COMPUTER NETWORKS

DCA 3303

SCHOOL OF SCIENCE AND TECHNOLOGY

BANGLADESH OPEN UNIVERSITY

SCHOOL OF SCIENCE AND TECHNOLOGY

DCA 3303

COMPUTER NETWORKS

Course Development Team

Writer

Prof. Dr. Md. Mozammel Huq Azad Khan
Computer Science and Engineering Discipline
Khulna University

Co-ordinator
Mohammod Shamim Hossain
School of Science and Technology
Bangladesh Open University

Editor
Anwar Sadat
School of Science and Technology
Bangladesh Open University

BANGLADESH OPEN UNIVERSITY

COMPUTER NETWORKS

Over All Supervision

Professor Saidur Rahman
Dean, School of Science and Technology
Bangladesh Open University

Published by : Publishing, Printing & Distribution Division
Bangladesh Open University, Gazipur-1704
September 1998

ISBN 984-34-4001-3

Computer Composed & Desktop Processing by : Md. Jakir Hossain Cover Design : Monirul Islam.
Printed by : Rupali Printing & Packages Ltd. 75, South Basabo, Dhaka- 1214.

Computer Networks
Contents

PREFACE

During the first two decades of their existence, computer systems were highly centralized, usually within a single large room. The old model of a single computer serving all of the organization’s computational needs has been obsolete and the computer workloads are continuously being decentralized. The need for communicating among the geographically dispersed computers has evolved computer networks. So computer network has become an essential part of computer science education. The purpose of this book is to present various concepts, protocols, standards, and applications related to computer networks. The materials of the book are mostly organized on the basis of different layers of the computer network architecture. The concept of data communications in the physical layer is given special attention. The other layers are discussed in relation to protocols and standards recently being used. Concepts and technologies of the local area networks are also given special emphasis. The book is divided into thirteen units covering all aspects of computer networks.

Unit 1 deals with definition, types, and topologies of computer networks.

Unit 2 introduces the architectural concepts of computer networks. The OSI Model and the TCP/IP protocol suite are presented.

Unit 3 presents various concepts related to signals and data transmission. Data transmission media and techniques are also presented.

Unit 4 deals with various techniques of data encoding for transmission.

Unit 5 discusses transmission of digital data. Error detection techniques and transmission line interface standards for digital data transmission are also discussed.

Unit 6 presents concepts, techniques, and protocols for data link control.

Unit 7 introduces multiplexing techniques for data link.

Unit 8 deals with switched data communication networking. Circuit switched networking is introduced briefly. Packet switching networking is discussed in details including one widely used protocol standard.

Unit 9 discusses concepts, technologies, and standards of local area networks.

Unit 10 presents services and protocols related to transport mechanism.

Unit 11 introduces session services and protocols.

Unit 12 discusses presentation concepts and protocols. Network security and virtual terminal protocol are also presented.

Unit 13 deals with some distributed applications including electronic mail system.

At the end of each lesson there is an exercise. The answers of the multiple choice questions are provided at the end of the book. A learner can check his/her understanding of the lesson by answering the questions.

Unit 1 : Introduction to Computer Networks

Introduction

Computer workloads are continuously being decentralized. The need for communicating among the geographically dispersed computers has evolved computer networks. In this unit, preliminary ideas of computer networks are introduced. Classification of computer networks and their topologies are also presented in this unit.

Lesson 1 : Computer Networks

1.1. Learning Objectives

On completion of this lesson you will be able to :

- grasp the elementary idea of computer networks
- understand the goals of computer networks
- grasp the idea of message transmission over a computer network

1.2. What is a Computer Network?

A computer network is an interconnected collection of autonomous computers.

A computer network is an interconnected collection of autonomous computers.

An autonomous computer is one whose start, stop and control do not depend on any other computer.

Two computers are said to be interconnected if they are able to exchange information. This connection between two computers may be using copper wire, fiber optics, microwaves, and communication satellites.

1.3. Computer Networks and Distributed Systems

There is a considerable confusion between a computer network and a distributed system. In a computer network, users explicitly log onto one computer, explicitly submit jobs remotely, explicitly move files around and generally handle all the network management personally.

In a distributed system, the existence of multiple autonomous computers is not visible to the user. A user can type a command to run a program, and it runs. It is up to the operating system to select best processor, find and transport all the input files to that processor, and put the results in the appropriate place. In a distributed system, nothing has to be done explicitly, it is all automatically done by the system without the user's knowledge. In effect, a distributed system is a software system built on top of a computer network.

1.4. Goals of Computer Networks

Computer networks have the following goals :

(i) **Resource sharing** : Programs, equipment, and data available to anyone on the network can be shared without regard to the physical location of resource and the user.

(ii) **High reliability** : Alternative sources of resource supply provide high reliability. For example, files could be placed on two or three computers, so if one of them is unavailable due to a hardware failure, the other copies could be used. In addition, for presence of multiple CPUs, if one goes down the other may be able to take over its work.

(iii) **Saving money** : Resource sharing provides considerable saving of money.

(iv) **Salability** : Computer network provides ability to increase system performance gradually as the workload grows just by adding more processor in the network.

(v) **Communication medium** : A computer network provides a powerful communication medium among widely separated people. For example, it is easy for two or more people who live far apart to write a report using a computer network.

1.5. Message Transmission over a Computer Network

A message in a computer network is a single unit of communication. For example, in an e-mail system, a message would consist of a document sent from one user to another. A message in an image transmission system could be a single figure, image, or diagram.

Long messages are normally broken up into shorter bit strings called packets.

To transmit a message over a computer network, it is usually represented as a string of bits. Transmitting long message as one complete unit is generally not done for various reasons. Long messages are normally broken up into shorter bit strings called packets. These packets are then sent through the network as individual units and are reassembled into complete message at the destination computer.

1.6. Exercise

1.6.1. Multiple choice questions

a. A computer network is an interconnected collection of

i) autonomous computers
ii) network nodes
iii) mainframe computers
iv) personal computers.

b. A distributed system is

i) basically a computer network
ii) a software system built on top of a computer network
iii) the operating system of a computer network
iv) none of the above.

1.6.2. Questions for short answers

a) What is a computer network?
b) What is a distributed system?
c) What is a message?
d) What is a packet?

1.6.3. Analytical questions

a) Discuss the difference between a computer network and a distributed system.
b) Discuss the goals of a computer networks.
c) Discuss the relationship between message and packet.

Lesson 2 : Types Of Computer Networks

2.1. Learning Objectives

On completion of this lesson you will be able to :

- classify computer networks based on transmission technology
- classify computer networks based on their scale
- grasp the idea of inter-networking.

2.2. Types of Computer Networks Based on Transmission Technology

Types of computer networks based on transmission technology.

There are two types of computer networks based on transmission technology :

(i) **Broadcast Networks** : Broadcast networks have a single communication channel that is shared by all the computers on the network. Packets sent by any computer are received by all the others. An address field within the packet specifies for whom it is intended. Upon receiving a packet, a computer checks the address field. If the packet is intended for itself, it process the packet; if the packet is intended for some other computer, it is just ignored.

(ii) **Point-to-point Networks** : Point-to-point networks consist of many connections between individual pairs of computers. To go from source to the destination, a packet on this type of network may have to first visit one or more intermediate computers.

2.3. Types of Computer Networks Based on Their Scale

Types of computer networks based on their scale.

There are three types of computer networks based on their scale :

(i) **Local Area Networks** : Local area networks, generally called LANs, are privately owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources and exchange information.

(ii) **Metropolitan Area Networks** : A metropolitan area network, or MAN, is basically a bigger version of a LAN and normally uses similar technologies. It might cover a group of nearby corporate offices or a city and might be either private or public.

(iii) **Wide Area Networks** : A wide are network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of computers intended for running user programs called hosts or end systems. The hosts are connected by a communication subnet, or just subnet for short.

2.4. Internetworks

Many computer networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. This desire requires connecting together different and frequently incompatible networks. The connection is made by using computers called gateways to provide the necessary translation both in terms of hardware and software. A collection of interconnected networks is called an internetwork or just internet.

A collection of interconnected networks is called an internetwork or just internet.

A common form of internet is a collection of LANs connected by a WAN.

The Internet is a specific world wide internet that is widely used to connect universities, government offices, companies, and private individuals.

2.5. Exercise

2.5.1. Multiple choice questions

a. A broadcast network has

i) a single communication channel shared by all computers
ii) many communication channels, each shared by a group of computers
iii) point-to-point communication channel between each pair of computers
iv) none of the above.

b. A LAN spans over

i) only few meters
ii) few kilometers

iii) hundreds of kilometers
iv) many countries.

2.5.2. Questions for short answers

a) What is a broadcast network?
b) What is a point-to-point channel?
c) What is a LAN?
d) What is a MAN?
e) What is a WAN?
f) What is a host?
g) What is a subnet?
h) What is an internet?
i) What is the Internet?
j) What is a gateway?

2.5.3. Analytical questions

a) Classify computer networks based on transmission technology.
b) Classify computer networks based on their scale.
c) Discuss the difference between internet and the Internet.

Lesson 3 : Network Topology

3.1. Learning Objectives

On completion of this lesson you will be able to :

- know the different topologies used in LANs
- know the different topologies used in the subnet of WANs.

3.2. Definition

The manner in which computers in a network are geometrically arranged and connected is known as the **topology** of the network.

3.3. Topologies used in LANs

Broadcast networks are commonly used in LANs. Figure 1.1 shows three commonly used topologies for LANs.

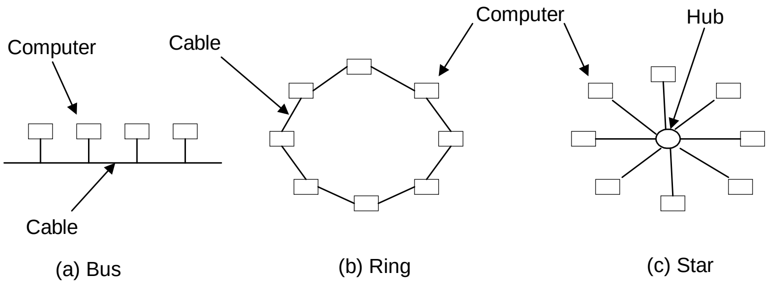


Fig. 1.1 : Topologies commonly used in LANs.

In a bus topology, only one pair of computers on the network can communicate at the same time.

Bus Topology : In a bus topology, all the computers are connected to a common transmission medium. As a result of this, only one pair of computers on the network can communicate at the same time. Each computer has a unique address which is used when information is transmitted. When a data packet is sent out, it propagates throughout the medium and is received by all computers. To receive messages, each computer continuously monitors the medium and copies those messages that are addressed to itself as the data packets go by. Since the transmission medium in a bus is generally time-shared, there must be some type of control mechanism to prevent several stations from transmitting simultaneously.

Ring Topology : In a ring topology, consecutive computers are connected by point-to-point links which are arranged to form a single closed path. Data are transmitted from node to node around the ring. The interface at each computer has the ability to recognize packets destined to it.

In a star topology, all computers are joined at a single point called the hub.

Star Topology : In a star topology, all computers are joined at a single point called the hub.

3.4. Topologies Used In WANs

A computer connected to the WAN is called **host** or end system. The hosts are connected by a communication subnet or **subnet** for short. The job of the subnet is to carry messages from host to host.

The job of the subnet is to carry messages from host to host.

In most WANs, the subnet consists of two distinct components: **transmission lines** (also called circuits, channels, or trunks) and **routers** (also called nodes or switching elements).

The transmission lines move packets between computers. The routers connect two or more transmission lines. Routers are specialized computers.

The routers connect two or more transmission lines.

The collection of transmission lines and routers form the subnet as shown in Figure 1.2.

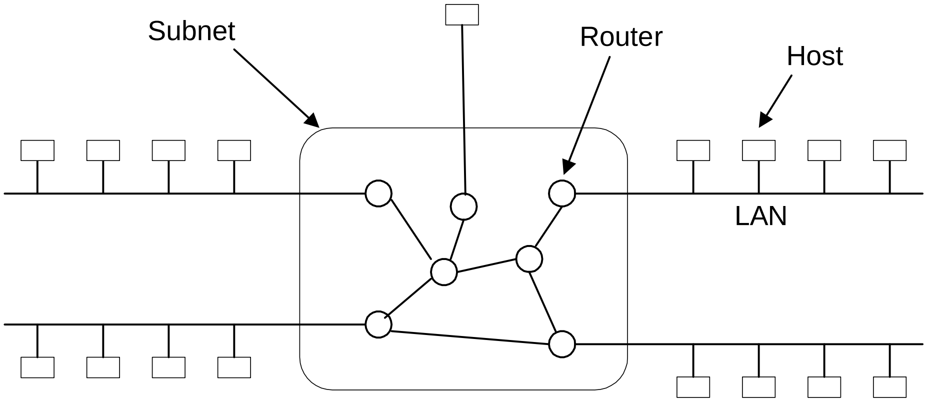
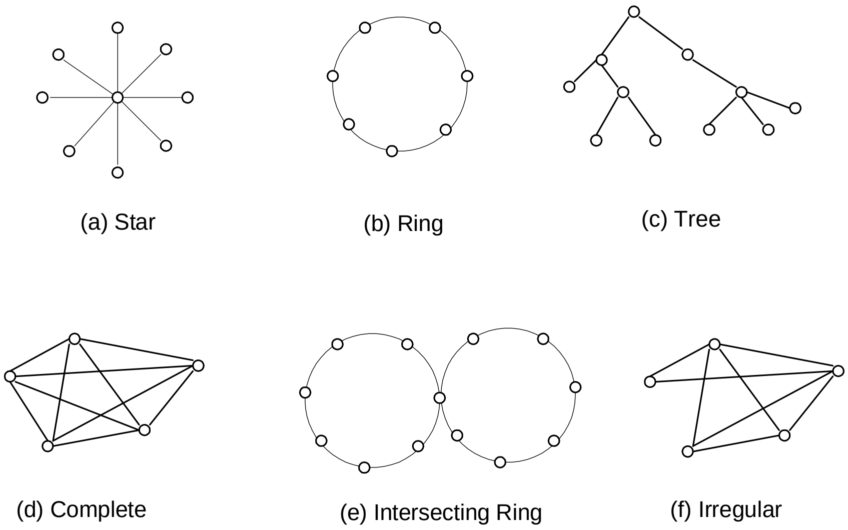


Fig. 1.2: Organization of a WAN.

If two routers that are not directly connected wish to communicate, they must do this via other intermediate routers. In this case, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet using this principle is called a **point-to-point** (also called store-and-forward or packet switching) subnet.

Figure 1.3 shows six possible topologies used in a point-to-point subnet.



(a) Star

(b) Ring

(c) Tree

(d) Complete

(e) Intersecting Ring

(f) Irregular

Fig. 1.3 : Topologies used in point-to-point subnet.

3.5. Exercise

3.5.1. Multiple choice questions

a. In a bus topology, all the computers are connected

i) to a common transmission medium
ii) by point-to-point lines
iii) by a ring
iv) none of the above.

b. A subnet consists of

i) transmission lines
ii) routers
iii) routers and transmission lines
iv) none of the above.

3.5.2. Questions for short answers

a) What is topology of a network?
b) What is a host?
c) What is a subnet?
d) What is a router?
e) What is a point-to-point subnet?

3.5.3. Analytical questions

a) Discuss different types of topologies used in LANs.
b) Discuss different types of topologies used in point-to-point subnet of a WAN.

Unit 2 : Computer Networks Architecture

Introduction

*Set of convention is referred to as **protocol**.*

Network hardware is reasonably standard and generally presents few problems. However, when communication is desired among heterogeneous (different vendors, different models of same vendor) computers or hosts, the software development effort can be a nightmare. A one-at-a-time special-purpose approach to network software development is too costly to be acceptable. The only alternative is for computer vendors to adopt and implement a common set of conventions. This set of convention is referred to as **protocol**. The task of communication in a truly cooperative way between applications on different computers is too complex to be handled as a unit. The problem must be decomposed into manageable parts. Hence before one can develop standards, there should be a structure or architecture that defines the communications task. In this unit, the concept of protocol and various architectural models of computer networks are discussed.

Lesson 1 : Protocols

1.1. Learning Objectives

On completion of this lesson you will be able to :

- grasp the concept of protocol used in computer networks
- grasp the characteristics and features of protocols.

1.2. Characteristics of Protocols

In computer networks, entities in different hosts need to communicate. Examples of entities are user application programs, file transfer packages, data base management systems, electronic mail facilities, and terminals. In general, an **entity** is anything capable of sending or receiving information.

For two entities to successfully communicate they must “speak the same language”. What is communicated, how it is communicated, and when it is communicated must conform to some mutually accepted set of conventions between the entities evolved. The set of conventions is referred to as **protocol**, which may be defined as set of rules governing the exchange of data between two entities. The key elements of a protocol are :

- **Syntax** : includes such things as data format, coding, and signal levels.
- **Semantics** : includes control information for coordination and error handling.
- **Timing** : includes speed matching and sequencing.

Some important characteristics of a protocol are :

Important characteristics of a protocol.

- Direct/indirect
- Monolithic/structured
- Symmetric/asymmetric
- Standard/nonstandard.

Direct/indirect : Communication between two entities may be direct or indirect. If two hosts share a point-to-point link, the entities in these hosts may communicate directly; that is, data and control information pass directly between entities with no intervening active agent. If hosts connect through a switched communication networks, the two entities must depend on the functioning of other entities to exchange data.

Monolithic/structured : A protocol may be monolithic or structured. The task of communication between entities on different hosts is too complex to be handled as a unit. An alternative is to use structured design and implementation techniques. Instead of a single protocol, there is a set of protocols that exhibit a hierarchical or layered structure. More primitive functions are implemented in lower-level entities that provide service to higher-level entities. When structured protocol design is used, we refer to the hardware and software used to implement the communications functions as a **network architecture**.

The symmetric protocols involve communication between peer entities.

Symmetric/asymmetric : Protocol may be symmetric or asymmetric. The symmetric protocols involve communication between peer entities. Asymmetric may be dictated by the logic of an exchange, or by the desire to keep one of the entities as simple as possible.

Standard/nonstandard : A protocol may be either standard or nonstandard. A nonstandard protocol is one built for a specific communication situation. The increasing use of distributed processing dictate that all vendors implement protocols that conform to an agreed upon standard.

1.3. Functions of Protocols

We can group protocol functions into the following categories:

- Segmentation and reassembly
- Encapsulation
- Connection control
- Ordered delivery
- Flow control
- Synchronization
- Addressing
- Multiplexing
- Transmission services.

Functions of Protocols

Segmentation and Reassembly : A protocol is concerned with exchanging streams of data between two entities. Usually, the transfer can be characterized as consisting of a sequence of blocks of data of some bounded size. Lower level protocols may need to break the data up into blocks of some smaller bounded size. This process is called segmentation, or fragmentation.

A block of data exchanged between two entities via a protocol is referred to as a **protocol data unit** (PDU). The counterpart of segmentation is reassembled.

Encapsulation : Each PDU contains not only data but control information. Indeed, some PDUs consists solely of control information and no data. The control information falls into three general categories :

- **Address** : The address of the sender and/or receiver may be indicated.
- **Error-detecting code** : Some sort of frame check sequence is often included for error detection.
- **Protocol control** : Additional information is included to implement the protocol function.

The addition of control information to data is referred to as encapsulation.

The addition of control information to data is referred to as encapsulation.

Connection Control : An entity may transmit data to another entity in an unplanned fashion and without prior coordination. This is known as **connectionless data transfer**. If stations anticipate a lengthy exchange of data and/or certain details of their protocol must be worked out dynamically, a logical connection is established between the entities. This is known as

connection-oriented data transfer. In connection-oriented data transfer, three phases occur :

- Connection establishment.
- Data transfer.
- Connection termination.

Ordered Delivery : If two communicating entities are in different hosts connected by a network, there is a risk that PDUs will not arrive in the order in which they are sent, because they may traverse different paths through the network. In connection-oriented protocols, it is generally required that PDU order be maintained.

Flow Control : Flow control is a function performed by a receiving entity to limit the amount or rate of data that is sent by a transmitting entity. Flow control is a function that must be implemented in several protocols.

Error Control : Techniques are needed to guard against loss or damage of data and control information. Most techniques involve error detection and PDU retransmission. Error control is a function that must be performed at various levels of protocols.

Synchronization : It is occasionally important that two communicating protocol entities simultaneously in a well-defined state, for example at initialization, check pointing, and termination. This is termed synchronization.

Addressing : For two entities to communicate, other than over a point-to-point link, they must somehow be able to identify each other.

Multiplexing : Multiplexing permits multiple simultaneous connection.

Transmission Services : A protocol may provide a variety of additional services to the entities that use it. Three common examples of services are :

- **Priority** : Certain message, such as control messages, may need to get through to the destination entity with minimum delay. Thus priority may be assigned on a message basis.
- **Grade of Service** : Certain classes of data may require a minimum throughput or a maximum delay threshold.
- **Security** : Security mechanism may be involved.

1.4. Exercise

1.4.1. Multiple choice question

a. An entity is

i) anything capable of sending or receiving information.
ii) a software capable of sending or receiving information.
iii) a hardware capable of sending or receiving information.
iv) none of the above.

1.4.2. Questions for short answers

a) What are protocol and network architecture?
b) What are the key elements of a protocol?

1.4.3. Analytical questions

a) Describe the important characteristics of a protocol.
b) Describe the various categories of functions of a protocol.

Lesson 2 : The OSI Model

2.1. Learning Objectives

On completion of this lesson you will be able to :

- grasp the concepts of OSI reference model
- know the names of seven layers of OSI model
- know the principle of operation of OSI model
- grasp the concept of service primitive and parameters.

2.2. Introduction

The OSI model provides the basis for connecting "open" systems for distributed processing.

The International Organization for Standardization (ISO) in 1977 established a subcommittee to develop a computer network architecture. The result was the **Open System Interconnection** (OSI) reference model, adopted in 1983, which is a framework for defining standards for linking heterogeneous computers. The OSI model provides the basis for connecting "open" systems for distributed processing. The term "open" denotes the ability of any two systems conforming to the reference model and the associated standards to connect.

2.3. Concepts

The layers are defined so that changes in one layer do not require changes in the other layers.

A widely accepted structuring technique is layering. The communication functions are partitioned into a vertical set of layers. Each layer performs a related subset of the functions required to communicate with another system. It relies on the next lower layer to perform more primitive functions and to conceal the details of these functions. It provides services to the next higher layer. The layers are defined so that changes in one layer do not require changes in the other layers.

The OSI reference model has seven layers as follows :

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer.

It takes two to communicate, so the same set of layered functions must exist in two systems. Communication is achieved by having corresponding ("peer") entities in the same layer in two different systems communicate via a protocol.

Figure 2.1 illustrates the OSI model. Each system contains the seven layers. Communication is between applications in the systems, labeled application X and application Y in the figure. If application X wishes to send a message to application Y, it invokes the application layer (layer 7). Layer 7 establishes a peer relationship with layer 7 of the target machine, using a layer 7 protocol. This protocol requires services from layer 6, so the two layer 6 entities use a protocol of their own, and so on down to the physical layer, which actually passes the bits through a transmission medium.

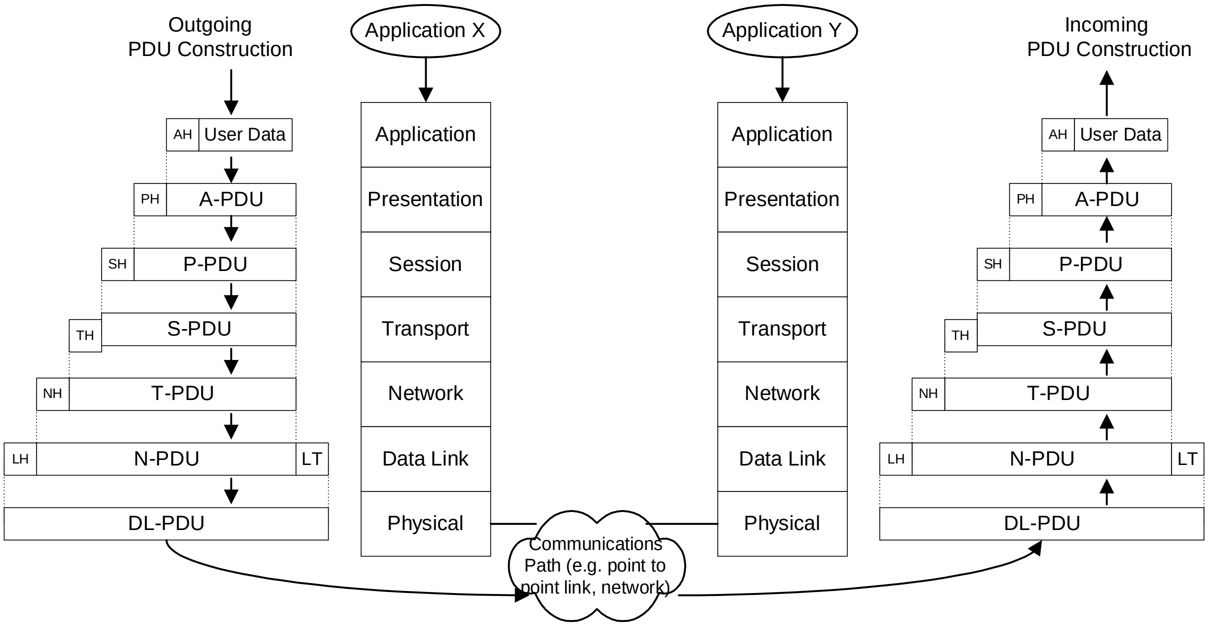


Fig. 2.1 : The OSI environment.

There is no direct communication between peer layers except at the physical layer. That is, above the physical layer, each protocol entity sends data down to the next lower layer in order to get the data across to its peer entity.

To assure the effective communication between two heterogeneous systems, standards are needed.

To assure the effective communication between two heterogeneous systems, standards are needed. Standards must define the functions and services to be provided by a layer (but not how it is to be done - that may differ from system to system). Standards must also define the protocols between peer layers (each protocol must be identical for the two peer layers). The OSI model, by defining a seven-layer architecture, provides a framework for defining these standards.

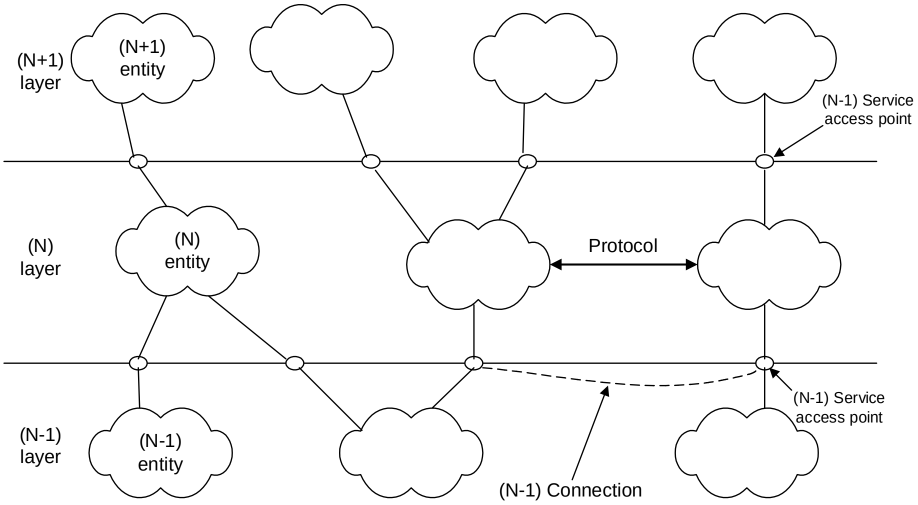


Fig. 2.2 : The layer concept.

Some useful OSI terminology is illustrated in Figure 2.2. For simplicity, any layer is referred to as the (N) layer, and names of constructs associated with that layer are also preceded by (N). Within a system, there are one or more active entities in each layer. An (N) entity implements functions of the (N) layer and also the protocol for communicating with (N) entities in other systems. There might be multiple identical (N) entities. There might also be different (N) entities, corresponding to different protocol standards at that level.

Service access points

Each entity communicates with entities in the layers above and below it across an interface. The interface is realized as one or more **service access points** (SAPs). The (N-1) entity provides services to an (N) entity via the invocation of primitives. A primitive specifies the function to be performed and is used to pass data and control information.

The OSI model is connection-oriented. Two (N) entities communicate, using a protocol, by means of an (N-1) connection. This logical connection is provided by (N-1) entities between (N-1) SAPs.

Figure 2.1 illustrates the OSI principle in operation. When application X has a message to send to application Y, it transfers these data to an application entity in the application layer. A header is appended to the data that contains the required information for the peer layer 7 protocol (encapsulation). The original data, plus the header, is now passed as a unit to layer 6. The presentation entity treats the whole unit as data, and appends its own header. This process continues down through layer2, which generally adds both a header and a trailer. This layer 2 unit, called a **frame**, is then passed by the physical layer onto the transmission medium. When the frame is received by the target system, the reverse process occurs. As the data ascend, each layer strips off the outer most header, acts on the protocol information contained therein, and passes the remainder up to the next layer.

2.4. Service Primitives and Parameters

Each layer is defined in two parts: the protocol between peer entities in different systems and the services provided by one layer to the next higher layer.

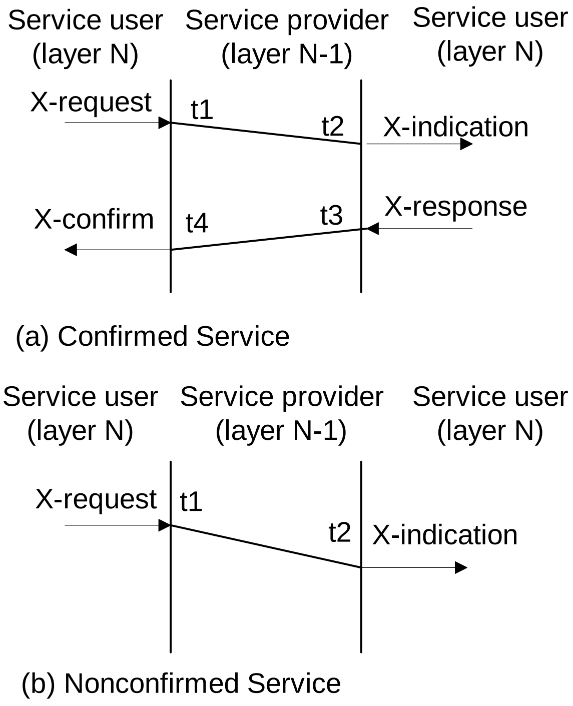
Each layer is defined in two parts: the protocol between peer entities in different systems and the services provided by one layer to the next higher layer in the same system. Protocols are defined in terms of the formats of protocol data units (PDUs) that are exchanged and the rules governing the use of those PDUs. The services between adjacent layers are expressed in terms of primitives and parameters. A primitive specifies the function to be performed, and the parameters are used to pass data and control information.

Four types of primitives are used in standards to define the interaction between adjacent layers in the architecture :

- **REQUEST** : A primitive issued by a service user to invoke some service and to pass the parameters needed to fully specify the requested service.
- **INDICATION** : A primitive issued by a service provider to either (i) indicate that a procedure has been invoked by the peer service user on the connection and to provide the associated parameters, or (ii) notify the service user of a provider-initiated action.
- **RESPONSE** : A primitive issued by a service user to acknowledge or complete some procedure previously invoked by an indication to that user.
- **CONFIRM** : A primitive issued by a service provider to acknowledge or complete some procedure previously invoked by a request by the service user.

The layout of figure 2.3 suggests the time ordering of these events. For example, consider the transfer of data from an (N) entity to a peer (N) entity in another system. The following steps occur :

1. The source (N) entity invokes its (N-1) entity with a DATA.request primitive. Associated with the primitive are the parameters needed, such as the data to be transmitted and the destination address.
2. The source (N-1) entity prepares an (N-1) PDU to be sent to its peer (N-1) entity.
3. The destination (N-1) entity delivers the data to the appropriate destination (N) entity via a DATA.indication, which includes the data and source address as parameters.
4. If an acknowledgment is called for, the destination (N) entity issues a DATA.response to its (N-1) entity.
5. The (N-1) entity conveys the acknowledgment in an (N-1) PDU.
6. The acknowledgment is delivered to the (N) entity as a DATA.confirm.



(a) Confirmed Service

(b) Nonconfirmed Service

Fig. 2.3 : Time sequence diagrams for primitives.

This sequence of events is referred to as a confirmed service, as the initiator receives confirmation that the requested service has had the desired effect at the other end. If only request and indication primitives are involved (corresponding to steps 1 through 3), then the service dialogue is a nonconfirmed service;

the initiator receives no confirmation that the requested action has taken place (figure 2.3b).

2.5. Exercise

2.5.1. Multiple choice questions

a. In the OSI reference model, which of the following is true?

i) layers N uses services provided by layer N-1
ii) layer N provides services to layer N+1
iii) layer N communicates with the peer layer N of the target machine
iv) all of the above.

b. In the OSI reference model, physical communication takes place in

i) Transport Layer
ii) Network Layer
iii) Data Link Layer
iv) Physical Layer.

2.5.2. Questions for short answers

a) Name the seven layers of the OSI reference model.
b) What is service access points (SAPs)?
c) What are primitives and parameters?

2.5.3. Analytical questions

a) Discuss the OSI reference model with neat diagram.
b) Discuss the four types of standard primitives used to define the interaction between adjacent layers.

Lesson 3 : Layers of the OSI Model

3.1. Learning Objective

On completion of this lesson you will be able to :

- know the functions of the seven layers of the OSI model
- know useful perspective on OSI architecture.

3.2. Layers of the OSI Model

Physical Layer

The physical layer covers the physical interface between devices and the rules by which bits are passed from one to another. The physical layer has four important characteristics :

The physical layer has four important characteristics.

- Mechanical
- Electrical
- Functional
- Procedural.

Data Link Layer

While the physical layer provides only a raw bit stream service, the data link layer attempts to make the physical link reliable and provides the means to activate, maintain, and deactivate the link. The principal service provided by the data link layer to the higher layers is that of error detection and control. Thus, with a fully functional data link layer protocol, the next higher layer may assume virtually error-free transmission over the link.

Network Layer

The network layer provides the transfer of information between end systems across some sort of communication network. It relieves higher layers of the need to know anything about the underlying data transmission and switching technologies used to connect systems. At this layer, the computer system engages in a dialogue with the network to specify the destination address and to request certain network facilities, such as priority.

Transport Layer

The transport layer ensures that data units are delivered error-free, in sequence, with no losses or duplications. The transport layer may also be concerned with optimizing the use of network services and providing a requested quality of service to session entities. For example, the session entity might specify acceptable error rates, maximum delay, priority, and security. In effect, the transport layer serves as the user's liaison with the communications facility.

Session Layer

The session layer provides the mechanism for controlling the dialogue between applications in end systems. The key services provided by the session layer include :

The key services provided by the session layer include.

- **Dialogue discipline** : This can be full duplex or half duplex.
- **Grouping** : The flow of data can be marked to define groups of data.
- **Recovery** : The session layer can provide a check pointing mechanism, so that if a failure of some sort occurs between checkpoints, the session entity can retransmit all data since the last checkpoint.

Presentation Layer

The presentation layer defines the syntax used between application entities.

The presentation layer is concerned with the syntax of the data exchanged between application entities. Its purpose is to resolve differences in format and data representation. The presentation layer defines the syntax used between application entities and provides for the selection and subsequent modification of the representation to be used.

Application Layer

The application layer provides a means for application process to access the OSI environment. This layer contains management functions and generally useful mechanisms to support distributed applications.

The lower two layers deal with the link between the host and the network. The next three layers are all involved in transferring data from one host to another.

Figure 2.4 provides a useful perspective on the OSI architecture. The annotation along the right-side suggests viewing the seven layers in three parts. The lower three layers contain the logic for a computer to interact with a network. The host is attached physically to the network, uses a data link protocol to reliably communicate with the network, and uses a network protocol to request data exchange with another device on the network and to request network services. Continuing from this perspective, the transport layer provides a reliable end-to-end service regardless of the intervening network facility; in effect, it is the user's liaison to the communications facility. Finally, the upper three layers, taken together, are involved in the exchange of data between end users, making use of a transport service for reliable data transfer.

3.3. Perspective on the OSI Architecture

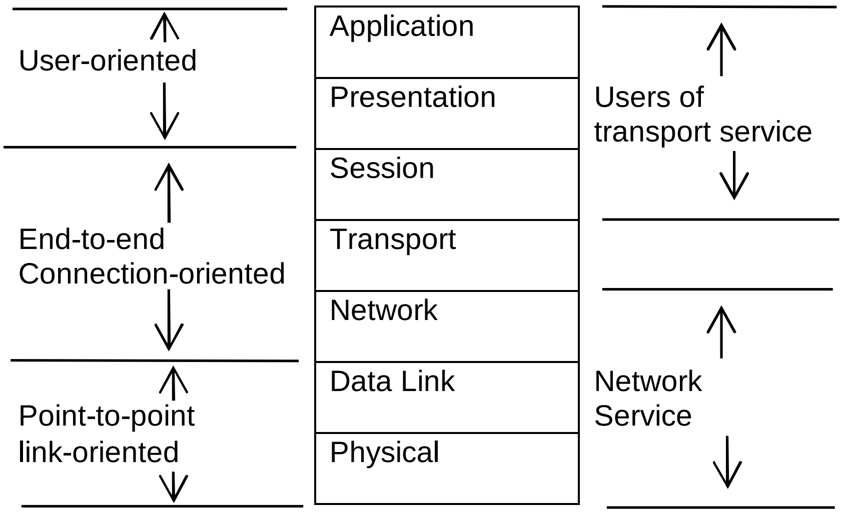


Fig. 2.4 : Perspective on the OSI Architecture.

Another perspective is suggested by the annotation to the left. The lower two layers deal with the link between the host and the network. The next three layers are all involved in transferring data from one host to another: The network layer makes use of the communication network facilities to transfer data from one host to another; the transport layer assures that the transfer is reliable; and the session layer manages the flow of data over the logical connection. Finally, the upper two layers are oriented to the user's concerns, including considerations of the application to be performed and any formatting issues.

3.4. Exercise

3.4.1. Multiple choice questions

a. The physical layer provides

i) only a raw bit stream service
ii) the means to activate, maintain, and deactivate the physical link

iii) for the transfer of information between end systems across some sort of communication network

iv) a means for application process to access the OSI environment.

b. The session layer provides

i) for the transfer of information between end systems across some sort of communication network

ii) the means to activate, maintain, and deactivate the physical link

iii) a means for application process to access the OSI environment

iv) the mechanism for controlling the dialogue between applications in end systems.

3.4.2. Questions for short answers

a) What is the principal service provided by the data link layer to the higher layers?

b) What are the key services provided by the session layer?

c) What is the purpose of the presentation layer?

3.4.3. Analytical questions

a) Briefly discuss the seven layers of OSI model.

b) Discuss the perspective of the OSI architecture.

Lesson 4 : The TCP/IP Protocol Suite

4.1. Learning Objectives

On completion of this lesson you will be able to :

- know the TCP/IP protocol architecture
- grasp the operation of TCP and IP protocols.

4.2. Introduction

The experience already gained in the development and use of protocols within ARPANET has led to the TCP/IP communications architecture. The TCP/IP protocol suite deals with communications among heterogeneous computers.

Four fundamental differences between the TCP/IP protocol suit and the OSI model.

There are four fundamental differences between the TCP/IP protocol suit and the OSI model :

- **Hierarchy versus Layering** : The OSI model is layered, but the TCP/IP protocol suit is modular and hierarchical and gives the designer more freedom to develop efficient, cost-effective, and rich protocols.
- **Internetworking** : Unlike the OSI model, the TCP/IP protocol suit places importance on internetworking between two different networks.
- **Connectionless Service** : A connectionless service is one in which data are transferred from one entity to another without the prior mutual construction of a connection (e.g., datagram). The TCP/IP protocol suit places equal importance on connectionless and connection-oriented services, whereas the OSI model is couched solely in terms of connection-oriented service. A primary use of the connectionless service within the TCP/IP protocol suit is in internetworking.
- **Management Functions** : The TCP/IP protocol suit and the OSI model differently treats the management-related functions.

The TCP/IP protocol suite is based on a view of communication that involves three agents: process, hosts, and networks.

4.3. TCP/IP Protocol Architecture

The TCP/IP protocol suite is based on a view of communication that involves three agents: process, hosts, and networks. **Processes** are the fundamental entities that communicate. A process executes on **hosts**, which can often support multiple simultaneous processes. Communication between processes takes place across **networks** to which the hosts are attached.
These three concepts yield a fundamental principle of the TCP/IP protocol suit: the transfer of information to a process can be accomplished by first getting it to the host in which the process resides and then getting it to the process within the host. These two levels of demultiplexing can be handled independently. Therefore, a network need only be concerned with routing data between hosts, as long as the hosts agree how to direct data to processes.

The protocols are organized into four layers :

- Network access layer
- Internet layer
- Host-host layer
- Process/application layer.

An entity in a layer may use the services of another entity in the same layer, or directly use the services of an entity in a lower but not adjacent layer.

The Network Access Layer

The **network access layer** contains those protocols that provide access to a communication networks. Protocols at this layer are between a communications node and an attached host. A function of all these protocols is to route data between hosts attached to the same network. Other services provided are flow control and error control between hosts, and various quality of service features such as priority and security. A network layer entity is typically invoked by an entity in either the internet or host-host layer, but may be invoked by a process/application layer entity.

A function of all these protocols is to route data between hosts attached to the same network.

The Internet Layer

A gateway is a processor connecting two networks whose primary function is to relay data between networks using an internetworks protocol.

The **internet layer** consists of the procedures required to allow data to traverse multiple networks between hosts. Thus it must provide a routing function. This protocol is usually implemented within hosts and gateways. A **gateway** is a processor connecting two networks whose primary function is to relay data between networks using an internetworks protocol.

The Host-Host layer

The **host-host layer** contains protocol entities with the ability to deliver data between two processes on different host computers. A protocol entity at this level may (or may not) provide a logical connection between higher-level entities. Other possible services include error and flow control and the ability to deal with control signals not associated with a logical data connection.

Four general types of protocols seen to be needed at this level :

- A reliable connection-oriented data protocol
- A datagram protocol
- A speech protocol
- A real-time data protocol.

The Process/Application Layer

TCP/IP protocol

The **process/application layer** contains protocols for resource sharing and remote access. Within the TCP/IP protocol suit architecture, there are the following protocol standards :

- **Internet layer** : **Internet Protocol (IP)**, which provides a connectionless service for end systems to communicate across one or more networks and does not assure the networks to be reliable.
- **Host-to-host layer** : **Transmission Control Protocol (TCP)**, which provides a reliable end-to-end data transfer service.
- **Process/application layer** :

  i) **File Transfer Protocol (FTP)**, which is a simple application for transfer of ASCII, EBCDIC, and binary files.
  ii) **Simple Mail Transfer Protocol (SMTP)**, which is a simple electronic mail facility.
  iii) **Telnet Protocol (TELNET)**, which provides a simple asynchronous terminal capability.

4.4. Operation of TCP and IP

Figure 4.5 indicates how TCP and IP protocols are configured for communications. The total communications facility may consist of multiple networks, the constituent networks are usually referred to as **subnetworks**. Some sort of network access protocol is used to connect a computer to a subnetwork. This protocol enables the host to send data across the subnetwork to another host or, in the case of a host on another subnetwork, to a router. IP is implemented in all of the end systems and the routers. It acts as a relay to move a block of data from one host, through one or more routers, to another host. TCP is implemented only in the end systems; it keeps track of the blocks of data and assure that all are delivered reliably to the appropriate application.

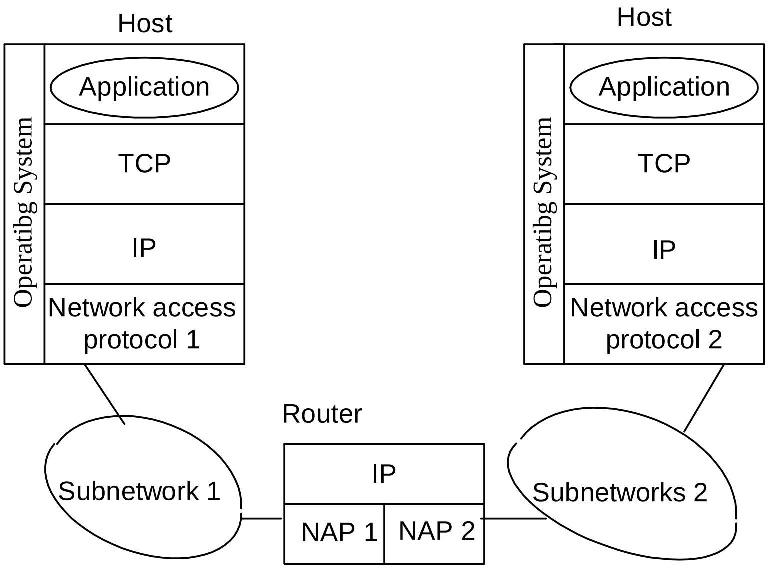


Fig. 4.5 : Communications using the TCP/IP protocol architecture.

Every entity in the overall system must have a unique address.

For successful communication, every entity in the overall system must have a unique address. Actually, two levels of addressing are needed. Each host on a subnetwork must have a unique global internet address; this allows the data to be delivered to the proper host. Each process with a host must have an address that is unique within the host; this allows the host-to-host protocol (TCP) to deliver data to the proper process. These latter addresses are known as **ports**.

Suppose that a process, associated with port 1 at host A, wishes to send a message to another process, associated with port 2 at host B. The process at A hands the message down to TCP with instructions to send it to host B, port 2. TCP hands the message down to IP with instructions to send it to host B. Next, IP hands the message down to the network access layer with instructions to send it to router X.

TCP appends control information known as the TCP header, forming a TCP segment.

To control this operation, control information as well as user data must be transmitted, as in figure 4.6. The sending process generates a block of data and passes this to TCP. TCP may break this block into smaller pieces to make it more manageable. To each of these pieces, TCP appends control information known as the TCP header, forming a **TCP segment**. The control information is to be used by the peer TCP protocol entity at host B. Examples of items that are included in this headed are Destination port, Sequence number, and Checksum.

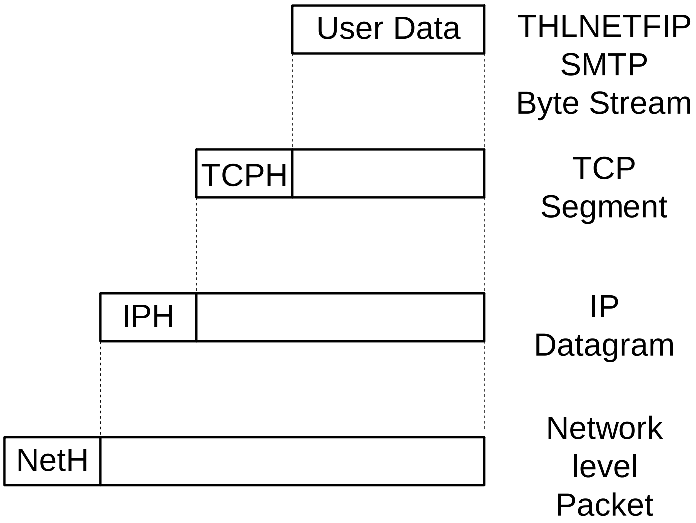


Fig. 4.6 : Protocol data units in the TCP/IP architecture.

Thus IP appends a header of control information to each segment to form an IP

Next, TCP hands each segment over to IP, with instructions to transmit it to B. These segments must be transmitted across one or more subnetworks and relayed through one or more intermediate routers. This operation requires the use of control information. Thus IP appends a header of control information to each segment to form an **IP datagram**. An example of an item stored in the IP header is the destination host address.

Finally, each IP datagram is presented to the network access layer for transmission across the first subnetwork in its journey to the destination. The network access layer appends its own header, creating a packet, or frame. The packet is transmitted acroos the subnetwork to router X. The packet header contains the information that the subnetwork needs to transfer the data across the subnetwork. Examples of items that may be contained in this header include Destination subnetwork address and Facilities requested.

At router X, the packet header is stripped off and the PP header examined. On the basis of the destination address information in the IP header, the router directs the datagram out across subnetwork 2 to B. To do this, the datagram is again augmented with a network access header.

When the data are received at B, the reverse process occurs. At each layer, the corresponding header is removed, and the remainder is passed on to the next higher layer until the original user data are delivered to the destination process.

4.5. Exercise

4.5.1. Multiple choice questions

a. A function of networks access layer protocols is to route data between

i) hosts attached to the same network
ii) hosts attached to different networks
iii) routers of different networks
iv) none of the above.

b. The host-host layer contain protocol entities with the ability to deliver data between

i) the process on the host and the process on the router
ii) two processes on different routers
iii) two processes on different host computers
iv) none of the above.

4.5.2. Questions for short answers

a) Define process, hosts, and networks with respect to TCP/IP protocol architecture.
b) What is a gateway?
c) Name the general types of protocols seen to be needed at host-host layer.
d) What is a subnetwork?
e) What is a port?

4.5.3. Analytical questions

a) Briefly discuss the differences between the TCP/IP protocol suit and the OSI model.
b) Discuss the layers of the TCP/IP protocol architecture.

c) Discuss the protocol standards within the TCP/IP protocol suit architecture.

d) Discuss the operation of TCP and IP protocols with suitable diagram.

Unit 3 : Data Transmission Fundamentals

Introduction

The major task of a computer network is to perform data communications between two hosts (computers), between two routers, or between host and routers. In this unit, elementary concepts of data and transmission are introduced. Transmission impairments and the maximum possible data rate of a transmission channel are presented. Transmission media and various transmission systems are also presented in this unit.

Lesson 1 : Basic Concepts

1.1. Learning Objectives

On completion of this lesson you will be able to:

- grasp the elementary concepts of data communications
- know the basic definitions pertaining to data communications.

1.2. A Communications Model

The fundamental purpose of data communications is to exchange information between two agents (hosts or routers) that are directly connected by a single transmission path.

The fundamental purpose of data communications is to exchange information between two agents.

Data: Data is a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human beings or by computers.

Information: Information is the meaning that is currently assigned to data by means of the conventions applied to these data.

A block diagram of a simplified communications system is shown in figure 3.1.

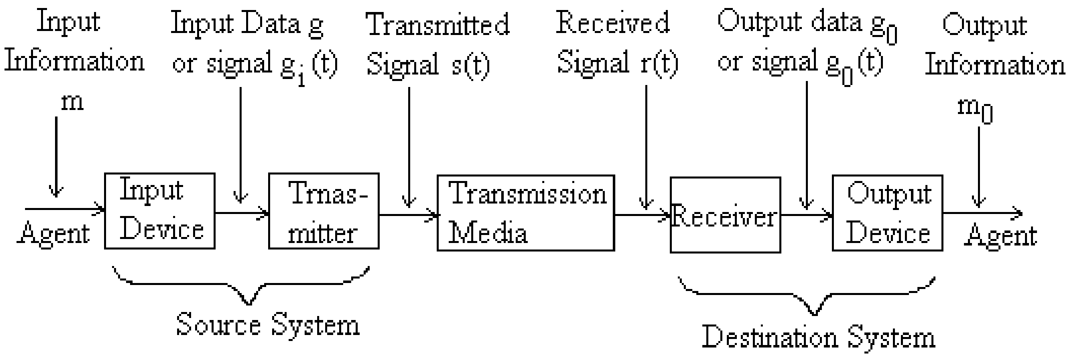


Fig. 3.1: Block diagram of a simplified communications system.

Concept of Analog and Digital

In figure 3.1, the information to be exchanged is a message labeled m. This information is represented as data g and is generally presented to a transmitter in the form of a time-varying signal, $g_i(t)$. The signal $g_i(t)$ is to be transmitted. Generally, the signal will not be in a form suitable for transmission and must be converted to a signal s(t) that is in some sense matched to the characteristics of the transmission medium. This sort of conversion is known as data encoding. The signal s(t) is then transmitted across the transmission medium. On the other end, a signal r(t) is received. This signal is then converted by a receiver into a form suitable for output. The converted signal $g_o(t)$, or data g_o, is an approximation of the input. Finally, the output device presents the approximated message, m_o, to the destination agent.

In a data communications system, the following concepts are very important:

- Data are entities that convey meaning.
- Signals are electric or electromagnetic encoding of data.
- Signaling is the act of propagating the signal along a suitable medium.
- Transmission is the communication of data by the propagation and processing of signals.

1.3. Concept of Analog and Digital

Analog Data: Analog data take on continuous values on some interval. For example, voice and video are continuously varying patterns of intensity.

Digital Data: Digital data take on discrete values. For example, text and integers are discrete.

Analog Signal: An analog signal is a continuously varying electromagnetic wave that may be propagated over a variety of media.

Digital Signal: A digital signal is a sequence of voltage pulses that may be transmitted over a medium. For example, a constant positive voltage level may represent binary 1 and a constant negative voltage level may represent binary 0.

Types of Data Transmission

Analog Transmission: Analog transmission is a means of transmitting analog signals without regard to their content; the signal may represent analog data or digital data.

Digital Transmission: Digital transmission is a means of transmitting digital signals.

1.4. Types of Data Transmission

Simplex Data Transmission: In simplex data transmission, signals are transmitted in only one direction; one station is transmitter and the other is receiver.

Half-Duplex Data Transmission: In Half-duplex data transmission, both station may transmit, but only one at a time.

Full-Duplex Data Transmission: In full-duplex data transmission, both stations may transmit simultaneously. In this case, the medium is carrying signals in both directions at the same time.

1.5. Exercise

1.5.1. Multiple choice questions

a. The fundamental purpose of data communications is to exchange information

i) among many agents connected by many lines
ii) between two agents connected by a single line
iii) among three agents connected by two lines
iv) none of the above.

b. Digital data take on

i) continuos values on an interval
ii) discrete values
iii) combination of continuos and discrete values
iv) none of the above.

1.5.2. Questions for short answers

a) What do you mean by data?
b) What do you mean by information?
c) What are signal and signaling?
d) What do you mean by transmission?

1.5.3. Analytical questions

a) Describe the simplified model of data communications.
b) Discuss the difference between analog and digital data.
c) Discuss the difference between analog and digital signaling.
d) Discuss the difference between analog and digital transmission.
e) Discuss different types of data transmission.

Lesson 2 : Frequency-Domain Consideration and Transmission Impairments

2.1. Learning Objectives

On completion of this lesson you will be able to:

- grasp the frequency-domain concept of signal
- know the different impairments of a transmission channel
- know the maximum data rate or capacity of a channel.

2.2. Frequency-Domain Concepts of Signals

A signal s(t) is a function of time. But it can also be expressed as a function of frequency. From Fourier Series analysis, we know that any signal is made up of components at various frequencies, in which each component is a sinusoid.

The **spectrum** of a signal is the range of frequencies that it contains.

Frequency-Domain Concepts of Signals

The **absolute bandwidth** of a signal is the width of the spectrum, that is, the difference between the highest and the lowest frequencies of the spectrum.

Many signals have an infinite bandwidth. However, most of the energy in the signal is contained in a relatively narrow band of frequencies. This band is referred to as the effective bandwidth, or just **bandwidth**.

If a signal includes a component of zero frequency, that component is a direct current (dc) or constant component. Although a given waveform may contain frequencies over a very broad range, as a practical matter any transmission medium that is used will be able to accommodate only a limited band of frequencies. This in turn limits the data rate that can be carried on the transmission medium. In general, any digital waveform will have infinite bandwidth. If we attempt to transmit this waveform as a signal over any medium, the nature of the medium will limit bandwidth that can be transmitted. This limiting of bandwidth will introduce distortion of the waveform and thus will introduce error in the receiver.

2.3. Transmission Impairments

With any communication system, the signal that is received will differ from the signal that is transmitted due to various transmission impairments. The most significant impairments are :

- ♦ Attenuation and attenuation distortion
- ♦ Delay distortion
- ♦ Noise.

The signal that is received will differ from the signal that is transmitted due to various transmission impairments.

Attenuation: The strength of a signal falls off with distance over any transmission medium. Attenuation of signal strength is higher for high frequency signals. If the signal strength falls below a certain level, the transmitter fails to recognize the signal.

Delay Distortion: The velocity of propagation of a signal through a medium varies with frequency. Thus various frequency components of a signal will arrive at the receiver at different times. The received signal is distorted due to variable delay in its components. This effect is referred to as delay distortion.

Noise: Sometimes the received signal may consist of the transmitted signal plus additional unwanted signals that are inserted somewhere between transmission and reception. These undesired signals are referred to as noise.

2.4. Channel Capacity

The rate at which digital data can be transmitted over a given communication path, or channel, under given conditions, is referred to as the channel capacity. In a finite bandwidth noise-free channel, the limitation on data rate is simply the bandwidth of the signal. Nyquist's formula for maximum data rate in a finite bandwidth noise-free channel is given below

The rate at which digital data can be transmitted over a given communication path, or channel, under given conditions, is referred to as the channel capacity.

$$C = 2W \log_2 M \qquad (3.1)$$

where C is the capacity or the maximum data rate of the channel in bits/sec (bps), W is the bandwidth of the channel in cycles/sec (Hz), and M is the number of discrete signal or voltage levels of the signal.

As a numerical example, if 8-level discrete signal is used and the bandwidth of the channel is 3100Hz, the $C = 2 \times 3100 \log_2 8 = 18{,}600$ bps, that is, the maximum possible data rate in this channel is 18,600 bps.

If a 2-level discrete (binary) signal is used, the equation (3.1) reduces to

$$C = 2W \qquad (3.2)$$

For a binary digital signal, the highest data rate that can be carried is 2W bps for a channel with W Hz bandwidth.

As a numerical example, if the bandwidth of the channel is 3100Hz, then C = 2 x 3100 = 6,200 bps, that is, the maximum possible data rate in this channel is 6,200 bps.

It must be noted that for error-free transmission, the bandwidth of the signal must not exceed the bandwidth of the channel.

For error-free transmission, the bandwidth of the signal must not exceed the bandwidth of the channel.

Shannon's formula for the maximum data rate in a finite-bandwidth noisy-channel is given below

$$C = W \log_2 (1 + S/N) \qquad (3.3)$$

where C is the capacity or the maximum data rate of the channel in bps, W is the bandwidth of the channel in Hz, S is the power in the signal and N is the power in the noise.

S/N is referred to as **signal-to-noise ratio** and often reported in decibels:

$$(S / N)_{dB} = 10 \log \frac{Signal\ Power}{Noise\ Power} = 10 \log \frac{S}{N} \qquad (3.4)$$

As a numerical example, suppose that the bandwidth of a channel is 3100Hz and S/N is 30dB. Here

$$30 = 10 \log S/N$$
$$\text{or} \quad S/N = \log^{-1} (30/10) = 1000$$

Then, $C = 3100 \log_2 (1 + 1000) = 30{,}898$ bps.

2.5. Exercise

2.5.1. Multiple choice questions

a. The spectrum of a signal is

i) the difference between the highest frequency and the lowest frequency of the signal.
ii) the range of frequencies of the signal.
iii) the power of the frequency components of the signal.
iv) none of the above.

b. The dc component of a signal is the component of the signal

i) where frequency is zero.
ii) where frequency is the lowest.
iii) where frequency is the highest.
iv) none of the above.
c. In general, a digital waveform has

i) finite bandwidth.
ii) infinite bandwidth.
iii) zero bandwidth.
iv) none of the above.

d. Attenuation of a signal strength is

i) lower for higher frequency
ii) higher for lower frequency
iii) higher for higher frequency
iv) none of the above.

2.5.2. Questions for short answers

a) Give the names of the most important transmission impairments.
b) State Nyquist's formula for capacity of a finite bandwidth noise-free channel.
c) State Shannon's formula for capacity in a finite-bandwidth noisy-channel.

2.5.3. Analytical questions

a) What is the difference between absolute bandwidth and effective bandwidth.
b) Discuss the various transmission impairments that affect the transmission of digital data.
c) The bandwidth of a given channel is 1600Hz. If 16 discrete levels are used for signal encoding, what will be the maximum data rate of the channel in bps?
d) The bandwidth of a given channel is 1600Hz. If the signal-to-noise ratio is 20dB, what will be the maximum data rate of the channel in bps?

Lesson 3 : Metallic Transmission Media

3.1. Learning Objectives

On completion of this lesson you will be able to:

- ♦ learn basic concepts of transmission media
- ♦ classify the transmission media
- ♦ grasp the physical description, uses and transmission characteristics of two commonly used types of metallic transmission media.

3.2. Introduction to Transmission Media

The characteristics and quality of data transmission are determined both by the nature of the signal and the nature of the medium.

The transmission medium is the physical path between transmitter and receiver in a data transmission system. The characteristics and quality of data transmission are determined both by the nature of the signal and the nature of the medium. Transmission media are of two types: Guided Media and Unguided Media. Guided media is subdivided into two groups: Metallic transmission media and Optical fiber. Commonly used metallic transmission media are twisted pair and coaxial cables. Commonly used unguided transmission techniques are terrestrial microwave, satellite microwave and radio.

3.3. Twisted Pair

Physical Description

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern (as shown in figure 3.2).

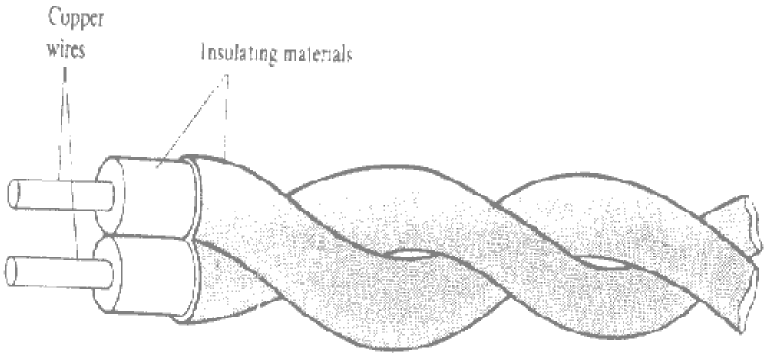


Figure 3.2 : Twisted-pair wire configuration.

A wire pair acts as a single communication link. Typically, a number of these pairs are bundled together into a cable by wrapping them in a tough protective sheath. The twisting of the individual pairs minimizes electromagnetic interference between the pairs.

The twisting of the individual pairs minimizes electromagnetic interference between the pairs.

Uses

By far the most common transmission medium for both analog and digital data is twisted pair. It is the backbone of the telephone system as well as the workhorse for intrabuilding communications.

Transmission Characteristics

Wire pairs may be used to transmit both analog and digital signals. For analog signals, amplifiers are required about every 5 to 6 km. For digital signals, repeaters are used every 2 or 3 km. For point-to-point analog signaling, a bandwidth of up to about 250 kHz is possible. For digital point-to-point lines, data rates of up to a few Mbps are possible.

3.4. Coaxial Cable

Physical Description

A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often as a closely woven braided mesh. The outer conductor is covered in a protective plastic sheath. A cutaway view of a coaxial cable is shown in figure 3.3.

Wire pairs may be used to transmit both analog and digital signals.

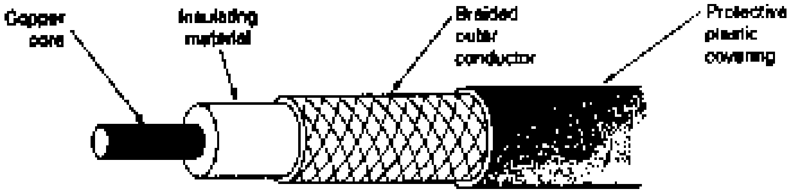


Fig. 3.3: A coaxial cable.

Uses

Coaxial cable has been perhaps the most versatile transmission medium and is enjoying utilization in a wide variety of applications. The most important of these are :

- Long-distance telephone and television transmission
- Television distribution
- Local area networks
- Short-run system links.

Transmission Characteristics

Coaxial cable is used to transmit both analog and digital signals. Coaxial cable has superior frequency characteristics to twisted pair, and can hence be used effectively at higher frequencies and data rates.

For long-distance transmission of analog signals, amplifiers are needed every few kilometers.

For long-distance transmission of analog signals, amplifiers are needed every few kilometers, with closer spacing requirement if higher frequencies are used. The usable spectrum for analog signaling extends to about 400 MHz. For digital signaling, repeaters are needed every kilometers or so, with closer spacing needed for higher data rates. On experimental systems, data rates as high as 800 Mbps have been achieved with a repeater spacing of 1.6 km.

3.5. Exercise

3.5.1. Multiple choice questions

a. The characteristics and quality of data transmission are determined by

i) the nature of the signal
ii) the nature of the medium
iii) both the nature of the signal and the nature of the medium
iv) none of the above.

b. Commonly used metallic transmission media are

i) twisted pair, coaxial cable and optical fiber.
ii) twisted pair and coaxial cable.
iii) optical fiber and microwave.
iv) microwave and radio.

c. Commonly used unguided transmission technologies are

i) terrestrial microwave, satellite microwave and radio.
ii) optical fiber, microwave and radio.
iii) coaxial cable, optical fiber and microwave.
iv) coaxial cable, microwave and radio.

d. The most commonly used transmission medium for both analog and digital data is

i) twisted pair
ii) coaxial cable
iii) optical fiber
iv) none of the above.

3.5.2. Questions for short answers

a) What is a transmission medium?
b) Give the names of different metallic transmission media.
c) Give the names of different unguided transmission techniques.
d) Why are pairs of wires twisted in twisted pair?
e) Name the applications of coaxial cable.

3.5.3. Analytical questions

a) Classify the transmission media.
b) Discuss the physical construction, uses, and transmission characteristics of twisted pair.
c) Discuss the physical construction, uses, and transmission characteristics of coaxial cable.

Lesson 4 : Optical Fiber

4.1. Learning Objective

On completion of this lesson you will be able to:

- grasp physical description,
- uses and transmission characteristics
- of optical fiber.

4.2. Optical Fiber

Physical Description

An optical fiber cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket.

An optical fiber is a thin, flexible medium capable of conducting an optical ray. An optical fiber cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket. The core is the innermost section and consists of one or more very thin strands, or fibers, made of glass or plastic. Each fiber is surrounded by its own cladding, a glass or plastic coating that has optical properties different from those of the core. The outermost layer, surrounding one or a bundle of cladded fibers, is the jacket. The jacket is composed of plastic and other materials layered to protect against moisture, abrasion, crushing, and other environmental dangers. A cutaway view of an optical fiber is shown in figure 3.4.

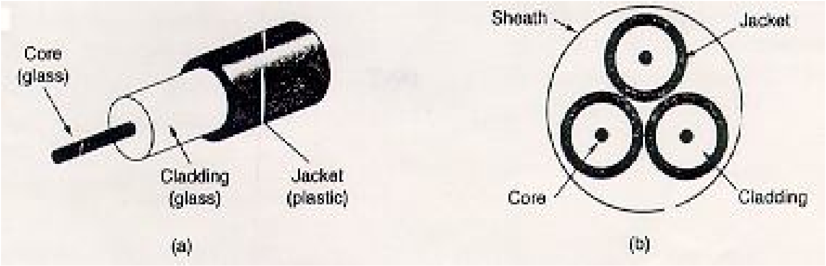


Fig. 3.4: (a) Side view of a single fiber. (b) End view of a sheath with three fibers.

Uses

The following characteristics distinguish optical fiber from twisted pair and coaxial cable:

- Greater bandwidth
- Smaller size and higher weight
- Lower attenuation

- Electromagnetic isolation
- Greater repeater spacing.

Five basic categories of applications have become important for optical fiber:

- Long-haul trunks
- Metropolitan trunks
- Rural exchange trunks
- Local loops
- Local area networks.

Transmission Characteristics

Optical fiber transmit a signal-encoded beam of light by means of total internal reflection. In effect, the optical fiber acts as a waveguide for frequencies in the range 10^{14} to 10^{15} Hz, which covers the visible spectrum and part of the infrared spectrum.

Optical fiber transmit a signal-encoded beam of light by means of total internal reflection.

Light from a source enters the cylindrical glass or plastic core. Rays at shallow angles are reflected and propagated along the fiber; other rays are absorbed by the surrounding material. Two different types of light source are used in fiber optic systems: the light emitting diode (LED) and the injection laser diode (ILD). Both are semiconductor devices that emit a beam of light when a voltage is applied. The detector used at the receiving end to convert the light into electrical energy is a photodiode.

In optical fiber, light propagates best in three distinct wavelength “windows”, centered on 850, 1300, and 1500 nanometers (nm). These are all in the infrared portion of the frequency spectrum. Most local application today use 850 nm LED light sources. It is generally limited to data rates under 100 Mbps and distance of a few km. To achieve higher data rates and longer distances, a 1300 nm LED or laser source is needed. The highest data rates and longest distances require 1500 nm laser sources.

4.3. Exercise

4.3.1. Multiple choice questions

a. Which of the following is used as light source in optical fiber systems?

i) Light Emitting Diode (LED) only.
ii) Injection Laser Diode (ILD) only.
iii) Both Light Emitting Diode (LED) and Injection Laser Diode (ILD).
iv) none of the above.

4.3.2. Questions for short answers

a) Give the names of applications of optical fiber.
b) Mention the characteristics that distinguish optical fiber from twisted pair and coaxial cable.

4.3.3. Analytical question

a) Discuss the physical construction, uses, and transmission characteristics of optical fiber.

Lesson 5 : Unguided Transmission Techniques

5.1. Learning Objective

On completion of this lesson you will be able to:

- grasp the physical description
- uses of three types of unguided transmission techniques
- transmission characteristics of three break into three sections.

5.2. Terrestrial Microwave

Physical Description

Microwave is commonly used for both voice and television transmission.

In terrestrial microwave, an antenna is fixed rigidly and focuses a narrow beam to achieve line-of-sight transmission to the receiving antenna. Two microwave antennas at a height of 100m may be as far as 82 km apart. To achieve long-distance transmission, a series of microwave relay towers is used.

Uses

The primary uses for terrestrial microwave systems is in long-haul telecommunications service. Microwave can support high data rates over long distances. Microwave is commonly used for both voice and television transmission. Another common use of microwave is for short point-to-point links between buildings for closed-circuit TV or as a data link between local networks. A potential use for terrestrial microwave is for providing digital data transmission in small region.

Transmission Characteristics

The higher the frequency used, the higher the potential bandwidth and therefore the higher the potential data rate.

The common frequencies used for microwave transmission are in the range 2 to 40 GHz. The higher the frequency used, the higher the potential bandwidth and therefore the higher the potential data rate. Bandwidth and data rate for some typical microwave systems are shown in table 2.1.

Table 2.1: Typical Digital Microwave Performances

Band (GHz)	Bandwidth (MHz)	Data Rate (Mbps)
2	7	12
6	30	90
11	40	90
18	220	274

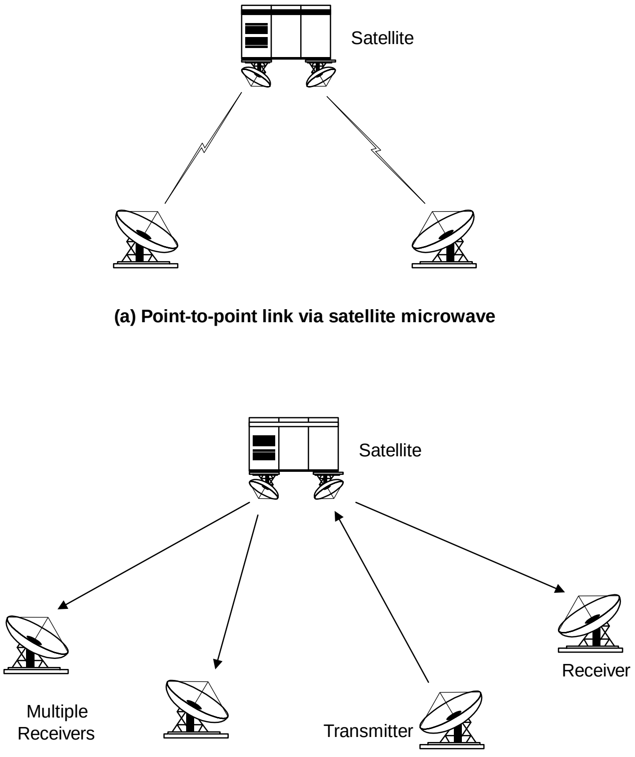
5.3. Satellite Microwave

Physical Description

A communication satellite is, in effect, a microwave relay station. It is used to link two or more ground-based microwave transmitter/receivers, know as earth stations or ground stations. The satellite receives transmission on one frequency band (up link), amplifies the signal for analog transmission or repeats the signal for digital transmission, and transmits it on another frequency (down link). A single orbiting satellite will operate on a number of frequency bands, called transponder channels, or simply transponder.

Two common uses of communications satellite are depicted in figure 3.5.

A single orbiting satellite will operate on a number of frequency bands, called transponder channels, or simply transponder.



(a) Point-to-point link via satellite microwave

(b) Broadcast link via satellite microwave

Fig. 3.5: Satellite communications configurations.

In the first use, the satellite is being used to provide a point-to-point link between two distant ground-based antennas. In the second use, the satellite provides communication between one ground-based transmitter and a number of ground-based receivers.

The very small aperture terminal (VSAT) system.

A recent development is the very small aperture terminal (VSAT) system. A typical VSAT configuration is depicted in figure 3.6.

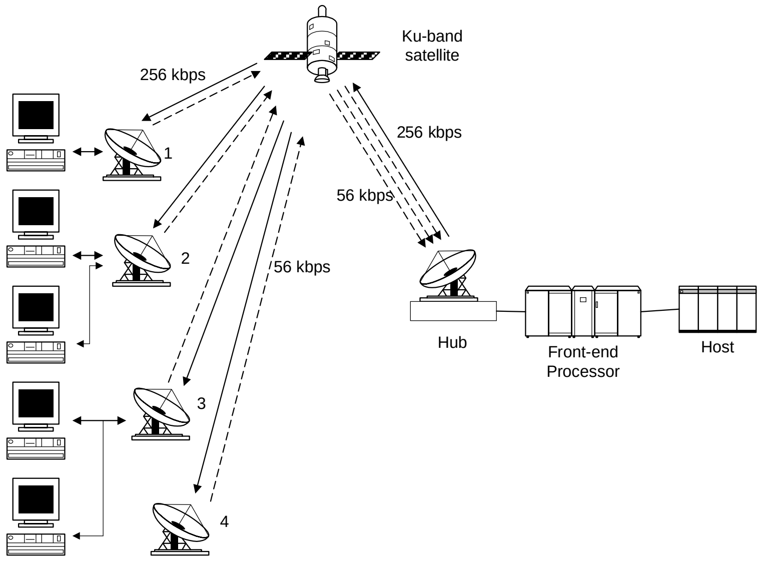


Fig. 3.6: VSAT configuration.

A number of subscriber stations are equipped with low-cost VSAT antennas. These stations share a satellite transmission capacity for transmission to a hub station. The hub station can exchange messages with each of the subscribers and can relay messages between subscribers.

To remain stationary, the satellite must have a period of rotation equal to the earth's period of rotation.

For a communication satellite to function effectively, it is generally required that it remains stationary with respect to its position over the earth. To remain stationary, the satellite must have a period of rotation equal to the earth's period of rotation. This match occurs at a height of 35,784 km.

Uses

The most important application for communications satellite are :

- Television distribution
- Long-distance telephone transmission.

Transmission Characteristics

The optimum frequency range for satellite transmission is the range 1 to 10 GHz. Most satellites providing point-to-point service today use a frequency bandwidth in the range 5.925 to 6.425 GHz for transmission from earth to satellite (up link) and a bandwidth in the range 3.7 to 4.2 GHz for transmission from satellite to earth (down link). This combination is referred to as the 4/6 GHz band, or C band.

5. 4. Radio

Physical Description

Radio is omnidirectional and the antennas need not be rigidly mounted to a precise alignment.

Uses

Radio covers 30MHz to 1 GHz band. This range covers FM radio and VHF and UHF television. A well-known use of radio for digital data communications is packet radio. A packet radio system uses ground-based antennas to link multiple sites in a data transmission network.

Transmission Characteristics

The range 30 MHz to 1 GHz is a very effective one for broadcast radio communications.

The range 30 MHz to 1 GHz is a very effective one for broadcast radio communications. The transmission is limited to the line of sight and distant transmitters will not interfere with each other due to reflection from the atmosphere. For digital communications, lower data rates are achieved in the kilobit range. Radio waves suffer less attenuation.

5.5. Exercise

5.5.1. Multiple choice questions

a. Two microwave antennas at a height of 100m may be as far as

i) 82 km
ii) 100 km
iii) 82 m
iv) 100 m.

b. The common frequencies used for microwave transmission are in the range of

i) 30 MHz to 1 GHz
ii) 2 to 40 GHz
iii) 0 to 30 MHz
iv) none of the above.

c. The common frequencies used for broadcast radio communications are in the range of

i) 30 MHz to 1 GHz
ii) 2 to 40 GHz
iii) 0 to 30 MHz
iv) none of the above.

5.5.2. Questions for short answers

b) What are the primary uses for terrestrial microwave?
c) What do you mean by up link and down link of a communication satellite?
d) What is a transponder?
e) At what height does a satellite remain stationary with respect to earth station?

5.5.3. Analytical questions

a) Discuss physical description, uses, and transmission characteristics of terrestrial microwave.
b) Discuss physical description, uses, and transmission characteristics of satellite microwave.
c) Discuss physical description, uses, and transmission characteristics of radio.
d) Briefly discuss the VSAT system.

Lesson 6 : Transmission Systems

6.1. Learning Objective

On completion of this lesson you will be able to:

- know the different types of transmission systems
- uses of transmission systems.

6.2. Types of Transmission Systems

Voice-Band Transmission System

The voice-grade channel of already existing worldwide and ubiquitous telephone networks is extensively used for data communications over long distances. Telephone networks evolved with the objective of providing good quality analog voice communication and for this reason the bandwidth is kept to 4000 Hz to accommodate the voice band of 300 to 3400 Hz. Analog signaling is mainly used and using suitable modulation of the signal an average data rate of 2400 bps can be achieved. Higher data rates can be achieved using advanced modulation techniques. The voice band transmission is bi-directional.

Baseband Transmission System

Baseband systems can extend only a limited distance, about a kilometer at most.

A baseband transmission system is defined as one that uses digital signaling. Digital signals are inserted on the line as voltage pulses. The entire frequency spectrum of the medium is used to form the signal. Transmission is bi-directional. The digital signaling requires a bus topology. Baseband systems can extend only a limited distance, about a kilometer at most.

The most popular form of baseband system uses coaxial cable. Most baseband coaxial systems use 50-ohm cable. Using 50-ohm cable with a 0.4-inch diameter, a data rate of 10 Mbps is achieved for a cable distance of 500 meters. To extend the length of the network, a repeater may be used between two segments.

Broadband Transmission System

A broadband transmission system is defined as one that uses analog signaling. In broadband system frequency-division multiplexing is possible. The frequency spectrum of the cable can be divided into channels or sections of bandwidth.

Separate channels can support data traffic, TV, or radio signals. A distance of tens of kilometers are possible with broadband system. Broadband is inherently a unidirectional medium. This unidirectional property means that only those stations downstream from a transmitting station can receive its signals. To achieve full connectivity, two data paths are needed. These paths are joined at a point on the network known as the headend. All stations transmit on one path toward the headend (inbound). Signals received at the headend are then propagated along a second data path away from the headend (outbound). All stations receive on the outbound path. Broadband systems use 75-ohm coaxial cable. Broadband is suitable for tens of kilometers' radius from the headend. The broadband system can be used to carry multiple channels, some used for analog signals, such as video and voice, and some for digital. Digital channels can generally carry a data rate of somewhere between 0.25 and 1 bps/Hz.

A distance of tens of kilometers are possible with broadband system.

Carrierband Transmission System

An abridged form of broadband, known as single-channel broadband or carrierband, is one in which the entire spectrum of the cable is devoted to a single transmission path for analog signals. In a single-channel broadband system, bi-directional transmission is employed using a bus topology. Hence there is no need for a headend.

6.3. Exercise

6.3.1. Multiple choice questions

a. Analog signaling is used in

i) voiceband transmission system only
ii) Baseband transmission system only
iii) Broadband transmission system only
iv) voiceband, broadband and carrierband transmission systems.

b. Digital signaling is used in

i) voiceband transmission system only.
ii) voiceband, baseband, broadband and carrierband transmission systems.
iii) carrierband transmission system only.
iv) baseband transmission system only.

6.3.2. Questions for short answers

a) What is the distance limit of a baseband transmission system?

b) What is the distance limit of a broadband transmission system?

c) What is a headend?

6.3.3. Analytical question

a) Briefly discuss various types of transmission systems.

Unit 4 : Data Encoding

Introduction

The main task of a data communications system is to transmit data over a physical transmission medium. The data to be transmitted may be either analog or digital data and is generally presented as a time-varying signal. The data signals will not be in a form suitable for transmission and must be converted to a signal that is in some sense matched to the characteristics of the physical transmission medium. Therefore, data encoding is required to achieve this sorts of conversion. The transmitted signal may be either analog or digital. Either form of data can be encoded into either form of signal. In this unit four types of data encoding are discussed.

Lesson 1 : Encoding of Digital Data into Digital Signals

1.1. Learning Objectives

On completion of this lesson you will be able to :

- learn basic definitions regarding digital encoding of digital data
- understand different techniques of digital encoding of digital data.

1.2. Basic Definitions and Concepts

Definitions and Concepts

Signal Element : A digital signal is a sequence of discrete, discontinuous voltage pulses. Each pulse is a signal element. Binary data are transmitted by encoding each data bit into signal elements.

Unipolar Signal : If the signal elements all have the same algebraic sign, that is, all positive or negative, then the signal is unipolar.

Bipolar : In bipolar signal, one logic state is represented by a positive voltage level, and the other by a negative voltage level.

Data Signaling Rate : The data signaling rate, or just rate, of a signal is the rate, in bits per second, that data are transmitted.

Bit Duration : The bit duration is the amount of time it takes for the transmitter to emit the bit. For a data rate R, the bit duration is 1/R.

Modulation Rate : The modulation rate is the rate at which signal level is changed. The modulation rate is expressed in baud, which means signal elements per second.

Mark and Space : The terms mark and space refer to the binary digit 1 and 0 respectively.

Digital encoding of digital data is generally used to generate or interpret digital data by terminals and other devices. It is also used for digital magnetic recording.

1.3. Techniques of Digital Encoding of Digital Data

Nonreturn-to-Zero-Level (NRZ-L) Coding

In this coding, two different voltage levels are used for the two binary digits as stated below :

Techniques of Digital Encoding

0 = high voltage level (more commonly a positive voltage level).
1 = low voltage level (more commonly a negative voltage level).

The voltage level remains constant for a bit duration.

This code is illustrated in figure 4.1.

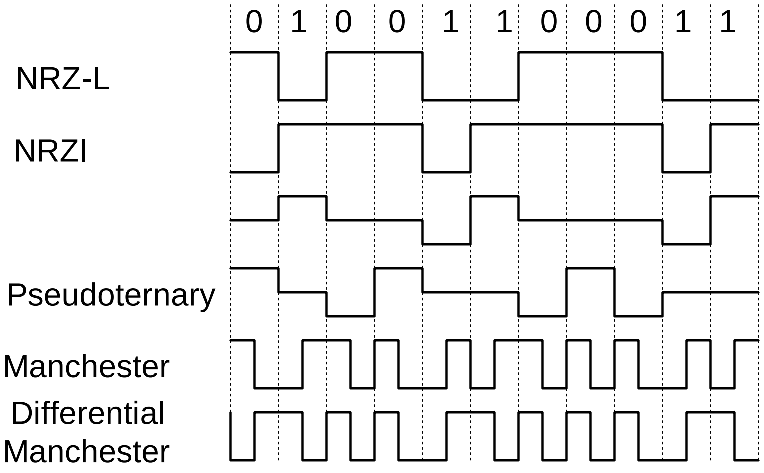


Fig. 4.1 : Digital signal encoding formats.

Nonreturn-to-Zero Inverted (NRZI) Coding

NRZI is a variation of NRZ. It maintains a constant voltage pulse for bit duration. The data are encoded as the presence or absence of a signal transition at the beginning of the bit duration as below:

0 = no transition at the beginning of bit duration.
1 = transition at the beginning of bit duration.

This code is illustrated in figure 4.1.

Bipolar-alternate mark inversion (Bipolar-AMI) Coding

In Bipolar-AMI coding, binary digit are represented as below :

0 = no line signal.
1 = positive or negative voltage level, alternating for successive ones.

This code is illustrated in figure 4.1.

Pseudoternary Coding

In pseudoternary coding, binary digits are represented as below:

0 = positive or negative voltage level, alternating for successive zeros.
1 = no line signal.

This code is illustrated in figure 4.1.

Manchester Coding

In the Manchester code, there is a transition at the middle of each bit duration and a binary digit is represented as below :

0 = transition from high to low in middle of bit duration.
1 = transition from low to high in middle of bit duration.

This code is illustrated in figure 4.1.

Differential Manchester Coding

In Differential Manchester code, there is always a transition at the middle of each bit duration and a binary digit is represented as below :

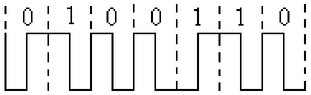
0 = transition at beginning of bit duration.
1 = no transition at beginning of bit duration.

This code is illustrated in figure 4.1.

1.4. Exercise

1.4.1. Multiple choice questions

a. The code depicted in the following figure uses



i) NRZ-L coding

ii) Bipolar-AMI coding

iii) Manchester coding

iv) Differential Manchester coding.

b. In NRZI coding, a 0 is represented by

i) no transition at beginning of bit duration

ii) transition from high to low in middle of bit duration

iii) transition at beginning of bit duration

iv) none of the above.

1.4.2. Questions for short answers

a) What is a signal element?

b) What is data rate?

c) What is bit duration?

d) Give the Manchester code for the binary string 0100110.

1.4.3. Analytical question

a) Discuss the various schemes of digital encoding of digital data.

Lesson 2 : Encoding of Digital Data into Analog Signals

2.1. Learning Objectives

On completion of this lesson you will be able to :

- understand different techniques of analog encoding of digital data.

2.2. Techniques of Analog Encoding of Digital Data

In analog encoding of digital data, modulation of carrier signal is involved. Modulation involves operation on one or more of the three characteristics of a carrier signal: amplitude, frequency, and phase. Accordingly, there are three encoding or modulation techniques for transmitting digital data into analog signals :

- Amplitude-shift keying (ASK)
- Frequency-shift keying (FSK)
- Phase-shift keying (PSK).

In all these cases, the resulting signal occupies a bandwidth centered on the carrier frequency.

Amplitude-Shift Keying (ASK)

In ASK, the two binary digits are represented by two different amplitudes of the carrier frequency.

In ASK, the two binary digits are represented by two different amplitudes of the carrier frequency. Binary digit 1 is represented by the presence, at constant amplitude, of the carrier, and binary 0 is represented by the absence of the carrier.

This encoding is illustrated in figure 4.2.

On voice-grade lines, ASK is typically used only up to 1200 bps. This technique is also used to transmit digital data over optical fiber.

Frequency-Shift Keying (FSK)

In FSK, the two binary digits are represented by two different frequencies near the carrier frequency. This encoding scheme is illustrated in figure 4.2. On voice-grade lines, FSK is typically used up to 1200 bps. It is also commonly used for high-frequency (3 to 30 MHz) radio transmission.

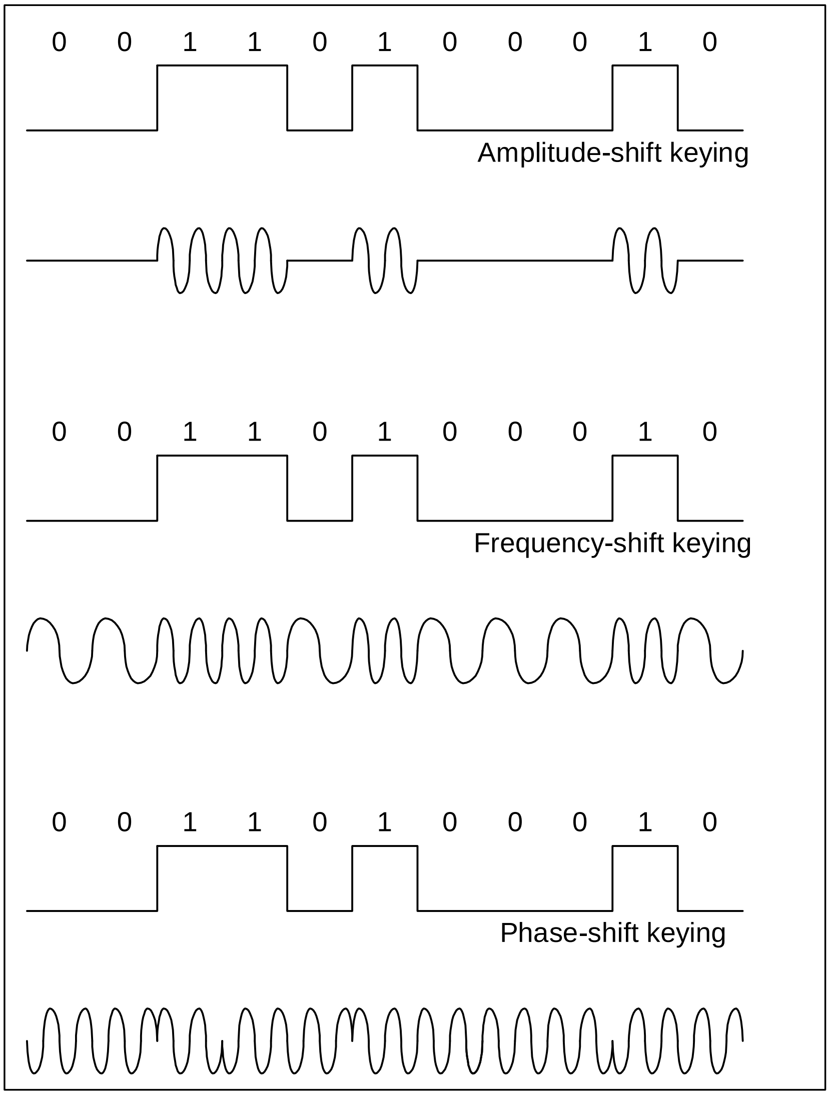


Fig. 4.2 : Modulation of analog signals for digital data.

Phase-Shift Keying (PSK)

In PSK, the phase of the carrier signal shifted to represent data. In this system, a binary 0 is represented by sending a signal burst of the same phase as the previous signal burst sent. A binary 1 is represented by sending a signal burst of opposite phase to the preceding one.

This encoding scheme is illustrated in figure 4.2.

2.3. Exercise

2.3.1. Multiple choice questions

a. In ASK, the following characteristics of the carrier signal is modulated

i) amplitude
ii) frequency
iii) phase
iv) amplitude and phase.

b. In PSK, a binary 0 is represented by

i) the absence of the carrier signal.
ii) changing the frequency of the carrier to a lower value.
iii) sending a signal burst of the same phase as the previous signal burst sent.
iv) sending a signal burst of opposite phase to the preceding one.

2.3.2. Questions for short answers

a) Give the names of different techniques of analog encoding of digital data.
b) What are the characteristics of a carrier signal that are modulated in analog encoding of digital data?

2.3.3. Analytical question

a) Discuss different techniques of analog encoding of digital data.

Lesson 3 : Encoding of Analog Data into Digital Signal

3.1. Learning Objectives

On completion of this lesson you will be able to :

- learn the basic concepts of digital encoding of analog signal
- learn various techniques of coding and decoding of analog data.

3.2. Basic Concepts

Analog data is first converted into digital data. The process of converting analog data into digital data is known as digitization. After digitization, one of the following three things is done :

i) The digital data is transmitted using NRZ-L.
ii) The digital data is encoded as a digital signal using a code other than NRZ-L.
iii) The digital data is converted into an analog signal using one of the ASK, FSK and PSK modulation techniques.

The device used for converting analog data into digital form for transmission, and subsequently recovering the original analog data from the digital is known as **codec** (coder-decoder).

Codec coder-decoder.

3.3. Techniques of Coding and Decoding of Analog Data

Pulse Code Modulation (PCM)

Pulse Code Modulation (PCM) is based on the sampling theorem, which is stated below:

Sampling Theorem : If a signal f(t) is sampled at regular intervals of time and at a rate higher than twice the highest significant signal frequency, then the samples contain all the information of the original signal. The function f(t) may be reconstructed from these samples by the use of a low-pass filter.

In PCM, the original signal is assumed to be bandlimited with a bandwidth of B. Samples are taken at a rate 2B, or once every 1/2B seconds. These samples are represented as narrow pulses whose amplitude is proportional to the value of the original signal. This process is known as pulse amplitude modulation (PAM). To produce PCM data, the PAM samples are quantized. That is, the amplitude of each PAM pulse is approximated by an n-bit integer. The PCM pulse is then converted into a block of n bits. This process is illustrated in figure 4.3.

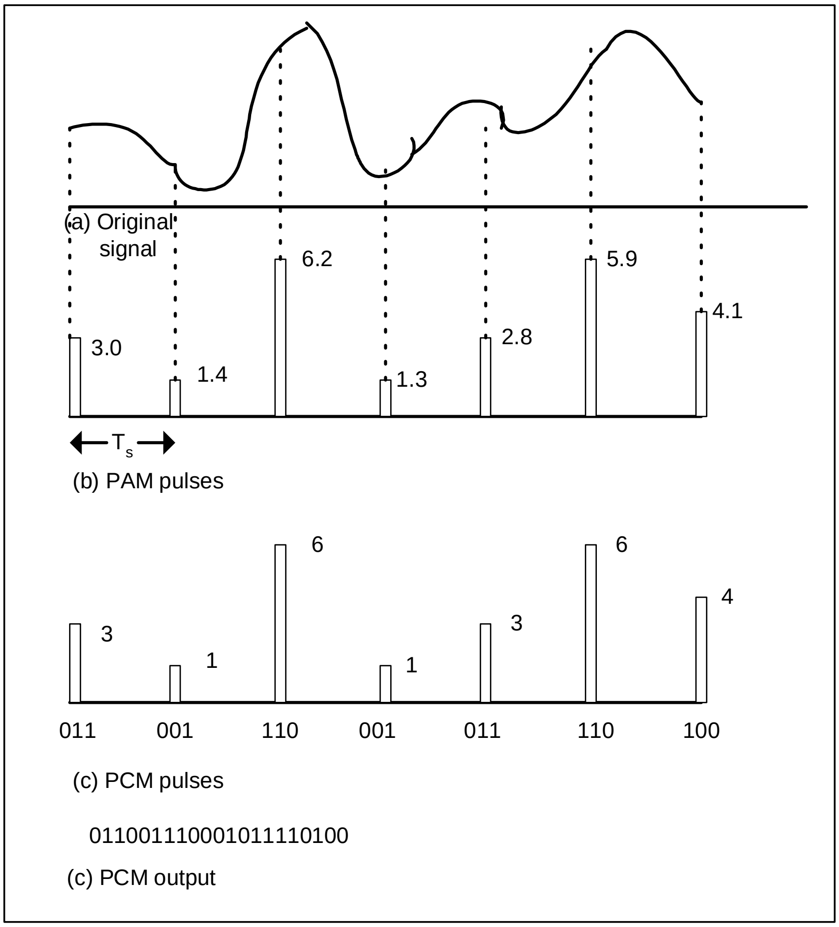


Fig. 4.3 : Pulse-code modulation.

The output of the delta modulation process is represented as a single binary digit for each sample.

Delta Modulation (DM)

In delta modulation, an analog input is approximated by a staircase function that moves up or down by one quantization level (δ) at each sampling interval (T_s). An example is shown in figure 4.4. At each sampling time, the staircase function moves up or down a constant amount δ. The output of the delta modulation process is represented as a single binary digit for each sample. In essence, a bit stream is produced where a 1 is generated if the staircase function is to go up during the next interval and a 0 is generated otherwise. For transmission, at each sampling point, the analog input is compared to the most recent value of the approximating staircase function. If the value of the sampled waveform exceeds that of the staircase function, a 1 is generated; otherwise, a 0 is generated. The output of DM process is a binary sequence that can be used at the receiver to reconstruct the staircase function. The staircase function can then be smoothed by some type of integration process or by passing it through a low-pass filter to produce an analog approximation of the analog input signal.

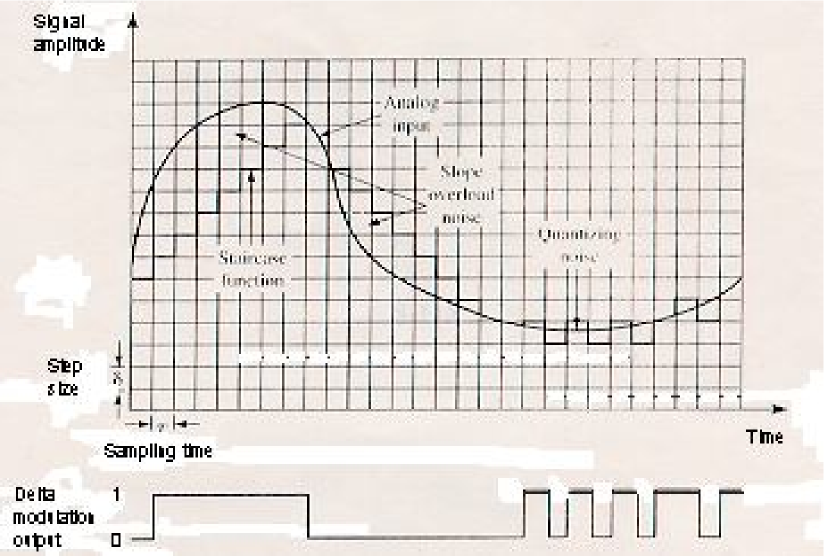


Fig. 4.4 : Example of delta modulation.

3.4. Exercise

3.4.1. Multiple choice questions

a. In analog to digital encoding, the digitized data

i) is always encoded using NRZ-L.
ii) is encoded using code other than NRZ-L.
iii) is encoded using ASK, FSK or PSK modulation techniques.
iv) is encoded either using NRZ-L or other coding or using ASK, FSK or PSK modulation techniques.

b. Suppose that bandwidth of an analog signal is 2B. In PCM, sampling is done

i) once every 1/B seconds.
ii) once every 1/2B seconds.
iii) once every 1/3B seconds.
iv) once every 1/4B seconds.

3.4.2. Questions for short answers

a) What is a codec?
b) What is PAM?
c) State sampling theorem.

3.4.3. Analytical questions

a) Discuss PCM technique of coding analog data.
b) Discuss DM technique of coding analog data.

Lesson 4 : Encoding of Analog Data into Analog Signal

4.1. Learning Objectives

On completion of this lesson you will be able to :

- learn various techniques of encoding analog data into analog signal
- techniques of modulation.

4.2. Introduction

Baseband Signal: If analog data are transmitted at their original spectrum, then the signal is referred to as baseband signal. In telephone lines, voice signals are transmitted as baseband signal.

In most of the analog transmission of analog data, some sorts of modulation of carrier signals by the baseband signal is done. The principal reasons are :

Modulation

- For unguided transmission, it is virtually impossible to transmit baseband signal, because the required antennas would be many kilometers in diameter.
- Modulation permits frequency-division multiplexing.

The principal techniques for modulation by analog data are :

- Amplitude Modulation (AM)
- Frequency Modulation (FM)
- Phase Modulation (PM).

Carrier : The signal that is modulated by the data is referred to as carrier.

Modulating Signal : The data signal by which the carrier is modulated is referred to as modulating signal.

In amplitude modulation (AM), input modulating signal is multiplied with the carrier signal.

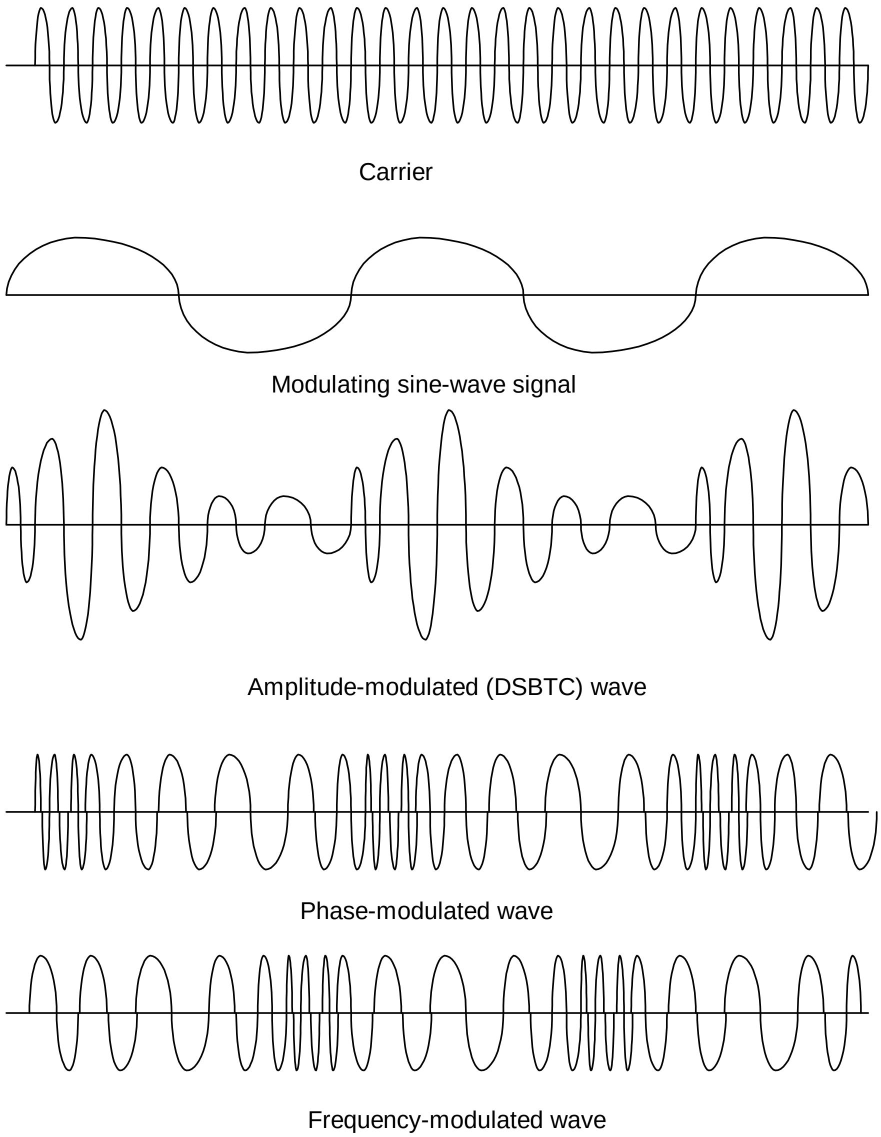
4.3. Techniques of Modulation

Amplitude Modulation (AM)

In amplitude modulation (AM), input modulating signal is multiplied with the carrier signal. The envelops of the resulting modulated signal exactly represents the original signal, that is, the envelop of the modulated signal is proportional to the amplitude of the modulating signal. This technique is shown in figure 4.5.

Frequency Modulation (FM)

In frequency modulation (FM), the carrier is modulated by the modulating signal in such a way that the frequency or the derivative of the phase of the modulated signal is proportional to the modulating signal. This process is shown in figure 4.5.



Carrier

Modulating sine-wave signal

Amplitude-modulated (DSBTC) wave

Phase-modulated wave

Frequency-modulated wave

Fig. 4.5 : Amplitude, phase and frequency modulation of a sine-wave carrier by a sine-wave signal.

Phase Modulation (PM)

In phase modulation (PM), the carrier is modulated by the modulating signal in such a way that the phase of the modulated signal is proportional to the modulating signal. This process is shown in figure 3.5.

4.4. Exercise

4.4.1. Multiple choice questions

a. In FM,

i) the frequency of the modulated signal is proportional to the modulating signal.
ii) the phase of the modulated signal is proportional to the modulating signal.
iii) the envelop of the modulated signal is proportional to the modulating signal.
iv) none of the above.

b. In AM, the envelop of the modulated signal is proportional to

i) the frequency of the modulating signal
ii) the phase of the modulating signal
iii) the derivative of the phase of the modulating signal
iv) the amplitude of the modulating signal.

4.4.2. Questions for short answers

a) What is a baseband signal?
b) What are the reasons for which an analog data is modulated for transmission?
c) Give the names of different modulation techniques by analog signals.

4.4.3. Analytical question

a) Discuss various types of modulation by analog signals.

Unit 5 : Digital Data Communications Techniques

Introduction

For two devices linked by a transmission medium to exchange data, a high degree of cooperation is required. Typically, data are transmitted one bit at a time over the medium. The timing of these bits must be the same for transmitter and receiver. Transmission modes to achieve this cooperation are discussed in this unit.

Data transmission is always subject to some sorts of errors. In this unit, means of accounting for data transmission errors are discussed.

Typically, digital data devices do not attach to and signal across a transmission medium directly. Rather, this process is mediated through a standardized interfaces. In this unit, standard transmission line interfaces are also discussed.

Lesson 1 : Transmission Mode

1.1. Learning Objectives

On completion of this lesson you will be able to :

Data are transmitted one bit at a time over the medium.

- grasp the two transmission modes used to achieve cooperation between transmitter and receiver
- asynchronous
- synchronous.

1.2. Introduction

For two devices linked by a transmission medium to exchange data, a high degree of cooperation is required. Typically, data are transmitted one bit at a time over the medium. The timing, that is, rate, duration and spacing of these bits must be the same for transmitter and receiver. To achieve this cooperation between transmitter and receiver, two modes of data transmission are used. They are :

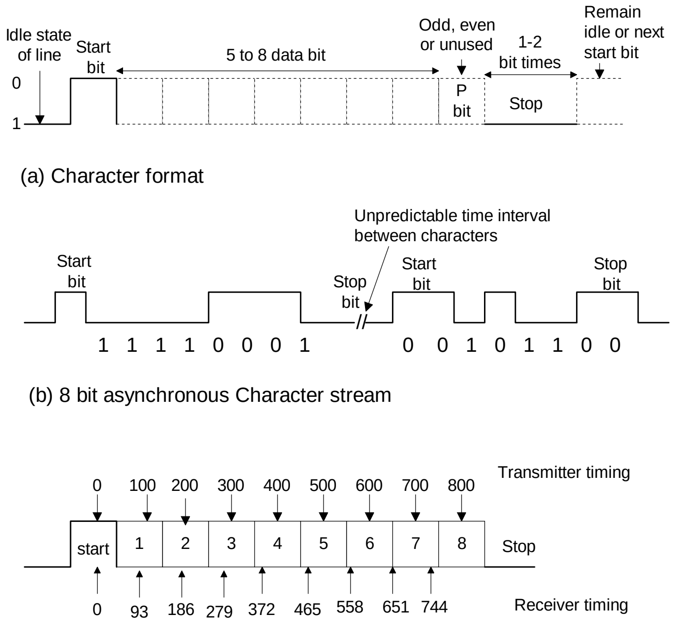
- Asynchronous Data Transmission
- Synchronous Data Transmission.

1.3. Asynchronous Data Transmission

In asynchronous data transmission, data are transmitted one character at a time, where each character is five to eight bits in length. Timing or synchronization is maintained within each character; the receiver has the opportunity to resynchronize at the beginning of each new character.

The technique is explained with reference to figure 4.1. When no character being transmitted, the line between transmitter and receiver is in an “idle” state. The definition of idle is equivalent to the signaling element for binary 1. The beginning of a character is signaled by a start bit with a value of binary 0. This is followed by the five to eight bits that actually make up the character. The bits of the character are transmitted starting with the least significant bit. Usually, the character bits are followed by a parity bit, which therefore is in the most-significant bit position. The parity bit is set by the transmitter such that the total number of ones in the character, including the parity bit, is even (even parity) or odd (odd parity), depending on the convention being used. The final element is a stop, which is a binary 1. A minimum length for the stop is specified, and this is usually 1, 1.5, or 2 times the duration of an ordinary bit. Since the stop is the same as the idle state, the transmitter will continue to transmit the stop signal until it is ready to send the next character.

When no character being transmitted, the line between transmitter and receiver is in an “idle” state.



(a) Character format

(b) 8 bit asynchronous Character stream

(c) Effect of timing error

Fig. 5.1 : Asynchronous data transmission.

If a steady stream of characters is sent, the interval between two characters is uniform and equal to the stop element. For example, if the stop bit has unit length and the ASCII character ABC are sent (without parity bit), the pattern is

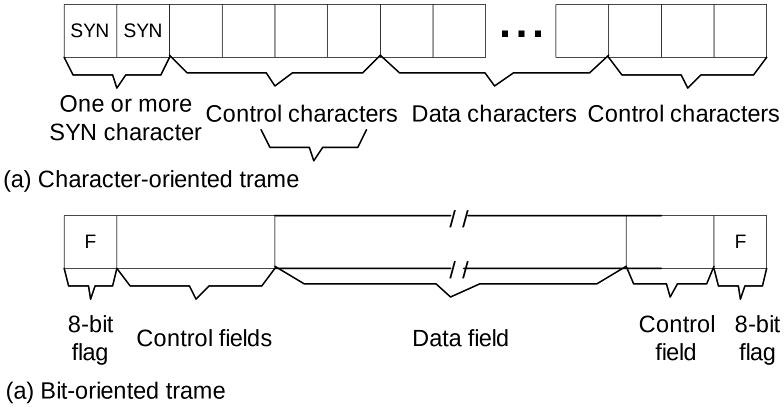
01000001100100001101100001 11…

The start bit (0) starts the timing sequence for the next eight elements, which are the 7-bit ASCII code and the stop bit. In the idle state, the receiver looks for a transition from 1 to 0 to begin the next character and then samples the input signal at one-bit intervals for seven intervals. It then looks for the next 1-to-0 transition.

1.4. Synchronous Data Transmission

In synchronous data transmission, blocks of characters or bits are transmitted. To synchronize the clocks of the transmitter and the receiver, the clocking information is embedded in the data signal with biphase encoding of digital signals. Each block begins with a preamble bit pattern and generally ends with postamble bit pattern. These patterns are control information rather than data. In addition, other control information is included. The data plus control information is called **frame**. There are two formats of the frame: character-oriented and bit-oriented. The frame format is shown in figure 5.2.

The data plus control information is called frame.



(a) Character-oriented trame

(a) Bit-oriented trame

Fig. 5.2 : Synchronous frame.

With character-oriented transmission, the block of data is treated as a sequence of characters (usually 8-bit characters). All control information is in character form. The frame begins with one or more “synchronization characters” (SYN). The SYN is a unique bit pattern that signals the receiver that this is the beginning of a block. The postamble is another unique character used in some schemes. The receiver thus is alerted to an incoming block of data by the SYN characters and accepts data until the postamble character is seen.

The SYN is a unique bit pattern that signals the receiver that this is the beginning of a block.

With bit-oriented transmission, the block of data is treated as a sequence of bits. A special bit pattern (flag) signals the beginning of a block. This preamble flag is eight bit long. The same flag is also used as a postamble.

1.5. Exercise

1.5.1. Multiple choice questions

a. In asynchronous mode of data transmission, the idle state is indicated by signaling element for

i) binary 1
ii) binary 0
iii) transition of 1-to-0
iv) none of the above.

b. In synchronous mode of data transmission, data are transmitted

i) one character at a time
ii) as blocks of characters
iii) as blocks of bits
iv) as blocks of characters or bits.

1.5.2. Questions for short answers

a) How many modes of data transmission are there? Name them.
b) What is a frame?
c) How many formats of frame are there and what are they?

1.5.3. Analytical questions

a) Discuss asynchronous mode of data transmission.
b) Discuss synchronous mode of data transmission.

Lesson 2 : Error Detection Techniques

2.1. Learning Objectives

On completion of this lesson you will be able to :

- know the classification of error detection techniques
- grasp the details of each of the error detection techniques.

2.2. Introduction

Regardless of the design of the transmission system, there will be errors. To ensure error-free transmission, three types of error-detection techniques are commonly used. They are :

- Parity check
- Longitudinal redundancy check
- Cyclic redundancy check.

2.3. Parity Check

Typically even parity is used for asynchronous transmission.

The simplest bit error detection scheme is to append a parity bit to the end of each word in the frame. A typical example is ASCII transmission, in which a parity bit is attached to each 7-bit ASCII character.

Even Parity : In even parity, the value of the parity bit is selected so that the word has an even number of 1’s. Typically even parity is used for asynchronous transmission.

Odd Parity : In odd parity, the value of the parity bit is selected so that the word has an odd number of 1’s. Typically odd parity is used for synchronous transmission.

For example, if the transmitter is transmitting an ASCII G (1110001) and using odd parity, it will append a 1 and transmit 1110001. The receiver examines the received character and if the total number of 1’s is odd, assumes that no error has occurred. If one bit (or any odd number of bits) is erroneously inverted during transmission (e. g., 11$\underline{0}$00011), then the receiver will detect an error. However, if any even number of bits are inverted, parity check will not detect the error.

2.4. Longitudinal Redundancy Check

In longitudinal redundancy check, the frame is viewed as a block of character arranged in two dimensions. To each character is appended a parity bit. In addition, a parity bit is generated for each bit position across all characters. That is, an additional character is generated in which the Ith bit of the character is a parity bit for the Ith bit of all other characters in the block. This technique is illustrated below :

	bit	1	2	3	4	5	6	7	Parity bit	
Character 1		1	0	1	1	0	1	1	1	
2		1	1	0	1	0	1	1	1	
3		0	0	1	1	1	0	1	0	
4		1	1	1	1	0	0	0	0	
5		1	0	0	0	1	0	1	1	
6		0	1	0	1	1	1	1	1	
Parity Check Character		0	1	1	1	1	1	1	0	← LRC
									↑ VRC	

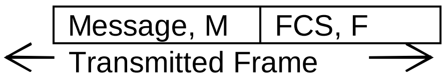
The parity bit at the end of each character (row parity bit) is generated using the bits of that character. For the parity check character, each bit is generated using the corresponding bits of all characters. The parity bit at the end of each character are referred to as the vertical redundancy check (VRC).

The parity bit at the end of each character are referred to as the vertical redundancy check (VRC).

The parity check character is referred to as the longitudinal redundancy check (LRC)

2.5. Cyclic Redundancy Check

A very powerful but easily implemented error detecting technique is cyclic redundancy check (CRC). In this technique, given a k-bit message, the transmitter generates an n-bit sequence, known as a frame check sequence (FCS), so that the resulting frame, consisting of k+n bits, is exactly divisible using modulo-2 division by some predetermined number. The receiver then divides the incoming frame by the same number and, if there is no remainder, assumes that there was no error. CRC frame is shown below :



Let us define the following :

T = (k+n)-bit frame to be transmitted, with n < k.
M = k-bit message, the first k bits of T.
F = n-bit FCS, the last n bits of T.
P = pattern of n+1 bits, the predetermined divisor.

We would like T/P to have no remainder. The problem is to find F.

As M occupies the most significant k bits of T, in respect to T, it can be viewed that M is shifted n bits left, that is, M is multiplied by 2^n. Then, it should be clear that

$$T = 2^nM + F \qquad (5.1)$$

It should be noted that the addition is modulo-2 addition.

Let us suppose that

$$\frac{2^n M}{P} = Q + \frac{R}{P} \qquad (5.2)$$

As P is an n+1 bit number, the remainder R is always an n bit number. The value of the remainder R is used as F, that is, F = R.

Then

$$T = 2^nM + R \qquad (5.3)$$

From (5.2), we have that

$$R = 2^nM + QP \qquad (5.4)$$

Substituting (5.4) in (5.3), we have that

$$T = 2^nM + 2^nM + QP = QP$$

That is, T is always divisible by P.

For example, let us consider that
Message M = 1010001101 (10 bits)
Pattern P = 110101 (6 bits)
FCS R = to be calculated (5 bits0

Multiplying M by 2^n yields 101000110100000. This product is divided by P

```
                 1101010110 ← Q
P →  110101 | 101000110100000 ← 2^nM
            | 110101
                111011
                110101
                   111010
                   110101
                      111110
                      110101
                         101100
                         110101
                          110010
                          110101
                              1110 ← R
```

The remainder R = 01110 is then added to 2^nM to have T :

```
        101000110100000
                  01110
T →     101000110101110
```

This T is transmitted.

If there are no errors, the receiver receives T intact. The received frame is then divided by P:

```
               1101010110
110101 | 101000110101110
       | 110101
           111011
           110101
              111010
              110101
                 111110
                 110101
                    101111
                    110101
                     110101
                     110101
                           00
```

Since there is no remainder, it is assumed that there have been no error.

The pattern P is chosen to be one bit larger than the desired FCS and both the high- and low-order bits of P must be 1.

A second way of viewing the CRC process is to express all values as polynomials in a dummy variable X with binary coefficients. The coefficients corresponds to the bits in the binary number. Thus for M = 110011, we have M(X) = X^5+X^4+X+1, and for P = 11001, we have P(X) = X^5+X^3+1. Arithmetic operations are modulo-2. The CRC process can now be described as

$$\frac{X^n M(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$

$$T(X) = X^n M(X) + R(X)$$

Four versions of P(X) are widely used :

CRC-12 = $X^{12}+X^{11}+X^3+X^2+X+1$
CRC-16 = $X^{16}+X^{15}+X^2+1$
CRC-CCITT = $X^{16}+X^{12}+X^5+1$
CRC-32=$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$

The CRC-12 system is used for transmission of streams of 6-bit characters and generates a 12-bit FCS. Both CRC-16 and CRC-CCITT are popular for 8-bit characters, in the United States and Europe respectively, and both results in a 16-bit FCS. CRC-32 is specified as an option in some point-to-point synchronous transmission standards, and generates a 32-bit FCS.

2.6. Exercise

2.6.1. Multiple choice questions

a. Typically even parity is used for

i) asynchronous transmission
ii) synchronous transmission
iii) both of the above
iv) none of the above.

b. Typically odd parity is used for

i) asynchronous transmission
ii) synchronous transmission
iii) both of the above
iv) none of the above.

2.6.2. Questions for short answers

a) Classify error detection techniques.
b) What is VRC?
c) What is LRC?
d) What is FCS?

2.6.3. Analytical questions

a) Discuss parity bit technique of error detection.
b) Discuss Longitudinal Redundancy Check technique of error detection.
c) Discuss Cyclic Redundancy Check technique of error detection.
d) Given that
Message M = 0101110010 (10 bits)
Pattern P = 100101
Calculate the FCS R (5bits).

Lesson 3 : Transmission Line Interfaces

3.1. Learning Objectives

On completion of this lesson you will be able to :

- know the preliminary ideas about various interface standards of digital data transmission
- EIA-232-D
- DIA-530
- ISDN physical interface.

3.2. Introduction

Most digital data processing devices do not attach directly to a transmission medium. The more common situation is depicted in Figure 5.3

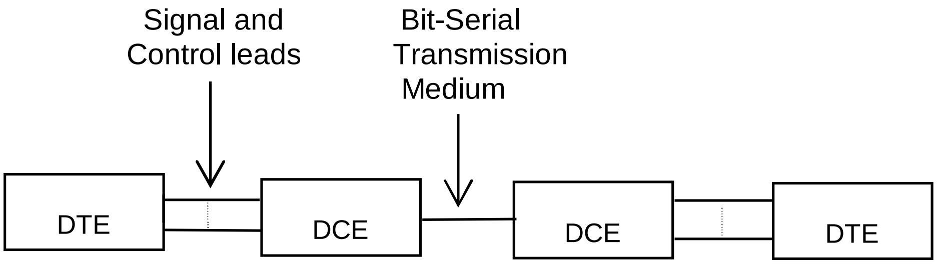


Fig. 5.3 : Generic interface to transmission medium.

The DCE is responsible for transmitting and receiving bits over a transmission medium.

The devices are generally referred to as data terminal equipment (DTE). A DTE makes use of the transmission system through the mediation of data circuit-terminating equipment (DCE). On one side, the DCE is responsible for transmitting and receiving bits over a transmission medium. On the other side, the DCE must interact with the DTE. In general, this requires both data and control information to be exchanged.

A variety of standards for interfacing between the DTE and the DCE exist. The most important interface standards are :

- EIA-232-D
- EIA-530
- ISDN Physical Interface.

3.3. EIA-232-D

By far the most common interface standard in the United States is the 232 standard issued by the Electronic Industries Association. The RS-232 standard was first issued in 1962, and its third version, RS-232-C, was published in 1969. EIA-232-D was introduced in 1987. It is compatible with RS-232-C. This interface is used to connect DTE devices to voice-grade modems for use on public analog telecommunications systems.

The mechanical specification for EIA-232-D calls for a 25-pin connector with a specific arrangement of leads. The electrical specification defines the signaling between DTE and DCE. Digital signaling is used on all interchange circuits. With respect to a common ground, a voltage more negative than -3 volts is interpreted as binary 1 and a voltage more positive than +3 volts is interpreted as binary 0. The interface is rated at a signal rate of <20 kbps and a distance of <15m. The same voltage levels apply to control signals: a voltage more negative than -3 volts is interpreted as an OFF condition and a voltage more positive than +3 volts is interpreted as an ON condition. The interchange circuits are grouped into categories of data, control, timing, and ground. There is one data circuit in each direction, so full-duplex operation is possible. In addition, there are two secondary data circuits that are useful when the device operates in half-duplex fashion.

The interchange circuits are grouped into categories of data, control, timing, and

There are fourteen control circuits. Eight of these relate to the transmission of data over the primary channel. For asynchronous transmission, six of these circuits are used. In addition to these six circuits, two other control circuits are used in synchronous transmission. There are three timing circuits that may be used with synchronous transmission; these provide clock pulses. The final set of circuits deal with grounding and shielding.

3.4. EIA-530

In 1987 EIA-530 was introduced. This standard is intended to operate at data rates from 20 kbps to 2 Mbps using the same 25-pin connector used by EIA-232-D and RS-232-C. In this standard, two modes of transmission are used: balanced transmission and unbalanced transmission. Balanced transmission line consists of two conductors. Signal are transmitted as a current that travels down one conductor and returns on the other, the two conductors form a complete circuit. Unbalanced transmission uses a single conductor to carry the signal, with ground providing the return

Two modes of transmission are used: balanced transmission and unbalanced transmission.

path. The balanced mode tolerates more, and produces less, noise than the unbalanced.
In the unbalanced case, a positive voltage of between 2 and 6 volts, with respect to ground, is interpreted as a binary 0, and a negative voltage of between 4 and 6 volts is interpreted as binary 1. In the balanced case, a voltage difference between the two circuits in the range 2 to 6 volts is interpreted as a binary digit, with the direction of the difference determining whether it is interpreted as binary 0 or binary 1.

3.5. ISDN Physical Connector

In Integrated Services Digital Network (ISDN) terminology, a physical connection is made between terminal equipment (TE) and network-terminating equipment (NT). These terms closely corresponds to DTE and DCE respectively. The physical connection, defined in ISO standard 8877 (ISO 8877), specifies that the NT and TE cables shall terminate in matching plugs that provide for 8 contacts. Two contact points each are needed to provide balanced transmission in each direction. These contact points are used to connect twisted-pair leads coming from the NT and TE devices.

Contact points are used to connect twisted-pair leads coming from the NT and TE devices.

The electrical specification for the interface dictates the use of a pseudoternary coding scheme. Binary one is represented by the absence of voltage, binary zero is represented by a positive or negative pulse of 750 mV ± 10%. The data rate is 192 kbps.

3.6. Exercise

3.6.1. Multiple choice questions

a. In EIA-232-D standard, the interchange circuits are grouped into the categories of

i) data and control
ii) data, control and timing
iii) data, control and ground
iv) data, control, timing and ground.

b. In EIA-232-D standard, the following are possible

i) full-duplex operation only
ii) half-duplex operation only
iii) both full- and half-duplex operations
iv) none of the above.

c. In EIA-232-D standard, the number of pins used for timing is

i) 3
ii) 14
iii) 8
iv) 6.

3.6.2. Question for short answer

a) Name the most important interface standards used in digital data transmission.

3.6.3. Analytical questions

a) Discuss EIA-232-D standard for interfacing digital devices.
b) Discuss EIA-530 standard for interfacing digital devices.
c) Discuss ISO 8877 standard for ISDN physical connection.

Unit 6 : Data Link Control

Introduction

The physical layer is concerned with sending signals over a transmission link. For effective digital data communications much more is needed to control and manage the exchange. This is done by the data link layer. The data link control or data link protocol is concerned with sending data over a data communications link. This unit, presents some of the key features of data link protocols, such as : **line configuration**, **flow control**, and **error control**. A specific **data link protocol** is also presented in this unit.

Lesson 1 : Line Configuration

1.1. Learning Objectives

On completion of this lesson you will be able to :

- review the concepts of topology and duplexity of data link
- understand the discipline of transmission link.

1.2. Topology and Duplexity

The **topology** of a data link refers to the physical arrangement of stations on a link. If there are only two stations, the link is **point-to-point**. If there are more than two stations, then it is a **multipoint** topology.

The topology of a data link refers to the physical arrangement of stations on a link.

The **duplexity** of a link refers to the direction and timing of signal flow. In **simplex** transmission, the signal flow is always in one direction. A **half-duplex** link can transmit and receive but not simultaneously. On a **full-duplex** link, two stations can simultaneously send and receive data from each other.

With digital signaling, full-duplex usually requires two separate transmission paths, while half-duplex requires only one. For analog signaling, duplexcity depends on frequency, whether guided or unguided transmission is used. If a station transmits and receives on the same frequency, it must operate in half-duplex mode. If a station transmits on one frequency and receives on another, it may operate in full-duplex mode.

1.3. Line Discipline

Some discipline is needed in the use of a transmission link. On a half-duplex line, only one station at a time should transmit. On either a half- or full-duplex line, a station should only transmit if it knows that the intended receiver is prepared to receive.

Point-to-point Links

Line discipline is simple with a point-to-point link. Let us consider first a half-duplex link in which either station may initiate an exchange. If either station wishes to send data to the other, it first performs an inquiry of the other station to see if it is prepared to receive. The second station responds with a positive acknowledgment to indicate that it is ready. The first station then sends some data. In asynchronous communication, the data would be sent as an asynchronous stream of character. In any case, after some quantum of data is sent, the first station pauses to await results. The second station acknowledges successful receipt of the data. The first station then sends an end of transmission message which terminates the exchange and return the system to its initial state.

There are three distinct phases in this communication control procedure :

- **Connection Establishment** : This determines which station is to transmit and which to connection receive, and that the receiver is prepared to receive.
- **Data Transfer** : The data are transferred in one or more acknowledgment blocks.
- **Termination** : This terminates the logical connection.

A common situation is to have one of the stations designated **primary** and the other **secondary**. The primary has the responsibility of initiating the exchange. If the secondary has data to send, it must wait for the primary to request the data, and only then enter a data transfer phase. If the link is full-duplex, data and control messages can be transmitted in both directions simultaneously.

Multipoint Links

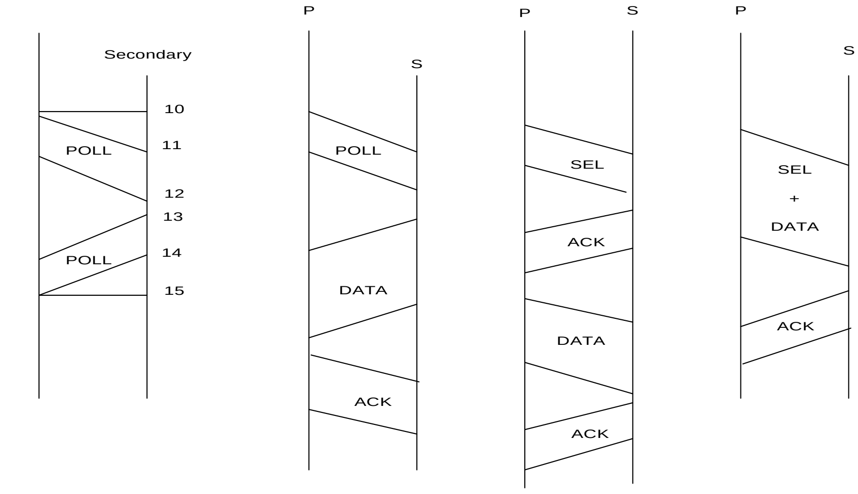
When there is a primary station, data are exchanged only between the primary and a secondary, not between two secondaries. The most common disciplines used in this situation are all variants of a scheme known as **poll and select** :

- **Poll** : The primary requests data from a secondary.
- **Select** : The primary has data to send and informs a secondary that data are coming.

Poll and select

Figure 6.1 illustrates these concepts. In figure 6.1(a), the primary polls a secondary by sending a brief polling message. In this case, the secondary has nothing to send and responds with some sort of negative acknowledgment (NAK) message. Figure 6.1(b) depicts the case of a successful poll. The most common form of polling is **roll-call polling**, in which the primary selectively polls each secondary in a predetermined sequence. In the simplest case, the primary polls each secondary in a round-robin fashion. Variants of roll-call polling permit priority handling by polling some stations more than once per cycle.

The most common form of polling is roll-call ...



(a) Polled terminal has nothing

(b) Polled terminal has Data to send

(c) Select

(d) Fast select

Fig. 6.1 : Poll and Select sequences.

The select function is shown in figure 6.1(c). Note that four separate transmissions are required to transfer data from the primary to the secondary. An alternative technique is **fast select**. In this case, the selection message includes the data to be transferred (figure 6.1(d)). The first reply from the secondary is an acknowledgment that indicate4s that the station was prepared to receive and did receive the data successfully. Fast selection is particularly well suited for applications where short messages are frequently transmitted and the transfer time for the message is not appreciably larger than the reply time.

the line is free; otherwise, it must wait.

Another form of line discipline is **contention**. In this mode, there is typically no primary but rather a collection of peer stations. A station can transmit if the line is free; otherwise, it must wait.

A characteristics of all multipoint line discipline is the need for addressing. In the case of roll-call polling, transmission from the primary must indicate the intended secondary; transmission from a secondary must identify the secondary. In a peer situation, both transmitter and receiver must be identified. Thus there are three cases :

- **Point-to-point** : no address needed.
- **Primary-secondary multipoint** : one address needed, to identify secondary.
- **Peer multipoint** : two addresses needed, to identify transmitter and receiver.

In practice, the first case is subsumed into the second, so that most data link control protocols require one address even for point-to-point transmission.

1.4. Exercise

1.4.1. Multiple choice question

a. In the contention line discipline

i) a station can transmit if the line is free in a peer multipoint link.
ii) a primary station can transmit to the secondary station in a primary-secondary multipoint link.
iii) a primary station can transmit to the secondary station in a point-to-point link.
iv) a secondary station can transmit to the primary station in a point-to-point link.

1.4.2. Questions for short answers

a) Define the terms topology and duplicity.
b) Define simplex, half-duplex, and full-duplex links.
c) Define primary and secondary stations.
d) Define poll and select.
e) What is roll-call polling?

1.4.3. Analytical questions

a) Discuss line discipline for point-to-point link.
b) Discuss line discipline for multipoint link.
c) Discuss need for addresses in line discipline.

Lesson 2 : Flow Control

2.1. Learning Objectives

On completion of this lesson you will be able to :

- know two mechanisms for flow control between a transmitting station and a receiving station.

2.2. Introduction

In the absence of flow control, the receiver's buffer may overflow while it is processing old data.

Flow control is a technique for assuring that a transmitting station does not overwhelm a receiving station with data. The receiver will typically allocate a data buffer with some maximum length. When data are received, it must do a certain amount of processing before it can clear the buffer and be prepared to receive more data. In the absence of flow control, the receiver's buffer may overflow while it is processing old data.

For asynchronous transmission, the data are sent in a sequence of frames with each frame containing a portion of the data and some control information. We assume that all frames that are transmitted are successfully received; no frames are lost and none arrive with errors. Furthermore, frames arrive in the same order in which they are sent. However, each transmitted frame suffers an arbitrary and variable amount of delay before reception.

There are two mechanisms for flow control.

There are two mechanisms for flow control in the absence of errors :

- Stop-and-wait flow control.
- The sliding window flow control.

2.3. Stop-and-wait Flow Control

Stop-and-wait flow control works as follows. A source entity transmits a frame. After reception, the destination entity indicates its willingness to accept another frame by sending back an acknowledgment to the frame just received. The source must wait until it receives the acknowledgment before sending the next frame. The destination can thus stop the flow of data by simply withholding acknowledgment.

2.4. The Sliding Window Flow Control

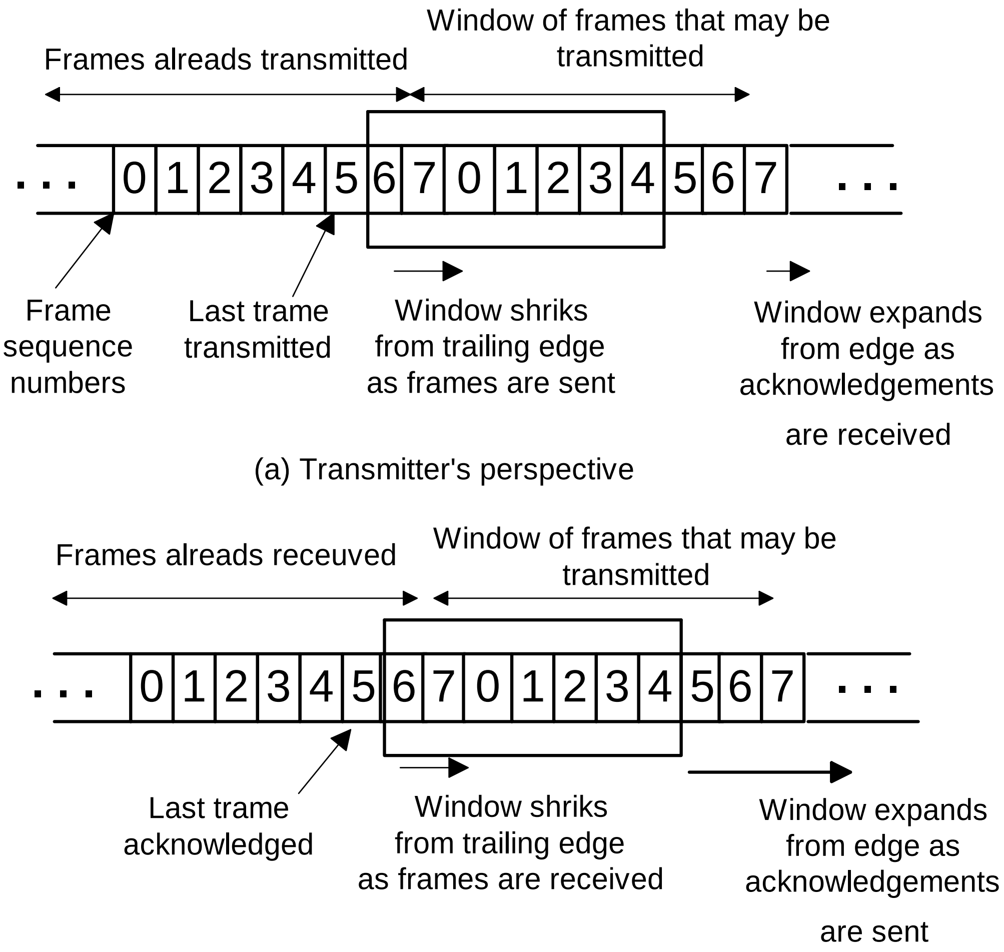
With the use of multiple frames for a single message, the simple stop-and-wait flow control procedure may be inadequate. This problem is overcome by using the sliding-window flow control.

Sliding-window flow control.

Let us suppose that two stations, A and B, are connected via a full-duplex link. Station B allocates buffer space for n frames. Thus station B can accept n frames, and station A is allowed to send n frames without waiting for an acknowledgment. To keep track of which frames have been acknowledgment, each is labeled with a sequence number. Station B acknowledges a frame by sending a acknowledgment that includes the sequence number of the next frame expected. This acknowledgment also implicitly announces that station B is prepared to receive the next n frames beginning with the number specified. This scheme can also be used to acknowledge multiple frames. For example, station B could receive frames 2, 3, and 4, but without acknowledgment until frame 4 has arrived. By then returning a acknowledgment with sequence number 5, station B acknowledges frames 2, 3, and 4 at one time. Station A maintains a list of sequence numbers that it is allowed to send and station B maintains a list of sequence numbers that it is prepared to receive. Each of these lists can be thought of as a **window** of frames. The operation is referred to as **sliding-window flow control**.

Since the sequence number to be used occupies a field in the frame, it is clearly of bounded size. For a k-bit field, the sequence number can range from 0 to (2^k - 1). Accordingly, frames are numbered modulo 2^k; that is, after sequence number (2^k - 1), the next number is zero.

Figure 6.2 depicts the sliding-window process. It assumes the use of a 3-bit sequence number, so that frames are numbered sequentially from 0 through 7, and then the same numbers are reused for subsequent frames. The shaded rectangle represents the window of frames that may be transmitted. The figure indicates that the sender may transmit 7 frames, beginning with frame 6. Each time a frame is sent, the shaded portion will shrink; each time a new acknowledgment is received, the shaded portion will grow.


Window of frames that may be transmitted
Frames alreads transmitted
. . . 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 . . .
Frame sequence numbers
Last trame transmitted
Window shriks from trailing edge as frames are sent
Window expands from edge as acknowledgements are received
Frames alreads receuved
Window of frames that may be transmitted
. . . 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 . . .
Last trame acknowledged
Window shriks from trailing edge as frames are received
Window expands from edge as acknowledgements are sent

(a) Transmitter's perspective

(b) Receiver's perspective

Fig. 6.2 : Example of sliding-window flow control.

An example is shown in Figure 6.2. The example assumes a 3-bit sequence number field and a maximum window size of seven. Initially, station A and station B have windows indicating that station A may transmit seven frames, beginning with frame 0 (F0). After transmitting three frames (F0, F1, F2) without acknowledgment, station A has shrunk its window to four frames. The window indicates that station A may transmit four frames, beginning with frame number 3. Station B then transmit an ACK3, which indicates that station B received all frames up through frame number 2 and now ready to receive seven frames beginning with frame number 3. With this acknowledgment, station A is back up to permission to transmit seven frames, still beginning with frame 3. Station A proceeds to transmit frames 3, 4, 5, and 6. Station B returns ACK4, which acknowledges frame 3, and allows the transmission of frames 4 through 2. But, by the time that this acknowledgment reaches station A, it has already transmitted frames 4, 5, and 6. The result is that station A may only open its window to permit the transmission of 4 frames, beginning with frame 7.

To supplement the above flow control, most protocols allow a station to completely cut off the flow of frames from the other side by sending a Receive Not Ready (RNR) message, which acknowledges former frames but forbids transfer of future frames. Thus RNR5 indicates that the station received all frames up through number 4 and now unable to accept any more. At some subsequent point, the station must send a normal acknowledgment to reopen the window.

2.5. Exercise

2.5.1. Multiple choice questions

a. In the sliding-window flow control mechanism, using a 4-bit sequence number, the frames are numbered

i) from 0 to 7
ii) from 0 to 16
iii) from 0 to 15
iv) none of the above.

b. In a sliding-window flow control mechanism with sequence number ranging from 0 to 7, a ACK4 from station B to station A indicates that

i) station B received all frames up through frame number 4 and now ready to receive seven frames beginning with frame number 5.
ii) station B received all frames up through frame number 3 and now ready to receive seven frames beginning with frame number 4.
iii) station A already transmitted 5 frames beginning from frame number 0.
iv) station A may transmit 5 frames beginning from frame number 0.

2.5.2. Questions for short answers

a) Why is flow control needed between a transmitting station and a receiving station?

b) Name the different mechanisms for flow control in absence of error.

c) What does ACK5 mean in a sliding-window flow control mechanism with frame sequence ranging from o to 7?

d) What does RNR5 mean in a sliding-window flow control mechanism with frame sequence ranging from o to 7?

2.5.3. Analytical questions

a) Discuss stop-and-wait flow control mechanism.

b) Discuss sliding-window flow control mechanism.

Lesson 3 : Error Control

3.1. Learning Objectives

On completion of this lesson you will be able to :

- know three mechanisms of error control between a transmitting station and a receiving station.

3.2. Introduction

Error control refers to mechanisms to detect and correct errors that occur in the transmission of frames.

There is possibility of two types of errors :

- **Lost frame** : A frame fails to arrive at the other side.
- **Damaged frame** : A frame does arrive but some of the bits are in error.

The most common techniques for error control are based on some or all of the following ingredients :

- **Error Detection** : Typically CRC is used.
- **Positive acknowledgment** : The destination returns a positive acknowledgment to successfully received, error-free frames.
- **Retransmission after time-out** : The source retransmits a frame that has not been acknowledged after a predetermined amount of time.
- **Negative acknowledgment and retransmission** : The destination returns a negative acknowledgment to frames in which an error is detected. The source retransmits such frames.

Automatic repeat request (ARQ).

Collectively, these mechanisms all referred to as **automatic repeat request (ARQ)**. Three versions of ARQ are in common use:

- Stop-and-wait ARQ

- Go-back-N ARQ
- Selective-reject ARQ.

All of these forms are based on the use of flow control techniques.

3.3. Stop-and-wait ARQ

Stop-and-wait ARQ is based on the stop-and-wait flow control technique, and is depicted in figure 6.3. The source station transmits a single frame and then must await an acknowledgment (ACK). No other data frames can be sent until the destination station's reply arrives at the source station.

Stop-and-wait ARQ is based on the stop-and-wait flow control technique.

The frame transmitted by the source could suffer an error. If the error is detected by the destination, it discards the frame and sends a negative acknowledgment (NAK), causing the source to retransmit the damaged frame. On the other hand, if the transmitted frame is so corrupted by noise as not to be received, the destination will not respond. To account for this possibility, the source is equipped with a timer. After a frame is transmitted, the source waits for an acknowledgment (ACK or NAK). If no recognizable acknowledgment is received during the time-out period, then the frame is retransmitted. Note that this system requires that the source maintain a copy of a transmitted frame until an ACK is received for that frame.

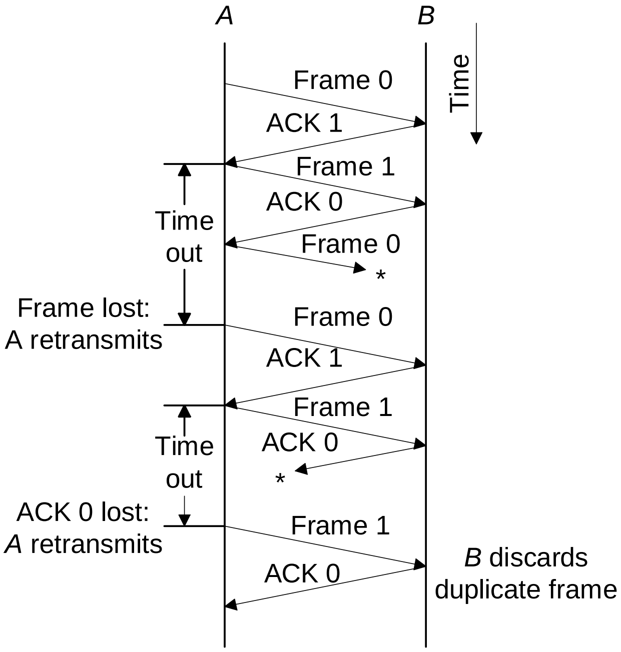


Fig. 6.3: Stop-and-wait ARQ.

If a frame is sent correctly but the acknowledgment is damaged in transit, then the source will time out and retransmit that frame. The destination will now receive and accept two copies of the same frame. To avoid this problem, frames are alternately labeled with 0 or 1 and positive acknowledgments are of the form ACK0 or ACK1: an ACK0 (ACK1) acknowledges receipt of a frame numbered 1(0) and indicates that the receiver is ready for a frame numbered 0(1).

3.4. Go-back-N ARQ

The sliding-window flow control technique can be adapted to provide more efficient error control and it is referred to as **continuous ARQ**. One variant of continuous ARQ is known as **go-back-N ARQ**. In this technique, a station may send a series of frames determined by window size, using the sliding-window flow control technique. While no errors occur, the destination will acknowledge (ACK) incoming frames as usual.

Go-back-N ARQ

Consider that station A is sending frames to station B. After each transmission, station A sets an acknowledgment timer for the frame just transmitted. The go-back-N technique takes into account the following contingencies :

1. Damaged frame : There are three subcases :

a) Station A transmits frame i. Station b detects an error and has previously successfully received frame (i-1). Station B sends a NAKi, indicating that frame i is rejected. When station A receives this NAK, it must retransmit frame i and all subsequent frames that it has transmitted.
b) Frame i is lost in transit. Station A subsequently sends frame (i+1). Station B receives frame (i+1) out of order, and send a NAKi.
c) Frame i is lost in transit and station A does not soon send additional frames. Station B receives nothing and returns neither an ACK or a NAK. Station A will time out and retransmit frame i.

2. Damaged ACK: There are two subcases :

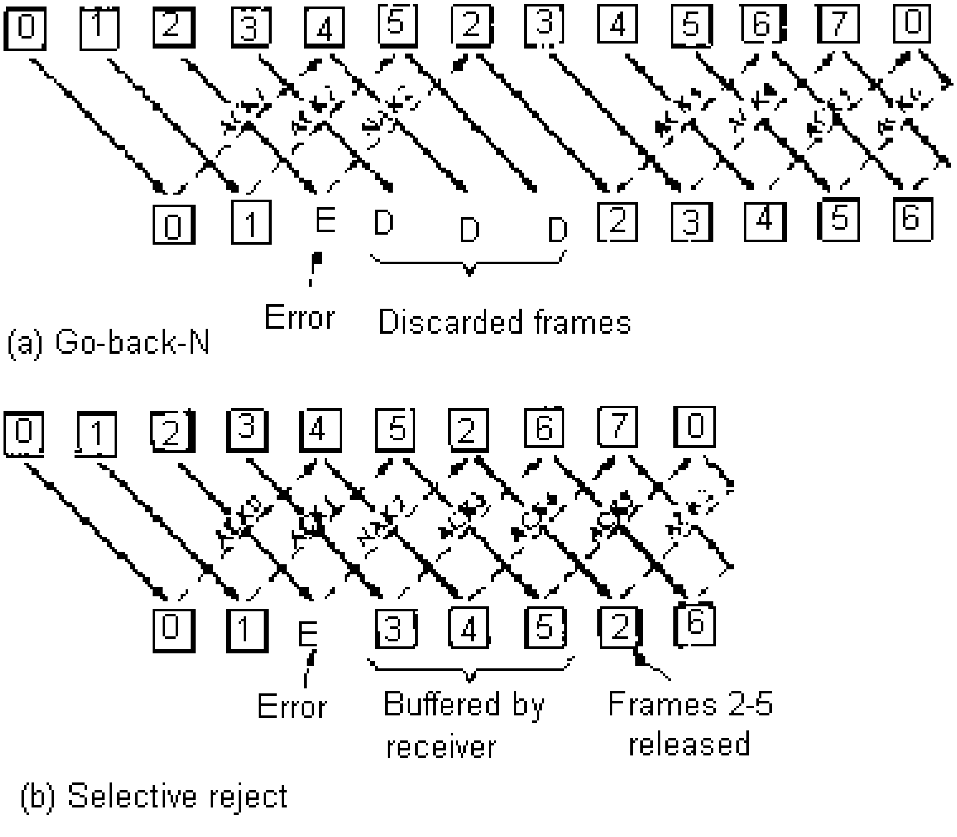
a) Station B receives frame i and sends ACK(i+1), which is lost in transit. Since ACKs are cumulative (e.g., ACK6 means that all frames through 5 are acknowledged), it may be that A will receive a subsequent ACK to a subsequent frame that will do the job of the lost ACK before the associated time expires.

b) If station A's time expires, station A retransmits frame i and all subsequent frames.

3. **Damaged NAK** : If a NAK is lost, station A will eventually time out on the associated frame and retransmit that frame and all subsequent frames.

Figure 6.4(a) shows the frame flow for go-back-N ARQ on a full-duplex line, assuming a 3-bit sequence number.

With go-back-N ARQ, it is not required that each individual frame be acknowledged. For example, station A sends frames 0, 1, 2, and 3. Station B responds with ACK1 after frame 0, but then does not respond to frames 1 and 2. After frame 3 is received, station B issues ACK4, indicating that frame 3 and all previous frames are accepted.



(a) Go-back-N

(b) Selective reject

Fig. 6.4. Examples of continuous ARQ.

In most continuous ARQ implementation, the receiving station sends acknowledgment with the next return frame using a fixed length acknowledgment field. This is known as **piggybacking**.

3.5. Selective-reject ARQ

With selective-reject ARQ, the only frames retransmitted are those that received a NAK or which time out.

With selective-reject ARQ, the only frames retransmitted are those that received a NAK or which time out. Figure 6.5(b), which exhibits the same error pattern as figure 6.5(a), illustrates selective-reject. Because of various complications, the selective-reject ARQ is rarely implemented.

3.6. Exercise

3.6.1. Multiple choice questions

a. In Go-back-N ARQ, a ACK5 means that

i) frame 5 and all subsequent frames are to be retransmitted
ii) frame 5 is to be retransmitted
iii) frame 4 and all subsequent frames are to be retransmitted
iv) none of the above.

b. In Go-back-N ARQ, if a NAK5 is lost, then

i) station A will eventually time out on the frame 4 and retransmit frame 4 and all subsequent frames.
ii) station A will eventually time out on the frame 5 and retransmit frame 5 and all the subsequent frames.
iii) station A will not be able to detect the case.
iv) none of the above.

3.6.2. Question for short answer

a) Briefly discuss the possible types of errors that occur in frame transmission between two stations.

3.6.3. Analytical questions

a) Briefly discuss the different ingredients of ARQ.
b) Discuss Stop-and-wait ARQ.
c) Discuss Go-back-N ARQ.
d) Discuss Selective-reject ARQ.

Lesson 4 : HDLC and Data Link Control Protocol

4.1. Learning Objectives

On completion of this lesson you will be able to :

- learn details of a widely used data link protocol named High-level Data Link Control (HDLC)
- learn names of other variants of HDLC.

4.2. Introduction

A number of very similar data link control protocols have achieved wide-spread use :

- **High-level Data Link Control (HDLC)** : developed by the International Organization for Standardization (ISO 3309, ISO 4335).
- **Advanced Data Communication Control Procedures (ADCCP)** : developed by the American National Standards Institution (ANSI X3.66). With very minor exceptions, ADCCP has been adopted by the U.S. National Bureau of Standards (FIPS PUB 71-1) for use of federal government procurements, and by the Federal Telecommunications Standards Committee (FED-STD-10034) as the standard for the national-defense-related national Communications Systems.
- **Link Access Procedure, Balanced (LAP-B)** : adopted by the International Telegraph and Telephone Consultative Committee (CCITT) as part of its X.25 packet switched network standard.
- **Synchronous Data Link Control (SDLC)** : used by IBM. This is not a standard, but is in wide-spread use.

There are virtually no differences between HDLC and ADCCP. LAP-B is a subset of HDLC. SDLC is also a subset HDLC, but also includes several minor additional features.

4.3. Basic Characteristics of HDLC

HDLC defines three types of stations, two link configurations, and three data transfer modes of operation.

The three station types are :

- **Primary station** : has the responsibility for controlling the operation of the link. Frames issued by the primary station are called **commands**.
- **Secondary station** : operates under the control of the primary station. Frames issued by the secondary station(s) are called **responses**. The primary maintains a separate logical link with each secondary station on the line.
- **Combined station** : combines the features of primary and secondary stations. A combined station may issue both commands and responses.

The two link configurations are :

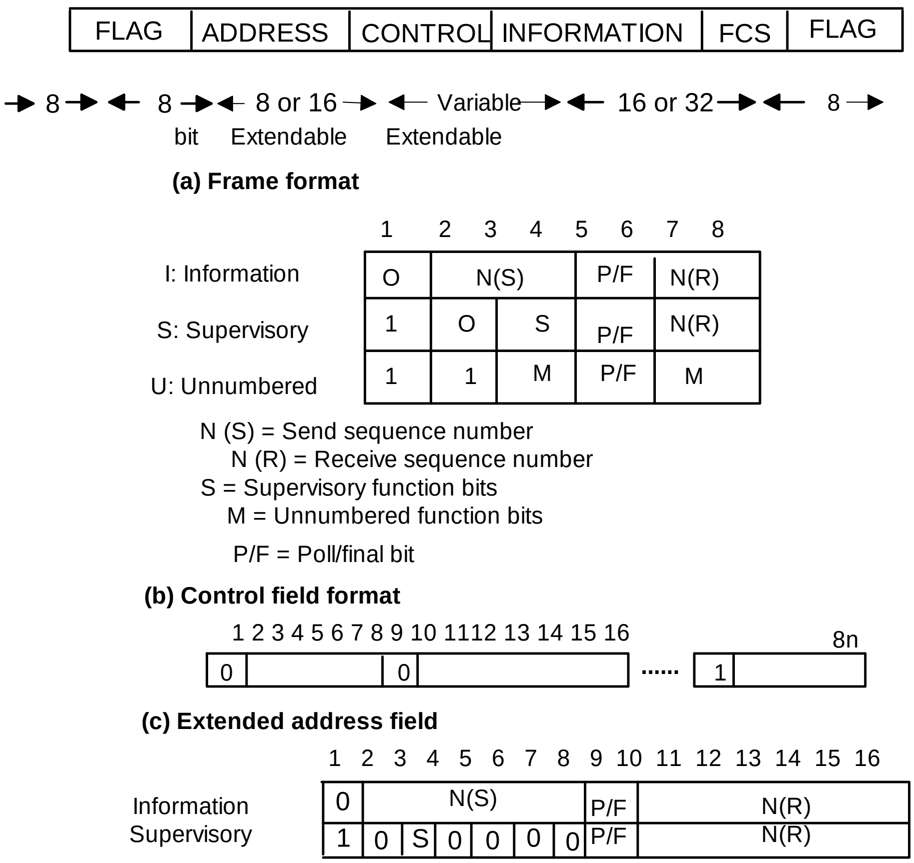
- **Unbalanced configuration** : used in point-to-point and multipoint operations. This configuration consists of one primary and one or more secondary stations and support both full-duplex and half-duplex transmissions.
- **Balanced configuration** : used only in point-to-point operation. This configuration consists of two combined stations and supports both full-duplex and half-duplex transmissions.

The three data transfer modes of operation are :

- **Normal Response Mode (NRM)** : This is an unbalanced configuration. The primary may initiate data transfer to a secondary, but a secondary may only transmit data in response to a poll from the primary.
- **Asynchronous Balanced Mode (ABM)** : This is a balanced configuration. Either combined station may initiate transmission without receiving permission from the other combined station.
- **Asynchronous Response Mode (ARM)** : This is an unbalanced configuration. In this mode, the secondary may initiate transmission without explicit permission of the primary (i.e., send a response without waiting for a command). The primary still retains responsibility for the line, including initialization, error recovery, and logical disconnection.

4.4. Frame Structure of HDLC

HDLC uses synchronous transmission. All transmissions are in frames, and a single frame format suffices for all types of data and control exchanges.



(a) Frame format

N (S) = Send sequence number
N (R) = Receive sequence number
S = Supervisory function bits
M = Unnumbered function bits
P/F = Poll/final bit

(b) Control field format

(c) Extended address field

(d) Extended control fields

Fig. 6.5: HDLC frame structure.

Figure 6.5 depicts the structure of the HDLC frame. The frame has the following fields :

- **Flag** : 8 bits
- **Address** : One or more octets
- **Control** : 8 or 16 bits
- **Information** : variable
- **Frame Check Sequence (FCS)** : 16 or 32 bits
- **Flag** : 8 bits.

The flag, address, and control fields that precede the data field are known as a **header**. The FCS and flag fields following the data field are referred to as a **trailer**.

Flag Fields

Flag fields delimit the frame at both ends with the unique pattern 01111110. A single flag may be used as the closing flag for one frame and the opening flag for the next. All active stations attached to the link are continuously hunting for the flag sequence to synchronize on the start of a frame. While receiving a frame, a station continues to hunt for that sequence to determine the end of the frame. However, since the HDLC frame allows arbitrary bit patterns, there is no assurance that the pattern 01111110 will not appear somewhere inside the frame, thus destroying frame-level synchronization. To avoid this problem, a procedure known as **bit stuffing** is used. The transmitter will always insert an extra 0 bit after each occurrence of five 1's in the frame. After detecting a starting flag, the receiver monitors the bit stream. When a pattern of five 1's appears, the sixth bit is examined. If this bit is 0, it is deleted. If the sixth bit is a 1 and the seventh bit is a 0, the combination is accepted as a flag. If the sixth and seventh bits are both 1, the sending station is signaling an abort condition. With the use of bit stuffing, arbitrary bit patterns can be inserted into the data field of the frame. This property is known as **data transparency**. An example of the bit stuffing is given below :

Bit stuffing

Original pattern : 111111111111011111101111110
After bit stuffing : 1111101111101101111101011111010

Address Field

The address field is used to identify the secondary station that transmitted or is to receive the frame. This field is not needed for point-to-point links, but is always included for the sake of uniformity. An address is normally eight bits long but, by prior agreement, an extended format may be used in which the address length is a multiple of seven bits. The least significant bit in each octet is 1 or 0 according as it is or is not the last octet of the address field. The remaining seven bits form part of the address. The single octet address of 11111111 is interpreted as the all-stations address in both basic and extended formats. It is used to allow the primary to broadcast a frame for reception by all secondaries.

Control Field

HDLC defines three types of frames, each with a different control field format. **Information frames (I-frames)** carry the data to be transmitted for the station, known as **used data**. Additionally, flow and error control data, using ARQ mechanism, may be piggybacked on an information frame. **Supervisory frames (S-frames)** provide the ARQ mechanism when piggybacking is not used, and **unnumbered frames (U-frames)** provide supplemental link control functions. The first one or two bits of the control field serves to identify the frame type, the remaining bit positions are organized into subfields as indicated in figure 6.6(b) and (d). Note that the basic control field for S- and I-frames uses 3-bit sequence numbers. With the appropriate set-mode command, an extended control field can be used for S- and I-frames that employs 7-bit sequence numbers.

Information Field

HDLC defines three types of frames, each with a different control field format.

The information field is present only in I-frames and some unnumbered frames. The field can contain any sequence of bits. Its length is undefined in the standard, but is generally limited by each implementation to a specified maximum.

Frame Check Sequence Field

The frame check sequence is applied to the remaining bits of the frame, exclusive of flags. The normal FCS is the 16-bit CRC-CCITT. An optional 32-bit FCS, using CRC-32, may be employed if the frame length or line reliability dictates this choice.

4.5. Exercise

4.5.1. Multiple choice questions

a. In HDLC, a command is issued by

i) primary station
ii) secondary station
iii) both primary and secondary stations
iv) none of the above.

b. In HDLC, a response is issued by

i) primary station
ii) secondary station
iii) both primary and secondary stations
iv) none of the above.

c. In HDLC, unbalanced configuration is used

i) only in point-to-point operation
ii) only in multipoint operation
iii) in both point-to-point and multipoint operations
iv) none of the above.

4.5.2. Questions for short answers

a) Name the different widely used data link protocol along with their standardizing organization.
b) What is a command in HDLC?
c) What is a response in HDLC?
d) What is a primary station in HDLC?
e) What is a secondary station in HDLC?
f) What is a combined station in HDLC?
g) Name the header fields and trailer fields of HDLC.
h) Name the different fields of HDLC.

4.5.3. Analytical questions

a) Discuss the characteristics of HDLC.
b) Discuss the different fields of HDLC frame format.
c) Discuss the bit stuffing procedure in HDLC.

Lesson 5 : Operation of HDLC

5.1. Learning Objectives

On completion of this lesson you will be able to :

- grasp the operation of HDLC.

5.2. Introduction

The operation of HDLC consists of the exchange of I-frames, S-frames, and U-frames between a primary and a secondary or between two primaries. To describe HDLC operation, we will discuss these three types of frames.

5.3. Information Frames

The basic operation of HDLC involves the exchange of information frames (I-frames) containing user-data. Each I-frame contains the sequence number of the transmitted frame as well as a piggybacked positive acknowledgment. The acknowledgment is the sequence number of the **next** frame expected. A maximum window size of 7 or 127 is allowed. The I-frame also contains a poll/final (P/F) bit. The bit is a poll bit for commands (from primary) and a final bit (from secondary) for responses. In normal response mode (NRM), the primary issues a poll giving permission to send by setting the poll bit to 1, and the secondary sets the final bit to 1 on the last I-frame of its response. In asynchronous response mode (ARM) and asynchronous balanced mode (ABM), the P/F bit is sometimes used to coordinate the exchange of S- and U-frames.

*The acknowledgment is the sequence number of the **next** frame expected.*

5.4. Supervisory Frames

The supervisory frames (S-frames) is used for flow and error control. Both go-back-N (REJ) and selective-reject (SREJ) ARQ are allowed. The latter is rarely implemented because of the buffering requirements. A frame may be positively acknowledged with a receive ready (RR) when an I-frame is not available for piggybacking. In addition, a receive not ready (RNR) is used to accept a frame but request that no more I-frames be sent until a subsequent RR is used. For the RR, RNR, and REJ frames, N(R) indicates the sequence number of the next expected I-frame. For SREJ, N(R) is the sequence number of the rejected frame.

The supervisory frames (S-frames) is used for flow and error control.

The P/F bit on a supervisory frame may be employed as follows. The primary may set the P bit in an RR frame to poll the secondary. This is done when the primary has no I-frame upon which to piggyback the poll. The secondary responds with an I-frame if it has one; otherwise, it sends an RR with the F bit set to indicate that it has no data to send. The primary (combined station) may set the P bit in the RNR command to solicit the receiver status of a secondary/combined station. The response will be an RR with the F bit set if the station can receive I-frames, and an RNR with the F bit set if the station is busy.

5.5. Unnumbered Frames

Unnumbered frames are used for a variety of control functions. These frames do not carry sequence numbers and do not alter the sequencing or flow of numbered I-frames. We can group these frames into the following categories :

- Mode-setting commands and responses.
- Information transfer commands and responses.
- Recovery commands and responses.
- Miscellaneous commands and responses.

Mode-setting commands are transmitted by the primary/combined station to initialize or change the mode of the secondary/combined station. The secondary/combined station acknowledges acceptance by responding with an unnumbered acknowledgment (UA) frame; the UA has the F bit set to the same value as the received P bit. Once established, a mode remains in effect at a secondary station until the next mode-setting command is accepted, and at a combined station until the next mode-setting command is either accepted or transmitted and acknowledged. Upon acceptance of any of the commands Set Normal Response/Extended Mode (SNRM/SNRME), Set Asynchronous Response/Extended Mode (SARM/SARME), Set Asynchronous Balanced/Extended Mode (SABM/SABME), the I-frame sequence numbers in both directions are set to 0. The Set Initialization Mode (SIM) command is used to cause the addressed secondary/combined station to initiate a station-specified procedure to initialize its data link control functions (e.g., accept a new program or update operational parameters). While in initialization mode, the required information is sent using unnumbered information (UI) frames. The Disconnect command (DISC) is used to inform the addressed station that the transmitting station is suspending operation.

The secondary/combined station acknowledges acceptance by responding with an unnumbered acknowledgment (UA).

Information transfer commands and responses are used to exchange information between stations. This is done primarily through the Unnumbered Information (UI) command/response. Example of UI frame information are higher-level status, operational interruption, time of day, and link initialization parameters. The Unnumbered Poll (UP) command is used to solicit an unnumbered response, as a way of establishing the status of the addressed station.

Recovery commands and responses are used when the normal ARQ mechanism does not apply or will not work. The Frame Reject (FRMR) response is used to report an error in a received frame, such as :

- Invalid control field.
- Data field to long.
- Data field not allowed with received frame type.
- Invalid receive count (i.e., a frame is acknowledged that has not yet been sent).

The Reset (RSET) command is used to clear the FRMR condition. RSET announces that the sending station is resetting its send sequence number, and the addressed station should reset its receive sequence number.

Miscellaneous commands/responses fit into no neat category. The Exchange Identification (XID) command/response is used for two stations to exchange station identification and the characteristics of the two stations. The actual information exchanged is implementation dependent. A Test (TEST) command/response is used for testing that the link and the addressed station are still functioning. A test command must be echoed with a test response at the earliest opportunity.

5.6. Exercise

5.6.1. Multiple choice question

a. The operation of HDLC consists of the exchange of

i) I-frames between a primary and a secondary or between two primaries.
ii) S-frames between a primary and a secondary or between two primaries.
iii) U-frames between a primary and a secondary or between two primaries.
iv) all of the above.

5.6.2. Questions for short answers

a) Name the categories of Unnumbered frames in HDLC.
b) Name the different mode-setting commands and responses in HDLC.
c) Name the different information transfer commands and responses in HDLC.
d) Name the different recovery commands and responses in HDLC.
e) Name the different miscellaneous commands and responses in HDLC.

5.6.3. Analytical question

a) Discuss different types of frames in HDLC.

Unit 7 : Multiplexing

Introduction

Transmission facilities are, by and large, expensive. It is often the case that two communicating stations will not utilize the full capacity of a data link. For efficiency, it should be possible to share that capacity. The generic term for such sharing is **multiplexing**. In this unit different types of multiplexing is discussed.

Lesson 1 : Frequency Division Multiplexing

1.1. Learning Objectives

On completion of this lesson you will be able to :

- know the classification of multiplexing techniques
- know details of frequency-division multiplexing technique.

1.2. Classification Of Multiplexing Techniques

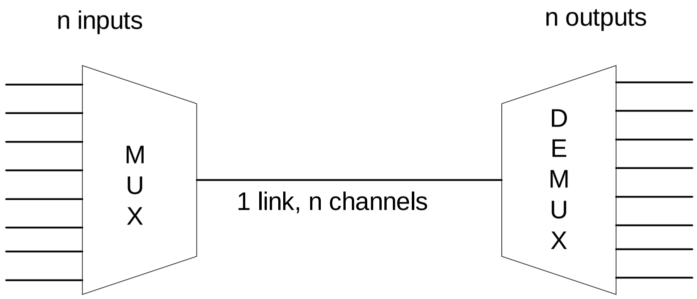


Fig. 7.1: Multiplexing.

Figure 7.1 depicts the multiplexing function generically. There are n inputs to a multiplexer. The multiplexer is connected by a single data link to a demultiplexer. The link is able to carry n separate **channels** of data. The multiplexer combines (multiplexes) data from the n input lines and transmits over a higher-capacity data link. The demultiplexer accepts the multiplexed data stream, separates (demultiplexes) the data according to channel, and delivers them to the appropriate output lines.

Multiplexing techniques are of two types:

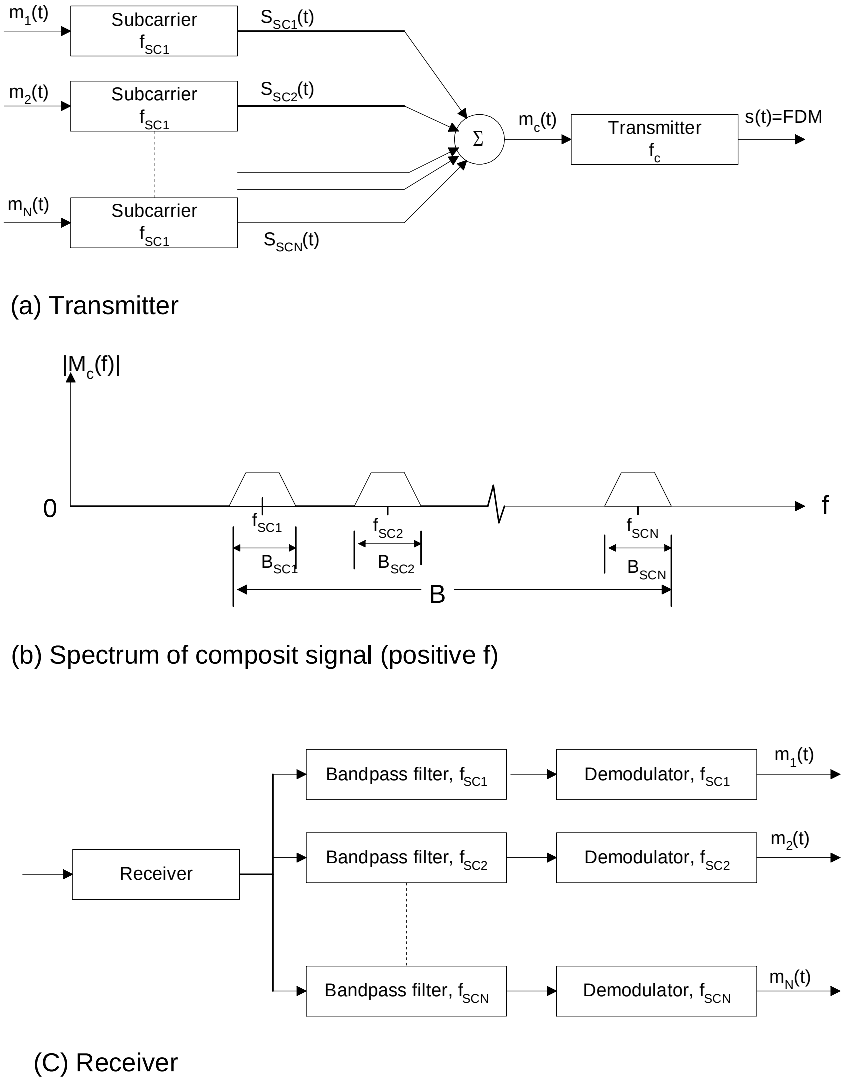
- Frequency-division multiplexing (FDM)
- Time-division multiplexing (TDM).

TDM are of two types:

- Synchronous TDM
- Statistical TDM.

1.3. Frequency Division Multiplexing

Frequency-division multiplexing (FDM) is possible when the useful bandwidth of the medium exceed the required bandwidth of signals to be transmitted. A number of signals can be carried simultaneously if each signal is modulated onto a different carrier frequency, and the carrier frequencies are sufficiently separated that the bandwidths of the signals do not overlap.



(a) Transmitter

(b) Spectrum of composit signal (positive f)

(C) Receiver

Fig. 7.2: Frequency division multiplexing.

Each modulated signal requires a certain bandwidth centered around its carrier frequency, referred to as a **channel**. To prevent interference, the channels are separated by **guard bands**, which are unused portion of the spectrum. The composite signal transmitted across the medium is analog. Note, however, that the input signals may be either digital or analog.

Each modulated signal requires a certain bandwidth centered around its carrier frequency, referred to as a channel.

A generic depiction of an FDM system is shown in figure 7.2. A number of analog or digital signals [$m_i(t)$, i=1,N] are to be multiplexed onto the same transmission medium. Each signal $m_i(t)$ is modulated onto a carrier f_{sci}; since multiple carrier are to be used, each is referred to as a **subcarrier**. Any type of modulation may be used. The resulting analog, modulated signals are then summed to produce a composite signal $m_c(t)$. Figure 7.2(b) shows the result. The spectrum of signal $m_c(t)$ is shifted to be centered on f_{sci}. For this scheme to work, f_{sci} must be chosen so that the bandwidth of the various signals do not overlap. Otherwise, it will be impossible to recover the original signals. The composite signal may then be shifted as a whole to another carrier frequency by an additional modulation step. This second modulation step need not use the same modulation techniques as the first. The composite signal has a total bandwidth, B, where $\mathbf{B} < \sum_{i=1}^{N} B_{sci}$. This analog signal may be transmitted over a suitable medium. At the receiving end, the composite signal is passed through N bandpass filters, each filter centered on f_{sci} and having width B_{sci}, for $1 \leq i \leq N$. In this way, the signal is again split into its component parts. Each component is then demodulated to recover the original signal.

1.4. Exercise

1.4.1. Multiple choice questions

a. In FDM, the composite signal transmitted across the medium is

i) analog
ii) digital
iii) either analog or digital
iv) both analog and digital.

b. In FDM, the composite signal has a total bandwidth B, where

i) $B = \sum_{i=1}^{N} B_{sci}$
ii) $B > \sum_{i=1}^{N} B_{sci}$
iii) $B < \sum_{i=1}^{N} B_{sci}$
iv) none of the above.

1.4.2. Questions for short answers

a) Give the classification of multiplexing techniques.
b) What is guard bands in FDM system?
c) What is a subcarrier in FDM system?

1.4.3. Analytical question

a) Discuss the FDM technique.

Lesson 2 : Time Division Multiplexing

2.1. Learning Objectives

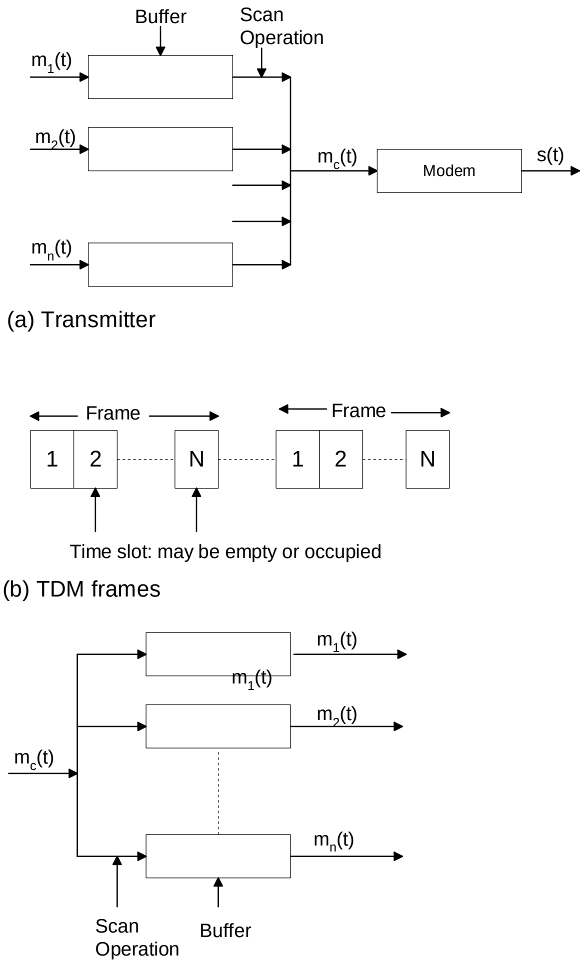
On completion of this lesson you will be able to :

- learn details of Synchronous TDM
- learn details of Statistical TDM.

2.2. Synchronous Time-Division Multiplexing

Synchronous time-division Multiplexing is possible when the achievable data rate of the medium exceeds the data rate of digital signals to be transmitted. Multiple digital signals (or analog signals carrying digital data) can be carried on a single transmission path by interleaving portions of each signal in time.

Multiple digital signals can be carried on a single transmission path by interleaving portions of each signal in time.



(a) Transmitter

(b) TDM frames

(c) Receiver

Fig. 7.3: Synchronous time-division multiplexing.

A generic depiction of a synchronous TDM system is provided in figure 7.3. A number of signals [$m_i(t)$, i=1,N] are to be multiplexed onto the same transmission medium. The signals carry digital data and are generally digital signals. The incoming data from each source are briefly buffered. Each buffer is typically one bit or one character in length. The buffers are scanned sequentially to form a composite digital data stream $m_c(t)$. The scan operation is sufficiently rapid so that each buffer is emptied before more data can arrive. Thus the data rate of $m_c(t)$ must at least equal the sum of the data rates of the $m_i(t)$. The digital signal $m_c(t)$ may be transmitted directly, or passed through a modem so that an analog signal is transmitted. In either case, transmission is typically synchronous. The transmitted data may have a format something like figure 7.3(b). The data are organized into frames. Each frame contains a cycle of time slots. In each frame, one or more slots is dedicated to each data source. The sequence of slots dedicated to one source, from frame to frame, is called a **channel**. The slot length equals the transmitted buffer length, typically a bit or a character. At the receiver, the interleaved data are demultiplexed and routed to the appropriate destination buffer. For each input source $m_i(t)$, there is an identical output source which will receive the input data at the same rate at which it was generated.

The slot length equals the transmitted buffer length, typically a bit or a character.

2.3. Statistical Time-Division Multiplexing

In a synchronous time-division multiplexing, it is generally the case that many of the time slots in a frame are wasted. An alternative to synchronous TDM is **statistical TDM**. The statistical multiplexer exploits this common property of data transmission by dynamically allocating time slots on demand. As with a synchronous TDM, the statistical multiplexer has a number of I/O lines on one side and a higher speed multiplexed line on the other. Each I/O line has a buffer associated with it. In the case of the statistical multiplexer, there are n I/O lines, but only k, where k < n, time slots available on the TDM frame. For input, the function of the multiplexer is to scan the input buffers, collecting data until a frame is filled, and then send the frame. On output, the multiplexer receives a frame and distributes the slots of data to the appropriate output buffers. Since data arrive from and are distributed to I/O lines unpredictably, address information is required to assure proper delivery.

The statistical multiplexer exploits this common property of data transmission by dynamically allocating time slots on demand.

2.4. Exercise

2.4.1. Multiple choice questions

a. TDM system is used for

i) only analog input signals
ii) only digital input signals
iii) both analog and digital signals
iv) none of the above.

b. The data rate of the composite signal $m_c(t)$ of a synchronous TDM system

i) must equal the sum of the data rates of the input signal $m_i(t)$.
ii) must at least equal the sum of the data rates of the input signal $m_i(t)$.
iii) must be less than the sum of the data rates of the input signal $m_i(t)$.
iv) none of the above.

c. In statistical TDM system, the number of time slots

i) is equal to the number of input I/O lines
ii) is greater than the number of input I/O lines.
iii) is less than the number of input I/O lines.
iv) none of the above.

2.4.2. Questions for short answer

a) Why is the number of time slots in statistical TDM system kept less than the number of input I/O lines?

2.4.3. Analytical questions

a) Discuss synchronous TDM system.
b) Discuss statistical TDM system.

Unit 8 : Switched Data Communication Networking

Introduction

In a computer network, generally computers are not connected by point-to-point links. Often they are connected to a data communication network.

Data communication networks can be categorized as follows:

- Switched networks
  - Circuit-switched networks
  - Packet-switched networks.

- Broadcast network
  - Local area networks (LANs)
  - Metropolitan area networks (MANs).

In this unit, switched networks, viz., circuit-switched networks and packet-switched networks are discussed. Broadcast networks are discussed in the next unit.

Lesson 1 : Circuit Switching

1.1. Learning Objectives

On completion of this lesson you will be able to :

- understand operation of switching networks
- understand circuit switching.

1.2. Switching Networks

A collection of devices that need to communicate; we refer to them generically as station. Each station attaches to a network node.

In a network, there is a collection of devices that need to communicate; we refer to them generically as **station**. Each station attaches to a network **node**. The set of nodes to which stations attach is the boundary of the communication network, which is capable of transferring data between pairs of attached stations. The communication network is not concerned with the content of the data exchanged between stations; its purpose is simply to move those data from source to destination.

A **switched communication network** consists of an interconnected collection of nodes; in which data are transmitted from source station to destination station by being routed through

Data entering the network from a station are routed to the destination by being switched from node to node.

the network of nodes. Figure 8.1 is a simplified illustration of the concept. The nodes are connected by transmission paths. Data entering the network from a station are routed to the destination by being switched from node to node. For example, data from station A intended for station F are sent to node 4. They may then be routed via nodes 5 and 6 or nodes 7 and 6 to the destination. Several observations are in order:

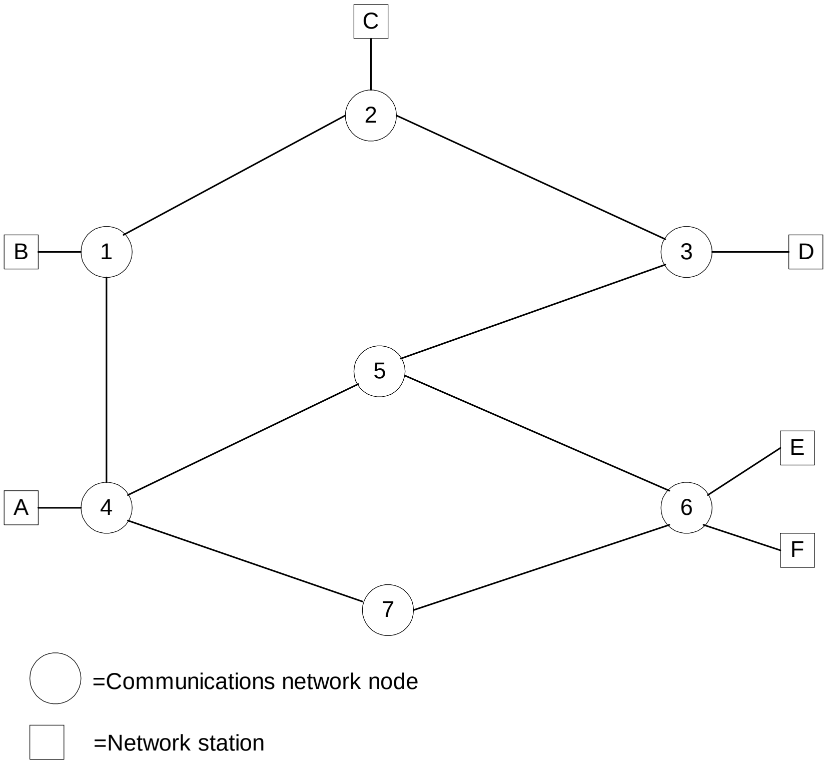


Fig. 8.1: Generic switching network.

1. Some nodes connect only to other nodes. Their sole task is the internal switching of data. Other nodes have one or more stations attached as well; in addition to their switching functions, such nodes accept data from and deliver data to the attached stations.
2. Node-node links are usually multiplexed links, using either FDM or TDM.
3. Usually, the network is not fully connected; that is, there is not a direct link between every possible pair of nodes. However, it is always desirable to have more than one possible path through the network for each pair of stations. This enhances the reliability of the network.

1.3. Circuit Switching

Communication via circuit switching implies that there is a dedicated communication path between two stations. That path is a connected sequence of links between network nodes. On each physical link, a channel is dedicated to the connection.

Communication via circuit switching involves three phases, which can be explained with reference to figure 8.1.

Communication via circuit switching implies that there is a dedicated communication path between two stations.

1. **Circuit establishment**. Before any signals can be transmitted, an end-to-end (station-to-station) circuit must be established. For example, station A sends a request to node 4 requesting a connection to station E. Typically, the link from A to 4 is a dedicated line, so that part of the connection already exists. Node 4 must find the next leg in a route leading to node 6. Based on routing information and measures of availability and perhaps cost, node 4 selects the link to node 5, allocates a free channel on that link and sends a message requesting connection to E. So far, a dedicated path has been established from A through 4 to 5. The remainder of the process proceeds similarly. Node 5 dedicates a channel to node 6 and internally ties that channel to the channel from node 4. Node 6 completes the connection to E. In completing the connection, a test is made to determine if E is busy or is prepared to accept the connection.
2. **Data transfer**: Information can now be transmitted from A through the network to E.
3. **Circuit disconnect**. After some period of data transfer, the connection is terminated, usually by the action of one of the two stations. Signals must be propagated to nodes 4, 5, and 6 to deallocate the dedicated resources.

Note that the connection path is established before data transmission begins and channel is dedicated for the duration of a connection, even if no data are being transferred. Thus circuit switching can be rather inefficient.

1.4. Exercise

1.4.1. Multiple choice question

a. In a circuit switching network

i) a dedicated communication path is established between two stations before data transfer begins.
ii) a communication path is established when data is ready for transmission.
iii) any of the above two may be adopted.
iv) none of the above.

1.4.2. Question for short answer

a) Define station and node in a switching network.

1.4.3. Analytical question

a) Discuss different phases of communication via a circuit-switching network.

Lesson 2 : Control Signaling in Circuit-Switched Network

2.1. Learning Objectives

On completion of this lesson you will be able to :

♦ learn details of control signaling needed in a circuit-switched network.

2.2. Signaling Functions

The functions performed by control signaling.

In a circuit-switched network, control signals are the means by which the network is managed and by which calls are established, maintained, and terminated. The functions performed by control signaling are as follows:

1. Audible communication with the station, including dial tone, ringing tone, busy signal, and so on.
2. Transmission of the number dialed to switching offices that will attempt to complete a connection.
3. Transmission of information between switches indicating that a call con not be completed.
4. Transmission of information between switches indicating that a call has ended and that the path can be disconnected.
5. A signal to make a station ring.
6. Transmission of information used for billing purposes.
7. Transmission of information giving the status of equipment or trunks in the network. This information may be used for routing and maintenance purposes.
8. Transmission of information used in diagnosing and isolating system failures.
9. Control of special equipment such as satellite channel equipment.

An example of the use of control signaling is shown in figure 8.2, which illustrates a typical connection sequence from one station to another in the same node. The steps involved appears as circled numbers in the figure:

1. Prior to the call, both stations are not in use (on-hook). The call begins when one station lifts the receiver (off-hook), which is automatically signaled to switch.
2. The switch responds with an audible dial tone, signaling the station that the number may be dialed.
3. The caller dials the number, which is communicated as a destination address to the switch.

4. If the called station is not busy, the switch alerts the station to an incoming call by sending a ringing signal, which causes the station to ring.

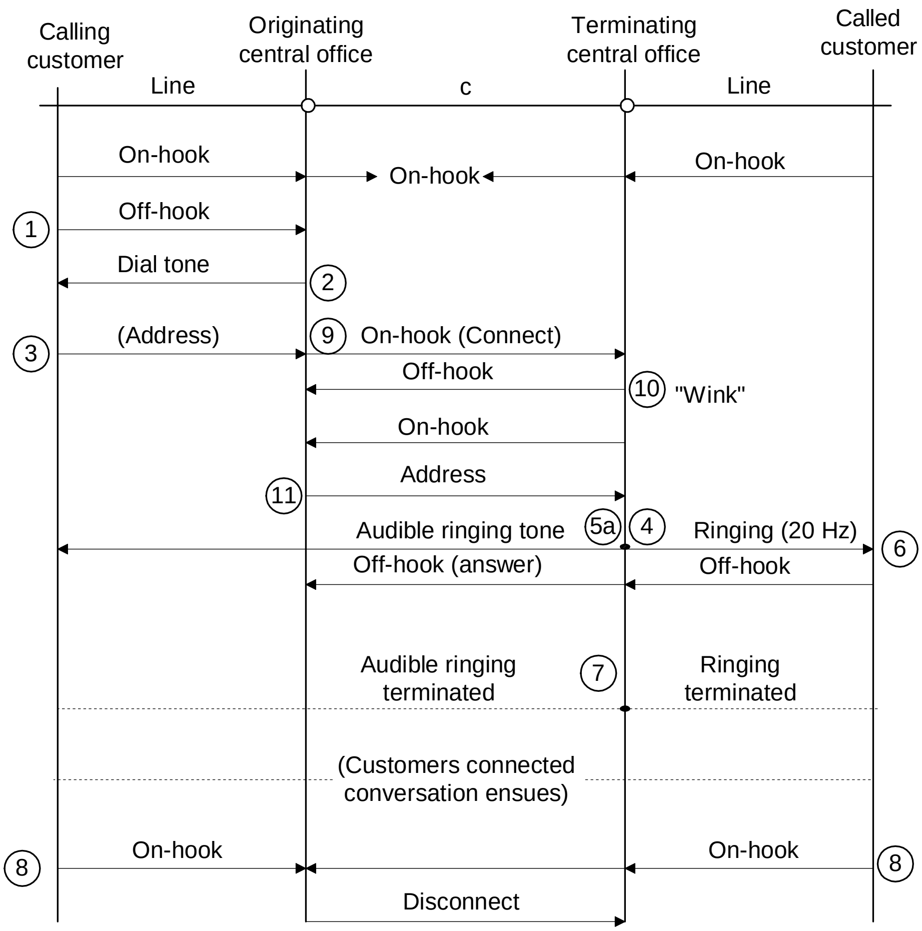


Fig. 8.2: Signaling on a typical completed call.

5. Feedback is provided to the calling station by the switch:

    a. If the called station is not busy, the switch returns an audible ringing tone to the caller while the ringing signal is being sent to the called station.
    b. If the called station is busy, the switch sends an audible busy signal to the caller.
    c. If the call cannot be completed through the switch, the switch sends an audible “reorder” message to the caller.

6. The called station accepts the call by lifting the receiver (off-hook), which is automatically signaled to the switch.

7. The switch terminates the ringing signal and the audible ringing tone, and establishes a connection between the two stations.
8. The connection is released when either station hangs up.

When the called station is attached to a different switch than the calling station, the following switch-to-switch trunk signaling functions are required:

1. The originating switch seizes an idle interswitch trunk, sends an off-hook indication on the trunk, and requests a digit register at the far end, so that the address may be communicated.
2. The terminating switch sends an off-hook followed by an on-hook signal, known as a "wink". This indicates a register-ready status.
3. The originating switch sends the address digits to the terminating switch.

The functions performed by control signals can be roughly grouped into the following category:

- Supervisory
- Address
- Call information
- Network management.

2.3. Location of Signaling

Control signaling needs to be considered in two contexts: signaling between a station and the network and signaling within the network. Typically, signaling operates differently within these two contexts.

Control signaling needs to be considered in two contexts: signaling between a station and the network and signaling within the network.

The signaling between a station and the switching office to which it attaches is, to a large extent, determined by the characteristics of the station and the needs of the human user. Signals within the network are entirely computer-to-computer. The internal signaling is concerned not only with the management of station calls but with the management of the network itself. Thus, for this internal signaling, a more complex repertoire of commands, responses, and set of parameters is needed.

Because two different signaling techniques are used, local switching office to which the station is attached must provide a mappings between the relatively less complex signaling technique used by the station and the more complex technique used within the network.

2.4. Types of Control Signaling

The facilities for signal transmission are shared with control signaling.

Traditional control signaling in circuit-switched networks has been on a per-trunk or inchannel basis. With inchannel signaling, the same channel is used to carry control signals as is used to carry the call to which the control signals relate. Such signaling begins at the originating station and follows the same path as the call itself. This has the merit that no additional transmission facilities are needed for signaling; the facilities for signal transmission are shared with control signaling.

Two forms of inchannel signaling are in use:

- Inband signaling
- Out-of-band signaling.

Inband signaling

Inband signaling uses not only the same physical path as the call it serves, it also uses the same frequency band as the signals that are carried. This form of signaling has several advantages. Because the control signals have the same electromagnetic properties as the signals, they can go anywhere that the signals go. Thus there are no limits on the use of inband signaling anywhere in the network, including places where analog-to-digital or digital-to-analog conversion takes place. In addition, it is impossible to set up a call on a faulty path, since the control signals that are used to set up that path would have to follow the same path.

Out-of-band signaling

In **out-of-band signaling**, a separate narrow signaling band is used to send control signals. The major advantage of this approach is that the control signals can be sent whether or not signals are on the line, thus allowing continuous supervision and control of a call. However, an out-of-band scheme needs extra electronics to handle the signaling band, and the signaling rates are slower because the signaling has been confined to a narrow bandwidth.

The information transfer rate is quite limited with inchannel signaling. It is difficult to accommodate, in a timely fashion, any but the simplest form of control messages. A second drawback of inchannel signaling is the amount of delay from the time a station enters an address and the connection is established. Both of these problems can be addressed with **common channel signaling**, in which control signals are carried over paths completely independent of the signal channel. One independent control signal path can carry the signals for a number of station channels, and hence is a common control channel for these station channels.

Two modes of operation are used in common channel signaling. In the **associated mode**, the common channel closely tracks along its entire length the interswitch trunk groups that are served between endpoints. The control signals are on different channels from the station signals, and inside the switch, the control signals are routed directly to a control signal processor. A more complex, but the more powerful, mode is the **nonassociated mode**. With this mode, the network is augmented by additional nodes, known as signal transfer points. There is now no close or simple assignment of control channels to trunk groups. In effect, there are now two separate networks, with links between them so that the control portion of the network can exercise control over the switching nodes that are servicing the station calls. Networks management is more easily exerted in the nonassociated mode since control channels can be assigned to task in a more flexible manner.

Two modes of operation are used in common channel signaling.

2.5. Exercise

2.5.1. Multiple choice questions

a. The signaling within the network is concerned with the management of

i) the station calls
ii) the networks
iii) all of the above
iv) none of the above.

b. With inchannel signaling

i) the same channel is used to carry control signals.
ii) a different channel on the same physical path is used to carry control signals.
iii) a different physical path is used to carry control signals.
iv) none of the above.

c. With common channel signaling

i) the same channel is used to carry control signals.
ii) a different channel on the same physical path is used to carry control signals.
iii) a different physical path is used to carry control signals.
iv) none of the above.

2.5.2. Questions for short answers

a) What is a “wink”?

b) Name the different categories of functions performed by control signals.

c) What is the merit of inchannel signaling?

d) Name the different types of inchannel signaling.

e) What are the demerits of inchannel signaling?

2.5.3. Analytical questions

a) Discuss the functions performed by control signaling.

b) With neat figure, illustrate the steps involved in a typical connection sequence from one station to another in the same node.

c) Discuss the function of switch-to-switch trunk signaling.

d) Discuss the advantages and disadvantages of out-of-band signaling.

e) Discuss the modes of operation of common channel signaling.

Lesson 3 : Packet Switching

3.1. Learning Objectives

On completion of this lesson you will be able to :

- introduce yourself to packet-switched network principles
- understands the switching technique used in packet-switched network.

3.2. Introduction

A key characteristic of circuit-switched networks is that resources within the network are dedicated to a particular call. For data connection on circuit-switched network, two shortcoming became apparent:

- In a typical terminal-to-host data connection, much of the time the line is idle.
- The connection provides for transmission at constant data rate. Thus each of the two devices that are connected must transmit and receive at the same data rate as the other. This limits the utility of the network in interconnecting a variety of host computers and terminals.

Each packet contains a portion (or all for a short message) of the user's data plus some control information.

Packet switching addresses these problems of circuit switching. In **packet switching** data are transmitted in short packets. If a source has a larger message to send, the message is broken up into a series of packets. Each packet contains a portion (or all for a short message) of the user's data plus some control information. At each node en route, the packet is received, stored briefly, and passed on to the next node. Let us consider figure 8.1, but now consider that this is a simple packet-switched network. Consider a packet to be sent from station A to station E. The packet will include control information that indicates that the intended destination is E. The packet is sent from station A to node 4. Node 4 stores the packet, determines the next leg of the route (say 5), and queues the packet to go out on that link (the 4-5 link). When the link is available, the packet is transmitted to node 5, which will forward the packet to node 6, and finally to station E.

Packet-switching has a number of advantages over circuit-switching:

- Line efficiency is greater, since a single node-to-node link can be dynamically shared by many packets over time.

- A packet-switched network can carry out data-rate conversion. Two stations of different data rates can exchange packets, since each connects to its node at its proper data rate.
- When traffic becomes heavy on a circuit-switched network, some calls are blocked; that is, the network refuses to accept additional connection requests until the load on the network decreases. On a packet-switched network, packets are still accepted, but delivery delay increases.
- Priorities can be used. Thus, if a node has a number of packets queued for transmission, it can transmit the higher-priority packet first.

3.3. Switching Technique

There are two approaches of routing stream of packets through the network and deliver them to the intended destination:

- Datagram
- Virtual circuit.

Two approaches of routing stream of packets through the network.

In the **datagram** approach, each packet is treated independently, with no reference to packets that have gone before. Suppose that station A in figure 8.1 has a three-packet message to send to station E. It transmits the packets, 1-2-3, to node 4. On each packet, node 4 must make a routing decision. Packet 1 arrives for delivery to station E. Node 4 could plausibly forward this packet to either node 5 or node 7 as the next step in the route. Similarly, node 4 could forward packets 2 and 3 to either node 5 or node 7. So the packets, each with the same destination address, do not all follow the same route. Thus it is possible that the packets will be delivered to station E in a different sequence from the one in which they were sent. It is up to station E to figure out how to reorder them and to detect the loss of a packet and figure out how to recover it. In this technique, each packet, treated independently, is referred to as a datagram.

In the **virtual circuit** approach, a preplanned route is established before any packets are sent. For example, suppose that, in figure 8.1, station A has one or more packets to send to station E. It first sends a special control packet, referred to as a Call Request packet, to node 4, requesting a logical connection to station E. Node 4 decides to route the request and all subsequent packets to node 5, which decides to route the request and all subsequent packets to node 6, which finally delivers the Call Request to station E. If station E is prepared to accept the connection, it sends a Call Accept packet to node 6. This packet is passed back through nodes 5 and 4 to station A. Stations A and E may now exchange data over the route that has been established. Because the route is fixed for the duration of the logical connection, it is some what similar to a circuit in a circuit-switching network and is referred to as a virtual circuit. Each packet now contains a virtual circuit identifier as well as data. Each node on the preestablished route knows where to direct such packets; no routing decisions are required. Eventually, one of the stations terminates the connection with a Clear Request packet. At any time, each station can have more than one virtual circuit to any other station and can have virtual circuits to more than one stations. The main characteristic of the virtual-circuit technique is that a route between stations is set up prior to data transfer. Note that this does not mean that this is a dedicated path, as in circuit switching.

The route is fixed for the duration of the logical.

3.4. Exercise

3.4.1. Multiple choice questions

a. In a virtual-circuit packet switching technique

i) a route between stations is set up prior to data transfer.
ii) a route between stations is set up independently for each packet.
iii) a physical path between stations is set up prior to data transfer.
iv) either (i) or (ii) may be used.

b. In a datagram packet switching technique

i) a route between stations is set up prior to data transfer.
ii) a route between stations is set up independently for each packet.
iii) a physical path between stations is set up prior to data transfer.
iv) either (i) or (ii) may be used.

3.4.2. Questions for short answers

a) What are the shortcomings of data connection on a circuit-switched network?
b) Name the different switching technique used in packet switching.

3.4.3. Analytical questions

a) Discuss the advantages of packet-switching over circuit-switching.
b) Discuss datagram technique of packet switching.
c) Discuss virtual circuit technique of packet switching.

Lesson 4 : Routing in Packet-Switched Network

4.1. Learning Objectives

On completion of this lesson you will be able to :

- introduce yourself to the routing function
- learn a least-cost routing algorithm
- learn routing strategies.

4.2. Introduction

The primary function of a packet-switched network is to accept packets from a source station and deliver them to a destination station. To accomplish this, a path or route through the network must be selected; generally, more than one route is possible. Thus a routing function must be performed. The desirable attributes of the routing function are:

- Correctness
- Simplicity
- Robustness
- Stability
- Fairness
- Optimality
- Efficiency.

The selection of a route is generally based on some performance criterion.

With these attributes in mind, the techniques of routing are employed. The selection of a route is generally based on some performance criterion. The simplest criterion is to chose the “shortest” route through the network. This results in the least number of hops per packet (one hop = traversal of one node-to-node link). A generalization of the shortest-route criterion is least-cost routing. In this case, a cost is associated with each link, and the route through the network that accumulates the least cost is sought. For example, figure 8.3 illustrates a network in which two arrowed lines between a pair of nodes represent a link between these nodes; the numbers on the lines represent the current link cost in each direction. The shortest path from node 1 to node 6 is 1-3-6, but the least cost path is 1-4-5-6. The cost assignment is intended to support one or more design objectives. For example, the cost could be related to the capacity of the link, or the current queueing delay to use the link.

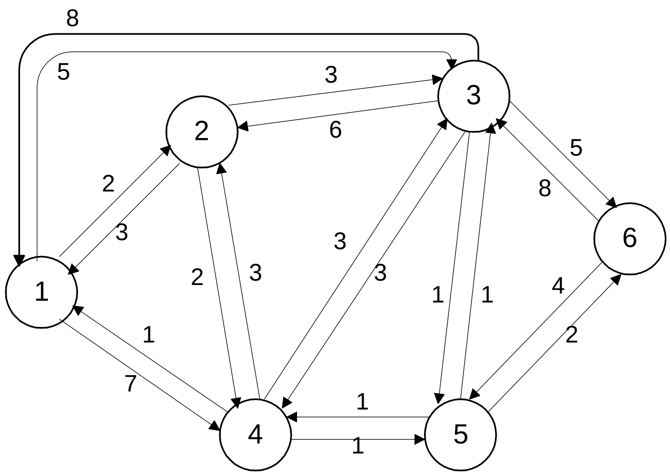


Fig. 8.3 : Example packet-switched network.

4.3. Least-Cost Routing Algorithm

Virtually all packet-switched networks base their routing decision on some form of least-cost criterion. The **least-cost routing algorithm** can be simply stated as:

Given a network of nodes connected by bidirectional links, where each link has a cost associated with it in each direction, define the cost of a path between two nodes as the sum of the costs of the links traversed. For each pair of nodes find the path with least cost.

One of the most common least-cost algorithm is **Dijkstra's algorithm**. The algorithm can be described as follows:

Dijkstra's algorithm

Define:

N = Set of nodes in the network
s = Source node
M = Set of nodes so far incorporated by the algorithm
d_{ij} = link cost from node i to node j; $d_{ii} = 0$, and $d_{ij} = \propto$ if the two nodes are not directly connected; $d_{ij} \geq 0$ if the two nodes are directly connected
D_n = cost of the least-cost path from node s to node n that is currently known to the algorithm

The algorithm has three steps; steps 2 and 3 are repeated until M = N.

1. Initialize:
   M = {s} i.e., set of nodes incorporated is only the source node.
   $D_n = d_{sn}$ for $n \neq s$ i.e., initial path costs to neighboring nodes are simply the link costs.
2. Find the neighboring node not in M that has the least-cost path from node s and incorporate that node into M:

   Find $w \notin M$ such that $D_w = \min\limits_{j \notin M} D_j$

   Add w to M.
3. Update least-cost paths:
   $D_n = \min[D_n, D_w + d_{wn}\}$ for all $n \notin M$

   If the latter term is the minimum, the path from s to n is now the path from s to w concatenated with the link from w to n.

One iteration of steps 2 and 3 adds one new node to M and defines the least-cost path from s to that node.

Table 8.1: Example of Dijkstra's Algorithm (s = 1) using figure 8.3.

Iteration	M	D_2	Path	D_3	Path	D_4	Path	D_5	Path	D_6	Path
1	{1}	2	1-2	5	1-3	1	1-4	$\propto$	-	$\propto$	-
2	{1,4}	2	1-2	4	1-4-3	1	1-4	2	1-4-5	$\propto$	-
3	{1,2,4}	2	1-2	4	1-4-3	1	1-4	2	1-4-5	$\propto$	-
4	{1,2,4,5}	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6
5	{1,2,3,4,5}	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6
6	{1,2,3,4,5,6}	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6

Table 8.1 shows the result of applying this algorithm to figure 8.3, using s = 1. Note that at each step the path to each node plus the total cost of that path is generated. After the final iteration, the least-cost path to each node and the cost of that path have been developed.

4.4. Routing Strategies

A large number of **routing strategies** have evolved. These are discussed below.

Fixed Routing

In fixed routing, a route is selected for each source-destination pair of nodes in the network using least-cost routing algorithm. The routes are fixed, or at least only change when there is a change in the topology of the network. In this routing, there is no difference between routing for datagrams and virtual circuits. All packets from a given source to a given destination follow the same route. The advantage of fixed routing is its simplicity, and it should work well in a reliable network with steady load. Its disadvantage is its lack of flexibility. It does not react to network congestion or failures.

Flooding

In flooding, a packet is sent by a source node to every one of its neighbors. At each node, an incoming packet is retransmitted on all outgoing links except for the link that it arrived from. As an example, consider figure 8.3. If node 1 has a packet to send to node 6, it sends a copy of that packet to nodes 2, 3, and 4. Node 2 will send a copy to nodes 3 and 4. Node 4 will send a copy to nodes 2, 3, and 5. And so it goes. Eventually, a number of copies of the packet will arrive at node 6. The packet must have some unique identifier (e. g. source node, sequence number; or virtual circuit number, sequence number) so that node 6 knows to discard all but the first copy.

In flooding, a packet is sent by a source node to every one of its neighbors.

The flooding technique has two remarkable properties:

- All possible routes between source and destination are tried. Thus, no mater what link or node outage have occurred, a packet will always get through as long as at least one path between source and destination exists.
- Because all routes are tried, at least one copy of the packet to arrive at the destination will have used a minimum-hop route.

Random Routing

Random routing is similar to flooding, but in this case, a node selects only one outgoing path for retransmission of an incoming packet. The outgoing link is chosen at random, generally excluding the link on which the packet arrived.

Adaptive Routing

Adaptive routing strategies are by far the most prevalent, for two reasons:

- An adaptive routing strategy can improve performance as seen by the network user.
- An adaptive strategy can aid traffic control.

In adaptive routing strategy, outgoing link is decided based on the measurable changing conditions of the links.

4.5. Exercise

4.5.1. Multiple choice question

a. In fixed routing,

i) all packets from a given source to a given destination follow the same route.
ii) different packets from a given source to a given destination may follow different route.
iii) either of the above two may be adopted.
iv) none of the above.

4.5.2. Questions for short answers

a) What are the attributes of the routing function?
b) State least-cost routing algorithm.
c) What are the advantages of fixed routing?
d) What are the remarkable properties of flooding?
e) What are the reasons for which the adaptive routing is by far the most prevalent?

4.5.3. Analytical questions

a) Discuss Dijkstra’s least-cost routing algorithm.
b) Discuss different routing strategies.

Lesson 5 : Traffic Control in Packet Switched Network

5.1. Learning Objectives

On completion of this lesson you will be able to :

- learn different types and strategies of traffic control in packet switched network.

5.2. Introduction

Traffic control deals with the control of the number of packets entering and using the network. It is concerned with preventing the network from becoming a bottleneck and in using it efficiently.

Traffic control mechanisms are of three general types:

- Flow control
- Congestion control
- Deadlock avoidance.

5.3. Flow Control

The basic purpose of flow control is to enable the receiver to control the rate at which it receives data.

Flow control is concerned with the regulation of the rate of data transmission between two points. The basic purpose of flow control is to enable the receiver to control the rate at which it receives data, so that it is not overwhelmed. Typically, flow control is exercised with some sort of sliding-window technique.

5.4. Congestion Control

The objective of congestion control is to maintain the number of packets within the network below the level at which performance falls off dramatically. In a packet switching network, any given node has a number of transmission links attached to it. On each link, packets arrive and depart. We can consider that there are two fixed-length buffers at each link, one to accept arriving packets, and one to hold packets that are waiting to depart. As packets arrive, they are stored in the input buffer of the corresponding link. The node examines each incoming packet to make a routing decision, and then moves the packet to the appropriate output buffer. Packets queued up for output are transmitted as rapidly as possible. Now, if packets arrive too fast for the node to process them or faster than packets can be cleaned from the outgoing buffers, then eventually packets will arrive for which no memory is available. When such a saturation point reached, one of two general strategies can be adopted:

- Simply discard any incoming packet for which there is no available buffer space.
- Exercise some sort of flow control over neighboring nodes so that the traffic flow remains manageable.

The objective of all congestion control techniques is to limit queue length at the nodes.

The objective of all congestion control techniques is to limit queue length at the nodes so as to avoid throughput collapse. A number of control mechanisms for congestion control have been suggested and tried.

1. Send a control packet from a congested node to some or all source nodes. This **choke packet** will have the effect of stopping or slowing the rate of transmission from sources and hence limit the total number of packets in the network.
2. Rely on routing information. Routing algorithms provide link delay information to other nodes, which influence routing decisions. This information could also be used to influence the rate at which new packets are produced.
3. Make use of an end-to-end probe packet. Such a packet could be time-stamped to measure the delay between two particular endpoints.
4. Allow packet switching nodes to add congestion information to packets as they go by. There are two possible approaches there;

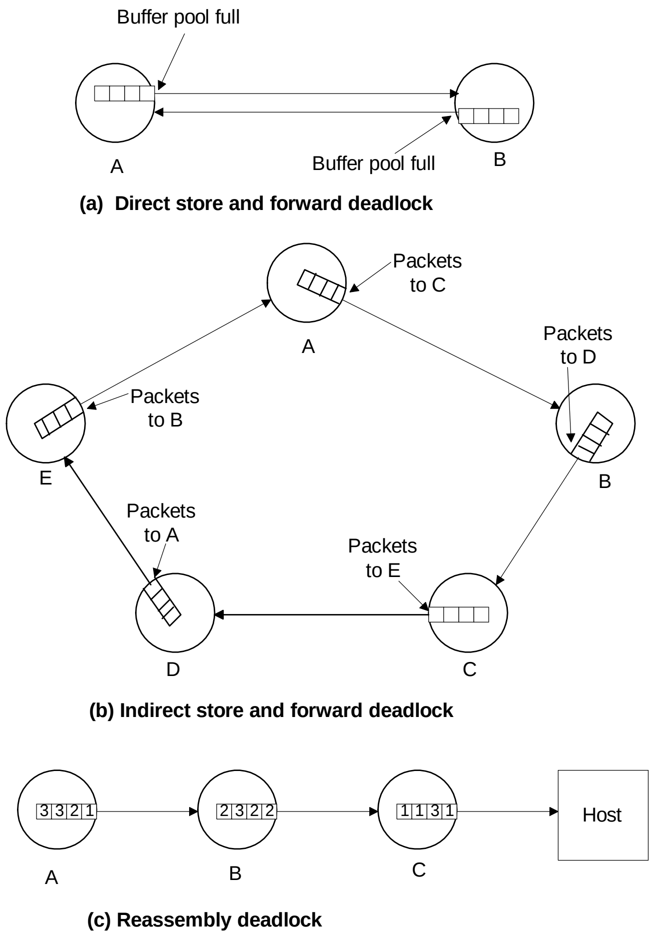
- A node could add such information to packets going in the direction opposite of the congestion. This information quickly reaches the source node, which can reduce the flow of packets into the network.
- A node could add such information to packets going in the same direction as the congestion. The destination either asks the source to adjust the load or returns the signal back to the source in the packets going in the reverse direction.

5.5. Deadlock Avoidance

Deadlock is a condition in which a set of nodes are unable to forward packets because no buffers are available. This condition can occur even without a heavy load. **Deadlock avoidance** techniques are used to design the network in such a way that deadlock can not occur. There are three types of deadlock to which a packet-switched network may be prone:

Three types of deadlock.

- Direct store-and-forward deadlock.
- Indirect store-and-forward deadlock.
- Reassembly deadlock.



(a) Direct store and forward deadlock

(b) Indirect store and forward deadlock

(c) Reassembly deadlock

Fig. 8.4: Types of deadlock.

Direct store-and-forward deadlock can be avoided by not allowing all buffers to end up dedicated to a single link.

Direct Store-and-Forward Deadlock

Direct store-and-forward deadlock can occur if a node uses a common buffer pool from which buffers are assigned to packets on demand. Figure 8.4(a) shows a situation in which all of the buffer space in node A is occupied with packets destined for node B. The reverse is true at node B. Neither node can accept any more packets since their buffers are full. Thus neither node can transmit or receive on any link.

Direct store-and-forward deadlock can be avoided by not allowing all buffers to end up dedicated to a single link. Using separate fixed-size buffers will achieve this prevention. Even if a common buffer pool is used, deadlock is avoided if no single link is allowed to acquire all of the buffer space.

Indirect Store-and-Forward Deadlock

Indirect store-and-forward deadlock is illustrated in figure 8.4(b). For each node, the queue to the adjacent node in one direction is full with packets destined for the next node beyond. One simple way to prevent this type of deadlock is to employ a structured buffer pool (figure 8.5). The buffers are organized in a hierarchical fashion. The pool of memory at level 0 is unrestricted; any incoming packet can be stored there. From level 1 to level N (where N is the maximum number of hops on any network path), buffers are reserved in the following way: Buffers at level k are reserved for packets that have traveled at least k hops so far. Thus, in heavy load conditions, buffers fill up progressively from level 0 to level N. If all buffers up through level k are filled, arriving packets that have covered k or less hops are discarded. It can be shown that this strategy eliminates direct and indirect store-and-forward deadlocks.

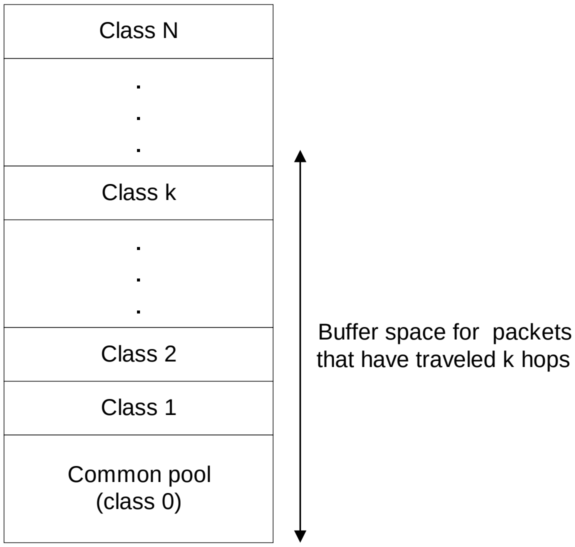


Fig. 8.5: Structured buffer pool for deadlock avoidance.

Reassembly Deadlock

Figure 8.4(c) shows a situation in which node C has three of four packets from message 1 and one from message 3. All of its buffers are full, so it can accept no more packets. Yet, because it has no complex message, it cannot reassemble packets and deliver them to the host. The solution is to require that a source node reserve space for each message in advance with a “request for buffer space” packet. When a destination node receives this request, and has available buffers for the packets that the message might contain, it returns an “allocation” packet. After the entire message is received and reassembled, the receiving node sends back an acknowledgment known as ready for next message (RFNM). If the node has buffer space for an additional message, it piggybacks an allocation packet with the RFNM. Thus, during stream transmission, the source node need not send request packets. A time may come when the source has no message to send but has collected one or more allocation permits. The source node is then obligated to send a "give back" packet to free up buffer space at the destination.

5.6. Exercise

5.6.1. Multiple choice question

a. Traffic control mechanisms concerned with

i) flow control
ii) congestion control
iii) deadlock avoidance
iv) all of the above.

b. Flow control is concerned with

i) the regulation of the rate of data transmission between two points.
ii) maintaining the number of packets within the network below the level at which performance falls off dramatically.
iii) both of the above.
iv) none of the above.

5.6.2. Questions for short answers

a) What is the objective of congestion control?
b) What are the strategies that can be adopted for congestion control?
c) What is a choke packet?
d) What is a deadlock?
e) Name the types of deadlock.

5.6.3. Analytical questions

a) Discuss control mechanisms for congestion control.
b) Discuss how direct store-and forward deadlock occurs and how it is eliminated.
c) Discuss how indirect store-and forward deadlock occurs and how it is eliminated.
d) Discuss how reassembly deadlock occurs and how it is eliminated.

Lesson 6 : X.25 Protocol Standard

6.1. Learning Objectives

On completion of this lesson you will be able to :

- grasp details of a most widely used protocol standard specifying an interface between a host system and a packet-switched network.

6.2. Basic Concepts of X.25 Protocol

Perhaps the best-known and most widely used protocol standard is X.25, which was originally approved in 1976 and subsequently revised many times. The standard specifies an interface between a host system and a packet-switched network.

X.25, standard specifies an interface between a host system and a packet-switched network.

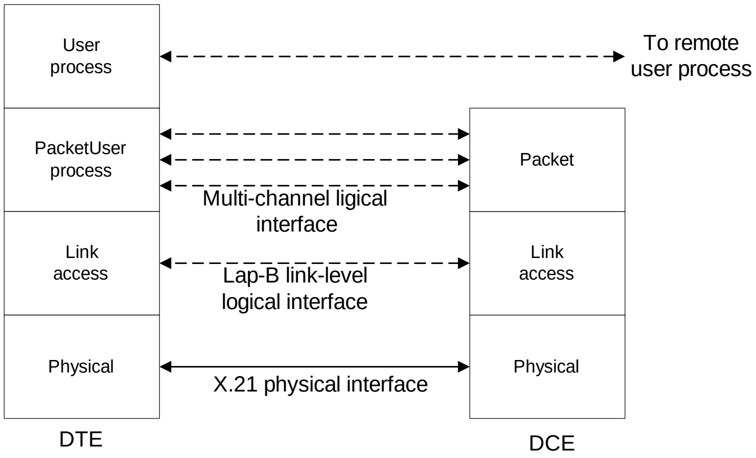


Fig. 8.6: X.25 interface.

The standard specifically calls out three layers of functionality (figure 8.6):

- Physical layer
- Link layer
- Packet layer.

These three layers corresponds to the lowest three layers of the OSI model. The physical layer deals with the physical interface between an attached station and the link that attaches that station to the packet-switching node. It makes use of the physical-layer specification in a standard known as X.21. The link layer provides for the reliable transfer of data across the physical link by transmitting the data as a sequence of frames. The link layer standard is referred to as LAP-B (Link Access Protocol-Balanced). LAP-B is a subset of HDLC. The packet layer provides an external virtual-circuit service.

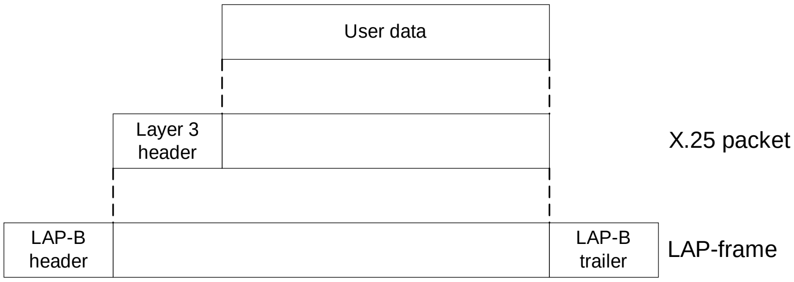


Fig. 8.7 User data and X.25 protocol control information.

X.25 standard refers to user machines as data terminal equipment (DTE) and to a packet-switching node to which a DTE is attached as data circuit-terminating equipment (DCE). Figure 8.7 illustrates the relationship between the levels of X.25. User data are passed down to X.25 level 3, which appends control information as a header, creating a packet. The entire X.25 packet is then passed down to the LAP-B entity, which appends control information at the front and back of the packet, forming a LAP-B frame.

6.3. Virtual-Circuit Service

With the X.25 packet layer, data are transmitted in packets over external virtual circuits. The virtual-circuit service of X.25 provides for two types of virtual circuits:

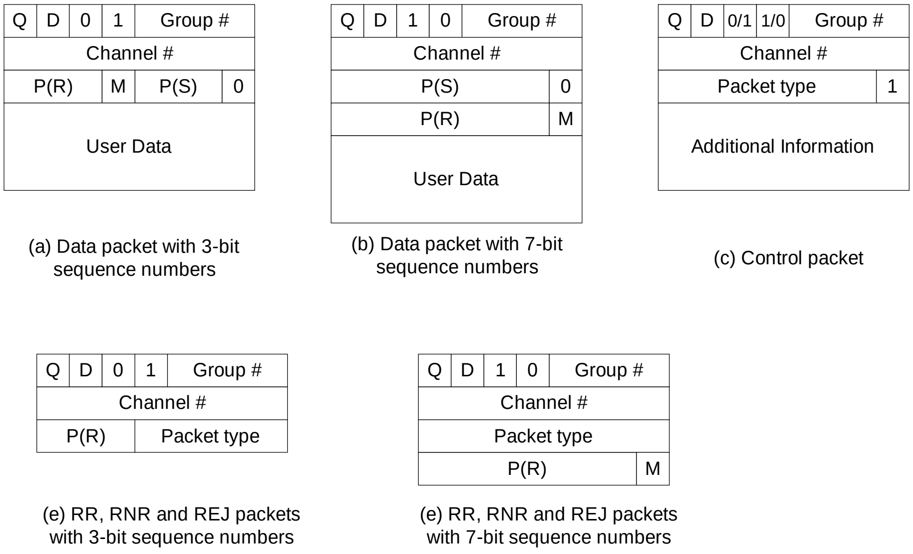
The virtual-circuit service of X.25 provides for two types of virtual circuits.

- Virtual call
- Permanent virtual circuit.

A **virtual call** is a dynamically established virtual circuit using a call setup and call cleaning procedure. A **permanent virtual circuit** is a fixed, network-assigned virtual circuit.

6.4. Packet Format

A variety of packet types are used, all using the same basic format, with variations (figure 8.8). For user data, the data are broken up into blocks of some maximum size, and a 24-bit or 32-bit header is appended to each block to form a **data packet**. The header includes a 12-bit virtual-circuit number (expressed as a 4-bit group number and an 8-bit channel number). The P(S) and P(R) fields support the functions of flow control and error control on a virtual circuit basis. The M and D bits are described in the following sections. The Q bit is not defined in the standard.



(a) Data packet with 3-bit sequence numbers

(b) Data packet with 7-bit sequence numbers

(c) Control packet

(e) RR, RNR and REJ packets with 3-bit sequence numbers

(e) RR, RNR and REJ packets with 7-bit sequence numbers

Fig. 8.8: X.25 packet formats.

In addition to transmitting user data, X.25 must transmit control information related to the establishment, maintenance, and termination of virtual circuits. Control information is transmitted in a **control packet**. Each control packet includes the virtual-circuit number; the packet type, which identifies the particular control functions; and additional control information related to that function.

6.5. Multiplexing

Perhaps the most important service provided by X.25 is multiplexing. A DTE is allowed to establish up to 4095 simultaneous virtual circuits with other DTEs over a single physical DTE-DCE link. The DTE can internally assign these circuits in any way it pleases. Individual virtual circuits could correspond to applications, processes, or terminals, for example. The DTE-DCE link provides full-duplex multiplexing. To sort out which packets belong to which virtual circuits, each packet contains a 12-bit virtual-circuit number (expressed as a 4-bit logical group number plus an 8-bit logical channel number).

The most important service provided by X.25 is multiplexing.

6.6. Flow and Error Control

Flow control and error control at the X.25 packet layer are virtually identical in format and procedure to flow control used for HDLC. A sliding-window protocol is used. Each data packet includes a send sequence number, P(S), and a receive sequence number, P(R). As a default, 3-bit sequence numbers are used. Optionally, A DTE may request, via the user facility mechanism, the use of extended 7-bit sequence numbers. As figure 8.8 indicates, for 3-bit sequence numbers, the third and fourth bits of all data and control packets are 01; for 7-bit sequence numbers, the bits are 10.

P(S) is assigned by the DTE on outgoing packets on a virtual circuit basis. P(R) contains the number of the next packet expected from the other side of a virtual circuit; this provides for piggybacked acknowledgment. If one side has no data to send, it may acknowledge incoming packets with the Receive Ready (RR) and Receive Not Ready (RNR)control packets. The default window size is 2, but it may be set as high as 7 for 3-bit sequence numbers and as high as 127 for 7-bit sequence numbers.

Acknowledgment, and hence flow control, may have either local or end-to-end significance, based on the setting of the D bit. When D =), (the usual case), acknowledgment is exercised between the DTE and the network. This is used by the local DCE and/or the network to acknowledge receipt of packets and control the flow from the DTE into the network. When D = 1, a acknowledgment come from the remote DTE.

The basic form of **error control** is go-back-N ARQ. Negative acknowledgment is in the form of a Reject (REJ) control packet. If a node receives a negative acknowledgment, it will retransmit the specified packet and all subsequent packets.

6.7. Packet Sequences

X.25 provides the capability to identify a contiguous sequence of data packets, which is called a complete packet sequence. This feature has several uses. On important use is by internetworking protocols, to allow longer blocks of data to be sent across a network with a smaller packet size restriction without losing the integrity of the block.

X.25 provides the capability to identify a contiguous sequence of data packets, which is called a complete packet sequence.

To specify this mechanism, X.25 defines two types of packets: A packets and B packets. An **A Packet** is one in which the M bit is set to 1, the D bit is set to 0, and the packet is full (equal to the maximum allowable packet length). A **B packet** is any packet that is not an A packet. A complete packet sequence consists of zero or more A packets followed by a B packet. The network may combine this sequence to make one longer packet. The network may also segment a B packet into smaller packets to produce a complete packet sequence.

6.8. Exercise

6.8.1. Multiple choice questions

a. In X.25 system, a virtual call is

i) a dynamically established virtual circuit
ii) a fixed, network assigned virtual circuit
iii) any of the above two
iv) none of the above.

b. In X.25 packet format, the header size is

i) 24 bit
ii) 32 bit
iii) any of the above two
iv) none of the above.

c. In X.25 system, the maximum allowable number of virtual circuits multiplexed over a single physical DTE-DCE link is

i) 1024
ii) 4095
iii) 2048
iv) 128.

d. In X.25 system, the default window size is

i) 2
ii) 7
iii) 127
iv) any of the above.

6.8.2. Questions for short answers

a) How many layers are there in X.25 standard? Name them.
b) How many types of virtual circuits are provided in X.25 system? Name them.
c) What are A packets and B packets in X.25 system?

6.8.3. Analytical questions

a) Discuss packet formats used in X.25 system.
b) Discuss multiplexing used in X.25 system.
c) Discuss how flow and error control are done in X.25 system.
d) Discuss the concept of complete packet sequence as used in X.25 system.

Unit 9 : Local Area Networks

Introduction

The local area networks (LANs) are distinguished from other types of data networks in that they are optimized for a moderate-size geographic area such as a single office building, a warehouse, or a campus. These networks share the characteristics of being packet broadcasting networks. The nature of a LAN is determined primarily by three factors: transmission medium, topology, and medium access control protocol. In this unit, these topics are discussed.

Lesson 1 : LAN Technology

1.1. Learning Objectives

On completion of this lesson you will be able to :

- learn details of transmission media and topology used in LAN technology.

1.2. Topology and Transmission Medium

Common topologies used for LAN are (figure 9.1):

- Ring
- Bus
- Tree
- Star.

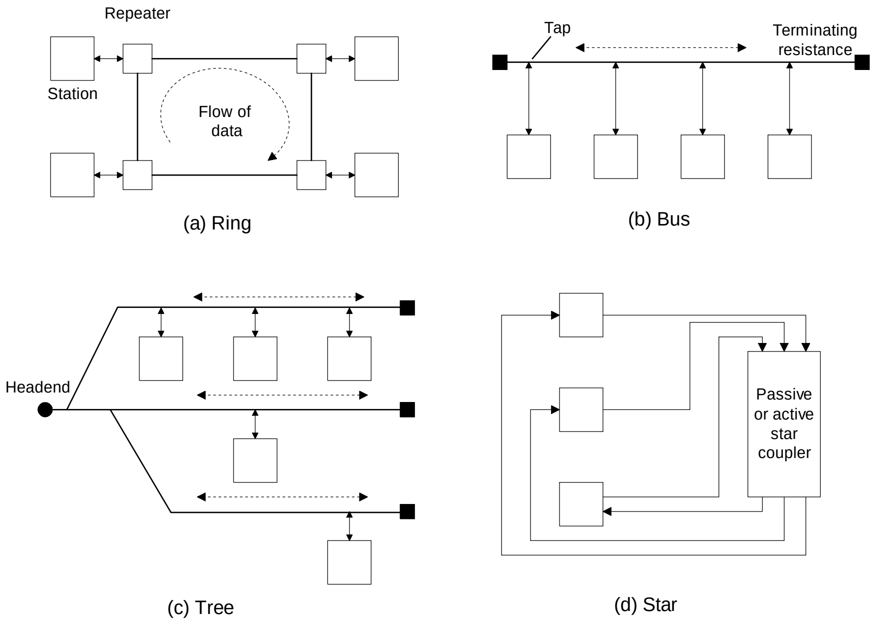
Ring Topology

The repeater is capable of receiving data on one link and transmitting it, bit by bit.

In the ring topology, the network consists of a set of repeaters joined by point-to-point links in a closed loop. The repeater is capable of receiving data on one link and transmitting it, bit by bit, on the other link as fast as it is received, with no buffering at the repeater. The links are unidirectional; that is, data are transmitted in one direction only, and all oriented in same way. Thus data circulate around the ring in one direction.

Each station attaches to the network at a repeater. Data are transmitted in packets inserted onto the ring by the stations. The packet containing source and destination address fields as well as other control information and user data. As a packet circulates, the destination station copies the data into a local buffer. Typically, the packet continues to circulate until it returns to the source station, where it is absorbed, removing from the ring. Since multiple devices share the ring, some form of medium access logic is needed to control the order and timing of packet transmissions.

Twisted pair, coaxial cable, and optical fiber are used for constructing the ring.



(a) Ring

(b) Bus

(c) Tree

(d) Star

Fig. 9.1: LAN topologies.

Twisted pair, coaxial cable, and optical fiber are used for constructing the ring. Table 9.1 summarizes representative parameters for transmission media for commercially-available ring LANs.

Table 9.1: Transmission Media for Ring LANs.

Transmission Medium	**Data Rate (Mbps)**	**Distance Between Repeaters (km)**	**Number of Repeaters**
Unshielded twisted pair	4	0.1	72
Shielded twisted pair	16	0.3	250
Baseband coaxial cable	16	1.0	250
Optical fiber	100	2.0	240

Bus and Tree Topologies

Both bus and tree topologies are characterized by the use of a multipoint medium. With the bus topology, all stations attach, through appropriate interfacing hardware, directly to a linear transmission medium, or bus. A transmission from any station propagates the length of the medium in both directions and can be received by all other stations.

In tree topology, the transmission medium is a branching cable with no closed loops. The tree layout begins at a point known as the **headend**. One or more cables start at the headend, and each of these may have branches. The branches in turn may have additional branches to allow quite complex layouts. Again, a transmission from any station propagates throughout the medium, can be received by all other stations, and is absorbed at the endpoints. The transmission is in the form of packets containing addresses and user data. Each station monitors the medium and copies packets addressed to itself. Because all stations share a common transmission link, only one station can successfully transmit at a time, and some form of medium access control technique is needed to regulate access.

Twisted pair, coaxial cable, and optical fiber are used as medium. Table 9.2 summarizes representative parameters for transmission media for commercially available bus/tree LANs.

Table 9.2: Transmission Media for Bus/Tree LANs.

Transmission Medium	Data Rate (Mbps)	Range (km)	Number of Taps
Twisted pair	1-10	<2	10’s
Baseband coaxial cable	10; 50 with limitations	<3	100’s
Broadband coaxial cable	500; 20 per channel	<30	1000’s
Optical fiber	45	<150	500’s

Star Topology

The star topology is also employed for implementing a packet-broadcasting LAN.

In the star topology, each station is directly connected to a common central switch. The star topology is also employed for implementing a packet-broadcasting LAN. In this case, each station attaches to a central node, referred to as the star coupler, via two point-to-point links, one for transmission in each direction. A transmission from any one station enters the central node and is retransmitted on all of the outgoing links. A transmission from any station is received by all other stations, and only one station at a time may successfully transmit. Thus, the medium access control techniques used for the packet star topology are the same as for bus and tree.

There are two ways of implementing the star coupler:

- Passive coupler.
- Active coupler.

In the case of optical fiber, the passive star coupling is achieved by fusing together a number of fibers, so that incoming light is automatically split among all of the outgoing fibers. In the case of coaxial cable or twisted pair, transformer coupling is used to split the incoming signal.

The star coupler

In active star coupler, there is digital logic in the central node that acts as a repeater. As bits arrive on any input line, they are automatically regenerated and repeated on all outgoing lines. If multiple input signals arrive simultaneously, a collision signal is transmitted on all outgoing lines. Table 9.3 summarizes representative parameters for transmission media for commercially available star LANs.

Table 9.3 : Transmission Media for passive or active star LANs.

Transmission Medium	**Data Rate (Mbps)**	**Distance from station to central switch (km)**	**Number of stations**
Unshielded twisted pair	1-10	0.5 (1 Mbps)-0.1 (10 Mbps)	10’s
Baseband coaxial cable	70	<1	10’s
Optical fiber	10-20	<1	10’s

1.3. LAN Implementation Using Metallic Transmission Media

Two transmission techniques are in use for bus/tree LANs using metallic transmission media:

- Baseband transmission.
- Broadband transmission.

The baseband digital signaling requires a bus topology.

Baseband, using digital signaling, can be employed on twisted pair or coaxial cable. Broadcast, using analog signaling in the RF range, employs coaxial cable. There is also a variant known as **carrierband** that uses analog signaling and the entire spectrum of the cable is devoted to a single transmission path.

Baseband System

The baseband digital signaling requires a bus topology. The most popular form of baseband bus LAN uses coaxial cable. Most baseband coax systems use a special 50-ohm cable. Table 9.4 summarizes the IEEE specifications for 10-Mbps baseband coaxial bus LANs. 10BASE5 is known as Ethernet and 10BASE2 is known as dubbed Cheapernet.

Table 9.4: IEEE specification for 10-Mbps Baseband Coaxial Bus LANs.

Parameter	10BASE5	10BASE2
Data rate	10Mbps	10Mbps
Maximum segment length	500m	200m
Network span	2500m	1000m
Nodes per segment	100	30
Node spacing	2.5m	0.5m
Cable diameter	0.4m	0.25m

To extend the length of the network, a repeater may be used. It consists, in essence, of two transceivers joined together and connected to two different segments of coax cable. The repeater passes digital signals in both directions between the two segments, amplifying and regenerating the signals as they pass through. A maximum of four repeaters is allowed in the path between any two stations, extending the effective cable length to 2.5 km. Figure 9.2 is an example of a baseband system with three segments and two repeaters.

A maximum of four repeaters is allowed in the path between any two stations, extending the effective cable length to 2.5 km.

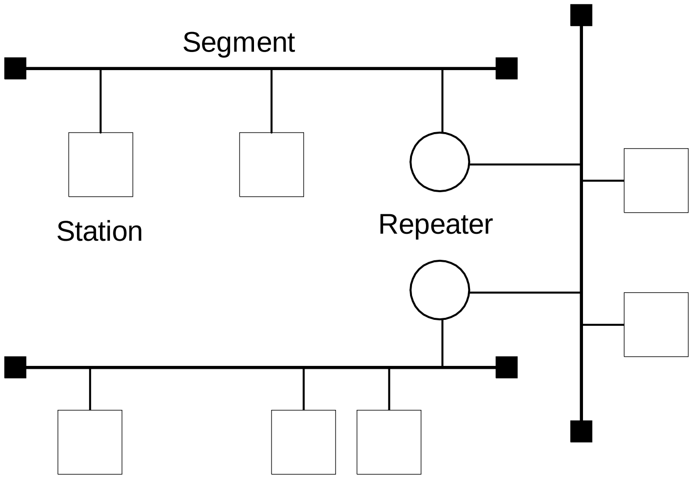


Fig. 9.2: Baseband configuration.

Unshielded twisted pair is used in baseband star LANs. The products on the market use a scheme suggested by figure 9.3, in which central element of the star is an active element, referred to as the **hub**. Each station is connected to the hub by two twisted pairs (transmit and receive). The hub acts as a repeater. Multiple levels of hubs can be cascaded in a hierarchical configuration. Figure 9.4 illustrates a two-level configuration. There is one **header hub** and one or more **intermediate hubs**. Each hub may have a mixture of stations and other hubs attached to it from below.

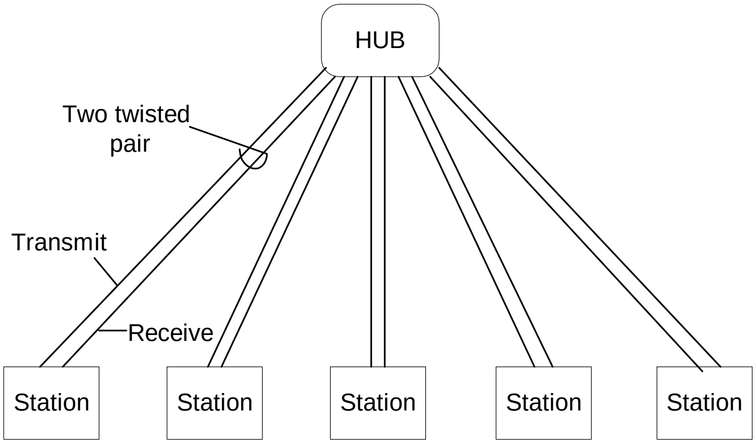


Fig. 9.3: Twisted-pair baseband star LAN.

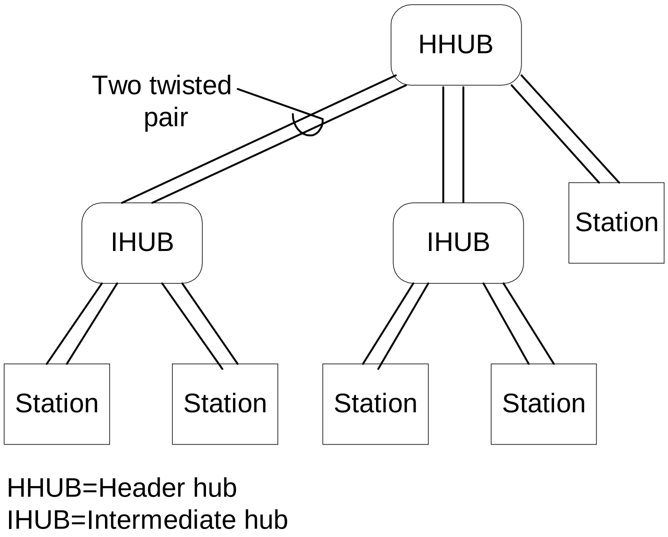


Fig. 9.4: Two-level hierarchy of twisted-pair baseband star LAN.

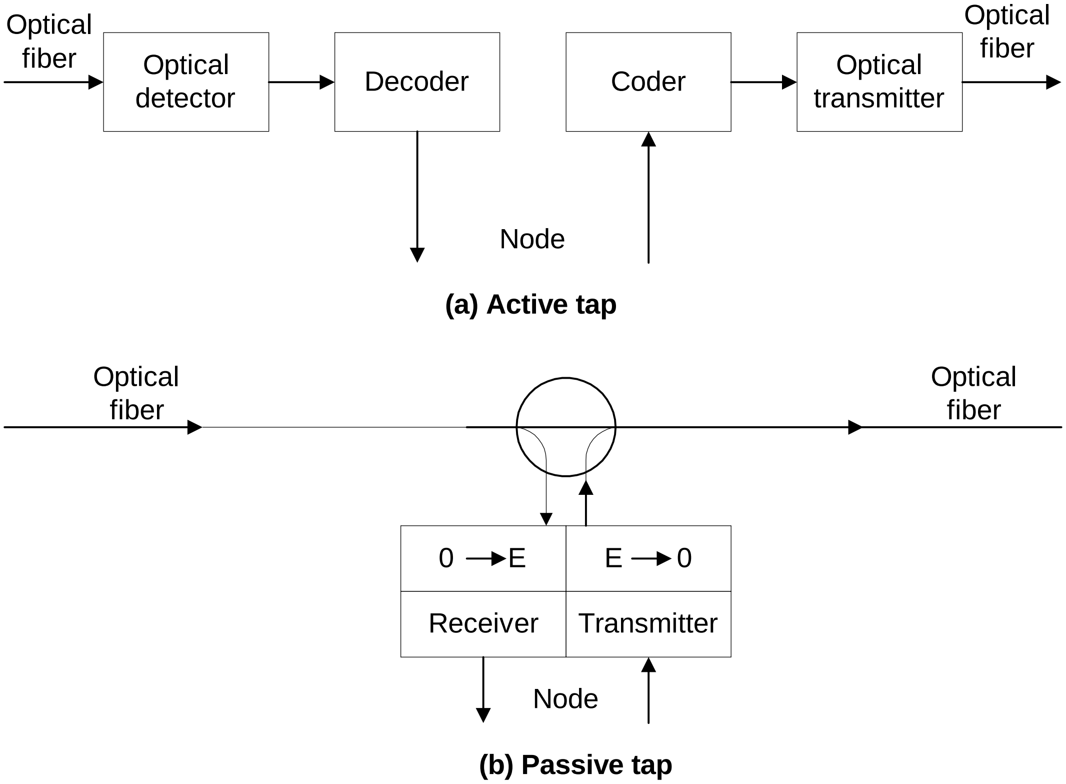
Broadband Systems

In broadband system, both bus and tree topologies are possible.

In broadband system, analog signaling is used and the frequency spectrum of the cable can be divided into channels using FDM. In broadband system, both bus and tree topologies are possible. Broadband is inherently a unidirectional medium; signals inserted onto the medium can propagate in only one direction. This means that only those stations "down stream" from a transmitting station can receive its signals. For full connectivity, two data paths are needed. These paths are joined at a point on the network known as the headend. For bus topology, the headend is simply one end of the bus. For tree topology, the headend is the root of the branching tree. All stations transmit on one path towards the headend (inbound). Signals received at the headend are then propagated along a second data path away from the headend (outbound). All stations receive on the outbound path. Broadband systems use 75-ohm coaxial cable.

1.4. LAN Implementation Using Optical Fiber

LAN is implemented using optical fiber in a bus topology. With an optical fiber bus, either an active or passive tap can be use.



(a) Active tap

(b) Passive tap

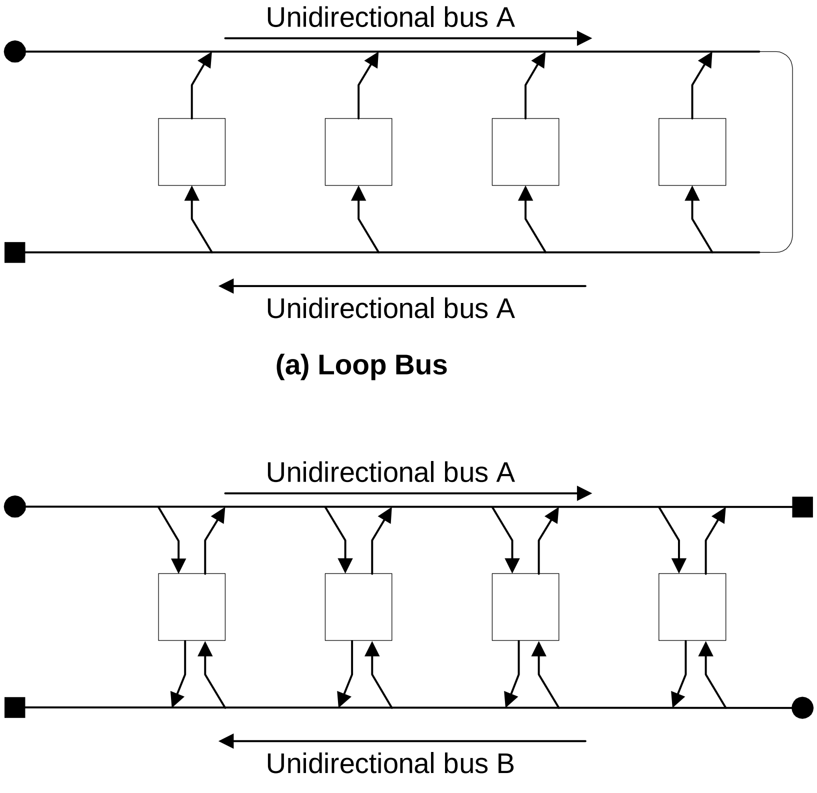
Fig. 9.5: Optical fiber taps.

In the case of an active tap (figure 9.5(a)), the following steps occur:

1. Optical signal energy enters the tap from the bus.
2. Clocking information is recovered from the signal and the signal is converted to an electrical signal.
3. The converted signal is presented to the node.
4. The optical output (a light beam) is modulated according to the electrical signal and launched into the bus.

Each tap actually consists of two of these active couplers and require two fibers.

In the case of a passive tap (figure 9.5(b)), the tap extracts a portion of the optical energy from the bus for reception and it injects optical energy directly into the medium for transmission. Thus, there is a single run of cable rather than a chain of point-to-point links. Each tap must connect to the bus twice, once for transmit and once for receive.



(a) Loop Bus

(b) Dual Bus

Fig 9.6: Optical fiber bus configuration.

Two configurations for the optical fiber bus have been proposed: those that use a single bus and those that use two buses. Figure 9.6(a) shows a typical single-bus configuration, referred to as a loop bus. Each station transmits on the bus in the direction toward the headend and receives on the bus in the direction away from the headend. Figure 9.6(b) shows the two-bus configuration. Each station attaches to both buses and has both transmit and receive taps on both buses.

1.5. LAN Implementation On Ring Topology

A ring consists of a number of repeaters, each connected to two others by unidirectional transmission links to for a single closed path. Data are transferred sequentially, bit by bit, around the ring from one repeater to the next. Each repeater regenerates and retransmits each bit.

For a ring to operate as a communication network, three functions are required:

- Data insertion
- Data reception
- Data removal.

These functions are provided by the repeaters. Data insertion is accomplished by the repeater. Data are transmitted in packets, each of which contains a destination address field. As a packet circulates past a repeater, the address field is copied. If the attached station recognize the address, the remainder of the packet is copied. Because the ring is a closed loop, a packet will circulate indefinitely unless it is removed. A packet may be removed by the addressed repeater. Alternatively, each packet could be removed by the transmitting repeater after it has made one trip around the loop.

The repeater can be seen to have two main purpose:

(1) To contribute to the proper functioning of the ring by passing on all the data that come its way.
(2) To provide a access point for attached stations to send and receive data.

Corresponding to these two purposes are two states (figure 9.7):

♦ The listen state.
♦ The transmit state.

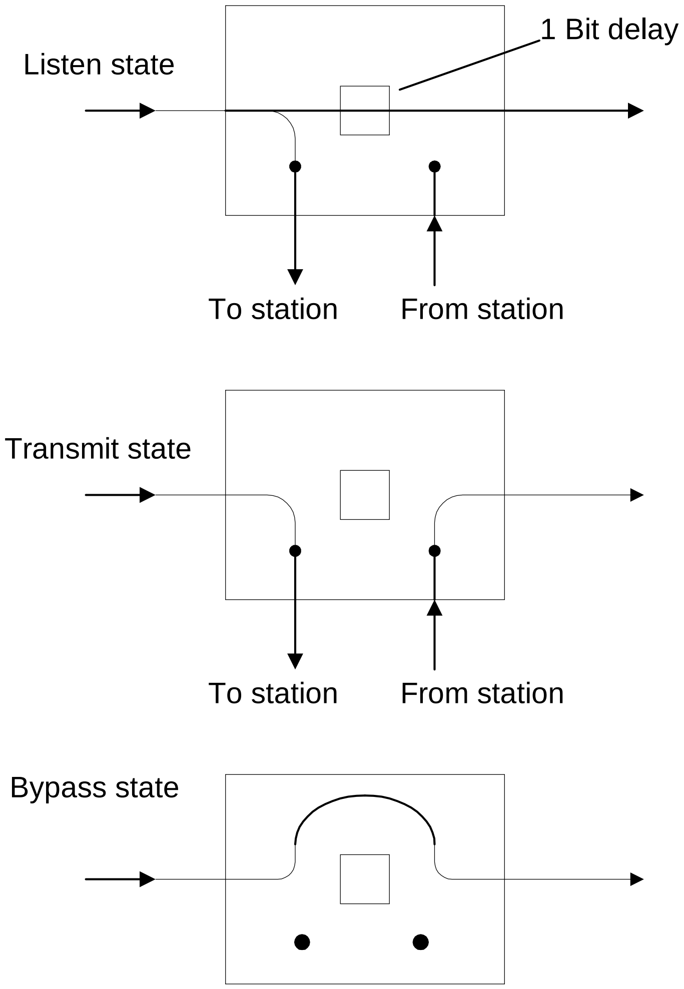


Fig. 9.7: Ring repeater states.

In the listen state, each received bit is retransmitted with a small delay. When a repeater's station has data to send and when the repeater has permission to send, the repeater enters the transmit state. In this state, the repeater receives bits from the station and retransmits them on its outgoing link. A third state, the bypass state, is also useful. In this state, a bypass relay can be activated, so that signals propagate past the repeater with no delay other than medium propagation.

1.6. Exercise

1.6.1. Multiple choice questions

a. In carrierband transmission

i) analog signaling is used and the entire spectrum of the cable is devoted to a single transmission path.
ii) digital signaling is used and the entire spectrum of the cable is devoted to a single transmission path.
iii) analog signaling is used and the spectrum of the cable is frequency multiplexed for several transmission paths.
iv) digital signaling is used and the spectrum of the cable is frequency multiplexed for several transmission paths.

b. Broadband system is

i) a bidirectional medium
ii) a unidirectional medium
iii) either of the above two
iv) none of the above.

1.6.2. Questions for short answers

a) Name the common topologies used in LANs.
b) How data is removed in a ring topology?
c) What is the function of a headend in bus and tree topologies?
d) How star coupler is implemented?
e) Name the different types of transmission technique used in LANs using metallic transmission media.
f) What is a hub and an intermediate hub?
g) Name the functions required in ring to operate as a communication network.
h) How many states are there in a ring repeater? Name them.

1.6.3. Analytical questions

a) Discuss the common topologies that used in LANs.
b) Discuss different types of transmission techniques used in LANs using metallic transmission medium.
c) Discuss the implementation of LANs using optical fiber.
d) Discuss the implementation of LANs on ring topology.

Lesson 2 : Medium Access Control Protocols

2.1. Learning Objectives

On completion of this lesson you will be able to :

- grasp medium access control techniques and protocols.

2.2. Medium Access Control Techniques

Medium access control techniques can be divided into two categories:

- Round robin.
- Contention.

Round Robin

With round robin, each station in turn is given the opportunity to transmit.

With round robin, each station in turn is given the opportunity to transmit. During that opportunity, the station may decline to transmit or may transmit subject to a specified upper bound, usually expressed as a maximum amount of data transmitted or time for this opportunity. In any case, the station, when it is finished, relinquishes its turn, and the right to transmit passes to the next station in logical sequence.

Contention

For bursty traffic (short, sporadic transmission), contention techniques are usually appropriate. With these techniques, no control is exercised to determine whose turn it is; all stations contend for time in a way that can be rather rough and tumble.

2.3. Carrier Sense Multiple Access With Collision Detection (CSMA/CD)

CSMA/CD is a contention technique used in bus topology.

CSMA/CD is a contention technique used in bus topology. In this technique, a station wishing to transmit first listens to the medium to determine if another transmission is in progress (carrier sense). If the medium is in use, the station must wait. If the medium is idle, the station may transmit. It may happen that two or more stations attempt to transmit at about the same time. If this happens, there will be a collision; the data from both transmission will be garbled and not received successfully.

The following is the rules for CSMA/CD:

1. If the medium is idle, transmit; other wise, go to step 2.
2. If the medium is busy, continue to listen until the channel is idle, then transmit immediately.
3. If a collision is detected during transmission, transmit a brief jamming signal to assure that all stations know that there has been a collision and then cease transmission.
4. After transmitting the jamming signal, wait a random amount of time, then attempt to transmit again (repeat from step 1).

Figure 9.8 illustrates the technique for a baseband bus. At time t_0, station A begins transmitting a packet addressed to station D. At time t_1, both station B and station C are ready to transmit. Station B senses a transmission and so defers. Station C, however, is still unaware of A’s transmission and begins its own transmission. When station A’s transmission reaches station C, at t_2, station C detects the collision and ceases transmission. The effect of the collision propagates back to station A, where it is detected some time later, t_3, at which time station A ceases transmission.

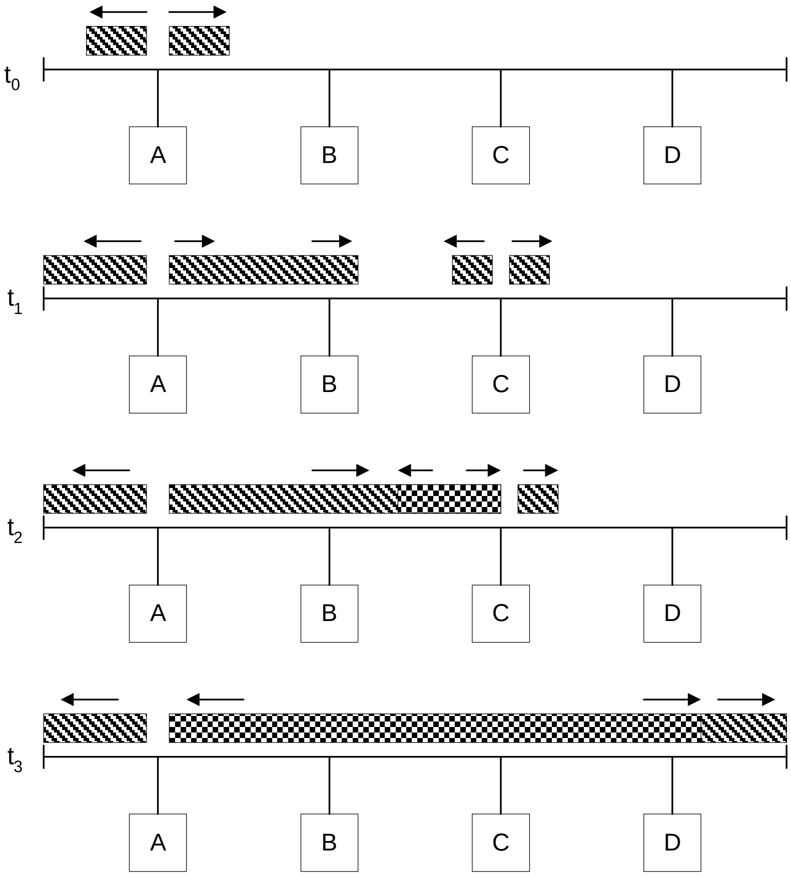


Fig. 9.8: CSMA/CD operation.

With CSMA/CD, a protocol is needed to specify what a station should do if the medium is found busy. Three approaches are used:

Nonresistant CSMA/CD:

A station wishing to transmit obeys the following rules:

1. If the medium is idle, transmit; otherwise go to step 2.
2. If the medium is busy, wait an amount of time drawn from a probability distribution (the retransmission delay) and repeat step 1.

1-persistent CSMA/CD:

A station wishing to transmit obeys the following rules:

1. If the medium is idle, transmit; otherwise go to step 2.
2. If the medium is busy, continue to listen until the channel is sensed idle; then transmit immediately.

p-persistent CSMA/CD:

A station wishing to transmit obeys the following rules:

1. If the medium is idle, transmit with probability p, and delay one time unit with probability (1-p). The time unit is typically equal to the maximum propagation delay.
2. If the medium is busy, continue to listen until the channel is sensed idle repeat step 1.
3. If transmission is delayed one time unit, repeat step 1.

The most common choice is 1-persistent CSMA/CD.

2.4. Token Bus

Token bus is a technique in which the stations of the bus or tree form a logical ring.

Token bus is a round robin technique used in bus topology; that is, the stations are assigned positions in an ordered sequence, with the last member of the sequence followed by the first. Each station knows the identity of the stations preceding and following it (figure 9.9).

A control packet known as the token regulates the right of access. When a station receives the token, it is granted control of the medium for a specified time. The station may transmit one or more packets. When the station is done, or time has expired, it passes the token to the next station in logical sequence. This station now has permission to transmit.

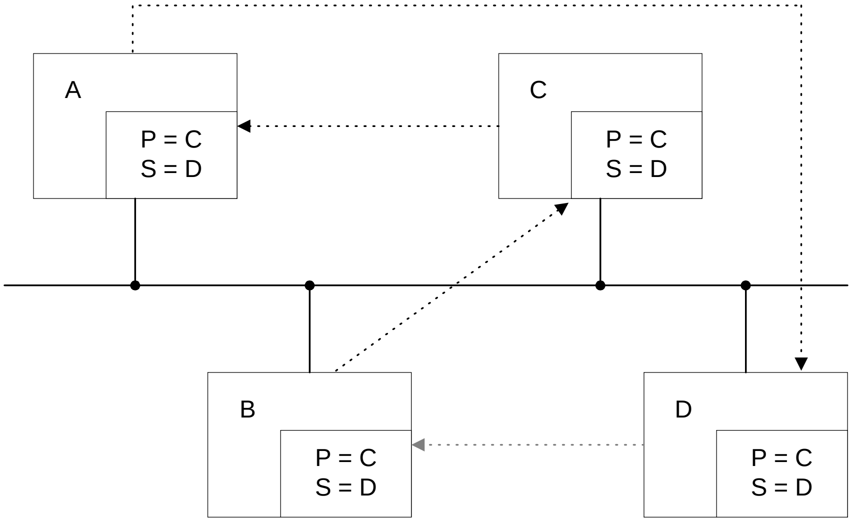


Fig. 9.9: Token bus.

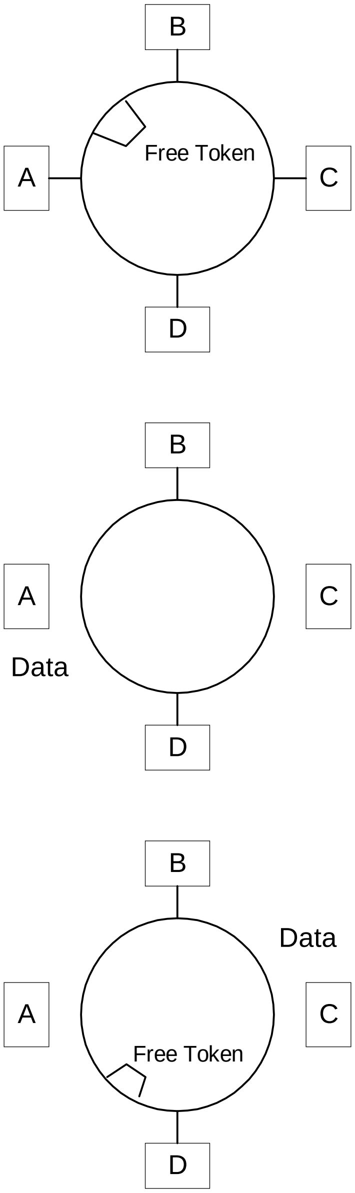
2.5. Token Ring

The token ring technique is based on the use of a small token packet that circulates around the ring.

Token ring is a round robin technique used in ring topology. The token ring technique is based on the use of a small token packet that circulates around the ring. When all stations are idle, the token packet is labeled as a “free token”. A station wishing to transmit must wait until it detects a token passing by. It then changes the token from “free token” to “busy token” by altering the bit pattern. The station then transmits a packet immediately following the busy token (figure 9.10). There is now no free token on the ring, so other stations wishing to transmit must wait. The packet on the ring will make a round trip and be purged by the transmitting stations. The transmitting station will insert a new free token on the ring when both of the following conditions have been met:

- The station has completed transmission of its packets.
- The busy token has returned to the station.

When a transmitting station releases a new free token, the next station downstream with data to send will be able to seize the token and transmit.



Sender looks for free token

Changes free token to busy token and appends data

Receiver copies data addressed to it

Sender generates free token upon receipt of physical transmission header (From addressee)

Fig. 9.10: Token Ring.

2.6. Exercise

2.6.1. Multiple choice questions

a. CSMA/CD is a

i) Contention technique used in bus topology.
ii) Contention technique used in ring topology.
iii) Round robin technique used in bus topology.
iv) Round robin technique used in ring topology.

b. Token bus is a

i) Contention technique used in bus topology.
ii) Contention technique used in ring topology.
iii) Round robin technique used in bus topology.
iv) Round robin technique used in ring topology.

c. Token ring is a

i) Contention technique used in bus topology.
ii) Contention technique used in ring topology.
iii) Round robin technique used in bus topology.
iv) Round robin technique used in ring topology.

2.6.2. Question for short answer

a) Classify the medium access control techniques.

2.6.3. Analytical questions

a) Discuss CSMA/CD protocol for MAC.
b) Discuss token bus protocol for MAC.
c) Discuss token ring protocol for MAC.

Lesson 3 : LAN Standards

3.1. Learning Objectives

On completion of this lesson you will be able to :

- grasp a logical link control standard for LAN
- grasp four physical layer and MAC standards for LAN.

3.2. Introduction

The standards for LANs were developed by a committee known as IEEE 802.

The standards for LANs were developed by a committee known as IEEE 802 and are organized as a three-layer protocol hierarchy. Logical link control (LLC) is responsible for addressing and data link control. It is independent of the topology, transmission medium, and medium access control technique chosen and was issued as a separate standard. Below logical link control are the medium access control (MAC) and physical layers. Figure 9.11 relates the LAN standards to the OSI architecture.

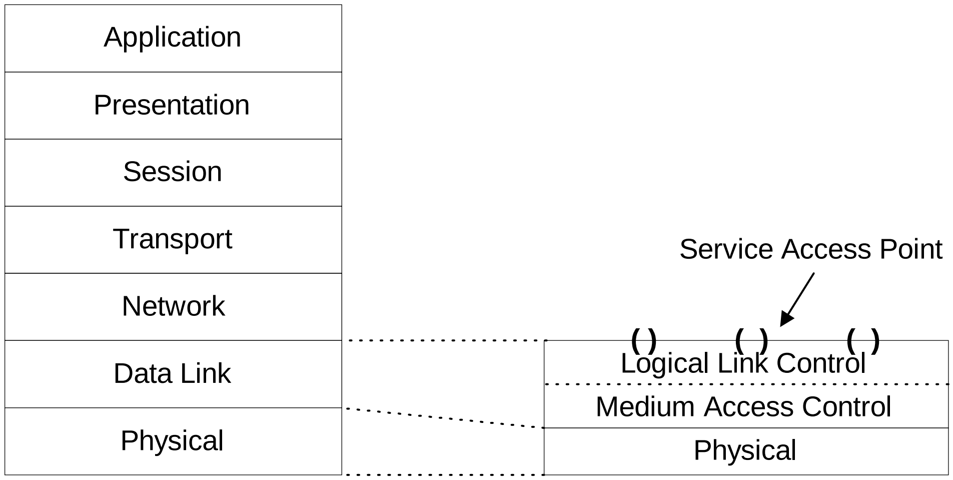


Fig. 9.11: IEEE 802 reference model relationship to OSI model.

Figure 9.12 illustrates the relation between the levels of the architecture and figure 9.13 shows the format of the LLC PDU and MAC frames.

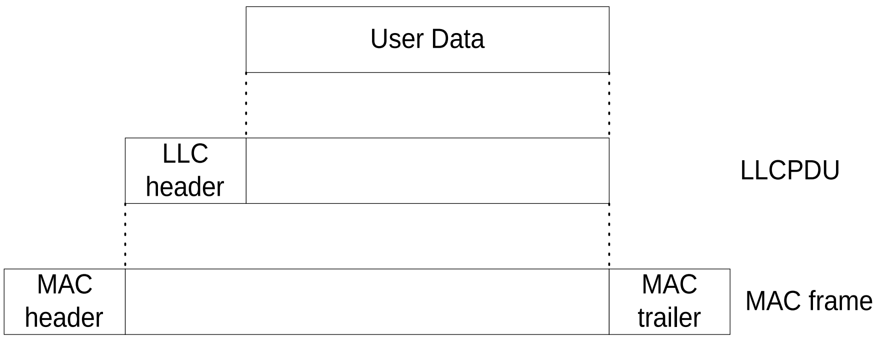


Fig. 9.12: User data and LAN protocol control information.

Logical Link Control (LLC)

1	1	1-2	N	bytes or octets
DSAP	SSAP	Control	DATA	

CSMA/CD

7	1	2,6	2,6	2	0-1500		4
Preamble	SFD	DA	SA	Length	LLC	PAD	FCS

Token Bus

>1	1	1	2,6	2,6	>0	4	1
Preamble	SD	FC	DA	SA	LLC	FCS	ED

Token Ring

1	1	1
SD	AC	ED

1	1	1	2,6	2,6	>0	4	1	1
SD	AC	FC	DA	SA	LLC	FCS	ED	FS

AC = Access Control
DA = Destination Address
DSAP = Destination Service Access Point
ED = Ending Delimiter
FC = Frame Control
FCS = Frame Check Sequence
FS = Frame Status
SA = Source Address
SD = Starting Delimiter
SFD = Start Frame Delimiter
SSAP = Source Service Access Point

Fig. 9.13: LAN standard formats.

3.3. Logical Link Control (LLC) Standard (IEEE 802.2)

LLC Services

LLC specifies the mechanisms for addressing stations across the medium and for controlling the exchange of data between two users. The operation and format of this standard is based on HDLC. Three services are provided as alternatives for attached devices using LLC:

- Unacknowledged connectionless service.
- Connection-mode service.
- Acknowledged connectionless service.

LLC Protocol

The basic LLC protocol is modeled after HDLC and has similar functions and formats. The differences between the two protocols can be summarized as follows:

1. LLC makes use of the asynchronous balanced mode of operation of HDLC, to support connection-mode LLC service; this is referred to as type 2 operation. The other HDLC modes are not employed.
2. LLC supports a connectionless service using the unnumbered information PDU; this is known as type 1 operation.
3. LLC supports an acknowledged connectionless service by using two new unnumbered PDUs; this is known as type 3 operation.
4. LLC permits multiplexing by the use of LLC service access points (LSAPs).

All three LLC protocols employ the same PDU format (figure 9.13). The DSAP and SSAP fields each contain 7-bit address, which specify the destination and source users of LLC. One bit of the DSAP indicates whether this is an individual or group address. One bit of the SSAP indicates whether it is a command or response PDU.

For type 1 operation, the unnumbered information (UI) PDU is used to transfer user data. There is no acknowledgment, flow control, or error control. However, there are error detection and discard at the MAC level.

With type 2 operation, a data link connection is established between two LLC SAPs prior to data exchange. Connection establishment is attempted by the type protocol in response to a request from a user. The LLC entity issues a SABME PDU to request a logical connection with the other LLC entity. If the connection is accepted by the LLC user designated by the DSAP, then the destination LLC entity returns an unnumbered acknowledgment (UA) PDSU. The connection is henceforth uniquely identified by the pair of user SAPS. If the destination LLC user rejects the connection request, its LLC entity returns a disconnected mode (DM) PDU. Once the connection is established, data are exchanged using information PDUs, as in HDLC. The information PDUs include send and receive sequence numbers, for sequencing and flow control. The supervisory PDUs are used, as in HDLC, for flow control and error control. Either LLC entity can terminate a logical LLC connection by issuing a disconnect (DISC) PDU.

With type 3 operation, each transmitted PDU is acknowledged. A new (not found in HDLC) unnumbered PDU, the Acknowledged Connectionless (AC) Information PDU, is defined. User data are sent in AC command PDUs and must be acknowledged using an AC response PDU. To guard against lost PDUs, a 1-bit sequence number is used.

3.4. CSMA/CD Standard (IEEE 802.3)

Medium Access Control

The 802.3 medium access control technique is CSMA/CD. In order to implement the CSMA/CD algorithm, data are transmitted in the form of packets, referred to as MAC frames, which contain user information and the control information needed for the algorithm. Figure 9.13 shows the format of the IEEE 802.3 MAC frame. The preamble is a special 7-octet pattern used by each receiver to establish bit synchronization. This is followed by a start frame delimiter (SFD) which is a special pattern that signals the beginning of the frame proper. The destination and source address specify the transmitting station and the intended receiving station respectively. The length field specify the number of data octets that follow. The pad field is inserted by the transmitter if needed to assure that the frame is long enough for proper collision detection operation. Finally, the frame check sequence is a 32-bit cyclic redundancy check for error detection.

The 802.3 medium access control technique is CSMA/CD.

Medium Options

Table 9.5: Physical layer specifications for IEEE 802.3 CSMA/CD LAN standard.

Option	Transmission Medium	Signaling Technique	Data Rate (Mbps)	Maximum Segment Length (m)	Maximum Number of Taps per Segment
10BASE5 (Ethernet)	Coaxial Cable (50 Ohms)	Baseband (Manchester)	10	500	100
10BASE2 (Cheapernet)	Coaxial Cable (50 Ohms)	Baseband (Manchester)	10	185	30
1BASE5 (Star LAN)	Unshielded Twisted Pair	Baseband (Manchester)	1	250	
10BASE-T	Unshielded Twisted Pair	Baseband (Manchester)	10	100	
10BROAD36	Coaxial Cable (75 Ohms)	Broadband (DPSK)	10	3600	

Table 9.5 summarizes the options defined for the IEEE 802.3 medium. 1BASE5 and 10BASE-T standard support passive-star topology.

3.5. Token Bus Standard (IEEE 802.4)

Medium Access Control

The 802.4 medium access control technique is the token bus algorithm. Figure 9.13 shows the MAC frame format. The only new field, compared to 802.3, is the frame control field. This field contains information needed for the proper operation of the algorithm.

Medium Options

Table 9.6: Physical layer specification for IEEE 802.4 (Token Bus) LAN standard.

Option	Transmission Medium	Signaling Technique	Data Rate (Mbps)	Maximum Segment Length (m)	Bandwidth MHz
Broadband	Coaxial Cable (75 Ohms)	Broadband (AM/PSK)	1,5,10	Not specified	1.5,6,12
Carrierband	Coaxial Cable (75 Ohms)	Broadband (FSK)	1,5,10	7600	
Optical Fiber	Optical Fiber	ASK-Manchester	5,10,20	Not specified	

The token bus standard specifies three physical layer options (table 9.6). For optical fiber option, either a passive or active star topology can be used.

3.6. Token Ring Standard (IEEE 802.5)

Medium Access Control

The 802.5 medium access control technique is token passing on a ring topology.

The 802.5 medium access control technique is token passing on a ring topology. Figure 9.13 shows the frame format. The access control field includes a token bit to indicate whether this is a frame or not. In the former case, the remainder of the frame simply consists of the ending delimiter. The access control field also includes a 3-bit priority and a 3-bit reservation, used in the capacity allocation algorithm. The frame control field serves the same function as in the 802.4 MAC frame. The frame status field contains bits that may be set by the receiver to indicate that it has recognized its address and copied the frame; these bits can then be read by the source station when it absorbs the frame.

Medium Option

The IEEE 802.5 physical layer options are given in table 9.7.

Table 9.7: Physical layer specification for IEEE 802.5 (Token Ring) LAN standard.

Transmission Medium	Signaling Technique	Data Rate (Mbps)	Maximum Number of Repeaters	Maximum Distance Between Repeaters (m)
Shielded Twisted Pair	Differential Manchester	4,16	250	Not specified
Unshielded Twisted Pair	Differential Manchester	4	250	Not specified

3.7. Fiber Distributed Data Interface (FDDI) Standard

Medium Access Control

The FDDI medium access control technique is also a token-passing ring technique.

The FDDI medium access control technique is also a token-passing ring technique. FDDI does not use the priority/reservation scheme of 802.5. Accordingly, the FDDI MAC frame (figure 9.13) is the same as that of 802.5 except that there is no access control field in the FDDI frame.

Medium Option

FDDI physical layer option is given in table 9.8.

Table 9.8: Physical layer specification for FDDI LAN standard.

Transmission Medium	Signaling Technique	Data Rate (Mbps)	Maximum Number of Repeaters	Maximum Distance Between Repeaters (m)
Optical Fiber	ASK-NRZI	100	1000	2000

3.8. Exercise

3.8.1. Multiple choice question

a. In LLC protocol for LANs, flow control is done for the following types of operations:

i) Type 1 operation only.
ii) Type 2 operation only.
iii) Type 3 operation only.
iv) Type 1 and 3 operations only.

3.8.2. Question for short answer

a) What are the services that are provided as alternatives for attached devices using LLC?

3.8.3. Analytical questions

a) Discuss LLC protocol (IEEE 802.2) for LAN.
b) Discuss CSMA/CD standard (IEEE 802.3) for LAN.
c) Discuss Token Bus standard (IEEE 802.4) for LAN.
d) Discuss Token Ring standard (IEEE 802.5) for LAN.
e) Discuss FDDI standard for LAN.

Unit 10 : Transport Protocols

Introduction

The transport protocol is the keystone of the whole concept of a computer-communications architecture. The transport protocol provides the basic end-to-end service of transforming data between users. Any process or application can be programmed to access directly the transport services without going through session and presentation layers. In this unit services provided by a transport protocol and the protocol mechanisms required to provide these services are discussed. As might be expected, the less the network service provides, the more the transport protocol must do. The types of network services and protocol standards are also discussed in this unit.

Lesson 1 : Transport Services and Protocol Mechanisms

1.1. Learning Objectives

On completion of this lesson you will be able to :

- learn services provided by a transport protocol
- the protocol mechanisms required to provide transport services.

1.2. Transport Services

The general service provided by a transport protocol is the end-to-end transport of data in a way that shields the user from the details of the underlying communications systems.

In a system, there is a transport entity which provides services to transport users, which might be an application process or a session protocol entity. This local transport entity communicates with some remote transport entity, using the services of some lower layer, such as the network layer. The general service provided by a transport protocol is the end-to-end transport of data in a way that shields the user from the details of the underlying communications systems. To be more specific, the following categories of service are useful for describing the transport service:

- Type of service.
- Quality of service.
- Data transfer.
- User interface.
- Connection management.
- Expedited delivery.

- Status reporting.
- Security.

Types of Service

Two basic types of services are possible:

- Connection-oriented service.
- Connectionless or datagram service.

Quality of Service

The transport protocol entity should allow the transport user to specify the quality of transmission service to be provided. Examples of services that might be required:

- Acceptable error and loss levels.
- Desired average and maximum delay.
- Desired average and minimum throughput.
- Priority levels.

Examples of services.

One approach to providing a variety of qualities of service is to include a quality of service facility within the protocol. An alternative is to provide a different transport protocol for different classes of traffic. Four types of transport protocol are suggested:

- A reliable connection-oriented protocol.
- A less reliable connectionless protocol.
- A speech protocol, requiring sequenced, timely delivery.
- A real-time protocol that requires high reliability and timeliness.

Data Transfer

The whole purpose of a transport protocol is to transfer data between two transport entities. Both user data and control data must be transferred, either on the same channel or separate channels. Full-duplex service must be provided.

The whole purpose of a transport protocol is to transfer data between two transport entities.

User Interface

The mechanism of the user interface to the transport protocol should be optimized to the station environment.

Connection Management

When connection-oriented service is provided, the transport entity is responsible for establishing and terminating connections.

Expedited Deliver

Some data submitted to the transport service may supersede data submitted previously. The transport entity will endeavor to have the transmission facility transfer the data as rapidly as possible. At the receiving end, the transport entity will interrupt the user to notify it of the receipt of urgent data.

Status Reporting

A status reporting service allows the transport user to obtain or be notified of information concerning the condition or attributes of the transport entity or a transport connection. Examples of status information:

- Performance characteristics of a connection.
- Addresses.
- Class of protocol in use.
- Current timer values.
- State of protocol "machine" supporting a connection.
- Degradation in requested quality of service.

Security

The transport entity may provide a variety of security services.

1.3. Protocol Mechanisms

As the network service is made less capable, the transport protocol becomes more complex. The ISO has defined three types of network service:

Three types of network service.

- **Type A**: network connections with acceptable residual error rate and acceptable rate of signaled failures.
- **Type B**: network connections with acceptable residual error rate but unacceptable rate of signaled failure.
- **Type C**: network connections with residual error rate not acceptable to the transport service user.

There are three subcases of Type A:

- Reliable, sequencing network service with arbitrary message size.
- Reliable, nonsequencing network service with arbitrary message size.
- Reliable, nonsequencing network service with maximum message size.

Reliable Sequencing Network service

In this case, we assume that the network service will accept messages of arbitrary length and will, with virtually 100% reliability, deliver them in sequence to the destination. These assumptions allow the development of the simplest possible transport protocol. Four issues need to be addressed.

- Addressing.
- Multiplexing.
- Flow control.
- Connection establishment/termination.

Reliable Nonsequencing Network Service

In this case, we assume that the network service will accept messages of arbitrary length and will, with virtually 100% reliability, deliver them to the destination. However, we now assume that the TPDU's may arrive out of sequence. This seemingly trivial change has a number of consequences:

- Sequence numbers are required on TPDU's for connection-oriented service. The transport entity is required to deliver data in sequence.
- The transport entity must keep track of control PDU's, both in relationship to each other and to data PDU's.

Reliable Nonsequencing Network Service With Maximum TPDU Size

In this case, the network service will only accept TPDU's of some maximum size for transfer. There are two types of data transfer required by the user: stream-oriented and block-oriented. A stream-oriented interface between transport and the user accepts data as if they were a continuous stream of bits and reproduce the stream at the other end without conveying any information about the breakpoints in the stream submitted by the sender. A more common occurrence is a transport user that sends data in blocks. If a block exceeds the maximum allowable TPDU size, the transport entity must segment the block before transmission, to be reassembled at reception prior to delivery to the user.

Two types of data transfer required by the user: stream-oriented and block-oriented.

Failure-Prone Network Service

This is a connection oriented network service and, while it delivers data reliably, it suffers from network failures that cause it to reset or restart network connections. Thus PDUs may be lost, but the loss is reported to the transport entities affected. In any case, the transport entity must cope with the problem of recovering from known loss of data and/or network connections.

Unreliable Network Service

In this case, TPDUs are occasionally lost, and TPDUs may arrive out of sequence. Six issues need to be addressed:

- ♦ Retransmission strategy.
- ♦ Duplication detection.
- ♦ Flow control.
- ♦ Connection establishment.
- ♦ Connection termination.
- ♦ Crash recovery.

1.4. Exercise

1.4.1. Multiple choice question

a. The transport protocol provides

i) end-to-end service of transferring data between users.
ii) service of transferring data between station and node to which the station is attached.
iii) service of transferring data between network nodes.
iv) none of the above.

1.4.2. Questions for short answers

a) Name the categories of transport service.
b) Name the types of service offered by transport protocol.
c) Name the quality of service that might be required for transport protocol.
d) Name the types of transport protocols.
e) Name the status information reported by transport protocol.
f) Name the issues need to be addressed in transport protocol for reliable sequencing network service.
g) Name the issues need to be addressed in transport protocols for unreliable network service.

1.4.3. Analytical question

a) Briefly discuss the types of network service defined by ISO.

Lesson 2 : Network Services And Transport Protocols

2.1. Learning Objectives

On completion of this lesson you will be able to :

- learn primitive used to provide a network service to a transport entity
- learn a family transport protocol developed by ISO
- learn transport-level protocols of TCP/IP protocol suite.

2.2. Network Services

To function, a transport protocol must make use of the services of some lower-level network-oriented protocol.

Service Primitives

ISO specified a set of primitives that might be used to provide a network service to a transport entity. The network service must provide a means of delivering TPDUs to a remote correspondent. The transport entity uses N-DATA.request primitive to transfer data to the network service for transmission. The network service passes up received data using N-DATA.indication primitive. If the service is not connection-oriented, address information must be included in the primitive invocation.

If the service is not connection-oriented, address information must be included in the primitive invocation.

If the network service is connection-oriented, additional primitives are needed: N-CONNECT.request primitive signals a request by a transport entity to open a connection. N-CONNECT.indication presents this request to the correspondent transport entity identified in the connection request. A transport entity signals its willingness to accept the connection with N-CONNECT.response. This willingness is communicated to the initiating transport entity with N-CONNECT.confirm. N-DISCONNECT.request and N-DISCONNECT.indication are used to terminate a connection.

Additional primitives may be provided by the network service for enhancing the capability and efficiency of the transport protocol. The N-DATA-ACKNOWLEDGE primitives permit the local exercise of flow control across the transport/network interface in both directions. N-EXPEDITED-DATA primitive provides direct support of the transport expedited data feature. The N-RESET primitives allow the transport entity to force a reset of the network connection.

2.3. The ISO Transport Standards

ISO developed a family of transport protocols as an international standard.

The Transport Protocol Family

In order to handle a variety of user service requirements and available network service, ISO has defined five classes of transport protocols:

ISO has defined five classes of transport protocols.

- **Class 0**: simple class.
- **Class 1**: basic error recovery class.
- **Class 2**: multiplexing class.
- **Class 3**: error recovery and multiplexing class.
- **Class 4**: error detection and recovery class.

Classes 0 and 2 are used with Type A networks; Classes 1 and 3 are used with Type B networks; and Class 4 is used with Type C networks. Class 0 was developed by CCITT and is oriented for teletex, a text-transmission system. It provides the simplest kind of transport connection. It provides a connection with flow control based on network-level flow control, and connection release based on the release of the network connection.

Class 1 was also developed by CCITT and is designed to run on X.25 network and provide minimal error recovery. Flow control is provided by the network layer. Expedited data transfer is also provided.

Class 2 is an enhancement to Class 0 that assumes a highly reliable network service. It provides multiplexing multiple transport connections onto a single network connection and explicit flow control on individual transport connection. A credit allocation scheme is used.

Class 3 is basically the union of the Class 1 and 2 capabilities. It provides the multiplexing and floe control capabilities of Class 2. It also contains the resynchronization and reassignment capabilities of Class 1, which are needed to cope with failure-prone networks.

Class 4 assumes that the underlying network service is unreliable. Thus most of the protocol mechanisms discussed in lesson 1 must be included.

Transport Services

The ISO specification is in the form of four primitive types and 10 primitives.

The transport service specification is the same for all classes. The ISO specification is in the form of four primitive types and 10 primitives. The T-CONNECT primitives are used to established a connection. The transport entity will either provide the requested quality of service, or indicate in the indication and confirm primitives a lesser quality of service that can be provided. T-DISCONNECT primitive provides for an abrupt connection termination. Termination can be initiated by either side or by one of the transport entities. T-DISCONNECT can also be used by the local transport entity or the remote addressee to reject a connection attempt. T-DATA and T-EXPEDITED-DATA primitives are used to transfer data over a transport connection.

Protocol Formats

The ISO protocol makes use of 10 types of transport protocol data units (TPDUs):

- Connection request (CR).
- Connection confirm (CC).
- Disconnect request (DR).
- Disconnect confirm (DC).
- Data (DT).
- Expedited data (ED).
- Acknowledgment (AK).
- Expedited acknowledgment (EA).
- Reject (RJ).
- TPDU error (ER).

Each TPDU consists of three parts:

- A fixed header.
- A variable header.
- A data field.

The latter two optionally may not be present in a TPDU. The fixed header contains the frequently occurring parameters and the variable header contains optional or infrequently occurring parameters.

Protocol Mechanisms

Protocol mechanisms are discussed under the following topics:

- Connection establishment.

- Data transfer.
- Connection termination.

Connection Establishment

The connection establishment phase requires the exchange of a CR and a CC TPDU. This two-way handshake suffices for Classes 0 through 3. For Class 4, a third TPDU is needed to acknowledge the CC; this may be an AK, DT, or ED. The purpose of this phase is to establish a transport connection with agreed-upon characteristics.

A transport connection invokes four different types of identifiers:

A transport connection invokes four different types of identifiers.

- User identifier (service access point).
- Transport/network address.
- Transport protocol identifier.
- Transport connection identifier.

Data Transfer

Normal data transfer over a connection is accomplished using DTs. DTs are numbered sequentially. This is used in Classes 2 through 4 for flow control. A credit-allocation scheme is used. The initial credit is set in the CC and CR TPDUs. Subsequent credit is granted with an AK. Acknowledgments are in separate TPDUs, and never piggybacked onto DTs. In Class 4, sequence numbers are also used for resequencing DTs that arrive out of order. Another mechanism unique to Class 4 is the DT checksum. If an error is detected, an ER is returned. Expedited data transfer uses the ED and EA data units. Sequence numbers are used, but only one ED may be outstanding at a time. The sender must receive an EA before sending another ED. In Classes 1 through 4, an ED is sent before any DTs queued for that connection. The Class 4 entity suspends the transfer of new DTs until an EA is received.

Normal data transfer over a connection is accomplished using DTs.

Connection Termination

An abrupt termination is achieved by the exchange of a DR and a DC. When a transport entity receive a disconnect request from its user, it discards any pending DTs and issues the DR. The entity that receives DR issues a DC, discarding any pending DTs, and informs its user.

2.4. TCP And UDP

The TCP/IP protocol suite includes two transport-level protocols:

- The Transmission Control Protocol (TCP), which is connection-oriented.
- The User Datagram Protocol (UDP), which is connectionless.

TCP Services

TCP is stream oriented, that is, TCP users exchange streams of data.

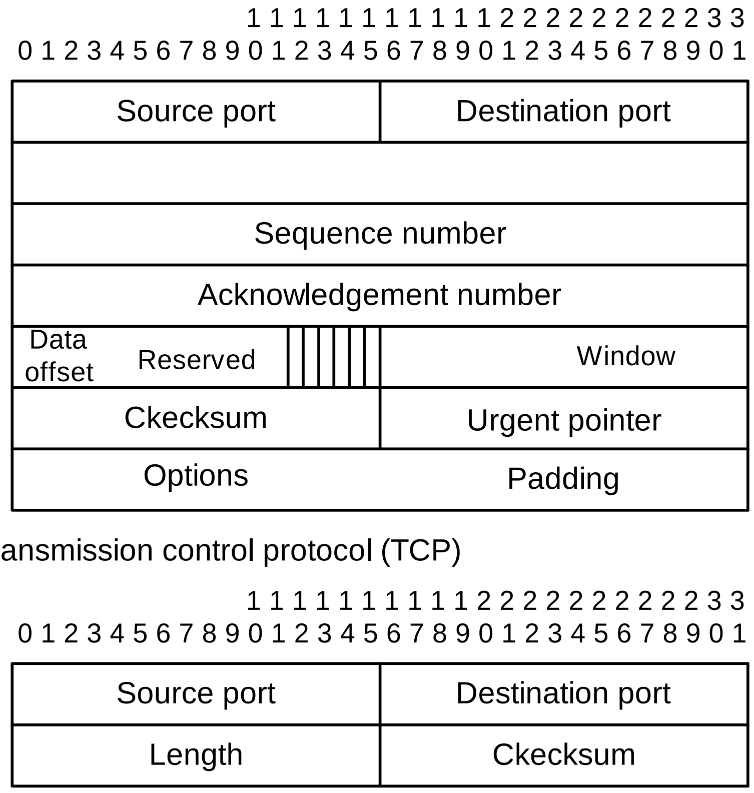
TCP is designed to provide reliable communication between pairs of processes (TCP users) across a variety of reliable and unreliable networks and internets. Functionally, it is equivalent to Class 4 ISO Transport. TCP is stream oriented, that is, TCP users exchange streams of data. The data are placed in allocated buffers and transmitted by TCP in segments (TPDUs0. TCP supports security and precedence labeling. In addition, TCP provides two useful facilities for labeling data: push and urgent. There are nine TCP service request (user to TCP) and eight TCP service response (TCP to user) primitives.

TCP Header Format

TCP uses only a single type of TPDU, called a TCP segment. The header is shown in figure 10.1(a). The header fields are:

- **Source port (16 bits)**: identifies source service access point.
- **Destination port (16 bits)**: identifies destination service access point.
- **Sequence number (32 bits)**:
- **Acknowledgment number (32 bits)**: a piggybacked acknowledgment.
- **Data offset (4 bits)**: number of 32-bit words in the header.
- **Reserved (6 bits)**: reserved for future use.
- **Flags (6 bits)**:
- **URG**: urgent pointer field significant.
- **ACK**: acknowledgment field significant.
- **PSH**: push function.
- **RST**: reset the connection.
- **SYN**: synchronize the sequence numbers.
- **FIN**: no more data from sender.
- **Window (16 bits)**: flow control credit allocation, in octets.
- **Checksum (16 bits)**:
- **Urgent Pointer (16 bits)**: points to the octet following the urgent data.

- **Options (variable)**: at present, only one option is defined, which specifies the maximum TPDU size that will be accepted.



(a) Transmission control protocol (TCP)

(b) User datagram protocol (UDP)

Fig. 10.1: TCP header format.

TCP Mechanism

Connection Establishment: Connection establishment in TCP always uses a three-way handshake. When the SYN flag is set, the TPDU is essentially a request for connection (RFC). To initiate a connection, an entity sends an RFC X, where X is the initial sequence number. The receiver responds with RFC Y, ACK X by setting both the SYN and ACK flags. Finally, the initiator responds with ACK Y. If both sides issue crossing RFCs, no problem results: Both sides respond with ACKs.

Connection establishment in TCP always uses a three-way handshake.

Data Transfer: Although data are transferred in TPDUs over a transport connection, data transfer is viewed logically as consisting of a stream of octets. Hence every octets is numbered, modulo 2^{32}. Each TPDU contains the sequence number of the first octet in the data field. Flow control is exercised using a credit allocation scheme in which the credit is a number of octets.

Data are buffered by the entity on both transmission and reception.

Data are buffered by the entity on both transmission and reception. TCP normally exercise its own discretion as to when to construct a TPDU for transmission and when to release received data to the user. The PUSH flag is used to force the data so far accumulated to be sent by the transmitter and passed on by the receiver. The user may specify a block of data as urgent. TCP will designate the end of that block with an urgent pointer and send it out in the ordinary data stream. The receiving user is alerted that urgent data are being received. If, during data exchange, a TPDU arrives which is apparently not meant for the current connection, the RST flag is set on an outgoing TPDU.

Connection Termination: For normal termination, each transport user must issue a CLOSE primitive. The transport entity sets the FIN bit on the last TPDU that it sends out, which also contains the last of the data to be sent on this connection.

An abrupt termination occurs if the user issues an ABORT primitive. In this case, the entity abandons all attempts to send or receive data and discards data in its transmission and reception buffers. An RST TPDU is sent to the other side.

User datagram Protocol (UDP)

UDP sits on top of IP. Essentially, it adds a port addressing capability to IP.

UDP provides a connectionless service for application-level procedures. Thus UDP is basically an unreliable service; delivery and duplicate protection are not guaranteed. UDP sits on top of IP. Essentially, it adds a port addressing capability to IP. This is best seen by examining the UDP header (figure 11.1(b)). The header includes a source port and destination port. The length field contains the length of the entire UDP segment, including header and data. The checksum applies to the entire UDP segment plus a pseudoheader prefixed to the UDP header at the time of calculation. If an error is detected, the segment is discarded and no further action is taken. The checksum field in UDP is optional. If it is not used, it is set to zero.

2.5. Exercise

2.5.1. Multiple choice question

a. Flow control is provided for the following ISO transport protocol class:

i) Class 1.
ii) Class 2.
iii) Class 3.
iv) all of the above.

2.5.2. Questions for short answers

a) How many classes of transport protocol are there defined by ISO? Name them.
b) How many types of transport protocol data units (TPDUs) are there in the ISO standard? Name them.
c) How many parts are there in ISO TPDU? Name them.
d) Name the different transport-level protocols of TCP/IP protocol suite.

2.5.3. Analytical questions

a) Discuss different classes of transport protocol defined by ISO.
b) Discuss protocol mechanisms of ISO transport protocol.
c) Discuss TCP service.
d) Discuss TCP header format.
e) Discuss TCP mechanisms.
f) Discuss UDP.

Unit 11 : Session Services and Protocols

Introduction

At the application level, users should be able to write their own applications that invoke the computer network functionality through a transport, session, or presentation interface, as appropriate. Whereas the OSI model calls for the inclusion of a session layer, the TCP/IP architecture sets face against a "session layer" as such, feeling that some of its presumed functions should be performed by transport and that other functions are peculiar to the process or applications that wish to communicate. This unit discusses the session layer. Session characteristics and requirements as well as standard developed by ISO are discussed.

Lesson 1 : Session Characteristics, Requirements And Standards

1.1. Learning Objectives

On completion of this lesson you will be able to :

- understand session characteristics
- learn OSI session service definition
- learn OSI session protocol definition.

1.2. Session Characteristics

The transport protocol is responsible for creating and maintaining a logical connection between endpoints.

The essential purpose of a session protocol is to provide a user-oriented connection service. The transport protocol is responsible for creating and maintaining a logical connection between endpoints. A session protocol provides a "user interface" by "adding value" to the basic connection service. The value-added functions can be grouped into the following categories:

- Session establishment and maintenance.
- Dialogue management.
- Recovery.

Session Establishment and Maintenance

The minimum service that a session protocol entity provides its user is the establishment, maintenance, and termination of sessions. When two users wish to establish a connection, their respective entities will create a session that is mapped onto a transport connection and negotiate the parameters of the session (e.g., data unit size).

The session entity accepts records from the session user and encapsulates each into a session protocol data unit (SPDU). SPDUs are, in turn, handed over the local transport entity to be sent over a transport connection in a sequence of transport protocol data units (TPDUs). The data are received on the other side and delivered to the user in the proper order. The sending transport entity may, at its discretion, segment SPDUs into multiple TPDUs if the SPDU size is too large. Alternatively, multiple records may be blocked into a single TPDU for efficiency of transmission. In any case, the receiving entity recovers the original records and passes these on to the receiving user.

Dialogue Management

The session entity may impose a structure on the interaction or dialogue between users. There are three modes of dialogue:

- Two-way simultaneous mode.
- Two-way alternate mode.
- One-way mode.

The two-way simultaneous mode is a full-duplex type of operation. Both sides can simultaneously send data. Once this mode is agreed upon in the session negotiation phase, there is no specific dialogue management task required. Similarly, the one-way mode requires no specific dialogue management mechanism once it is established. All user data flows in one direction only. The most complex of the three modes is two-way alternate. In this mode, the two sides take turns sending data. The session entity enforces the alternating interaction by informing each user when it is its turn.

The two-way simultaneous mode is a full-duplex type of operation.

Recovery

Another potential feature of a session protocol is a recovery support service. This feature could be provided by defining a session recovery unit, which corresponds to the interval between checkpoints. Each user specifies the point at which a recovery unit ends, and the recovery units are numbered sequentially. To recover lost data, a user can issue a command to recover, using the recovery unit number to identify the point to which the session should be backed up.

1.3. OSI Session Service Definition

The definition of OSI session services developed and standardized by ISO and CCITT is presented here.

Session Services

The services provided to a session-service user (SS-user) by the session service consists of the following:

1. Establish a connection with another SS-user, exchange data with that user in a synchronized manner, and release the connection in an orderly manner.
2. Negotiate for the use of tokens to exchange data, synchronize and release the connection, and to arrange for data exchange to be half-duplex or full-duplex.
3. Establish synchronization points within the dialogue and, in the event of errors, resume the dialogue from an agreed synchronization point.
4. Interrupt a dialogue and resume it later at a prearranged point.

The use of Tokens

A token is an attribute of a session connection that is dynamically assigned to one user at a time and that grants that user the exclusive right to invoke certain services.

In the context of the OSI standard, a token is an attribute of a session connection that is dynamically assigned to one user at a time and that grants that user the exclusive right to invoke certain services. There are certain services which can only be invoked by the current token holder. A simple example is a token that grants the right to transmit data. This token enforces a half-duplex mode of operation. Only the holder of the token can send data. At any time, the token holder can pass the token to the other user, at which time the other user becomes the possessor of the right to transmit.

Service Primitives and Parameters

There are 21 types and 56 session service primitives. A service action on the part of one of the session users usually results in action between the two session protocol entities at the two ends of the session connection. This protocol action is invisible to the session user and only manifests itself as a resultant service primitive.

For the connection establishment phase, the S-CONNECT primitives are used. The parameters that are provided are:

- **Identifier**: a unique identifier of this connection.

- **Calling and called SSAP**: service access points that serve as the address of the session users.
- **Quality of service**: a list of parameters that are negotiated as part of the connection establishment process. For the most part, these parameters are passed down to the transport service. The session provider indicates the quality of service that can be provided on the basis of the transport service.
- **Requirements**: a list of functional options that may be requested.
- **Serial number**: when synchronization services are to be employed, this is the proposed initial serial number.
- **Token**: a list of the initial side to which the available tokens are assigned.
- **Data**: certain session user data.

1.4. OSI Session Protocol Definition

It is the job of the session protocol to bridge the gap between the services provided by the transport layer and those required by the session user. In essence, the transport layer provides three services:

The transport layer provides three services.

- Establishment, maintenance, and release of a transport service with certain quality-of-service characteristics.
- Reliable transfer of data.
- Reliable transfer of expedited data.

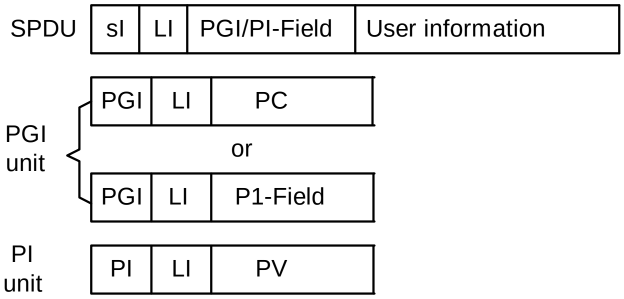
The session service provides a variety of services relating to the management and structuring of the exchange of data. Hence, it is the job of the session protocol to provide these structuring mechanisms on top of these transport services.

OSI session protocol includes 36 types of session protocol data units (SPDUs). The session protocol basically provides a rather straightforward mapping of session service primitives into session protocol data units, and makes use of the comparatively simple, reliable interface to the transport layer to exchange these primitives.

Session Protocol Formats

The number of parameters that is sent with an SPDU varies widely. Furthermore, the length of parameters is variable. The ISO standard provides a flexible formatting scheme to accommodate these variations. Figure 11.1 shows the general structure of an SPDU. Each SPDU has up to four fields. The first field is the SPDU identifier (SI), which specifies one of the 34 types of

SPDUs. The next field is the length indicator, which specifies the length of the header. If the SPDU contains any parameters, then the next field contains these parameters. Finally, there may be a field for session user information.



SI = SPDU identifier
LI = Length indicator
PGI/P1-Field = One or more PGI and/or PI units
PGI = Parameter group identifier
PV = Parameter value
PI-Field = One or more PI units
PI = Parameter identifier

Fig. 11.1: SPDU format.

The parameter field may take on one of several general forms, depending on the way in which particular parameters are expressed. In its simplest form, a parameter is expressed with three subfields: a parameter identifier, a length indicator, and the parameter value. This form is know as a PI unit, and the SPDU may contain one or more such units. Alternatively, related parameters may be expressed in a PGI unit, which consists of a parameter group identifier, a length indicator, and either a single parameter value or one or more PI units.

A parameter is expressed with three subfields: a parameter identifier, a length indicator, and the parameter value.

Transport Connection

Session connection must be mapped into transport connections by the session protocol entity. The ISO standard contains specific guidance on the way this is to be done. Most important is the requirement that a transport connection be dedicated to a single session connection.

When a session is terminated, the session protocol entity that initially set up the corresponding transport connection has the option of terminating that connection or not. If the transport connection is retained, then it may be used to support a new session connection request, provided that it meets the required quality of service.

1.5. Exercise

1.5.1. Multiple choice questions

a. A logical connection between endpoints is created by

i) a session protocol
ii) a transport protocol
iii) any one of the above two
iv) none of the above.

b. When a session is terminated, the session protocol entity that initially set up the corresponding transport connection

i) must terminate that connection.
ii) may terminate that connection.
iii) may not terminate that connection.
iv) may or may not terminate that connection.

1.5.2. Questions for short answers

a) Name the parameters that are provided to S-CONNECT primitives during the connection establishment phase.
b) Mention the services provided by the transport layer to the session layer.

1.5.3. Analytical questions

a) Discuss session establishment and maintenance.
b) Discuss dialogue management of session service.
c) Discuss the services provided to a session-service user by the session service.
d) Discuss the use of tokens in session service.
e) Discuss the SPDU format.
f) Discuss transport connection in relation to session connection.

Unit 12 : Presentation Facilities

Introduction

Presentation facilities deal with representation of information of concern to applications. In general, we can consider two categories of presentation facilities:

- Those concerned with data to be transferred between application entities in different systems. Presentation facilities may provide a representation to be used for the transfer of information as well as mechanisms for translating between local representations and the representation used for information exchange. Examples of such facilities include encryption and compression.
- Those concerned with data structures that applications refer to in their communication. An example of such a facility are concerned with the representation of management information for network management.

In this unit, presentation concept and Abstract Syntax Notation One (ASN.1), which has become an all-important universal language for defining representations are discussed. Encryption, an example of translation facility, and concept of virtual terminal protocols are also discussed in this unit.

Lesson 1 : Presentation Concepts and Abstract Syntax Notation one (ASN.1)

1.1. Learning Objectives

On completion of this lesson you will be able to :

- briefly introduce yourself to presentation concept
- briefly introduce yourself to ASN.1 standard.

Two major components

1.2. Presentation Concepts

Figure 12.1 illustrates the underlying concepts of presentation. For purposes of discussion, a communications architecture in an end system can be considered to have two major components:

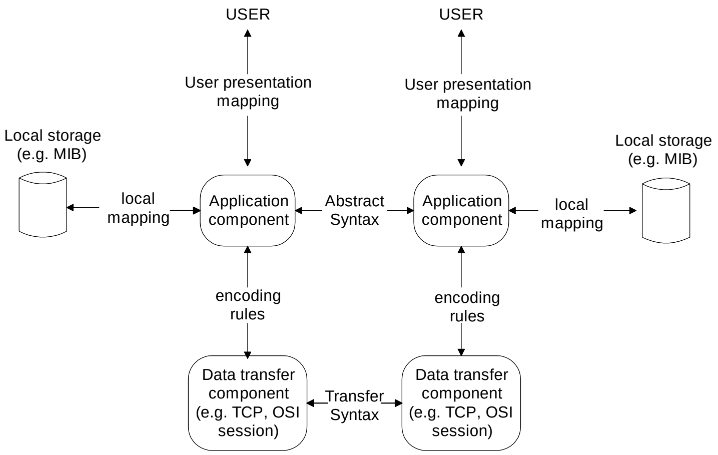


Fig. 12.1: The use of abstract and transfer syntaxes.

- **The data transfer component** is concerned with the mechanisms for the transfer of data between end systems. In the case of the TCP/IP protocol suite, this component would consist of TCP or UDP on down. In the case of the OSI architecture, this component would consist of the session layer on down.
- **The application component** is the user of the data transfer component and is concerned with the end user's application. In the case of the TCP/IP protocol suite, this component would consist of an application, such as SNMP, FTP, SMTP, or TELNET. In the case of OSI, this component actually consists of the application layer.

Application protocols describe their PDUs in terms of an abstract syntax.

As we cross the boundary from the application to the data transfer component, there is a significant change in the way the data are viewed. For the data transfer component, the data received from an application are specified as the binary values of a sequence of octets. This binary value can be directly assembled into service data units (SDUs) for passing between layers and into protocol data units (PDUs) for passing between protocol entities within a layer. The application component, however, is concerned with a user's view of data. For the application component, information is represented in a abstract syntax that deals with data types and data values. The abstract syntax formally specifies data independently from any specific representation. Application protocols describe their PDUs in terms of an abstract syntax.

This abstract syntax is used for the exchange of information between application components in different systems. The exchange consists of application level PDUs within a system, the information represented using an abstract syntax must be mapped into some form for presentation to the human user. Similarly, this abstract syntax must be mapped into some local format for storage.

A transfer syntax that describes the data values in a binary form, suitable for interaction with the data transfer component.

The application must also translate between the abstract syntax of the application and a transfer syntax that describes the data values in a binary form, suitable for interaction with the data transfer component. For example, an abstract syntax may include a data type of character; the transfer syntax could specify ACSII or EBCDIC encoding.

The transfer syntax thus defines the representation of the data to be exchanged between data transfer components. The translation from abstract syntax to the transfer syntax is accomplished by means of encoding rules that specify the representation of each data value of each data type.

This approach for the exchange of application data solves the two problems that relate to data representation in a distributed, heterogeneous environment:

- There is a common representation for the exchange of data between differing systems.
- Internal to a system, an application uses some particular representation of data. The abstract/transfer syntax scheme automatically resolves differences in representation between cooperating application entities.

1.3. Abstract Syntax Notation one (ASN.1)

ASN.1 is an abstract syntax standard and is widely used both in the development of OSI-related standards and TCP/IP-related standards. It is used to define the format of protocol data units (PDUs), the representation of distributed information, and operations performed on transmitted data.

ASN.1 is a language that can be used to define data structure.

The basic building block of an ASN.1 specification is the module. ASN.1 is a language that can be used to define data structure. A structure definition is in the form of a named module. The name of the module can then be used to reference the structure. Modules have the basic form

```
< modulereference > DEFINITIONS ::=
        BEGIN
                EXPORTS
                IMPORTS
                Assignment List
        End
```

The module reference is a module name followed optionally by an object identifier to identify the module. The EXPORTS construct indicates which definitions in this module may be imported by other modules. The IMPORTS construct indicates which type and value definitions from other modules are to be imported into this module. The assignment list consists of type assignments, value assignments, and macro definitions.

Type and value assignments have the form
    < name > ::= < description >

ASN.1 structures, types, and values are expressed in a notation similar to that of a programming language. ASN.1 is a notation for abstract data types and their values. The number of values that a type may take on may be infinite. For example, the type INTEGER has an infinite number of values.

We can classify types into four categories:

- **Simple**: These are atomic types, with no components.
- **Structured**: A structured type has components.
- **Tagged**: These are types derived from other type.
- **Other**: This category includes the CHOICE and ANY types.

The tag consists of class name and a nonnegative integer tag number.

Every ASN.1 data type, with the exception of CHOICE and ANY, has an associated tag. The tag consists of class name and a nonnegative integer tag number. There are four classes of data types, or four classes of tag:

- **Universal**: Generally useful, application-independent types and construction mechanism; these are defined in the standard.
- **Application-Wide**: Relevant to a particular application; these are defined in other standards.
- **Context-Specific**: Also relevant to a particular application, but applicable in a limited context.
- **Private**: Types defined by users and not covered by any standard.

Name:	Abdul Karim
Title:	Professor
Employee Number:	100
Date of Joining:	01 March 1999
Name of Spouse:	Momota Karim
Number of Children:	2

Child Information

Name:	Matin Karim
Date of Birth:	11 February 1990

Child Information

Name:	Matia Karim
Date of Birth:	15 January 1193

(a) Informal description of personnel record

```
Personnel Record ::=[APPLICATION 0] IMPLICIT SET {
        Name,
        title[0] VisibleString,
        number EmployeeNumber,
        dateOfJoining [1] Date,
        nameOfSpouse [2] Name,
        children [3] IMPLICIT SEQUENCE OF ChildInformation
        DEFAULT {}}
ChildInformation ::= SET{
        Name,
        dateOfBirth [0] Date}
Name ::= [APPLICATION 1] IMPLICIT SEQUENCE {
        givenName VisibleString,
        initial VisibleString,
        familyName VisibleString}
EmployeeNumber ::= [APPLICATION 2] IMPLICIT INTEGER
Date ::= [APPLICATION 3] IMPLICIT VisibleString - DDMMYYYY
```

(b) ASN.1 description of the record structure

```
{                       {givenName “Abdul”, familyName “Karim”},
title                   “Professor”
number                  100
dateOfJoining           “01031999”
nameOfSpouse            {givenName     “Momota”,     familyName
“Karim”},
children
{{                      {givenName “Matin”, familyName “Karim”}
  dateOfBirth           “11021990”},
  {                     {givenName “Matia”, familyName “Karim”},
   dateOfBirth          “15011993”}}}
```

(c) ASN.1 description of a record value

Fig. 12.2: Example of use of ASN.1.

To give an idea, without going into details, an example that defines the structure of a personal record is given in figure 12.2. Part (a) of the figure depicts the personal record informally by giving an example of a specific record. Such a display might correspond to the user presentation in figure 12.1. In part (b), we see the formal description, or abstract syntax, of the data structure. Part (c) is an example of a particular value for the personal record, expressed in the abstract syntax.

The most common encoding specification for translating from an abstract syntax to a bit pattern is known as Basic Encoding Rules (BER).

ASN.1 macro notation allows the user to extend the syntax of ASN.1 to define new types and their values. The subject of ASN.1

macro is a complex one, and is not discussed here. ASN.1 specifies the syntax or format of information in an abstract representation. To actually store or exchange information, it needs to be encoded as a bit pattern. The most common encoding specification for translating from an abstract syntax to a bit pattern is known as Basic Encoding Rules (BER). BER describes a method for encoding values of each ASN.1 type as a string of octets. Details of BER is not discussed here.

1.4. Exercise

1.4.1. Multiple choice questions

a. Application protocols describe their PDUs in terms of

i) abstract syntax.
ii) transfer syntax.
iii) absolute syntax.
iv) any one of the above.

b. The basic building block of a ASN.1 specification is

i) the type
ii) the module
iii) the macro
iv) none of the above.

c. In ASN.1, the number of values that a type may take on

i) must be infinite
ii) must be finite
iii) may be infinite
iv) none of the above.

1.4.2. Questions for short answers

a) What is the importance of abstract/transfer syntax scheme in data representation in a distributed, heterogeneous environment?
b) Name the different categories of types as used in ASN.1.
c) Name the different classes of tags as used in ASN.1

1.4.3. Analytical questions

a) Briefly discuss the module definition as used in ASN.1.
b) Briefly discuss the type definition as used in ASN.1.

Lesson 2 : Network Security : Encryption and Authentication

2.1. Learning Objectives

On completion of this lesson you will be able to :

- grasp the concept of text encryption concealing the meaning of the text for security purpose
- know different methods of message authentication for security purpose.

2.2. Network Security

One of the most important automated tools for computer network security is encryption. **Encryption** is a process that conceals meaning by changing intelligible messages into unintelligible messages. Encryption can be by means of either of the following two systems:

Message authentication.

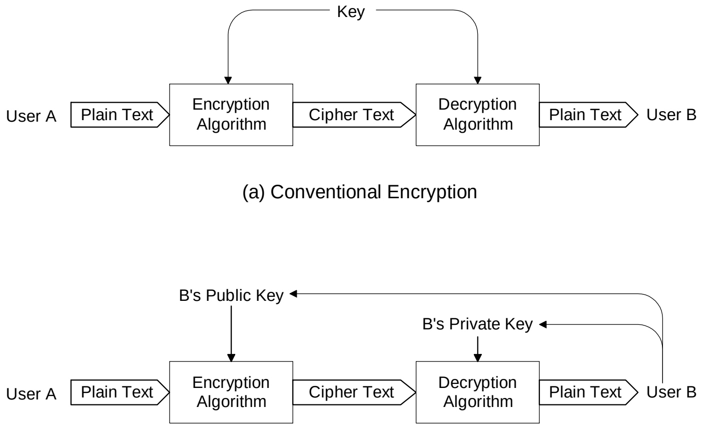
- **Code**: A code system uses a predefined table or dictionary to substitute a meaningless word or phrase for each message or part of message.
- **Cipher**: A cipher uses a computable algorithm that can translate any stream of message bits into an unintelligible cryptogram.

Because cipher techniques lend themselves more readily to automation, these are used in contemporary computer and network security facilities. Encryption protects against passive attack (eavesdropping). A different requirement is to protect against active attack (falsification of data and transmission). Protection against such attacks is known as message authentication.

2.3. Conventional Encryption

The encryption process consists of an algorithm and a key.

Figure 12.3(a) illustrates the conventional encryption process. The original intelligible message, referred to as **plaintext**, is converted into apparently random nonsense, referred to as **ciphertext**. The encryption process consists of an algorithm and a key. The **Key** is a relatively short bit string that controls the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. Changing the key radically changes the output of the algorithm.



(a) Conventional Encryption

Fig. 12.3: Encryption.

Once the ciphertext is produced, it is transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

The security of conventional encryption depends on the security of the key, not the security of the algorithm. We don't need to keep the algorithm secret; we only need to keep the key secret. With the use of conventional encryption, the principal security problem is maintaining the secrecy of the key.

Public-Key Encryption

2.4. Public-Key Encryption

One of the major difficulties with conventional encryption scheme is the need to distribute the keys in a secure manner. A clever way around this requirement is an encryption scheme that does not require key distribution. This scheme, known as public-key encryption, is illustrated in figure 12.3(b). For conventional encryption schemes, the keys used for encryption and decryption are the same. In public-key encryption, the algorithm uses one key for encryption and a companion but different key for decryption. The technique works as follows:

1. Each end system in a network generates a pair of keys to be used for encryption and decryption of messages that it will receive.
2. Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.
3. If A wishes to send a message to B, it encrypts the message using B's public key.

4. When B receives the message, it decrypts it using B's private key. No other recipient can decrypt the message since only B knows B's private key.

As long as a system controls its private key, its incoming communication is secure. At any time, a system can change its private key and publish the companion public key to place its old public key.

2.5. Message Authentication

A message, file, document, or other collection of data is said to be authentic when it is genuine and came from its alleged source. Message authentication is a procedure that allows the communicating parties to verify that received messages are authentic. The important aspects that are to be verified are:

- The contents of the message have not been altered.
- The source is authentic.
- The message is timely, that is, it has not been artificially delayed and replayed.
- The sequence relative to other messages flowing between two parties is correct.

Authentication using Conventional Encryption

Authentication using conventional encryption protects two parties exchanging messages from any third party.

It is possible to perform authentication simply by the use of conventional encryption. If we assume that only the sender and receiver share a key, then only the genuine sender would be able to successfully encrypt a message for the other participant. Furthermore, if the message includes an error-detection code and a sequence number, the receiver is assured that no alteration have been made and that sequencing is proper. If the message also includes a time stamp, the receiver is assured that the message has not been delayed beyond that normally expected for network transit.

Digital Signature using Public-Key Encryption

Authentication using conventional encryption protects two parties exchanging messages from any third party. However, it does not protect the two parties against each other. In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution is the digital signature. It must have the following properties:

- It must be able to verify the author and the date and time of the signature.
- It must be able to authenticate the contents at the time of the signature.
- The signature must be verifiable by third parties, to resolve disputes.

Thus the digital signature function includes the authentication function.

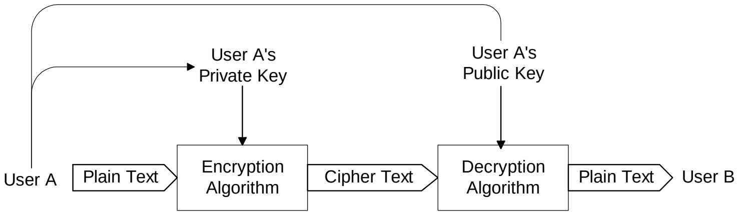


Fig. 12.4 : (a) Simple digital signature scheme proividing Authentication

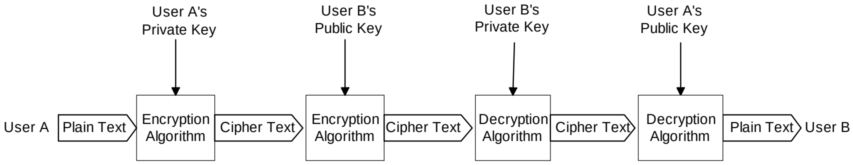


Fig. 12.4 : (b) Digital signature scheme providing authentication and secrecy

A simple digital signature scheme using public-key encryption.

Figure 12.4(a) illustrates a simple digital signature scheme using public-key encryption. This scheme exploits an important characteristics of all public-key encryption algorithms: The two keys can be used in either order. That is, one can encrypt with the public key and decrypt with the matching private key, or encrypt with the private key and decrypt with the matching public key. Figure 12.4(a) illustrates the latter application. A prepares a message to B and encrypts it using A’s private key before transmitting it. B can decrypt the message using A’s public key. Because the message was encrypted using A’s private key, only A could have prepared the message. Therefore, the entire encrypted message serves as the signature. In addition, it is impossible to alter the message without access to A’s private key, so the message is authenticated.

The encryption process just described does not provide secrecy. That is, the message being sent is safe from alteration but not safe from eavesdropping. It is, however, possible to provide both the digital signature function, which includes authentication, and secrecy by a double use of the public-key scheme. This is illustrated in figure 12.4(b). In this case, we begin by encrypting a message using the sender's private key. This provide the digital signature. Next, we encrypt again, using the receiver's public key. The final ciphertext can only be decrypted by the intended receiver, who alone possesses the matching private key. Thus secrecy is provided.

2.6. Message Authentication Without Message Encryption

Message Authentication Without Message Encryption

There are situations in which message authentication without secrecy is preferable. In message authentication without message encryption, an authentication tag is generated and appended to each message for transmission. The message itself is not encrypted and can be read at the destination independent of the authentication function at the destination.

Message Authentication Code

One authentication technique involves the use of a secret key to generate a small block of data, known as a message authentication code, that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key K_{AB}. When A has a message to send to B, it calculates the message authentication code as a function of the message and the key: $MAC_M = F(K_{AB}, M)$.The message plus code are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new message authentication code. The received code is compared to the calculated code. If we assume that only the receiver and the sender know the identity of the secret key, and if the received code matches the calculated code, then

1. The receiver is assured that the message has not been altered.
2. The receiver is assured that the message is from the alleged sender.
3. If the message includes a sequence number, then the receiver can be assured of the proper sequence.

2.7. Exercise

2.7.1. Multiple choice questions

a. The security of conventional encryption depends on

i) the secrecy of the key
ii) the secrecy of the encryption/decryption algorithm
iii) both of the above
iv) none of the above.

b. In public-key encryption, the algorithm uses

i) same key for both encryption and decryption.
ii) two different and independent keys for encryption and decryption.
iii) one key for encryption and a companion but different key for decryption.
iv) none of the above.

2.7.2. Questions for short answers

a) What do you mean by encryption?
b) Define plaintext, ciphertext and key.
c) What do you mean by message authentication?
d) List the aspects that are required to verify in message authentication.
e) What are the properties of digital signature?

2.7.3. Analytical questions

a) Discuss conventional encryption method.
b) Discuss public-key encryption method.
c) Discuss message authentication using conventional encryption.
d) Discuss digital signature using public-key encryption.
e) Discuss message authentication code.

Lesson 3 : Virtual Terminal Protocols: Telnet and the ISO Standard

3.1. Learning Objectives

On completion of this lesson you will be able to :

- grasp the need for virtual terminal protocol
- understand general principles of a virtual terminal protocol
- know two standards of virtual terminal protocol, namely TELNET and the ISO virtual terminal protocol (VTP) standard.

3.2. Introduction to Virtual Terminal Protocol

Most of our discussion has implicitly assumed that communication is between "peer" entities, that is, entities of roughly equal capabilities that wish to do roughly similar kinds of things. There are exceptions to this rule, and perhaps the most significant is the case of terminal-to-application communication.

Introduction to Virtual Terminal Protocol

In the case of a terminal directly connected to a computer, the computer will have an I/O driver that handles the terminal and a mechanism for communication between that driver and the application program. If the terminal and computer are connected via a network, the network must transparently pass the data between the terminal and a computer I/O port. This seems to be a requirement since a number of terminal devices do not have the capability of implementing the various OSI layers. Consider a network with N types of terminals and M types of host computers. For complete connectivity, each host type must contain a package for handling each terminal type. In the worst case MN I/O packages must be developed. This is practically impossible. To solve this problem, some sort of virtual terminal protocol (VTP) is needed.

VTP includes the following functions:

- Establishing and maintaining a connection between two application-level entities.
- Controlling a dialogue for negotiating the allowable actions to be performed across the connection.
- Creating and maintaining a data structure that represents the "state" of the terminal.
- Translating between actual terminal characteristics and a standardized representation.

The principal purpose of the VTP is to transform the characteristics of a real terminal into a standardized form or virtual terminal.

There are four classes of terminals:

- **Scroll mode**: These are terminals with no local intelligence, including keyboard-printer and keyboard-display devices. Characters are transmitted as they are entered, and incoming characters are printed or displayed as they come in. On a display, as the screen fills, the top line is scrolled off.
- **Page mode**: These are keyboard-display terminals with a cursor-addressable character matrix display. Either user or host can modify random-accessed portion of the display. I/O can be a page at a time.
- **Form/data entry mode**: These are similar to page mode terminals, but allow definition of fixed and variable fields on the display. This permits a number of features, such as transmitting only the variable part, and defining field attributes to be used as validity checks.
- **Graphics mode**: These allow the creation of arbitrary two-dimensional patterns.

There are basically four phases of operations.

For any VTP, there are basically four phases of operations;

- **Connection management**: includes session-layer-related functions, such as connection request and termination.
- **Negotiation**: used to determine a mutually agreeable set of characteristics between the two correspondents.
- **Control**: exchange of control information and commands.
- **Data**: transfer of data between two correspondents.

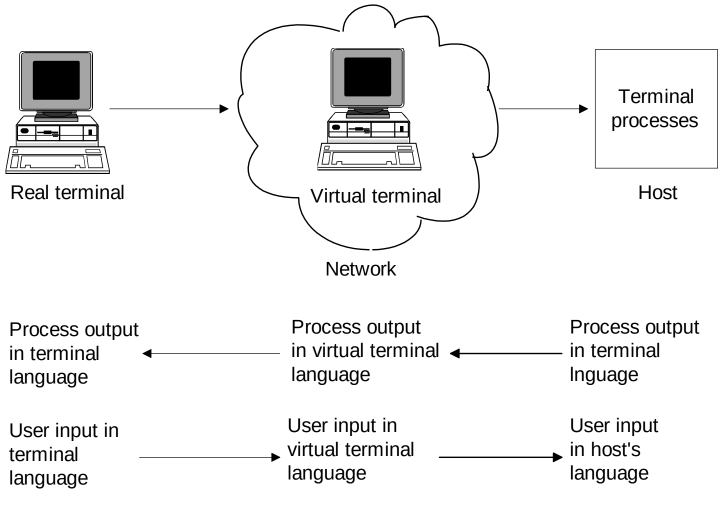

Real terminal
Virtual terminal
Network
Terminal processes
Host
Process output in terminal language
Process output in virtual terminal language
Process output in terminal lnguage
User input in terminal language
User input in virtual terminal language
User input in host's language

Fig. 12.5: Virtual Terminal mode.

Figure 12.5 illustrates the process involved. Upon user input, the characteristics of a real terminal are transformed into the agreed format, or “virtual terminal”. These formatted data are transmitted over a network to a host system. In the host computer, the virtual terminal structure is translated into the terminal format normally used by the host. The reverse process is performed for host-to-terminal traffic. Thus, a virtual terminal service must understand the virtual terminal format and be able to employ a data-transfer mechanism, such as that provided in the OSI architecture.

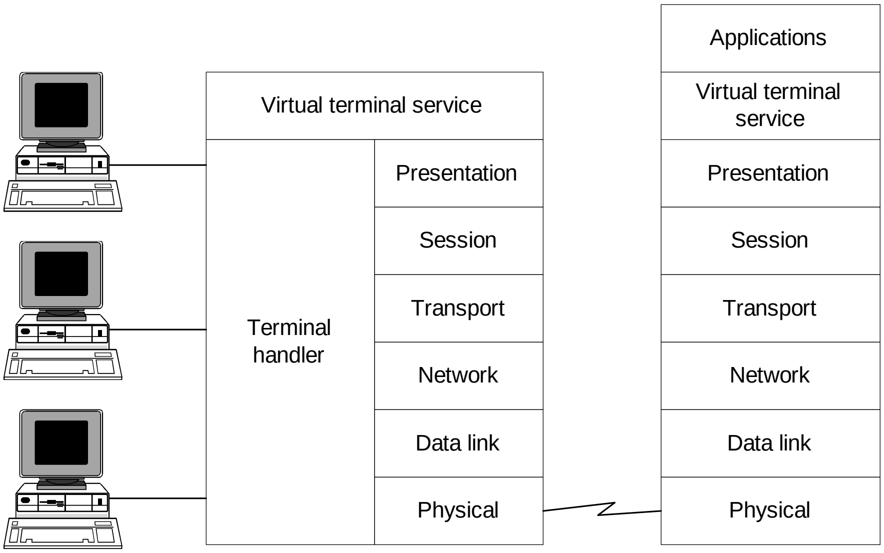


Fig. 12.6: Architecture for virtual terminal service.

Some terminal-handler software module is needed to communicate with the terminals; this is usually part of the operating system.

Figure 12.6 relates the virtual terminal service to the OSI architecture. Terminal are connected locally to a device that may be a terminal cluster controller, some other sort of communications processor, or a general-purpose computer. Some terminal-handler software module is needed to communicate with the terminals; this is usually part of the operating system. The purpose of this module is to link the terminal user to some application in the system. In this case, the user is linked to the virtual terminal service. This service is at the application layer of the OSI architecture and makes use of the lower six layers of OSI to establish a connection with a virtual terminal service module on a remote computer. On the remote computer, the virtual terminal service module provides an interface to various applications. To the application, terminal traffic coming in through the virtual terminal service appears to be coming from a local terminal through the usual terminal-handler software. Thus, for both the user and the application, it appears as though the user is locally connected to the remote computer.

3.3. TELNET

One of the first attempts to develop a true virtual terminal protocol is TELNET, which was developed as part of the TCP/IP protocol suite and is still widely used.

TELNET is built on three main principles:

- The concept of a network virtual terminal (NVT).
- A symmetric view of terminals and process.
- The principle of negotiated options.

The NVT is an imaginary device that provides an intermediate representation of a canonical terminal. If the communicating entity is a process, a module is needed (Server TELNET) to convert between the NVT representation and the process representation. If the communicating entity is a terminal, a module is needed (User TELNET) to map the characteristics of the terminal into those of NVT.

Communication can occur between two terminals, two processes, or a process and a terminal.

Communication can occur between two terminals, two processes, or a process and a terminal. It is expected that the communication will be over a TCP connection. TELNET enforces two-way alternate mode of communication to accommodate half-duplex terminals. TELNET assumes that the ASCII code will be used. Each TELNET connection begins with a negotiated option phase. Four commands are used in this phase: WILL, WONT, DO, DONT. WILL X is sent by either party to indicate that party's desire (offer) to begin performing option X; DO X and DONT X are positive and negative acknowledgments, respectively. DO X is sent to indicate a desire (request) that the other party begin performing option X; WILL X and WONT X are the positive and negative response.

In addition to the negotiation phase, there are other times when control information needs to be exchanged. This is achieved by the use of commands inserted into the data stream and preceded by an escape character.

3.4. The ISO Virtual Terminal Standard

The ISO virtual terminal service is an application-layer service defined within the framework of the OSI model. The standard defines a module for a virtual terminal, which is an abstract representation of a real terminal. The standard defines operations that can be performed, such as reading text from the virtual keyboard, writing text on the virtual screen, and moving a cursor to a particular position on the virtual screen. The standard also defines a virtual terminal protocol for the exchange of data and control messages between a terminal and an application via the virtual terminal service. The protocol standard specifies the display data stream structure and the control messages by which the two sides can agree on the details of the terminal capabilities to be supported.

Rather than defining a single virtual terminal for all possible applications, the standard provides its users with the tools to define a virtual terminal suited to the application at hand and the physical limitations of the terminal.

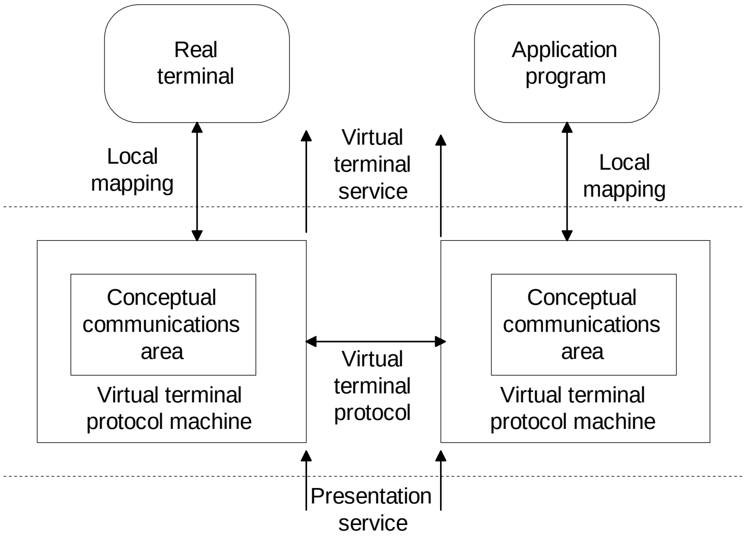

Real terminal
Application program
Local mapping
Virtual terminal service
Local mapping
Conceptual communications area
Virtual terminal protocol machine
Virtual terminal protocol
Conceptual communications area
Virtual terminal protocol machine
Presentation service

Fig. 12.7: The structure of the virtual terminal environment.

A virtual terminal is modeled as being made up of several parts.

The structure of the ISO standard is suggested by figure 12.7. A virtual terminal is modeled as being made up of several parts, all of which reside in the conceptual communication area, which is an abstraction used to model the interaction between two systems. A separate copy is maintained by each communicating entity, and it forms the basis for the protocol between the4 two sides. The Virtual Terminal Protocol is specified on terms of interactions between protocol entities in the two systems that affect the objects in the conceptual communications area. Each entity provides a Virtual Terminal Service to its user. The service user can be thought of as a local mapping from a real terminal or application to the virtual terminal context.

Classes of services: The ISO standard provides the following classes of service:

- Basic.
- Forms.
- Graphics.

Modes of operations: The virtual terminal standard supports two modes of operations:

- Two-way alternate (half-duplex).
- Two-way simultaneous (full-duplex).

Delivery control: Delivery control allows one side to control delivery of data to the other side to co-ordinate multiple actions. Normally, any data entered at a terminal are automatically delivered to the application on the other side as soon as possible, and any data transmitted by the application are delivered to the terminal as soon as possible.

Echo control: Echo control is concerned with the control of how characters typed on a keyboard will cause updates to display.

3.5. Exercise

3.5.1. Multiple choice question

a. The principal purpose of a virtual terminal protocol is

i) to transform characteristics of a real terminal into a virtual terminal.
ii) to transform characteristics of a real terminal into another real terminal.
iii) to transform characteristics of a virtual terminal into a real terminal.
iv) to transform characteristics of a virtual terminal into another virtual terminal.

3.5.2. Questions for short answer

a) Why is a virtual terminal protocol needed?
b) Briefly discuss the phases of operation of a virtual terminal protocol.
c) What is a network virtual terminal?
d) Name the classes of ISO VTP standard.
e) Name the modes of operation of ISO VTP standard.

3.5.3. Analytical questions

a) Discuss the functions of a virtual terminal protocol.
b) Discuss the different classes of terminals usually used.
c) Discuss the architecture for virtual terminal service.
d) Discuss TELNET protocol.
e) Discuss the ISO virtual terminal standard.

Unit 13 : Distributed Applications

Introduction

All of the protocols and functions are geared toward the support of distributed applications that involve the interaction of multiple independent systems. In the OSI model, such applications occupy the application layer and are directly supported by the presentation layer. In the TCP/IP protocol suite, such applications typically rely on TCP or UDP for support. In this unit, tree distributed applications supported by a network architecture are discussed.

Lesson 1 : Network Management: SNMPv2

1.1. Learning Objectives

On completion of this lesson you will be able to :

- understand the concept of network management systems
- introduce yourself to a widely used network management standard.

1.2. Network Management Systems

A large network cannot be put together and managed by human effort alone. The complexity of such a system dictates the use of automated network management tools. A network management system is a collection of tools for network monitoring and control.

A network management system consists of incremental hardware and software additions implemented among existing network components. The software used in accomplishing the network management tasks reside in the host computers and communications processors. A network management system is designed to view the entire network as a unified architecture, with addresses and labels assigned to each point and the specific attributes of such element and link known to the system. The active elements of the network provide regular feedback of status information to the network control center.

A network management system is a collection of tools for network monitoring and control.

A network management system consists of the following key elements:

- Management station, or manager.
- Agent.

- Management information base.
- Network management protocol.

The **management station** is typically a stand-alone device but may be a capacity implemented on a shared system. In either case, the management station serves as the interface for the human network manager into network management system. The management station will have:

- A set of management applications for data analysis, fault recovery, and so on.
- An interface by which the network manager may monitor and control the network.
- The capability of translating the network manager's requirements into the actual monitoring and control of remote elements in the network.
- A database of network management information extracted from the databases of all the managed entities in the network.

Agent is an active element in the network management system.

Agent is an active element in the network management system. Hosts, bridges, routers, and hubs may be equipped with agent software so that they may be managed from a management station. The agents responds to requests for information from a management station, responds to requests for actions from the management station, and may asynchronously provide the management station with important but unsolicited information.

The collection of objects is referred to as management information base (MIB).

The means by which resources in the network may be managed is to represent these resources as objects. Each object is a data variable that represents one aspect of the managed agent. The collection of objects is referred to as **management information base (MIB)**. The MIB functions as a collection of access points at the agent for the management station. A management station performs the monitoring function by retrieving the value of MIB objects.

The management station and agents are linked by a **network management protocol**. The protocol used for the management of TCP/IP networks is the simple network management protocol (SNMP). An enhanced version of SNMP, known as SNMPv2, is intended for both TCP/IP- and OSI-based networks. The protocol includes the following key capabilities:

- **Get**: enables the management stations to retrieve the value of objects at the agent.
- **Set**: enables the management station to set the value of objects at the agent.
- **Notify**: enables an agent to notify the management station of significant events.

1.3. Simple Network Management Protocol Version 2 (SNMPv2)

SNMP is a simple tool for network management. It defines a limited, easily implemented management information base (MIB) of scalar variables and two-dimensional tables, and it defines a streamlined protocol to enable a manager to get and set MIB variables and to enable an agent to issue unsolicited notifications, called traps. SNMPv2 is an enhanced version of SNMP.

The Elements of SNMPv2

SNMPv2 provides the infrastructure for network management.

SNMPv2 does not provide network management at all. SNMPv2 instead provides a framework on which network management applications can be built. SNMPv2 provides the infrastructure for network management. Figure 13.1 is an example of a configuration that illustrates that infrastructure.

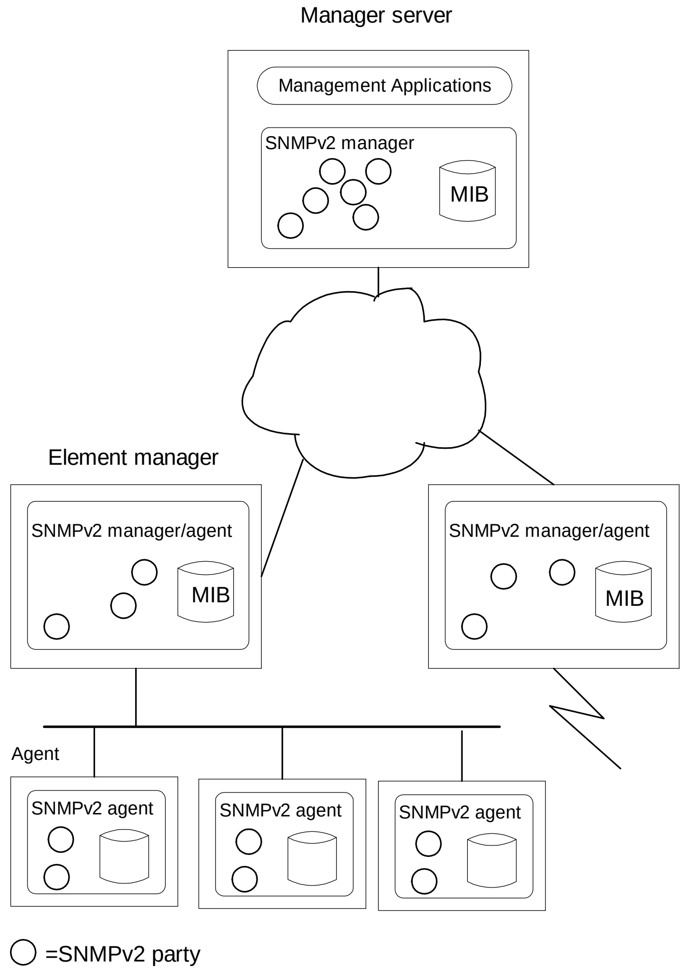


Fig. 13.1: SNMPv2-managed configuration.

The essence of SNMPv2 is a protocol that is used to exchange management information. Each "player" in the network management system maintains a local database of information relevant to network management, known as the management information base (MIB). The SNMPv2 standard defines the structure of this information and the allowable data types; this definition is known as the structure of management information (SMI). This is the language for defining management information. The standard also supplies a number of MIBs that are generally useful for network management. In addition, new MIBs may be defined by venders and users groups. At least one system in the configuration must be responsible for network management. There may be more than one of these management stations. Most other systems act in the role of agent. An agent collects information locally and stores it for later access by a manger.

The structure of management information (SMI).

SNMPv2 will support either highly centralized network management strategy or a distributed one. In the case of distributed network management, some systems operate both in the role of manager and of agent. All of information exchanges take place using the SNMPv2 protocol, which is a simple request/response type of protocol.

The actual exchange of information takes place between two parties. The use of parties allows systems to define access control and security policies that differ depending on the combination of manager, agent, and desired information. This gives the user considerable flexibility in setting up a network management system and assigning various levels of authorization to different persons.

1.4. Exercise

1.4.1. Multiple choice questions

a. The management station in a network management system is implemented on

i) s stand-alone system.
ii) s shared system.
iii) any one of (i) and (ii).
iv) none of (i) and (ii).

b. SNMPv2 is intended for

i) TCP/IP-based networks.
ii) OSI-based networks.
iii) both TCP/IP- and OSI-based networks.
iv) none of the above.

c. Which of the following is not correct

i) SNMPv2 provides all network management functions.
ii) SNMPv2 provides a framework on which network management applications can be built.
iii) SNMPv2 provides the infrastructure for network management.
iv) At least one system in the SNMPv2 configuration must be responsible for network management.

1.4.2. Questions for short answers

a) What is a network management system?
b) What are the key elements of a network management system?
c) What is a management station in a network management system?
d) What is an agent in a network management system?

1.4.3. Analytical question

a) Briefly discuss the elements of SNMPv2.

Lesson 2 : File Transfer: FTAM

2.1. Learning Objectives

On completion of this lesson you will be able to :

- learn the general principle of file transfer protocols
- have a general appreciation of the ISO file transfer standard FTAM.

2.2. Architecture

The purpose of a file transfer protocol (FTP) is to transfer a file or a portion of a file from one system to another, under command of an FTP user.

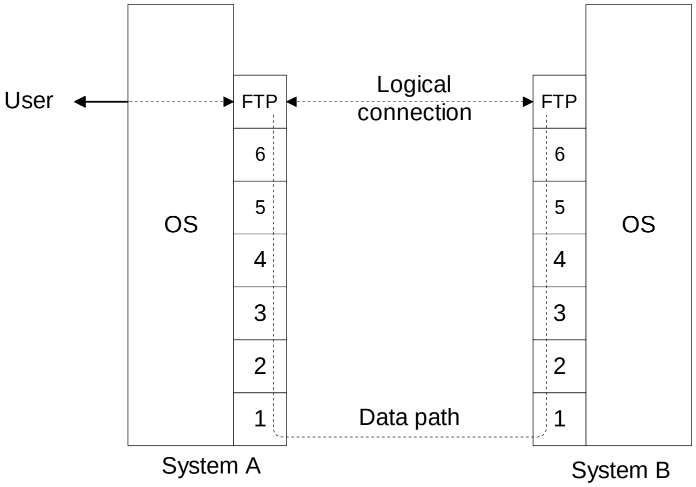


Fig. 13.2: Architecture context of a file transfer protocol.

A view of FTP as a application-level protocol.

Figure 13.2 shows a view of FTP as a application-level protocol. Here, FTP is viewed as the top layer of a seven-layer network architecture that is supported by the station's operating system. Typically, FTP is used interactively by an on-line user. The user's communications with FTP is mediated by the operating system, which contains I/O drivers. If the user on system A wishes access to a file on system B, then system A's FTP establishes a logical connection to system B's FTP. The actual path for control and user data is through the layers of the architecture.

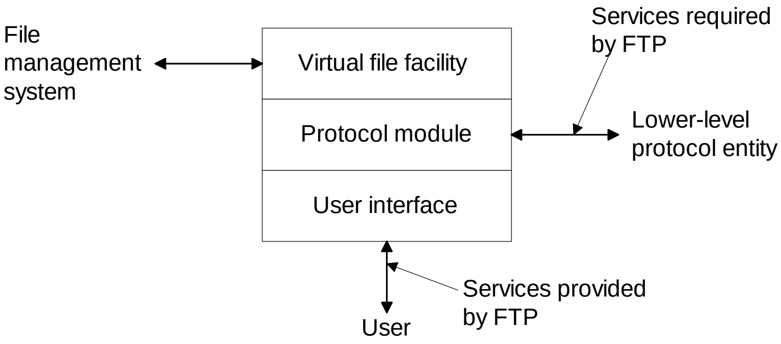


Fig. 13.3: Generic FTP structure.

The user connects to the local FTP in order to transfer all or part of a file. FTP must interact with three entities, as depicted in figure 13.3. First, there must be a user interface to accept request from an interactive user or, possibly, a program. Of course, this interaction only takes place at the requesting system. The remote FTP in a file transfer event does not interact with a user. Second, FTP must be able to communicate with other FTPs to achieve file transfer. Typically, this is done by interfacing to a lower-level protocol entity. Finally, to transfer a file, FTP must be able to get at the file. For this, an interface is needed to the local file management system.

A transformation is needed between the virtual file format and the local file format.

To avoid the problem of heterogeneous file structure, a general purpose virtual file structure is defined. Only virtual files are exchanged between FTPs. Locally, a transformation is needed between the virtual file format and the local file format. A virtual file consists of the following:

- A filename, that allows it to be referred unambiguously.
- Other descriptive attributes which express common properties of the file, such as size, accounting information, history, and so on.
- Attributes describing the logical structure and dimensions of the data stored in the file.
- Any data forming the contents of the file.

2.3. Characteristics

File transfer protocols can be characterized by the services they provide and the protocol mechanisms the employ.

Service Features

The following are the service features for file transfer protocols:

- **Access control**: There is some access control mechanism to protect the file system. A user must have an ID and password to gain access to the system at all. Then individual files may maintain access control lists with specific permissions (read, write) by user. The mechanism must be mediated by the FTP.
- **Processing mode**: The normal processing mode of a file transfer is immediate. That is, when the transfer is requested, FTP will endeavor to achieve the transfer right away and report back. If, however, the transfer is not urgent, the user could indicate that the transfer could take place in a background mode.
- **File naming**: A file naming facility is needed to identify the source and destination station and the source and destination file. A virtual file name would be used, to be translated locally by FTP.
- **Alternative operations**: The basic operation of FTP is to duplicate a file and send it to another system, where it is stored with a new local name. Alternative operations include: transfer of a portion of a file, copy a file only if an empty destination file already exists, and append a file to the contents of a destination file.
- **File management**: An FTP can mediate user access to certain file management facilities, either local or remote. The following three are found in most file transfer protocols: File allocation, file deletion, and listing file names in a directory.
- **Error recovery**: An error recovery facility would provide for recovery from errors or failure in the file system or operating system.
- **Flow control**: A simple stop-and-wait flow-control scheme is a useful addition to an FTP.
- **File structuring**: For handling heterogeneous file system, file structuring service is needed with an FTP.
- **Status reporting**: File transfer can be lengthy process, particularly if performed in background mode. Status report should be provided that indicate the start and completion of a transfer. The user should be able to interrogate FTP to determine the current status of any ongoing file transfer.

Protocol Features

The following are the features of a file transfer protocol:

- **Transmission of commands**: An FTP entity must communicate with a peer counterpart to coordinate and control the data transfer.
- **File attributes**: The source FTP must communicate file attributes to the recipient system.

- **Negotiation**: A flexible file transfer protocol is bound to have a number of options, for example, use of error recovery, flow control, buffer size, and so on. A process of negotiation is required for two FTP entities to agree on a common level of service.
- **Text formatting**: In text files, there will be certain control codes that affect the format of the text. A text formatting mechanism indicates which control code are in the file and how they are to be interpreted.
- **Security**: In addition to specific access control mechanisms that control access to files by identified users, file may be designated with a security label. FTP must cooperate with the file system's security mechanism to maintain security.
- **Statistics**: Statistics can be gathered by FTP to provide information to a central control authority and to provide the user with information to be used when allocating local resources.

2.4. The ISO FTAM Standard

The ISO file transfer, access, and management (FTAM) standard is quit complex and is organized into three parts:

- Virtual filestore definition.
- File service definition.
- File protocol specification.

Virtual Filestore Definition

The virtual filestore in FTAM is defined in terms of the structure of files, the attributes that can be assigned to files; and the allowable actions on files and file elements.

There are four aspects of the structure of a file:

Four aspects of the structure of a file.

- File access structure.
- Presentation structure.
- Transfer structure.
- Identification structure.

File attributes represent properties of the file itself.

Each file has associated with a number of properties, known as attributes. Two classes of attributes are defined: file attributes and activity attributes. File attributes represent properties of the file itself, independent of any FTAM action occurring over an ISO session connection. Three groups of file attributes are defined in FTAM. The kernel group is the minimum that must be supported; it provides the basic information needed for the act of file transfer.

The storage group defines concept related to the physical storage of files. It is concerned with the physical properties of the file, such as size, as well as information about accessors. The security group provides for file-related security information.

The other classes of attributes are activity attributes. These are relevant only to the file service session in progress. As with file attributes, activity attributes are divided into kernel, storage, and security groups. Some allowable actions are defined on complete file; these fall within the scope of file management. The other allowable actions are related to the access of individual file access data units within a file.

File Service Definition

The services provided by FTAM are defined as a set of primitives and parameters.

The file service definition defines the services available to users for accessing and manipulating the virtual files. The FTAM service and its supporting protocol are concerned with creating, in a series of stages, a working environment in which the user's desired activities can take place. The services provided by FTAM are defined as a set of primitives and parameters. There are eight groups and a total of 24 primitives defined in FTAM.

File Protocol Specification

The FTAM protocol provides a rather direct support of the FTAM service. By and large, there is a one-to-one mapping from service primitives to protocol data units. The FTAM protocol will set up a session connection and insert checkpoints in the flow of data.

2.5. Exercise

2.5.1. Multiple choice question

a. Which of the following is correct

i) Only physical files are exchanged between FTPs.
ii) Only virtual files are exchanged between FTPs.
iii) Physical or virtual file may be exchanged between FTPs.
iv) none of the above.

2.5.2. Questions for short answers

a) What is the purpose of a file transfer protocol?
b) Name the different components of a virtual file.

2.5.3. Analytical questions

a) Discuss the service feature for file transfer protocols.
b) Discuss the features of a file transfer protocol.
c) Discuss the ISO FTAM standards.

Lesson 3 : Electronic Mail: X.400

3.1. Learning Objectives

On completion of this lesson you will be able to :

- understand concepts of electronic mail
- learn basic ideas of an electronic mail standard known as CCITT X.4000 family of standard.

3.2. Single-System Electronic Mail

Electronic mail, also known as a computer-based message system (CBMS), is a facility that allows users at terminals to compose and exchange messages. Some electronic mail systems serve only users on a single computer and known as single-system electronic mail; others provide service across a network of computers and known as network electronic mail.

The mailbox is actually an entity maintained by the file management system, and is in the nature of a file directory.

The simplest form of electronic mail is the single-system facility. This facility allows all the users of a shared computer system to exchange messages. Each user is registered on the system and has a unique identifier. Associated with each user is a mailbox. The electronic mail facility is an application program available to any user logged on to the system. A user may invoke the electronic mail facility, prepare a message, and “send” it to any other user on the system. The act of sending simply involves putting the message in the recipient’s mailbox. The mailbox is actually an entity maintained by the file management system, and is in the nature of a file directory. On mailbox is associated with each user. Any “incoming” mail is simply stored as a file under that user’s mailbox directory. The user may later go and fetch that file to read the message. The user reads messages by invoking the mail facility and “reading”. In most systems, when the user logs on, he or she is informed if there is any new mail in that user’s mailbox.

A basic electronic mail system performs four functions;

- **Creation**: A user creates and edits a message.
- **Sending**: The user designates the recipient (or recipients) of the message, and the facility stores the message in the appropriate mailbox(es).
- **Reception**: The intended recipient may invoke the electronic mail facility to access and read the delivered mail.
- **Storage**: Both sender and recipient may choose to save the message in a file for more permanent storage.

3.3. Network Electronic Mail

With a single-system electronic mail facility, massages can only be exchanged among users of that particular system. In a distributed environment, we would like to be able to exchange messages with users attached to other systems. Thus, electronic mail is treated as an application-layer protocol that makes use of lower-layer protocols to transmit message.

Electronic mail is treated as an application-layer protocol that makes use of lower-layer protocols to transmit message.

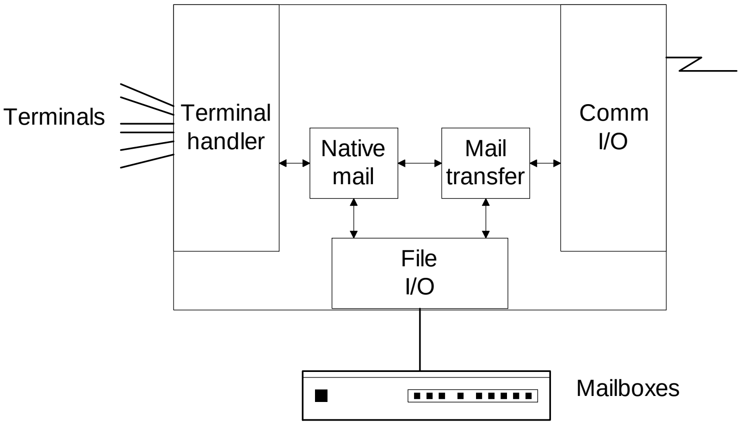


Fig. 13.4: Conceptual structure of electronic mail system.

Figure 13.4 suggests the internal system architecture required. Let us refer to a single-system mail facility as a **native mail** facility. For native mail, three major modules are needed. Users will interact with native mail via terminals; hence, terminal-handling software is needed. Mail is stored as files in the file system, so file-handling software is needed. Finally, there must be a native mail package that contains all the logic for providing mail-related services to users.

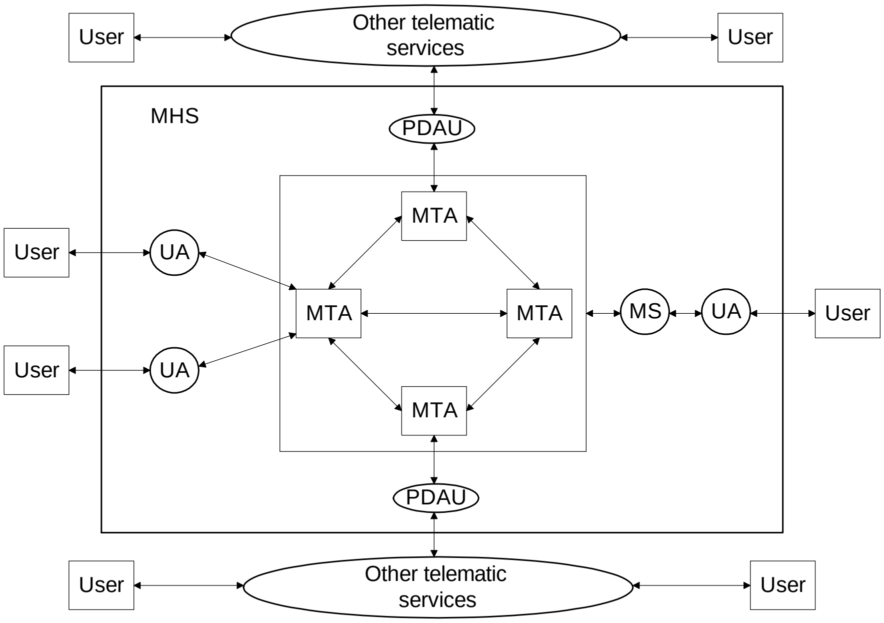
To extend this system to **network mail**, two more modules are needed. Since we are going to communicate across some sort of network or transmission system, communication I/O logic is needed; in the most general case, this would encompass layers 1 through 6 of the OSI model. Mail transfer logic is also needed, that knows how to invoke the communications functions, to specify the network address of the recipient, and to request whatever communication services are needed. If the user designates a local recipient, the message is stored in a local mailbox. If a remote recipient is designated, the native mail module passes the message to the mail transfer module for transmission across the network. Incoming mail from the network is routed to the appropriate mailbox.

3.4. The CCITT X.400 Family of Standard

The CCITT standards for Message Handling Systems (MHS) encompasses the requirements for network electronic mail. The standards do not deal with the user interface or the services available directly to the user. They specify services that are available for use in sending messages across the network and thus provide the base for building the user interface.

The X.400 family comprises of nine recommendations.

MHS Functional Model



MHS=Message handling system
MTS=Message transfer system
MTA=Message transfer agent
MS=Message store
UA=User agent
AU=Access unit
PDAU=Physical delivery access unit

Fig. 13.5: X.400 MHS functional model.

X.400 defines a functional model for the message handling system, as shown in figure 13.5.

The actual work of message transfer is done in the **message transfer system (MTS)**, which consists of an interconnected set of **message transfer agents (MTAs)**. The MTA accepts messages from a **user agent (UA)** for delivery to other UAs or to a **message store (MS)**. Some times the MTA that accepts submission of a message delivers it directly to the destination UA or MS. In other cases, it is necessary for the message to be relayed through a services of MTAs to the destination. For example, if only some MTAs have access to the proper long-distance communication paths, a message addressed to a distant UA might be relayed in several stages. Using relays also eliminates the need to have all UAs and MTAs available on a 24-hour basis.

The other elements of the message handling system are users of the MTS. The **user agent (UA)** operates on behalf of a user. The UA submits messages to an MTA for transmission across the network.

The **message store (MS)** has the following functionalities:

- One MS acts on behalf of one user.
- When a UA subscribes to an MS, all messages destined for the UA are delivered to the MS; when a message is delivered to an MS the role of the MTS in the transfer process is complete. Note that the MS does not store submitted messages, only delivered messages.
- It is possible to request an alert when a certain message arrives.
- Message submission from the UA to its MTA, via the MS, is transparent.
- Users are provided with general message retrieval, delete, and list.

Finally, various **access units (AUs)** allow MHS users to communicate with other message-based systems. The rules for coded information conversion are defined, making it possible to standardize the conversion of message contents for transfer of message between dissimilar systems.

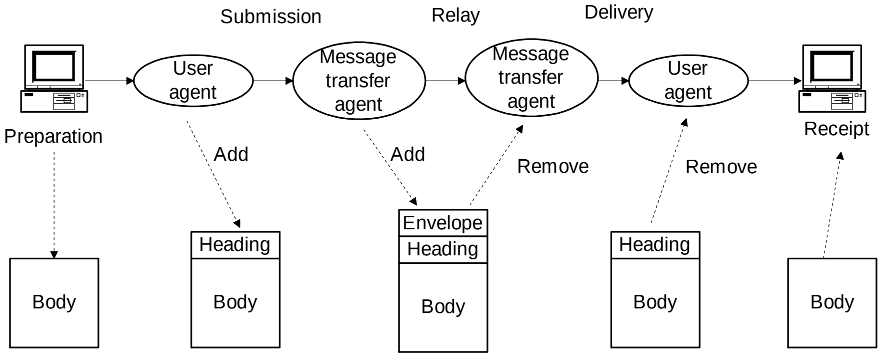


Fig. 13.6: X.400 message flow.

Figure 13.6 suggests the way in which messages are constructed and transmitted. The user prepares the **body** of a message outside of the scope of X.400, using some sort of word processor or editor. The user presents this body to the user agent software, together with a description, which might include recipient, subject, and priority. The user agent appends a **header** containing this qualifying information to the message, forming a complete message. This message is submitted to a message transfer agent. The MTA appends an **envelop** to the message; the envelop contains the source and destination address plus other control information needed for relaying the message through the network.

The X.400 Protocol Architecture

The message-handling protocols defined in the X.400 series are located in the application layer of the OSI model. X.400 family has the following protocols:

- Message transfer protocol (P1).
- Remote UA access protocol (P3).
- MS access protocol (P7).

The P1 protocol is used to transfer a message from the originator’s MTA to the recipients MTA through zero or more intermediate MTAs. The protocol is also used for transferring a notification of delivery or nondelivery back to the originator’s MTA.

Three types of protocol data units are defined: user, delivery report, and probe. The user PDU consists of the UA sublayer PDU plus a header, known as the **envelope**. The envelope contains the information needed for handling the message, including a network name for the recipient that will allow routing, a unique identifier, and information on how to process the PDU, such as the priority and whether a delivery report is required.

The delivery report includes a header that consists of a unique identifier, the name of the originator that submitted the message to which this report refers, and trace information, which indicates the route that the delivery report followed. The body of the delivery report PDU includes the identifier of the original user PDU plus information about the delivery.

The probe PDU is similar to the envelope portion of a user PDU. Its purpose is to determine if a particular delivery is possible without actually sending a user message. Delivery reports will be returned on probe PDUs.

X.400 Series

X.400 series are divided into two groups:

- Message transfer services.
- Interpersonal messaging service.

For both sets of services, the services are divided into three categories:

- Basic.
- Essential optional.
- Additional optional.

Basic services are inherent in the message handling system and must be implemented. Essential optional user facilities must be offered by the service provider, but it up to the user to select or not select the option. Additional optional user facility may or may not be offered by the provider.

Message Transfer Layer Services (X.401) include eight basic services, nine essential services, and six additional services. Interpersonal Messaging Services (X.401) include two basic services, four essential optional services, and fourteen essential/additional optional services.

3.5. Exercise

3.5.1. Multiple choice questions

a. In single-system electronic mail, a mailbox

i) is associated with each user.
ii) is associated with all users.
iii) any one of (i) and (ii).
iv) none of the above.

b. In X.400 MHS system, the MS stores

i) submitted messages.
ii) delivered messages.
iii) both of (i) and (ii).
iv) none of the above.

c. The following protocol is used in X.400 system to transfer a message from the originator's MTA to the recipient's MTA:

i) P1
ii) P3
iii) P7
iv) none of the above.

3.5.2. Questions for short answers

a) What is an electronic mail?
b) What are single-system and network electronic mail?
c) What is a mailbox?
d) Briefly state the functions performed by an electronic mail system.
e) What are native mail and network mail in an electronic mail system?
f) Name the different protocols of X.400 family.
g) How many protocol data units are defined in X.400 system? Name them.

3.5.3. Analytical questions

a) Differentiate between single-system electronic mail and network electronic mail.
b) Discuss the conceptual structure of electronic mail system.
c) Discuss the X.400 MHS functional mode.
d) Discuss how messages are constructed and transmitted in X.400 system.

COMPUTER NETWORKS

DCA 3303

COMPUTER NETWORKS

Computer network is
introduced in a self learning style
of distance education under Open university
system. The book covers detailed study of data
communications, different layers of computer
architecture, local area networks, widely used
standards in computer networks, and various
distributed applications. The book is suitable
for a self learner, for students, and
professionals.

SCHOOL OF SCIENCE AND TECHNOLOGY

BANGLADESH OPEN UNIVERSITY