 to 25 percent of the overall signal power; thus the carrier consumes75 to 80 percent of the power.This makes AM an inefficient mode.If an attempt is made to increase the modulating data input amplitude beyond these limits, the signal will become distorted, and will occupy a much greater bandwidth than it should.This is called ***overmodulation***, and can result in interference to signals on nearby frequencies.

## 2. FREQUENCY MODULATION

Frequency modulation (FM) is a method of impressing data onto an alternating-current (AC) wave by varying the instantaneous frequency of the wave. This scheme can be used with analog or digital data.
In analog FM, the frequency of the AC signal wave, also called the *carrier*, varies in a continuous manner. Thus, there are infinitely many possible carrier frequencies. In *narrowband FM*, commonly used in two-way wirelesscommunications, the instantaneous carrier frequency varies by up to 5 kilohertz (kHz, where 1 kHz = 1000 hertz or alternating cycles per second) above and below the frequency of the carrier with no modulation. In *wideband FM*, used in wireless broadcasting, the instantaneous frequency varies by up to several megahertz (MHz, where 1 MHz = 1,000,000 Hz). When the instantaneous input wave has positive polarity, the carrier frequency shifts in one direction; when the instantaneous input wave has negative polarity, the carrier frequency shifts in the opposite direction. At every instant in time, the extent of carrier-frequency shift (the *deviation*) is directly proportional to the extent to which the signal amplitude is positive or negative.

In digital FM, the carrier frequency shifts abruptly, rather than varying continuously. The number of possible carrier frequency states is usually a power of 2. If there are only two possible frequency states, the mode is called frequency-shift keying (FSK). In more complex modes, there can be four, eight, or more different frequency states. Each specific carrier frequency represents a specific digital input data state.

Frequency modulation is similar in practice to phase modulation (PM). When the instantaneous frequency of a carrier is varied, the instantaneous phase changes as well. The converse also holds: When the instantaneous phase is varied, the instantaneous frequency changes. But FM and PM are not exactly equivalent, especially in analog applications. When an FM receiver is used to demodulate a PM signal, or when an FM signal is intercepted by a receiver designed for PM, the audio is distorted. This is because the relationship between frequency and phase variations is not linear; that is, frequency and phase do not vary in direct proportion.

### 3. PHASE MODULATION

Phase modulation (PM) is a method of impressing data onto an alternating-current (AC) waveform by varying the instantaneous phase of the wave. This scheme can be used with analog or digital data.

In analog PM, the phase of the AC signal wave, also called the ***carrier***, varies in a continuous manner. Thus, there are infinitely many possible carrier phase states. When the instantaneous data input waveform has positive polarity, the carrier phase shifts in one direction; when the instantaneous data input waveform has negative polarity, the carrier phase shifts in the opposite direction. At every instant in time, the extent of carrier-phase shift (the ***phase angle***) is directly proportional to the extent to which the signal amplitude is positive or negative.

In digital PM, the carrier phase shifts abruptly, rather than continuously back and forth. The number of possible carrier phase states is usually a power of 2. If there are only two possible phase states, the mode is called ***biphase modulation***. In more complex modes, there can be four, eight, or more different phase states. Each phase angle (that is, each shift from one phase state to another) represents a specific digital input data state.

Phase modulation is similar in practice to frequency modulation (FM). When the instantaneous phase of a carrier is varied, the instantaneous frequency changes as well. The converse also holds: When the instantaneous frequency is varied, the instantaneous phase changes. But PM and FM are not exactly equivalent, especially in analog applications. When an FM receiver is used to demodulate a PM signal, or when an FM signal is intercepted by a receiver designed for PM, the audio is distorted. This is because the relationship between phase and frequency variations is not linear; that is, phase and frequency do not vary in direct proportion

## 5.4Digital Transmission

- is the transmittal of digital signals between two or more points in a communications system
- The signals can be binary or any other form of discrete-level digital pulses.
- the original source information may be in digital form, or it could be analog signals that have been converted to digital pulses prior to transmission and converted back to analog signals in the receiver.

- with digital transmission systems, a physical facility (pair of wires, coaxial cable, or an optical fiber cable) is required to interconnect the various points within the system

### *Advantages of Digital Transmission*

- noise immunity
  - pulses are evaluated during a precise time interval and a simple determination is made whether the pulse is above or below a prescribed reference level
- better suited than analog signals for processing and combining using a technique called *multiplexing*
- more resistant than analog systems to additive noise because they use signal *regeneration* rather than signal amplification
- simpler to measure and evaluate

### *Disadvantages of Digital Transmission*

- the transmission of digitally encoded analog signals requires significantly more bandwidth than simply transmitting the original analog signal
- needs additional encoding and decoding circuitry because analog signals must be converted to digital pulse prior to transmission and converted back to their original analog form at the receiver
- digital transmission requires precise time synchronization between the clocks in the transmitters and receivers
- incompatible with older analog transmission systems

## *Pulse Modulation*

- consists essentially of sampling analog information signals and then converting those samples into discrete pulses and transporting the pulses from a source to a destination over a physical transmission medium

### *The four predominant methods of pulse modulation:*

I. pulse width modulation
II. pulse position modulation
III. pulse amplitude modulation
IV. pulse code modulation

### *Pulse Width Modulation (PWM)*

- is sometimes called ***pulse duration modulation (PDM)*** or ***pulse length modulation (PLM)***
- the width of a constant amplitude pulse is varied proportional to the amplitude of the analog signal at the time the signal is sampled
- used in special-purpose communications system mainly for the military but are seldom used for commercial digital transmission

***Pulse Position Modulation (PPM)***

- the position of a constant-width pulse within a prescribed time slot is varied according to the amplitude of the sample of the analog signal
- the higher the amplitude of the sample, the farther to the right the pulse is positioned within the prescribed time slot
- the highest amplitude sample produces a pulse to the far right, and the lowest amplitude sample produces a pulse to the far left
- also used in special-purpose communications system mainly for the military but are seldom used for commercial digital transmission

***Pulse Amplitude Modulation (PAM)***

- the amplitude of a constant width, constant-position pulse is varied according to the amplitude of the sample of the analog signal
- PAM waveforms resemble the original analog signal more than the waveforms for PWM or PPM
- this is used as an intermediate form of modulation with PSK, QAM, and PCM, although it is seldom used by itself

***Pulse Code Modulation (PCM)***

- the analog signal is sampled and then converted to a serial *n*-bit binary code for transmission
- each code has the same number of bits and requires the same length of time for transmission
- is by far the most prevalent form of pulse modulation

***Pulse Code Modulation***

- invented by Alex Reeves in 1937 at AT&T laboratories in Paris
- this is the preferred method of communications within the public switched telephone network
- with PCM, it is easy to combine digitized voice and digital data into a single, high-speed digital signal and propagate it over either metallic or optical fiber cables
- it is not really a type of modulation but rather a form of digitally coding analog signals
- pulses are of fixed length and fixed amplitude

- this is a binary system where a pulse or lack of pulse within a prescribed time slot represents either a logic 1 or a logic 0 condition

***PCM Sampling***

- the function of a sampling circuit in a PCM transmitter is to periodically sample the continually changing analog input voltage and convert those samples to a series of constant-amplitude pulses that can be more easily be converted to binary PCM code
- For the ADC to accurately convert a voltage to binary code, the voltage must be relatively constant so that the ADC can complete the conversion before the voltage level changes. If not, the ADC would be continually attempting to follow the changes and may never stabilize on any PCM code.
-
    - ***Two basic techniques used to perform the sampling function:***
        - **natural sampling**
        - **flat-top sampling**

**Natural sampling**

- is when the tops of the sample pulses retain their natural shape during the sample interval, making it difficult for an ADC to convert the sample to a PCM code

**Flat-top sampling**

- is the most common method used for sampling voice signals in PCM systems, which is accomplished in a ***sample-and-hold circuit***
- the purpose of a sample-and-hold circuit is to periodically sample the continually changing analog input voltage and convert those samples to a series of constant-amplitude PAM voltage levels

***Aperture error*** – is when the amplitude of the sampled signal changes during the sample pulse time

***Aperture*** or ***acquisition time*** – the time that the FET, $Q_1$, of a sample-and-hold circuit is on

***Aperture distortion*** – if the input to the ADC is changing while it is performing the conversion

***Droop*** – a gradual discharge across the capacitor of a sample-and-hold circuit during conversion time caused by the capacitor discharging through its own leakage resistance and the input impedance of the voltage follower $Z_2$

## 5.5 Transmission Impairments

Analog signal consist of varying a voltage with time to represent an information steam. If the transmission media were perfectly, the receiver could receive exactly the same signal that the transmitter sent. But communication lines are usually not perfect, so they receive signal is not the same as the transmitted signal. For digital data this difference can lead to errors. Transmission lines suffers from three major problems

1. Attenuation
2. Delay distoration
3. Noise

**Attenuation:**

It is the loss of energy as the signal propagates outward. The amount of energy depends on the frequency. If the attenuation is too much, the receiver may not be able to detect the signal at all, or the signal may fall below the noise level. For reliable communication, the attenuation and delay over the range of frequencies of transmission should be constant.

**Destortion:**

The second transmission impairment is delay distortion. Communication line have distributed inductance and capacitance which distort the amplitude of signals and also delay the signals at different frequencies by different amounts. It is caused by the fact that different Fourier components travel at different speed. For digital data, fast components from one bit may catch up and over take slow component from bit ahead, mixing the two bits and increasing the probability of incorrect reception.

**Noise:**

Noise is a third impairment. It can be define as unwanted energy from sources other than the transmitter. Thermal noise is caused by the random motion of the electrons in a wire and is unavoidable.

**Cross talk:**

Similarly cross talk is a noise that is caused by the inductive coupling between two wires that are closed to each other. Sometime when talking on the telephone, you can hear another conversation in the background. That is cross talk

## 5.6 Unit Summary

- Analog signals can be converted into digital signals by using a modem.
- Digital signals use binary values to send and receive data between computers.
- Digital signals are easier and more reliable to transmit with fewer errors.
- Analog signal are replicas of sound waves that can be distorted with noise and drop the quality of transmission.
- Digital data has a faster rate of transmission when compared to analog, and gives better productivity.

## 5.7 Keywords

ASK, PSK, FSK, AM, FM, PM, Sampling, Attenuation

## 5.8 Exercise

1. Discuss different type's digital to analog conversion techniques with their applications
2. Explain various methods for analog to analog conversion
3. What are the major problems Transmission lines suffers? explain in details
4. What is the difference between analog and digital signal for data transmission?

## 5.9 Reference

1. Data Communications and Networking – Behrouz A. Forouzan, 4th Edition, Tata McGraw-Hill 2006.
2. Computer and Communication Networks – Nader F. Mir, Pearson Education, 2007.
3. Data and Computer Communication, William Stallings, 8th Edition, Pearson Education, 2007.

# UNIT-6: Digital to Digital, Analog to Digital, Digital to Analog

## Structure

## 6.0 OBJECTIVES

After studying this unit you will be able to

- Explain the basic concepts of signal conversion
- Explain different aspects of ASK, FSK, PSK conversion techniques
- Explain bandwidth and power requirement

## 6.1 Introduction

A signal is any time-varying or spatial-varying quantity. In the physical world, any quantity measurable through time or over space can be taken as a signal. Within a complex society, any set of human information or machine data can also be taken as a signal. Such information or machine data (for example, the dots on a screen, the ink making up text on a paper page, or the words now flowing into the reader's mind) must all be part of systems existing in the physical world – either living or non-living.

Despite the complexity of such systems, their outputs and inputs can often be represented as simple quantities measurable through time or across space. In the latter half of the 20th century, electrical engineering itself separated into several disciplines, specializing in the design and analysis of physical signals and systems, on the one hand, and in the functional behavior and conceptual structure of the complex human and machine systems, on the other. These engineering disciplines have led the way in the design, study, and implementation of systems that take advantage of signals as simple measurable quantities in order to facilitate the transmission, storage, and manipulation of information.

## 6.2 ANALOG AND DIGITAL SIGNALS

Less formally than the theoretical distinctions mentioned above, two main types of signals encountered in practice are analog and digital. In short, the difference between them is that digital signals are discrete and quantized, as defined below, while analog signals possess neither property.

**Discretization**

One of the fundamental distinctions between different types of signals is between continuous and discrete time. In the mathematical abstraction, the domain of a continuous-time (CT) signal is the set of real numbers (or some interval thereof), whereas the domain of a discrete-time (DT) signal is the set of integers (or some interval). What these integers represent depends on the nature of the signal.

DT signals often arise via sampling of CT signals. An audio signal, for example consists of a continually fluctuating voltage on a line that can be digitized by an ADC circuit, wherein the circuit will read the voltage level on the line, say, every 50 $\mu$s. The resulting stream of numbers is stored as digital data on a discrete-time signal. Computers and other digital devices are restricted to discrete time.

**Quantization**

If a signal is to be represented as a sequence of numbers, it is impossible to maintain arbitrarily high precision - each number in the sequence must have a finite number of digits. As a result, the values of such a signal are restricted to belong to a finite set; in other words, it is quantized.

### ANALOG SIGNALS

An analog or analogue signal is any continuous signal for which the time varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal. It differs from a digital signal in terms of small fluctuations in the signal which are meaningful. Analog is usually thought of in an electrical context; however, mechanical, pneumatic, hydraulic, and other systems may also convey analog signals.

An analog signal uses some property of the medium to convey the signal's information. For example, an aneroid barometer uses rotary position as the signal to convey pressure information. Electrically, the property most commonly used is voltage followed closely by frequency, current, and charge.

Any information may be conveyed by an analog signal; often such a signal is a measured response to changes in physical phenomena, such as sound, light, temperature, position, or pressure, and is achieved using a transducer.

For example, in sound recording, fluctuations in air pressure (that is to say, sound) strike the diaphragm of a microphone which induces corresponding fluctuations in the current produced by a coil in an electromagnetic microphone, or the voltage produced by a condenser microphone. The voltage or the current is said to be an "analog" of the sound.

An analog signal has a theoretically infinite resolution. In practice an analog signal is subject to noise and a finite slew rate. Therefore, both analog and digital systems are subject to limitations in resolution and bandwidth. As analog systems become more complex, effects such as non-linearity and noise ultimately degrade analog resolution to such an extent that the performance of digital systems may surpass it. Similarly, as digital systems become more complex, errors can occur in the digital data stream. A comparable performing digital system is more complex and requires more bandwidth than its analog counterpartIn analog systems, it is difficult to detect when such degradation occurs. However, in digital systems, degradation can not only be detected but corrected as well.

**Advantages**

The main advantage is the fine definition of the analog signal which has the potential for an infinite amount of signal resolution. Compared to digital signals, analog signals are of higher density.

Another advantage with analog signals is that their processing may be achieved more simply than with the digital equivalent. An analog signal may be processed directly by analog components, though some processes aren't available except in digital form.

**Disadvantages**

The primary disadvantage of analog signaling is that any system has noise – i.e., random unwanted variation. As the signal is copied and re-copied, or transmitted over long distances, these apparently random variations become dominant. Electrically, these losses can be diminished by shielding, good connections, and several cable types such as coaxial or twisted pair.

The effects of noise create signal loss and distortion. This is impossible to recover, since amplifying the signal to recover attenuated parts of the signal amplifies the noise (distortion/interference) as well. Even if the resolution of an analog signal is higher than a comparable digital signal, the difference can be overshadowed by the noise in the signal.

Most of the analog systems also suffer from generation loss.

## DIGITAL SIGNALS

The term digital signal is used, to refer to more than one concept. It can refer to discrete-time signals that have a discrete number of levels, for example a sampled and quantified analog signal, or to the continuous-time waveform signals in a digital system, representing a bit-stream. In the first case, a signal that is generated by means of a digital modulation method which is considered as converted to an analogue signal, while it is considered as a digital signal in the second case.

**Advantages**

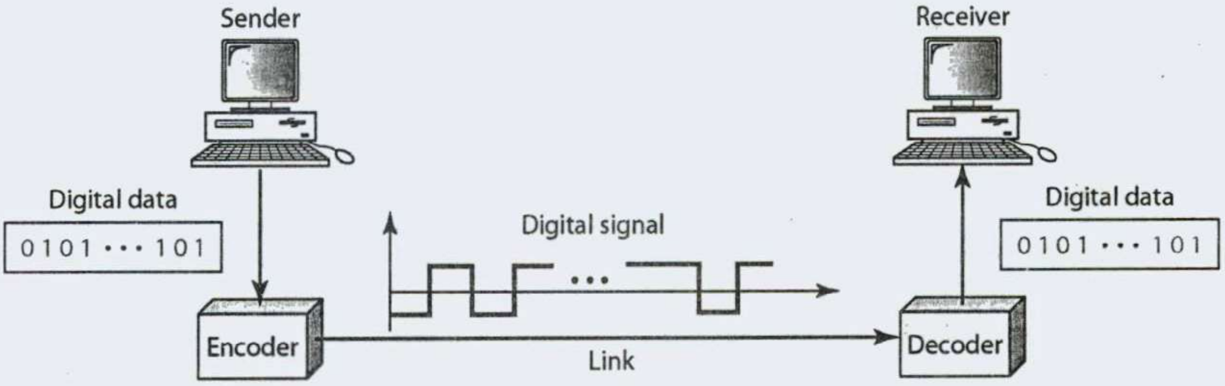
- Less expensive
- More reliable
- Easy to manipulate
- Flexible
- Compatibility with other digital systems
- Only digitized information can be transported through a noisy channel without degradation Integrated networks

**Disadvantages**

- Sampling Error
- Digital communications require greater bandwidth than analogue to transmit the same information.
- The detection of digital signals requires the communications system to be synchronised, whereas generally speaking this is not the case with analogue systems.

## 6.3 DIGITAL DATA TO DIGITAL SIGNAL CONVERSION

In this section, we see how we can represent digital data by using digital signals. The conversion involves three techniques: line coding, block coding, and scrambling. Line coding is always needed; block coding and scrambling may or may not be needed.



1. **LINE CODING**

The sent data needs to be somehow coded into an electromagnetic signal to be sent over the wire, and later decoded back. There are many ways of encoding signals, with each scheme having some pros and cons.

Primarily, there are three major categories of line coding: Unipolar, Polar, and Bipolar.

**Unipolar**

The most primitive encoding technique is Unipolar. The signal is basically this: high voltage on a '1' bit, and low (zero) voltage on a '0' bit. There is no synchronization information, and the signal has a DC component.

**Polar**

There are three categories of Polar line coding: NRZ, RZ, and Biphase.

**NRZ:** NRZ is Nonreturn to Zero. This basically means that after each bit is transmitted, the signal doesn't return to zero voltage. There are two major categories of NRZ, the NRZ-L, and NRZ-I. The NRZ-L is similar to Unipolar, in that the voltage directly depends on the bit it represents. A positive voltage generally represents a '1', and a negative voltage represents a '0' (or vice versa). Unlike the unipolar scheme, NRZ-L alleviates the problem of the DC component. The NRZ-I does a voltage transition (positive to negative, or negative to positive) on a '1' bit, and no change on a '0' bit. It is the change in the voltage that matters, not the actual voltage itself. NRZ-I is better than NRZ-L because the destination can use the voltage change to synchronize its clock with the sender—assuming messages don't have long sequences of '0' bits (which don't have a transition).

**RZ:** A pretty simple scheme. Positive voltage indicates a '1', negative voltage indicates a '0'. The voltage goes down to zero in the middle of every tick.

**Biphase:** There are two primary Biphase coding schemes: Manchester (Ethernet LANs), and Differential Manchester (Token Ring LANs). Manchester, like RZ has a transition in the middle of a bit interval. There is a transition for every bit. A low to high transition indicates a '1' bit, and a high to low transition indicates a '0' bit. Differential Manchester is somewhat similar to

NRZ-I. In the beginning of a bit interval, there is a voltage change on a '0' bit, and no voltage switch on a '1' bit. There is always a voltage change in the middle of a bit interval.

**Bipolar**

Bipolar scheme is similar to RZ (also has 3 voltage levels). It uses zero voltage to represent a '0' bit, and a '1' bit is represented by either a positive or negative voltage (alternating).

2. **Block coding**

- For a code to be capable of error detection, we need to add redundancy, i.e., extra bits to the data bits.
- Synchronization also requires redundancy - transitions are important in the signal flow and must occur frequently.
- Block coding is done in three steps: division, substitution and combination.
- It is distinguished from multilevel coding by use of the slash - xB/yB.
- The resulting bit stream prevents certain bit combinations that when used with line encoding would result in DC components or poor sync. Quality.

3. **Scrambling**

- The best code is one that does not increase the bandwidth for synchronization and has no DC components.
- Scrambling is a technique used to create a sequence of bits that has the required c/c's for transmission - self clocking, no low frequencies, no wide bandwidth.
- It is implemented at the same time as encoding, the bit stream is created on the fly.
- It replaces 'unfriendly' runs of bits with a violation code that is easy to recognize and removes the unfriendly c/c.

## 6.4 ANALOG TO DIGITAL CONVERSION

The compliment to the digital to analog converter is the analog to digital converter. An analog to digital converter converts analog voltages to digital information that can be used by a computer.

It is useful to note that the digital data produced by an analog to digital converter is only approximately proportional to the analog input. That's because a perfect conversion is impossible due to the fact that digital information changes in steps, whereas analog is virtually continuous, at least down to the subatomic level.

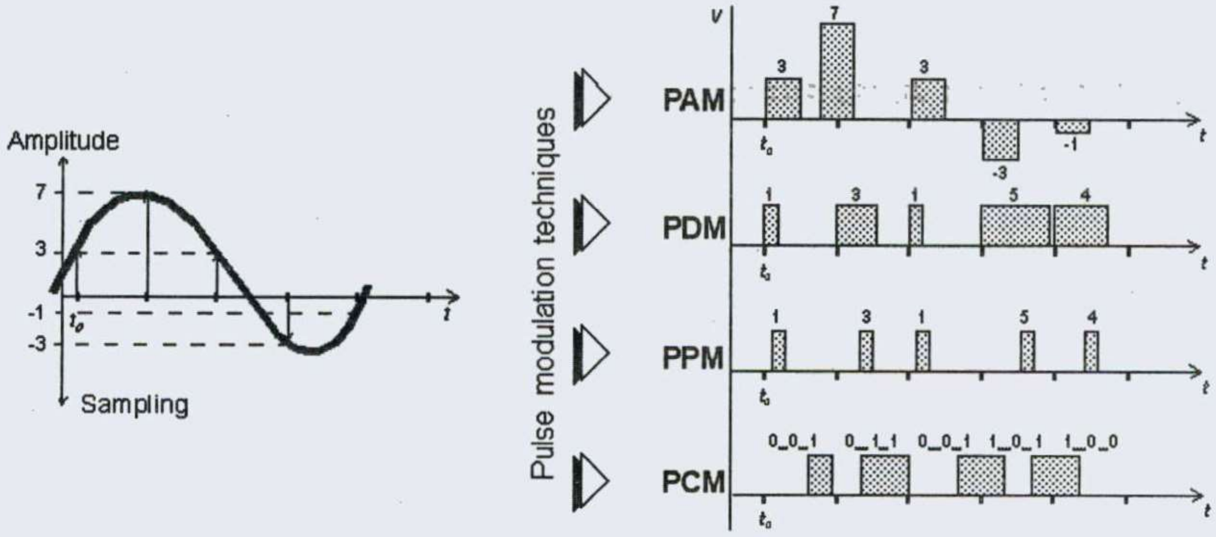
**Pulse code modulation (PCM)**

For digital communications it is necessary to transform the signals from the analog source of information into signals that are compatible with the digital processing they will undergo. This transformation is known as formatting the signal: Based on the information generated by the source, digital symbols are obtained. Formatting the information involves three processes: sampling, quantification and coding.

Nyquist demonstrated that an analog signal could be completely reconstructed without any loss of information based on a set of its periodic discrete samples, provided the following criterion is met:

$$\mathbf{fm < 2B}$$

Where B is the analog bandwidth [B]: Hz, and fm the sampling frequency [fm]: samples/s.



When sampling, values are taken from the analog signal every 1/fm seconds (sampling period). Quantification assigns these analog values a digital value by approximation and in accordance with the curves defined by the ITU. Finally, each quantified value is assigned a binary code (a series of zeros and ones) that constitutes the symbol to be transmitted. This process is called pulse code modulation (PCM).

PCM technology was patented and developed in France in the 30s (1938) but could not be used because the suitable technology was not available until during the Second World War. The first commercial PCM system was set up in 1962 by Bell Labs (USA). Its initial goal was that of converting an analog voice telephone channel to digital.