XPRESS LEARNING
easy...fast...result-oriented

Data Communications and Computer Networks

- Overview of Data Communications and Networking
- Reference Models and Network Devices
- Analog and Digital Transmission
- Transmission Media
- Multiplexing and Switching
- Error Detection and Correction
- Flow and Error Control
- Media Access Control
- Ethernet, Virtual Circuit Networks and SONET
- Routing and Congestion Control
- Quality of Service and Protocols
- Internet Transport Protocols
- Application Layer Protocols
- Multimedia
- Network Security

ITL Education Solutions Limited

Data Communications and Computer Networks

This page is intentionally left blank.

Data Communications and Computer Networks

ITL Education Solutions Limited
Research and Development Wing
New Delhi

ISBN 9788131761274
eISBN 9788131776209

Head Office: A-8(A), Sector 62, Knowledge Boulevard, 7th Floor, NOIDA 201 309, India
Registered Office: 11 Local Shopping Centre, Panchsheel Park, New Delhi 110 017, India

Contents

Unit VI Application Layer

Unit VII Security

Preface

Data communications and computer networks are two aspects of a multifarious field that caters to both telecommunications and computing industries. Over the past 10 years, an enormous growth has been seen in this field. Nowadays, when we talk about communications and networking, we are not restricted to just traditional telephone networks or wired LANs such as Ethernet; rather, we have plentiful new developments including Wi-Fi, 2G and 3G mobile networks, Bluetooth, WAP and wireless local loops. Because of these technological advancements, the demand for the courses on data communications and computer networks has been continuously increasing. Keeping pace with this trend, almost all universities have integrated the study of data communications and computer networks in B.Tech. (CSE and IT), M.C.A. and M.B.A. courses. This book, *Data Communications and Computer Networks*, in its unique easy-to-understand question-and-answer format, directly addresses the need of students enrolled in these courses.

The questions and corresponding answers in this book have been designed and selected to cover all the necessary material in data communications and networking as per the syllabi of most universities. The text has been designed to make it particularly easy for students having little or even no background in data communications and networking to grasp the concepts. The students can use it as a textbook for one- or two-semester course while interested professionals can use it as a self-study guide. The organized and accessible format allows students to quickly find the questions on specific topic

This book is a part of series named *Express Learning Series* which has a number of books designed as quick reference guides.

Unique Features

1. This book is designed as a student-friendly and self-learning guide. In addition, it is written in a clear, concise and lucid manner.
2. It has been prepared in an easy-to-understand question-and-answer format.
3. The chapters of this book include previously asked as well as new questions.
4. The chapters cover various types of questions such as multiple choice, short and long questions.
5. Solutions to numerical questions asked in various examinations are provided in this book.
6. All ideas and concepts included in this book are presented with clear examples.
7. All concepts are well structured and supported with suitable illustrations.
8. To help readers, the inter-chapter dependencies are kept to a minimum.
9. A comprehensive index, which is set at the end of the book, will be useful for readers to access the desired topics quickly.

Chapter Organization

All questions and answers are organized into seven units with each unit consisting of one or more chapters. A brief description of these units is as follows:

- **Unit I: Introduction**
  This unit covers the introductory concepts of data communications and computer networks in two chapters. *Chapter 1* discusses the differences between communication and transmission, the components of data communications, the categories and applications of computer networks, network topologies, protocols and standards and the general idea of the Internet. *Chapter 2* introduces two standard networking models, which are open systems interconnection (OSI) and the Internet model (TCP/IP), along with a brief idea about the different layers of these models. It also describes various network devices such as switch, hub, bridge and gateway. This unit serves as a prelude to the rest of the book.

- **Unit II: Physical Layer**
  This unit focuses on the physical layer of reference models and consists of three chapters. *Chapter 3* deals with analog and digital transmissions. It describes various techniques to convert digital/analog data to analog or digital signals. *Chapter 4* spells out the characteristics of transmission media and various guided and unguided media such as twisted-pair cables, coaxial cables, fibre optic cables, radio waves, microwaves, infrared waves and satellite communication. *Chapter 5* discusses how the available bandwidth of a channel can be utilized efficiently using multiplexing and spreading. It also explains the concept of switching which is not only related to this layer but also to several layers. The use of two common public networks, telephone and cable TV networks, for data transfer is also covered in the chapter.

- **Unit III: Data Link Layer**
  This unit discusses, in detail, the data link layer of reference models and consists of four chapters. *Chapter 6* outlines various design issues and types of services provided by the data link layer. It also discusses how to detect and correct the errors that occur due to certain transmission impairments. *Chapter 7* spells out two main responsibilities of data link layer: flow control and error control. It first discusses the protocols needed to implement flow and error control and then the discussion moves on to bit-oriented protocols such as high-level data link control (HDLC) protocol and byte-oriented protocols such as point-to-point protocol (PPP). *Chapter 8* familiarizes the reader with a sub-layer of data link layer named media access control (MAC) layer that is responsible for resolving access to shared media. It discusses a number of multiple-access protocols such as ALOHA, CSMA, CSMA/CD, CSMA/CA, reservation, polling, token passing, FDMA, TDMA and CDMA that have been devised to control access to shared media. *Chapter 9* throws light on various IEEE 802 standards specified for wired and wireless LANs. It discusses, in detail, the Ethernet—a wired LAN, Bluetooth—a short-range wireless technology, X.25—a virtual circuit network, frame relay and asynchronous transfer mode (ATM)—switched WANs, and synchronous optical network (SONET)—a high-speed WAN that uses fibre-optic technolog .

- **Unit IV: Network Layer**
  This unit is all about the network layer of reference models and consists of two chapters. *Chapter 10* explores major design issues in switched data networks and Internet which are routing and congestion control. It includes discussion on IP addressing and various routing algorithms for

designing optimal routes through the network, so that the network can be used efficientl . It also describes what the congestion is, when it occurs, what its effects are and how it can be controlled. *Chapter 11* familiarizes the reader with the meaning of quality of service (QoS) of a network and the ways to help improve the QoS. It includes discussion on the major protocol defined at the network layer which is Internet protocol (IP). It also discusses other network layer protocols such as ARP and ICMP that assist IP to perform its function.

- **Unit V: Transport Layer**
  This unit comprises a single chapter detailing the transport layer of reference models. *Chapter 12* provides an overview of transport layer and explains the duties and services of this layer. It also discusses two transport layer protocols, which are user datagram protocol (UDP) and transmission control protocol (TCP).

- **Unit VI: Application Layer**
  This unit revolves around the application layer of reference models and consists of two chapters. *Chapter 13* describes a client/server application named domain name system (DNS) that is responsible for providing name services for other applications. It also expounds on three common applications in the Internet, which are TELNET, e-mail and file transfer protocol (FTP). The chapter concludes with a brief discussion on the famous World Wide Web (www), hypertext transfer protocol (HTTP), which is used to access the Web, and the network management protocol named as simple network management protocol (SNMP). *Chapter 14* details multimedia and some new protocols that have been developed to deal with specific problems related to multimedia in other layers.

- **Unit VII: Security**
  This unit consists of a single chapter that discusses, in detail, the security in the network. *Chapter 15* describes the importance of security in communications and networking. It discusses cryptography, different cryptographic algorithms, such as data encryption standard (DES), triple-DES and RSA, hash functions and digital signatures. It also discusses the role of firewall in the network and the means of user authentication and message authentication.

Acknowledgements

We would like to thank the publisher, Pearson Education, their editorial team and panel of reviewers for their valuable contributions towards content enrichment. We are indebted to the technical and editorial consultants for devoting their precious time to improve the quality of the book. In addition, we are grateful to the members of our research and development team who have put in their sincere efforts to bring out a high-quality book.

Feedback

For any suggestions and comments about this book, please send an e-mail to **itlesl@rediffmail.com**.

We hope that you will enjoy reading this book as much as we have enjoyed writing it.

Rohit Khurana
Founder and CEO
ITL ESL

This page is intentionally left blank.

1

Overview of Data Communications and Networking

1. What is the difference between communication and transmission?

Ans: Both communication and transmission deal with the exchange of information. However, a few differences between them are listed in Table 1.1.

Table 1.1 Differences Between Communication and Transmission

Communication	Transmission
• It refers to exchange of meaningful information between two communicating devices.	• It refers to the physical movement of information.
• It is a two-way scheme.	• It is a one-way scheme.

2. What is meant by data communication? What are the characteristics of an efficien data communication system?

Ans: Data communication refers to the exchange of data between two devices through some form of wired or wireless transmission medium. It includes the transfer of data, the method of transfer and the preservation of the data during the transfer process. To initiate data communication, the communicating devices should be a part of a data communication system that is formed by the collection of physical equipments (hardware) and programs (software). The characteristics of an efficient data communication system are as follows:

- **Reliable Delivery:** Data sent from a source across the communication system must be delivered only to the intended destination.
- **Accuracy:** Data must be delivered at the destination without any alteration. If the data is altered or changed during its transmission, it may become unusable.
- **Timely Delivery:** Data must be delivered in time without much time lags; otherwise, it may be useless for the receiver. As in case of video and audio transmissions, timely delivery means

delivering data at the same time it is produced, in the same order in which it is produced and also without any delay.

- **Jitter:** It refers to the differences in the delays experienced during the arrival of packets. It is uneven delay in the arrival time of audio or video data packets. These packets must be delivered at a constant rate; otherwise, the quality of the video will be poor.

3. What are the components of data communication system?

Ans: There are five basic components of a data communication system (Figure 1.1)

- **Message:** It refers to the information that is to be communicated. It can be in the form of text, numbers, images, audio or video.
- **Sender:** It refers to the device, such as a computer, video camera and workstation, which sends the message.
- **Receiver**: It refers to the device, such as a computer, video camera and workstation, for which the message is intended.
- **Transmission Medium:** It refers to the path which communicates the message from sender to receiver. It can be wired such as twisted-pair cable and coaxial cable or wireless such as satellite.
- **Protocol:** It refers to a set of rules (agreed upon by the sender and the receiver) that coordinates the exchange of information. Both sender and receiver should follow the same protocol to communicate with each other. Without the protocol, the sender and the receiver cannot communicate. For example, consider two persons; one of which speaks only English while another speaks only Hindi. Now, these persons can communicate with each other only if they use a translator (protocol) that converts the messages in English to Hindi and vice versa.

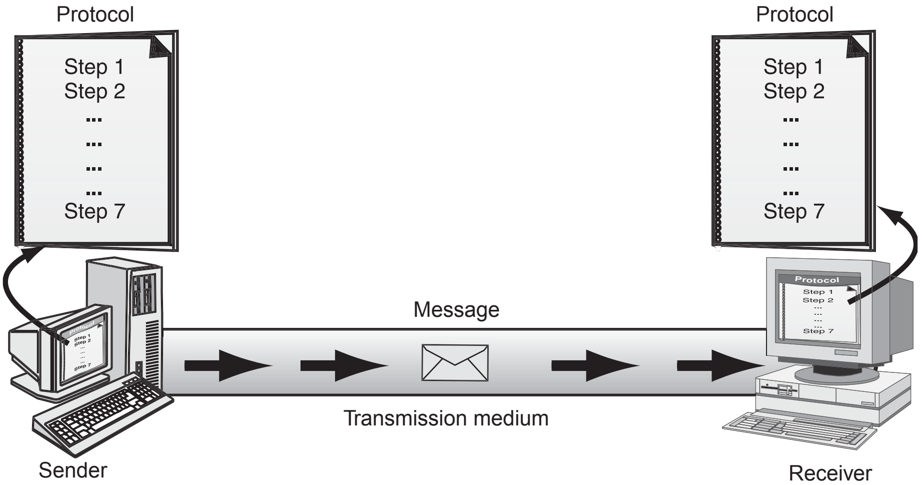


Figure 1.1 Components of a Data Communication System

4. What are the different forms of data representation? Explain in detail any two coding schemes used for data representation.

Ans: Data can be available in various forms such as text, numbers, images, audio and video. In networking, data has to be transmitted from source to destination in binary form. Thus, information such as alphabets (a–z, A–Z), numbers (0, 1, 2, …, 9), special symbols (!, @, #, $ etc.) and images (in the form of pixels/picture elements) has to be converted into sequences of bits, that is, 0 and 1. Audio and video data have to be converted from analog to digital signal for transmission with the help of different encoding schemes (explained in Chapter 03). There are various coding schemes including Unicode, ASCII and EBCDIC which are used these days to represent the data. Here, we discuss only ASCII and EBCDIC.

American Standard Code for Information Interchange (ASCII)

The standard binary code for the alphanumeric characters is ASCII. This code was originally designed as a seven-bit code. In addition, ASCII is often used with a parity bit which is the eighth bit. This bit is used at the most significant bit (MSB) position and is used for detecting errors during transmission. ASCII is commonly used in the transmission of data through data communication and is used almost exclusively to represent the data internally in the microcomputers.

In ASCII, uppercase letters are assigned codes beginning with hexadecimal value 41 and continuing sequentially through hexadecimal value 5A and lowercase letters are assigned hexadecimal values of 61 through 7A. The decimal values 1–9 are assigned the zone code 011 in ASCII. Table 1.2 of ASCII-7 coding chart shows uppercase and lowercase alphabetic characters, numeric digits 0–9 and special characters. The standard ASCII-7 code defines 128 character codes (0–127), of which, the first 32 are control codes (non-printable) and other are printable characters.

Table 1.2 ASCII-7 Coding Chart

Alphabetic characters							
Uppercase				Lowercase			
	ASCII-7 code				ASCII-7 code		
	In binary		In hexadecimal		In binary		In hexadecimal
Prints as	Zone	Digit		Prints as	Zone	Digit	
A	100	0001	41	a	110	0001	61
B	100	0010	42	b	110	0010	62
C	100	0011	43	c	110	0011	63
D	100	0100	44	d	110	0100	64
E	100	0101	45	e	110	0101	65
F	100	0110	46	f	110	0110	66
G	100	0111	47	g	110	0111	67
H	100	1000	48	h	110	1000	68
I	100	1001	49	i	110	1001	69
J	100	1010	4A	j	110	1010	6A
K	100	1011	4B	k	110	1011	6B
L	100	1100	4C	l	110	1100	6C
M	100	1101	4D	m	110	1101	6D

(*Continued*)

Table 1.2 ASCII-7 Coding Chart–(*Continued*)

Alphabetic characters							
Uppercase				Lowercase			
	ASCII-7 code				ASCII-7 code		
	In binary		In		In binary		In
Prints as	Zone	Digit	hexadecimal	Prints as	Zone	Digit	hexadecimal
N	100	1110	4E	n	110	1110	6E
O	100	1111	4F	o	110	1111	6F
P	101	0000	50	p	111	0000	70
Q	101	0001	51	q	111	0001	71
R	101	0010	52	r	111	0010	72
S	101	0011	53	s	111	0011	73
T	101	0100	54	t	111	0100	74
U	101	0101	55	u	111	0101	75
V	101	0110	56	v	111	0110	76
W	101	0111	57	w	111	0111	77
X	101	1000	58	x	111	1000	78
Y	101	1001	59	y	111	1001	79
Z	101	1010	5A	z	111	1010	7A
Numeric characters							
0	011	0000	30	5	011	0101	35
1	011	0001	31	6	011	0110	36
2	011	0010	32	7	011	0111	37
3	011	0011	33	8	011	1000	38
4	011	0100	34	9	011	1001	39
Special characters							
SPACE	010	0000	20	:	011	1010	3A
!	010	0001	21	;	011	1011	3B
“	010	0010	22	<	011	1100	3C
#	010	0011	23	=	011	1101	3D
$	010	0100	24	>	011	1110	3E
%	010	0101	25	?	011	1111	3F
&	010	0110	26	[	101	1011	5B
‘	010	0111	27	\	101	1100	5C
(	010	1000	28	]	101	1101	5D
)	010	1001	29	^	101	1110	5E
*	010	1010	2A	—	101	1111	5F
+	010	1011	2B	`	110	0000	60

(*Continued*)

Table 1.2 ASCII-7 Coding Chart–(*Continued*)

Alphabetic characters							
Uppercase				Lowercase			
	ASCII-7 code				ASCII-7 code		
	In binary		In		In binary		In
Prints as	Zone	Digit	hexadecimal	Prints as	Zone	Digit	hexadecimal
’	010	1100	2C	{	111	1011	7B
-	010	1101	2D	|	111	1100	7C
.	010	1110	2E	}	111	1101	7D
/	010	1111	2F	∼	111	1110	7E
@	100	0000	40	□	111	1111	7F

Extended Binary Coded Decimal Interchange Code (EBCDIC)

EBCDIC uses eight bits for each character; therefore, it is possible to represent 256 different characters or bit combinations (Table 1.3). This provides a unique code for each decimal value from 0 to 9 (for a total of 10), each uppercase and lowercase letters (for a total of 52), and for a variety of special characters. Since it is an eight-bit code, each group of the eight bits makes up one alphabetic, numeric, or special character and is called a **byte**.

In EBCDIC, the bit pattern 1100 is the zone combination (zone and digit) used for the alphabetic characters A through I, 1101 is used for the characters J through R and 1110 is the zone combination used for characters S through Z. The bit pattern 1111 is the zone combination used when representing decimal digits. Other zone combinations are used when forming special characters.

The concepts and advantages of ASCII are identical to those of EBCDIC. The important difference between EBCDIC and ASCII coding systems lies in the eight-bit combinations assigned to represent the various alphabetic, numeric and special characters. While using ASCII eight-bit code, we notice that the selection of bit patterns used in the positions differs from those used in EBCDIC.

Table 1.3 EBCDIC Coding Chart

Alphabetic characters							
Uppercase				Lowercase			
	EBCDIC				EBCDIC		
	In binary		In		In binary		In
Prints as	Zone	Digit	hexadecimal	Prints as	Zone	Digit	hexadecimal
A	1100	0001	C1	a	1000	0001	81
B	1100	0010	C2	b	1000	0010	82
C	1100	0011	C3	c	1000	0011	83
D	1100	0100	C4	d	1000	0100	84
E	1100	0101	C5	e	1000	0101	85

(*Continued*)

Table 1.3 EBCDIC Coding Chart–(*Continued*)

Alphabetic characters							
Uppercase				Lowercase			
	EBCDIC				EBCDIC		
	In binary		In		In binary		In
Prints as	Zone	Digit	hexadecimal	Prints as	Zone	Digit	hexadecimal
F	1100	0110	C6	f	1000	0110	86
G	1100	0111	C7	g	1000	0111	87
H	1100	1000	C8	h	1000	1000	88
I	1100	1001	C9	i	1000	1001	89
J	1101	0001	D1	j	1001	0001	91
K	1101	0010	D2	k	1001	0010	92
L	1101	0011	D3	l	1001	0011	93
M	1101	0100	D4	m	1001	0100	94
N	1101	0101	D5	n	1001	0101	95
O	1101	0110	D6	o	1001	0110	96
P	1101	0111	D7	p	1001	0111	97
Q	1101	1000	D8	q	1001	1000	98
R	1101	1001	D9	r	1001	1001	99
S	1110	0010	E2	s	1010	0010	A2
T	1110	0011	D3	t	1010	0011	A3
U	1110	0100	E4	u	1010	0100	A4
V	1110	0101	E5	v	1010	0101	A5
W	1110	0110	E6	w	1010	0110	A6
X	1110	0111	E7	x	1010	0111	A7
Y	1110	1000	E8	y	1010	1000	A8
Z	1110	1001	E9	z	1010	1001	A9
Numeric characters							
0	1111	0000	F0	5	1111	0101	F5
1	1111	0001	F1	6	1111	0110	F6
2	1111	0010	F2	7	1111	0111	F7
3	1111	0011	F3	8	1111	1000	F8
4	1111	0100	F4	9	1111	1001	F9

5. Explain different modes of data transmission between two devices.

Ans: There are three types of transmission modes: *simplex*, *half-duplex* and *full-duplex* (Figure 1.2).

- **Simplex:** This mode of transmission is unidirectional. The information flows in one direction across the circuit, with no capability to support response in the other direction. Only one of the communicating devices transmits information; however, the other can only receive it. Television

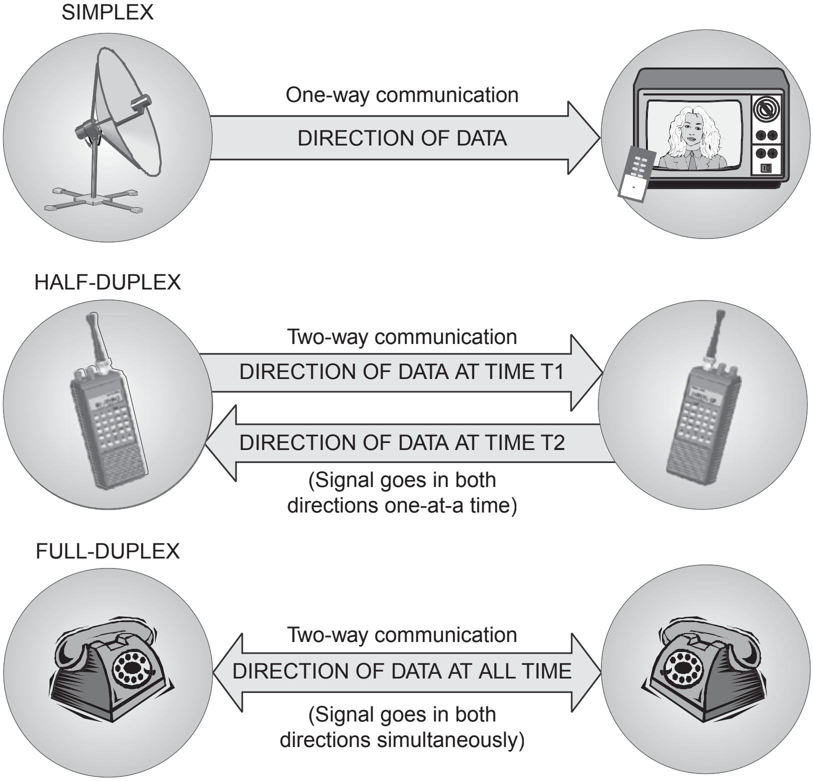

SIMPLEX
One-way communication
DIRECTION OF DATA
HALF-DUPLEX
Two-way communication
DIRECTION OF DATA AT TIME T1
DIRECTION OF DATA AT TIME T2
(Signal goes in both directions one-at-a time)
FULL-DUPLEX
Two-way communication
DIRECTION OF DATA AT ALL TIME
(Signal goes in both directions simultaneously)

Figure 1.2 Data Transmission Modes

transmission can be considered as an example of simplex mode of transmission where the satellite only transmits the data to the television, vice versa is not possible.

- ❑ **Half-Duplex:** In this transmission mode, each communicating device can receive and transmit information, but not at the same time. When one device is sending, the other can only receive at that point of time. In half-duplex transmission mode, the entire capacity of the transmission medium is taken over by the device, which is transmitting at that moment. Radio wireless set is an example of half-duplex transmission mode where one party speaks and the other party listens.
- ❑ **Full-Duplex:** This transmission mode allows both the communicating devices to transmit and receive data simultaneously. A full-duplex mode can be compared to a two-way road with traffic flowing in both directions. A standard voice telephone call is a full-duplex call because both parties can talk at the same time and be heard.

6. Defin computer network. What are the different criteria that a network should meet?

Ans: A **computer network** refers to a collection of two or more computers (nodes) which are connected together to share information and resources. Nodes are connected if they are capable of exchanging information with each other. To be able to provide effective communication, a network must meet a certain number of criteria, some of which are as follows:

- ❑ **Performance:** Performance of a network can be determined by considering some factors such as *transit time*, *response time*, *throughput* and *delay*. The amount of time taken by a message to travel from one device to another is known as **transit time** and the time elapsed between the user initiates a request and the system starts responding to this request is called the **response time**. The amount of work done in a unit of time is known as **throughput**. To achieve greater performance, we need to improve throughput and reduce the transit time, response time and delay. However, increasing the throughput by sending more data to the network often leads to traffic congestion in the network and thus, increases the delay. Some other factors that affect the performance of a network are the type of transmission medium, the total number of users connected to the network and the efficiency of connected hardware and software.

- **Reliability:** An efficient network must be reliable and robust. Reliability of a network is determined by the factors such as how frequently the failure is occurring and how much time is being spent in recovering from a link failure.
- **Security:** A network must also provide security by protecting important data from damage and unauthorized access. In addition, there must be procedures and policies to handle theft and recovery of data.

7. What are the various advantages of a computer network?

Ans: Today, computer networks are being used in every facet of life, as they provide the following advantages.

- **Sharing Information:** This is one of the most important advantages of a computer network. In the absence of a network, transferring information from one computer to another requires the use of a compact disk, floppy disk, printer, etc. However, if the communicating systems are geographically apart, sharing information becomes even harder. Computer networks solve this problem, as computers connected to a network can share information as if they are in the same building even when they are located geographically apart. For example, when we connect to the Internet and open a website on our computer, we can access information that is not stored in our own computers. In such a networked system, all information is stored on a central and powerful computer known as a **server**. All other computers in the network can easily access information from the server as if it was located on their own computer.
- **Sharing Hardware Resources:** A network facilitates sharing of hardware resources in an effective and user-friendly manner. When computers are connected to a network, they can share peripherals such as printer and hard disk drives, with any other computer. For example, in an office having five to ten computers and one printer, in the absence of network, only the computer that is connected to the printer can be used to print data. If others have to access the printer, then they would first need to transfer their data over to the computer connected to the printer. Contrastive to this, in a networked environment, the printer can be shared on the network and every computer on the network can easily access the printer without having the need to transfer data.
- **Sharing Software Resources:** Software resources are the programs or applications that are used by computers to perform any useful function or to carry out daily basis task. In an environment where networking is not available, users will have to install and configure any applications that they need individually. However, if the computers are connected via a network, the required software or application can be installed and configured centrally on a server and shared by all. This saves the valuable time and disk space.
- **Preserve Information:** In addition to sharing information, a networked environment helps to preserve information as well. It is difficult to maintain regular backups of data on a number of standalone computers and without backup, important data can be lost in case of some accident or failure

of computer. However, in a networked environment, a copy of the important data can be kept on the server as well as on other connected computers on the network. In this case, failure of one computer will not result in loss of information, as the data can still be accessed from other computers whenever required.

- **Communication:** Computer networks have revolutionized the way people communicate. Rather than exchanging memos and directives on paper, which involves a lot of printing costs and delays, network users can instantly send messages to others and even check whether or not their messages have been received.

8. What are the various applications of a computer network?

Ans: Nowadays, computer networks have become an essential part of industry, entertainment world, business as well as our daily lives. Some of the applications of a computer network in different fields are as follows:

- **Business Applications:** There is a need of effective resource sharing in companies for the exchange of ideas. This can be achieved by connecting a number of computers with each other. It allows transferring of business information effectively without using paper. For example, an employee of one department can access the required information about another department using network.
- **Marketing and Sales:** Marketing firms utilize networks for conducting surveys to gather and analyze data from the customers. This helps them to understand the requirements of a customer and use this information in the development of the product. Sales professionals can use various applications such as online shopping, teleshopping and online reservation for airlines, hotel rooms etc. in order to increase the revenue of their organization.
- **Financial Services:** Computer networks play a major role in providing financial services to people across the globe. For example, the financial application such as electronic fund transfer helps the user to transfer money without going into a bank. Some other financial applications that are entirely dependent on the use of networks include ATM, foreign exchange and investment services, credit history searches and many more.
- **Directory and Information Services:** Directory services permit a large number of files to be stored a central location thereby speeding up the worldwide search operations. Information services of Internet such as bulletin boards and data banks provide a vast amount of information to the users within seconds.
- **Manufacturing:** Computer networks are widely being used in manufacturing. For example, the applications such as computer-aided design (CAD) and computer-assisted manufacturing (CAM) use network services to help design and manufacture the products.
- **E-mail Services:** This is one of the most widely used applications of network. With the help of computer networks, one can send e-mails across the world within a few seconds and without using paper.
- **Mobile Applications:** With the help of mobile applications such as cellular phones and wireless phones, people wishing to communicate are not bound by the limitation of being connected by fixed physical connections. Cellular networks allow people to communicate with each other even while travelling across large distances.
- **Conferencing:** With the help of networking, conferencing (teleconferencing or videoconferencing) can be conducted that allows remotely located participants to communicate with each other as if they are present in the same room.

9. Discuss two types of computer network architectures.

Ans: The **computer network architecture** specifies how the physical and logical components of a computer network are assembled and connected with each other to facilitate information exchange and resource sharing. The two major types of network architectures are *client/server* and *peer-to-peer* architectures.

Client/Server Architecture

In this architecture, each computer is either a client or a server. To complete a particular task, there exists a centralized powerful host computer known as **server** and a user's individual workstation known as **client** (Figure 1.3). The client requests for services (file sharing, resource sharing etc.) from the server and the server responds by providing that service. The servers provide access to resources, while the clients have access to the resources available only on the servers. In addition, no clients can communicate directly with each other in this architecture. A typical example of client/server architecture is accessing a website (server) from home with the help of a browser (client). When a client makes a request for an object to the server, then the server responds by sending the object to the client. In addition, it must be noticed that two browsers accessing the same website, never communicate with each other.

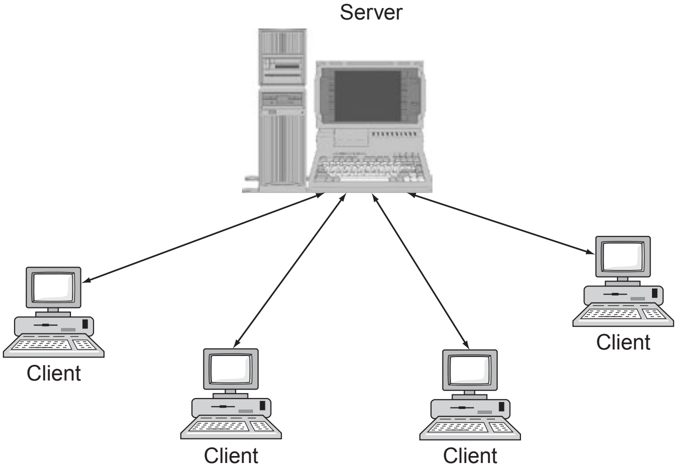


Figure 1.3 Client/Server Architecture

An advantage of client/server architecture is that the IP address of the server is always fixed and the server is always available on the network for clients. However, the disadvantage of this architecture is that with time as the number of clients starts to increase, the number of requests to the server also increases rapidly. In this scenario, we might need more than one server to serve larger number of requests.

Peer-to-Peer (P2P) Architecture

This architecture does not rely on dedicated servers for communication; instead, it uses direct connections between clients (**peers**) (Figure 1.4). A pure P2P architecture does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. That is, every node is able to initiate or complete any supported transaction (file transfer) with the other connected node and every node can directly communicate with anothe .

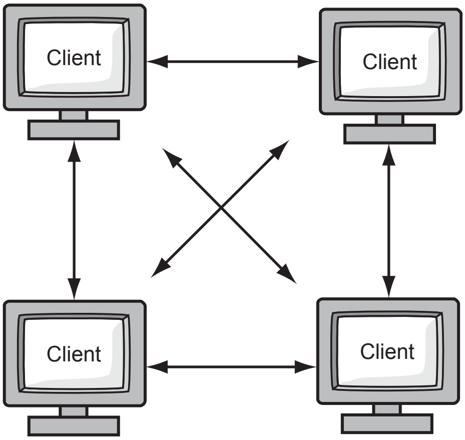


Figure 1.4 Point-to-Point Architecture

The upper limit of the number of nodes that can function as both clients and servers on a P2P network is between 10 and 25. If there are more nodes, then a P2P machine can be used as a dedicated server with additional high-performance hardware. An advantage of P2P architecture is that it is very scalable, that is, millions of nodes can be connected to the network to contribute to resources irrespective of the differences in their local configuration, processing speed, network and storage capacity. However, the highly decentralized approach of P2P architecture can be tough to manage. For example, during file sharing with other remote clients, the only client having a specific file might log off from the network. Examples of P2P networks are file-sharing applications such as Morpheus and Kaaza

10. Differentiate between P2P and client/server architecture.

Ans: Both P2P and client/server networks have associated advantages and disadvantages. These advantages and disadvantages form a part of distinction between the two. These differences are listed in Table 1.4.

Table 1.4 Differences Between P2P Architecture and Client/Server Architecture

Basis	P2P architecture	Client/server architecture
Centralized	There is no central repository for files and applications in this architecture.	Resources and data security are controlled through the server.
Maintenance	It incurs low maintenance cost.	A large network requires extra staff to ensure efficient operation.
Installation	It can be easily installed.	It requires experts for proper installation of the network.
Cost	It does not require a dedicated server; thus, it is not much expensive.	It is expensive, as it requires a dedicated server.
Security	Lack of proper security policies is the biggest drawback.	It provides high level of security.
Dependence	All nodes are independent of each other. Failure occurring in one node does not affect the functioning of other nodes in the network.	When server goes down, it affects functioning of the entire network.

11. Distinguish between point-to-point and multipoint connections? Give suitable diagrams.

Ans: In order to communicate with each other, two or more devices must be connected using a link. A **link** is a physical path using which data can be transferred between two or more devices. The two possible types of connections between two or more devices are *point-to-point* and *multipoint connections*.

- ❑ **Point-to-Point:** In a point-to-point connection, there is a dedicated link between the communicating devices (Figure 1.5). The link is totally reserved for transmission specifically for those two devices. Most point-to-point connections are established with cable or wire though satellite or microwave links are also possible. For example, operating any device such as television using a remote control establishes a point-to-point connection between the device and the remote control.

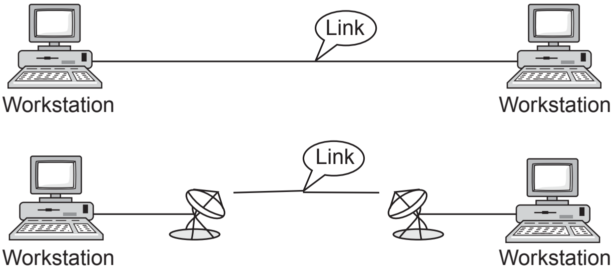


Figure 1.5 Point-to-Point Connection

- ❑ **Multipoint:** In a multipoint (**multidrop**) connection, a single link is shared between two or more devices, that is, there is no dedicated link between the communicating devices (Figure 1.6). If the shared link can be utilized by many devices simultaneously, it is known as a **spatially shared connection** whereas if devices need to take turns to utilize the link, it is known as a **timeshared connection**.

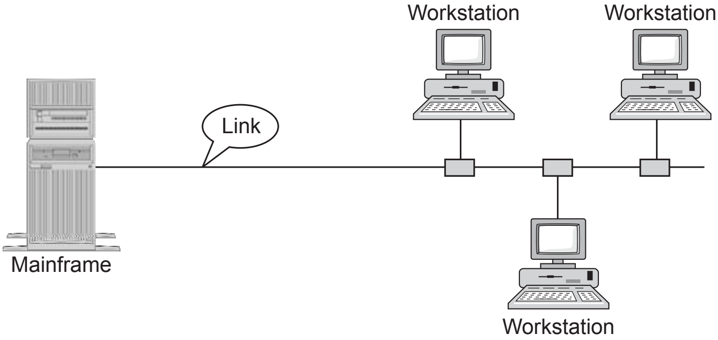


Figure 1.6 Multipoint Connection

12. What do you understand by the term network topology?

Ans: The term **topology** refers to the way a network is laid out, either physically or logically. A topology can be considered as the network's shape. It is the geometric representation of the relationship of all the links. There are five basic topologies: bus, ring, sta , tree and mesh.

13. Discuss bus and mesh topology. Compare them.

Ans: Bus and mesh topology are detailed as under.

Bus Topology

Bus topology uses a common bus or backbone (a single cable) to connect all devices with terminators at both ends. The backbone acts as a shared communication medium and each node (file server, workstations and peripherals) is attached to it with an interface connector. Whenever a message is to be transmitted on the network, it is passed back and forth along the cable, past the stations (computers) and between the two terminators, from one end of the network to the other. As the message passes each station, the station checks the message's destination address. If the address in the message matches the station's address, the station receives the message. If the addresses do not match, the bus carries the message to the next station and so on. Figure 1.7 illustrates how devices such as file servers, workstations and printers are connected to the linear cable or the backbone.

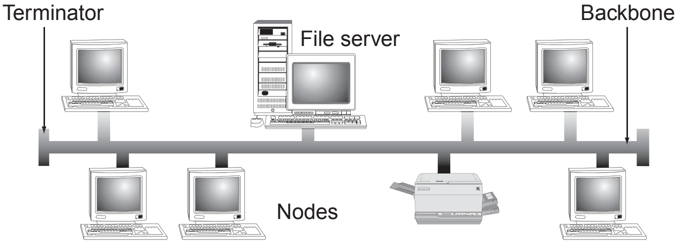


Figure 1.7 Bus Topology

Mesh Topology

In a mesh topology, every node has a dedicated point-to-point link to every other node (Figure 1.8). Messages sent on a mesh network can take any of several possible paths from source to destination. A fully connected mesh network has $n(n - 1)/2$ physical links to link n devices. For example, if an organization has five nodes and wants to implement a mesh topology, then 5(5−1)/2, that is, 10 links are required. In addition, to accommodate those links, every device on the network must have $n - 1$ communication (input/output) ports.

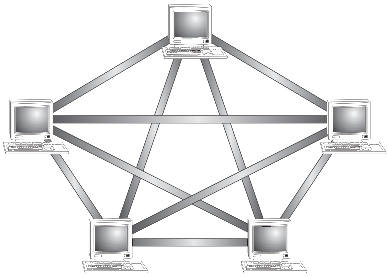


Figure 1.8 Mesh Topology

A comparison of bus topology and mesh topology is given in Table 1.5.

Table 1.5 Comparison of Bus and Mesh Topology

Bus topology	Mesh topology
• It uses a single cable to connect all devices with terminators at both ends.	• It has a dedicated point-to-point link to every other node.
• It requires least amount of cabling.	• It requires more amount of cabling.
• It incurs less cost.	• It is expensive.

(*Continued*)

Table 1.5 Continued

Bus topology	Mesh topology
• Entire network shuts down if there is failure in backbone (cable).	• If one link becomes unusable, it does not disable entire system.
• It is easy to install and reconfigure.	• It is difficult to install and reconfigure.
• An example of this topology is cable TV network.	• An example of this topology is mobile ad hoc network (MANet).

14. **Explain ring, star and tree topologies along with their advantages and disadvantages.**

Ans: The ring, star and tree topology are detailed as under.

Ring Topology

In this topology, computers are placed on a circle of cable without any terminated ends since there are no unconnected ends (Figure 1.9). Every node has exactly two neighbours for communication purposes. All messages travel through a ring in the same direction (clockwise or counterclockwise) until it reaches its destination. Each node in the ring incorporates a repeater. When a node receives a signal intended for another device, its repeater regenerates the bits and passes them along the wire.

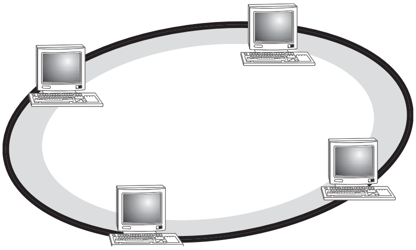


Figure 1.9 Ring Topology

The advantages of ring topology are as follows:

- ❑ It is easy to install and reconfigure
- ❑ Every computer is given equal access to the ring. Hence, no single computer can monopolize the network.

The disadvantages of ring topology are as follows:

- ❑ Failure in any cable or node breaks the loop and can take down the entire network.
- ❑ Maximum ring length and number of nodes are limited.

Star Topology

In this topology, devices are not directly linked to each other; however, they are connected via a centralized network component known as **hub** or **concentrator** (Figure 1.10). The hub acts as a central controller and if a node wants to send data to another node, it boosts up the message and sends the message to the intended node. This topology commonly uses twisted-pair cable; however, coaxial cable or fibre-optic cable can also be used

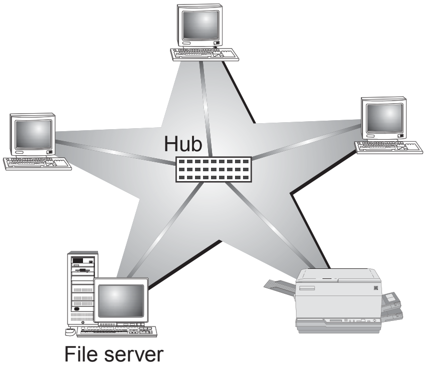


Figure 1.10 Star Topology

The advantages of star topology are as follows:

- It is easy to install and wire.
- The network is not disrupted even if a node fails or is removed from the network.
- Fault detection and removal of faulty parts are easier in star topology.

The disadvantages of star topology are as follows:

- It requires a longer length of cable.
- If the hub fails, nodes attached to it are disabled.
- The cost of the hub makes the network expensive when compared to bus and ring topologies.

Tree Topology

A tree topology combines characteristics of linear bus and star topologies (Figure 1.11). It consists of groups of star-configured workstations connected to a bus backbone cable. Not every node plugs directly to the cen-

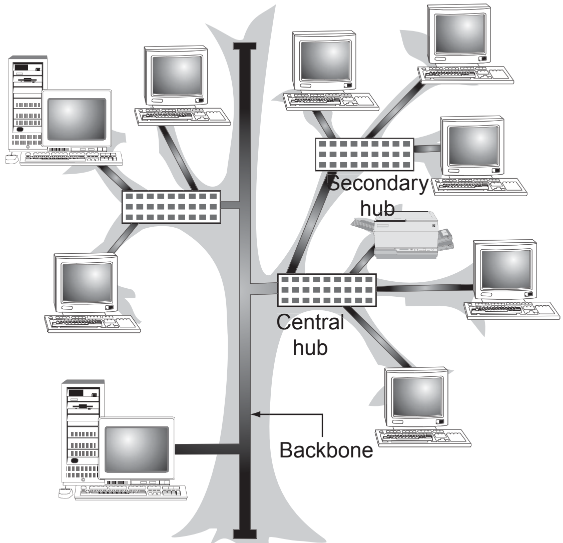


Figure 1.11 Tree Topology

tral hub. The majority of nodes connect to a secondary hub that, in turn, is connected to the central hub. Each secondary hub in this topology functions as the originating point of a branch to which other nodes connect. A tree topology is best suited when the network is widely spread and partitioned into many branches.

The advantages of tree topology are as follows:

- The distance a signal can travel increases, as the signal passes through a chain of hubs.
- It allows isolating and prioritizing communications from different nodes.
- It allows for easy expansion of an existing network, which enables organizations to configure a network to meet their needs.

The disadvantages of tree topology are as follows:

- If the backbone line breaks, the entire segment goes down.
- It is more difficult to configure and wire than other topologie

15. What are the different categories of a network?

Ans: There are no generally accepted criteria to classify the computer networks; however, two dimensions are considered more important, which are scale and transmission technology. On the basis of scale, computer networks can be classified into three types: local area network (LAN), metropolitan area network (MAN) and wide area network (WAN). On the basis of transmission technology, computer networks can be categorized as point-to-point networks and broadcast networks.

16. Explain the categories of networks based on scale.

Ans: A network can be as few as several personal computers on a small network or as large as the Internet, a worldwide network of computers. Today, when talking about networks, we are generally referring to three primary categories: LAN, MAN, and WAN.

Local Area Network

A LAN is a computer network that covers only a small geographical area (usually within a square mile or less) such as an office, home or building (Figure 1.12). In a LAN, connected computers have a network operating system installed onto them. One computer is designated as the **fil server**, which stores all the software that controls the network. It also stores the software that can be shared by the computers attached to the network. Other computers connected to the file server are called **workstations**. The workstations can be less powerful than the file server and they may have additional software on their hard drives. On most LANs, cables are used to connect the computers. Generally, LAN offers a bandwidth of 10–100 Mbps.

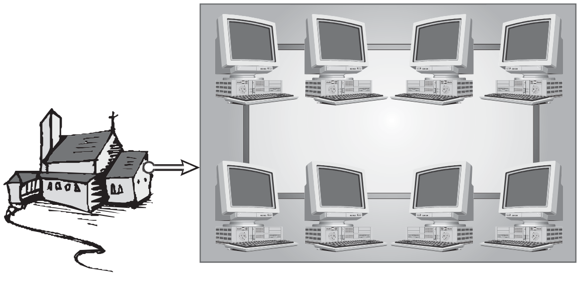


Figure 1.12 Local Area Network

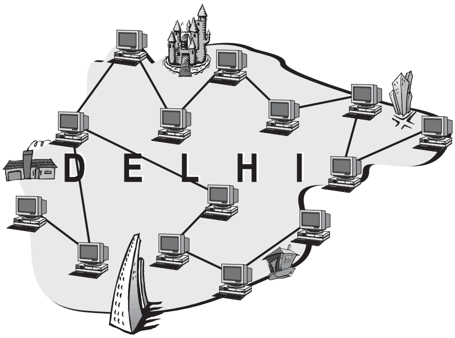


Figure 1.13 Metropolitan Area Network

Metropolitan Area Network

A MAN is a network of computers spread over a "metropolitan" area such as a city and its suburbs (Figure 1.13). As the name suggests, this sort of network is usually reserved for metropolitan areas where the city bridges its LANs with a series of backbones, making one large network for the entire city. It may be a single network such as a cable television network or it may be a means of connecting a number of LANs. Note that MAN may be operated by one organization (a corporate with several offices in one city) or be shared and used by several o ganizations in the same city.

Wide Area Network

A WAN is a system of interconnecting many computers over a large geographical area such as cities, states, countries or even the whole world (Figure 1.14). These kinds of networks use telephone lines, satellite links and other long-range communication technologies to connect. Such networks are designed to serve an area of hundreds or thousands of miles such as public and private packet switching networks and national telephone networks. For example, a company with offices in New Delhi, Chennai, and Mumbai may connect the LANs for each of those locations to each other through a WAN. Although a WAN may be owned or rented by private business, it is usually a public network designed to connect small and intermediate sized networks together. The largest WAN in existence is the Internet.

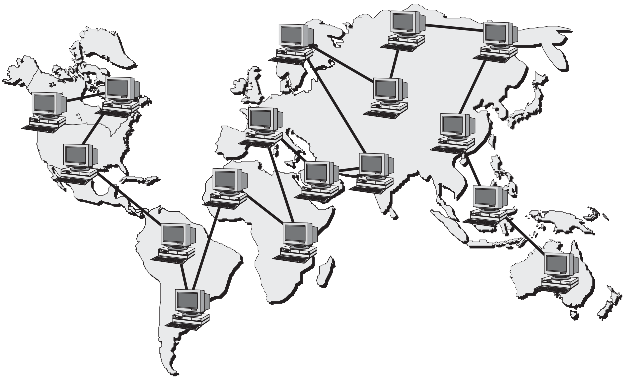


Figure 1.14 Wide Area Network

WAN offers many advantages to business organizations. Some of them are as follows:

- It offers flexibility of location because not all the people using the same data have to work at the same site.
- Communication between branch offices can be improved using e-mail and file sharin
- It facilitates a centralized company wide data backup system.
- Companies located in a number of small and interrelated offices can store files centrally and access each other's information.

17. What are the two types of transmission technology available?

Ans: The two types of transmission technology that are available include broadcast networks and point-to-point networks.

In **broadcast networks**, a single communication channel is shared by all the machines of that network. When a short message, let us say a packet is sent by any machine, it is received by all the other machines on that network. This packet contains an address field which stores the address of the intended recipient. Once a machine receives a packet, it checks the address field. If the address mentioned in the address field of packet is matched with the address of the recipient machine, it is processed; otherwise, the packet is ignored. In broadcast systems, there is a special code in the address field of the packet which is intended for all the destinations. When a packet with this code is transmitted, it is supposed to be received and processed by all the machines on that network. This mode of operation is called **broadcasting**. Some of the networks also support transmission to a subset of machines what is called **multicasting**.

In **point-to-point networks**, there could be various intermediate machines (such as switching devices called **nodes**) between the pair of end points called **stations**. Thus, there could be various possible routes of different lengths for a packet to travel from the source to the destination. Various routing algorithms are considered and finall , one of them is chosen for the packets to travel from the source to the destination.

Generally, for small geographically localized network (such as LAN), broadcasting is considered favourable while larger networks (such as WAN) use point-to-point networks. If there is specifically one sender and one receiver in any point-to-point network, it is sometimes considered as **unicasting**.

18. Defin Internet and write a brief history on Internet.

Ans: The word **Internet** is derived from two words**: Interconnection** and **Networks**. Also known as "the Net", Internet is a worldwide system of computer networks, that is, a network of networks, which allows the participants (users) to share information. It consists of thousands of separately administered networks of various sizes and types. Each of these networks comprises tens of thousands of computers. Moreover, the total number of users of the Internet is known to be in millions. This high level of connectivity encourages an unparalleled degree of communication, resource sharing and information access.

The foundation of Internet was laid in 1969 by the Department of Defense (DOD) of United States of America. They wanted to create a computer network that could continue to function in the event of a disaster, such as a nuclear war. Even if a part of the network was damaged or destroyed, the rest of the system would continue to work. That network was known as **ARPANET (Advanced Research Projects Agency Network),** which linked US scientific and academic researchers. It was the forerunner of today's Internet. Later in 1980, another agency, the National Science Foundation (NSF) created a new network of computers based on ARPANET, called **NSFNET**, which turned out to be more efficient and capable. Initially, NSFNET was designed to link five super computers situated at the major universities of NSF and allowed only academic research. Over the time, this network expanded to include sites for business, universities, government etc. and finally becoming a network consisting of millions of computers, now known as the Internet. Now, it is probably the most powerful and important technological advancement since the introduction of the desktop computer. With the advancement of Internet, the quality, quantity and variety of information also grew. Today, the Internet is a repository of every type of information. Nowadays, an Internet user can get all sorts of information ranging from how to add to the design of a functional spaceship to how to choose a product for personal use.

19. Defin protocol. Describe the key elements of protocols.

Ans: **Protocol** refers to a set of rules that coordinates the exchange of information between the sender and receiver. It determines what is to be communicated, and how and when it is to be communicated. Both sender and receiver should follow the same protocol to communicate data. Without the protocol, the sender and receiver cannot communicate with each other. The main elements of a protocol are as follows:

- **Syntax:** It refers to the format of the data that is to be transmitted.
- **Semantics:** It refers to the meaning and interpretation of each bit of data.
- **Timing:** It defines when the data should be sent and with what speed

20. What do you understand by the standards? Explain briefl .

Ans: Standards are crucial for establishing an open and worldwide marketplace for the manufacturers, vendors, suppliers, government agencies and other service providers to provide them worldwide interconnectivity. **Standards** define some common set of rules and guidelines which ensure universal interoperability of data and communication technology and processes. The standards for data communication are classified into two categories, which are *de facto* and *de jure* standards.

- **De facto:** This is a Latin word which means "from the fact" or "by convention". This category includes standards that have not been approved formally by some authority but have been accepted as standards because of their widespread use. For instance, the UNIX operating system has largely been used in computer science departments of most universities and thus has been adopted as the standard. Similarly, many manufacturers prefer to copy IBM machines while developing PCs for small office and home computers and thus, IBM PCs are the *de facto* standard. The *de facto* standards are usually founded by the manufacturers in an attempt to specify the functionality of some new technology or product.
- **De jure:** This is also a Latin word which means "by law" or "by regulation". Unlike *de facto* standards, the *de jure* standards are formally declared as legal standards by recognized standardization authorities. The international standardization authorities governing *de jure* standards may be established by treaty among governments of different nations or may comprise volunteers from different standard organizations without nay treaty.

21. Write short notes on intranet and extranet.

Ans:

- **Intranet:** This is a private network that is set up within an organization and also controlled by the organization; nobody outside the organization is permitted to access the network. Intranet utilizes the same protocols as used for accessing the Internet through a web browser. The users of intranet can access the basic services of the Internet such as e-mail. The difference between an intranet and the Internet is that an intranet user can view only those websites that are owned and maintained by the organization hosting the intranet. On the other hand, an Internet user may visit any website without any permission.

- **Extranet:** This is an extended intranet owned, operated and controlled by an organization. In addition to allow access to members of an organization, an extranet uses firewalls, access profiles and privacy protocols to allow access to users from outside the organization. In essence, an extranet is a private network that uses Internet protocols and public networks to securely share resources with customers, suppliers, vendors, partners or other businesses.

22. Represent the message 5A.dat in ASCII code. Assume parity bit position (eighth bit) as 0.

Ans: Using the ASCII coding chart shown in Table 1.2, 5A.dat will be coded as shown here.

Bit positions	7	6	5	4	3	2	1	0
5	0	0	1	1	0	1	0	1
A	0	1	0	0	0	0	0	1
.	0	0	1	0	1	1	1	0
d	0	1	1	0	0	1	0	0
a	0	1	1	0	0	0	0	1
t	0	1	1	1	0	1	0	0

23. Represent HelLO34 in EBCDIC code.

Ans: Using the EBCDIC coding chart shown in Table 1.3, HelLO34 will be coded as shown here.

Bit positions	7	6	5	4	3	2	1	0
H	1	1	0	0	1	0	0	0
e	1	0	0	0	0	1	0	1
l	1	0	0	1	0	0	1	1
L	1	1	0	1	0	0	1	1
O	1	1	0	1	0	1	1	0
3	1	1	1	1	0	0	1	1
4	1	1	1	1	0	1	0	0

24. What is hybrid topology?

(a) Draw a hybrid topology with a star backbone and three bus networks.
(b) Draw a hybrid topology with a star backbone and four ring networks.

Ans: Hybrid topology is the combination of two or more topologies such that the resultant network does not retain the characteristics of any of the basic topologies including star, bus, ring and tree. A hybrid topology is created when two different basic topologies are connected.

(a) A hybrid topology with star backbone and three bus networks is shown in Figure 1.15.

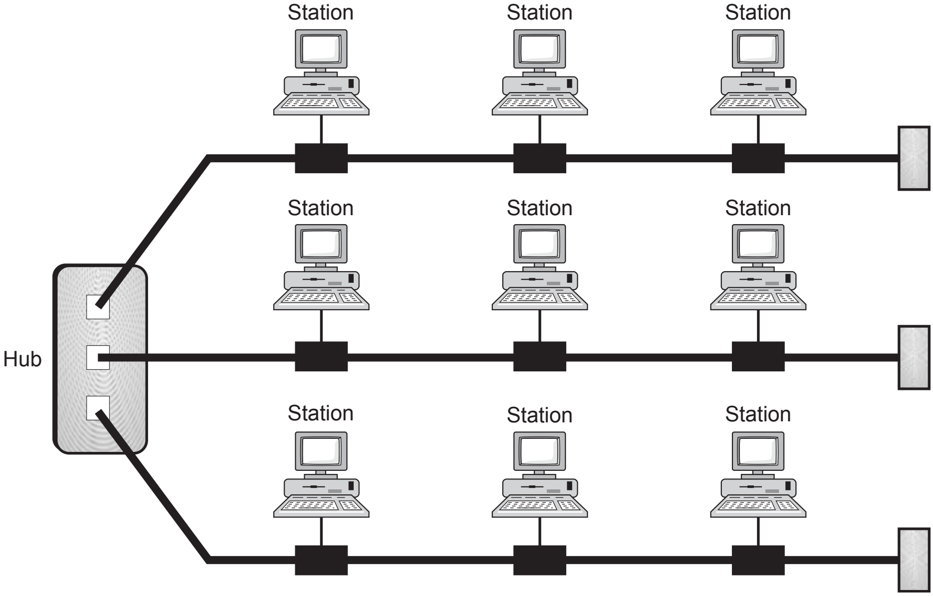


Figure 1.15 Hybrid Topology with a Star Backbone and Three Bus Networks

(b) A hybrid topology with star backbone and four ring topologies is shown in Figure 1.16.

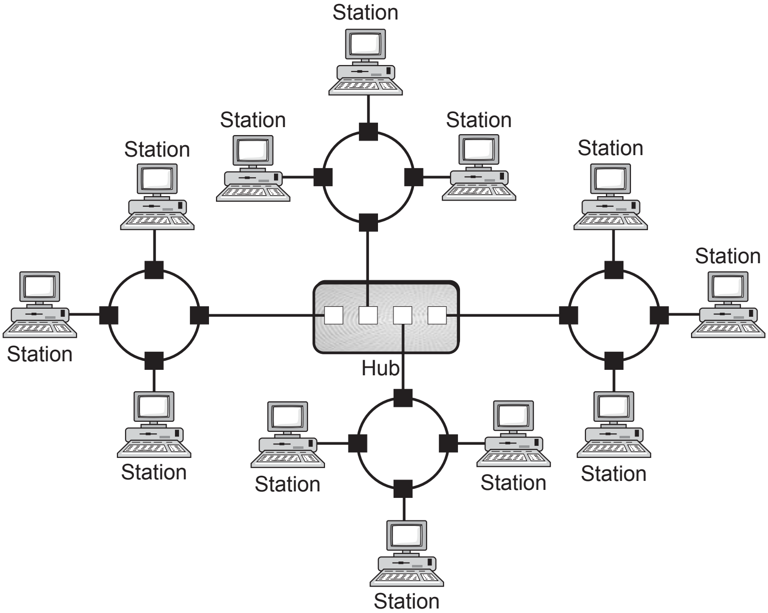


Figure 1.16 Hybrid Topology with a Star Backbone and Four Ring Networks

25. Assume a network with *n* devices. Calculate how many links are required to set up this network with mesh, ring, bus and star topologies?

Ans: The number of links required to set up this network with the various topologies are listed in Table 1.6.

Table 1.6 Topology along with Number of Links

Topology	Number of links
Mesh	$(n(n-1))/2$
Ring	n
Bus	(n drop lines + one line for bus)
Star	n

Multiple Choice Questions

1. Which of these is the part of a data communication system?
   (a) Sender (b) Message
   (c) Protocol (d) All of these

2. ASCII stands for
   (a) American standard code for information identificatio
   (b) American standard code for information interchange
   (c) American standard coding for information interchange
   (d) American standard coding for information identificatio

3. EBCDIC uses __________ bits for each character.
   (a) Six (b) Seven
   (c) Eight (d) Two

4. In _______ transmission mode, the flow of information is bidirectional at the same time.
   (a) Half-duplex (b) Simplex
   (c) Full-duplex (d) None of these

5. The amount of time taken by a message to travel from one device to another is known as
   (a) Delay
   (b) Response time
   (c) Transit time
   (d) Throughput

6. In star topology, devices are connected via a centralized network component known as
   (a) Node (b) Client
   (c) Bus (d) Hub

7. The network topology which uses hierarchy of nodes is
   (a) Ring (b) Tree
   (c) Bus (d) Fully connected

8. A MAN is ___________ in size as compared to a LAN.
   (a) Larger (b) Smaller
   (c) Equal (d) None of these

9. Internet is a
   (a) LAN (b) WAN
   (c) MAN (d) Both LAN and MAN

10. Which of these is not the key element of a protocol?
    (a) Syntax (b) Standard
    (c) Semantics (d) Timing

Answers

1. (d) 2. (b) 3. (c) 4. (c) 5. (c) 6. (d) 7. (b) 8. (a) 9. (b) 10. (b)

2

Reference Models and Network Devices

1. What is meant by a reference model? Why do we need it?

Ans: A **reference model** is a conceptual layout that describes how communication between devices should occur. For efficient communication, the reference model identifies the tasks involved in inter-computer communication and divides them in logical groups called **layers**, with each layer performing a specific function. A communication system designed in such a manner is referred to as **layered architecture**. We need a reference model, as it provides various advantages, some of which are as follows:

- It permits different types of network software and hardware to communicate with each other.
- It defines standards for building network components thereby permitting multiple-vendor development.
- It defines which functions should be performed at each layer of the model thereby promoting the standardization of network.
- It divides the overall communication function into simpler and smaller components thus, helps in component development and reducing trouble shooting.

2. What are the advantages of layering in a network?

Ans: The main aim behind building a layered architecture is to reduce the design complexity of a computer network. Other advantages of layering in a computer network are as follows:

- Layering can resolve complicated tasks by breaking it into smaller and manageable pieces.
- Each layer can be analyzed and tested independently.
- By layering, the functionalities are carried out in logical sequential manner.
- Implementation of layers can be changed without disturbing other layers, as the details of all the layers are hidden from each other.
- Layering allows reuse in a way that once a common functionality is implemented in a lower layer, the upper layers can share it.

3. Why standardization of network architecture is important?

Ans: Due to the advantages of layered architecture, many network vendors and suppliers used the concept of layered architecture for designing most computer systems, but the set of protocols and interfaces defined by each vendor were not same. In addition, the partition of layers defined by each vendor was alike. All this resulted into the integration incompatibility of different architectures defined by different vendors. Thus, to allow different vendor's network architectures to interoperate, the need for standardization of network architecture was felt. The standardization of architecture also tends to reduce the effort required to develop interfaces for the networking of different architectures.

4. What is Open Systems Interconnection (OSI) reference model? What are the principles used in defining the OSI layers

Ans: OSI is a standard reference model for communication between end users in a network. By the term open system, we mean a set of protocols using which a system can communicate with any other system irrespective of the differences in their underlying hardware and software. In 1983, International Organization for Standardization (ISO) published a document called 'The Basic Reference Model for Open Systems Interconnection', which visualizes network protocols as a seven-layered model. The OSI model consists of seven separate but related layers, namely, *physical*, *data link*, *network*, *transport*, *session*, *presentation* and *application* layers as shown in Figure 2.1.

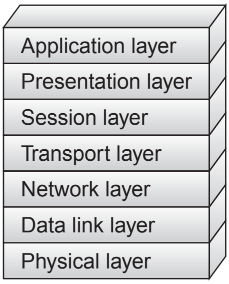


Figure 2.1 Layers in the OSI Model

With in a single machine, a layer in OSI model communicates with two other OSI layers. It services to the layer that is located directly above it while uses the services offered by the layer that is located directly below it. For example, the data link layer provides services to the network layer while calls upon the services of the physical layer. In contrast, during communication between two machines, each layer on source machine communicates with the corresponding layer (called the **peer layer**) on the destination machine using a set of protocols that are appropriate for the layer.

In 1983**, Day and Zimmermann** laid down certain principles which were used in defining the OSI layers. These principles are as follows:

- ❑ Each layer should perform a well-defined function
- ❑ The functionality of each layer should be defined keeping in mind the internationally standardized protocols.
- ❑ Changes made in any layer should not affect the other layers.
- ❑ The numbers of layers should be more enough, so that each layer is associated with distinct functions.
- ❑ A different layer should be made when the abstraction level changes.

5. Explain how data flows between the layers in OSI model

Ans: When data is sent from one machine to another, it travels down sequentially from layer to layer on the source machine and as it reaches the destination machine, it moves up through the layers. While the data passes through layers on source machine, each layer adds header (and sometimes, trailer which is usually added at data link layer) to it and passes the whole unit to the layer directly below it. The header attached at each layer contains control information such as sequence numbers and size of data.

Figure 2.2 shows the data flow in OSI model during communication between two processes on machines A and B. Initially, the application layer (layer 7) of machine A adds an application header (AH) to the data and passes the package to the presentation layer (layer 6), which further adds its own

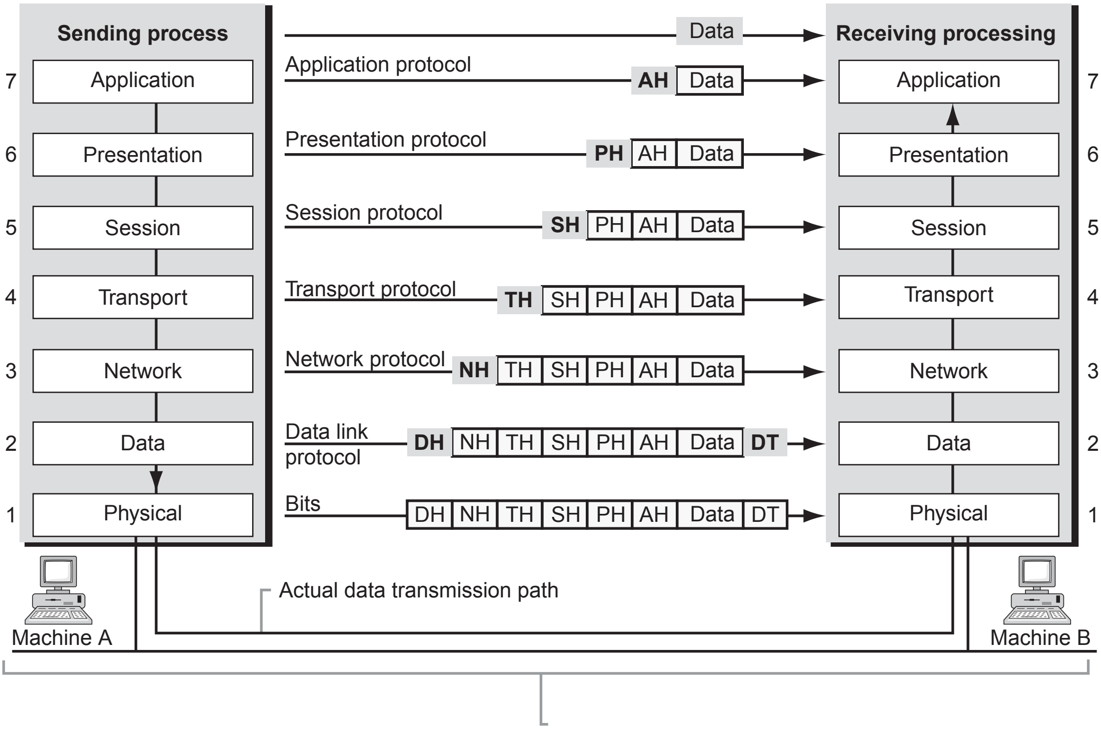


Figure 2.2 Data Flow in OSI Model

header PH to the received data and passes it to the session layer. The same process is repeated at the session (layer 5), transport (layer 4) and network layers (layer 3). At the data link layer (layer 2), a trailer DT is also added to the data received from network layer along with the header DH. Finally, the entire package (data plus headers and trailer) reaches the physical layer where it is transformed into a form (electromagnetic signals) that can be transmitted to the machine B.

At machine B, the reverse process happens. The physical layer transforms the electromagnetic signals back into digital form. As the data travels up through the layers, each layer strips off the header (or trailer) added by its peer layer and passes the rest package to the layer directly above it. For example, the data link layer removes DH and DT from the package received from the physical layer and passes the resultant package to the network layer. The network layer then removes NH and passes the rest package to the transport layer and so on. Ultimately, the data reaching the application layer of machine B is in a format appropriate for the receiving process on machine B and thus is passed to the process.

6. Explain the duties of each layer in OSI model.

Ans: The seven layers of OSI model are divided into two groups according to their functionalities. Physical, data link and network layers are put in one group, as all these layers help to move data between devices. Transport, session, presentation and application layers are kept in other group, because they allow interoperability among different software. The functions of each layer are discussed as follows:

1. **Physical Layer:** This layer defines the physical and electrical characteristics of the network. It acts as a conduit between computers' networking hardware and their networking software.

It handles the transfer of bits (0s and 1s) from one computer to another. This is where the bits are actually converted into electrical signals that travel across the physical circuit. Physical layer communication media include various types of copper or fibre-optic cable, as well as many different wireless media.

2. **Data Link Layer:** This layer is responsible for reliable delivery of data from node to node and for providing services to the network layer. At sender's side, the data link layer divides the packets received from the network layer into manageable form known as **frames**. These data frames are then transmitted sequentially to the receiver. At the receiver's end, data link layer detects and corrects any errors in the transmitted data, which it gets from the physical layer. Other functions of data link layer are *error control* and *flow control*. **Error control** ensures that all frames have finally been delivered to the destination network layer and in the proper order. **Flow control** manages the sender to send frames according to the receiving capability of the recipient.
3. **Network Layer:** This layer provides end-to-end communication and is responsible for transporting traffic between devices that are not locally attached. Data in the network layer is called **packet** (group of bits) which in addition to data contains source and destination address. Packets are sent from node to node with the help of any of two approaches, namely, *virtual circuit* (connection-oriented) and *datagram* (connectionless). In **virtual circuit method**, route is decided while establishing connection between two users and the same path is followed for the transmission of all packets. In **datagram method**, there is no connection established; therefore, sequenced packets take different paths to reach destination. Therefore, virtual circuit method resembles telephone system and datagram method resembles postal system. Other functions of network layer include *routing*, *deadlock prevention* and *congestion control*. Network layer makes routing decisions with the help of **routing algorithms** to ensure the best route for packet from source to destination. **Congestion control** tries to reduce the traffic on the network, so that delay can be reduced and overall performance can be increased.
4. **Transport Layer:** The basic function of this layer is to handle error recognition and recovery of the data packets. It provides end-to-end communication between processes which are executing on different machines. It establishes, maintains and terminates communications between the sender process and the receiver process. It splits the message at the sender's end and passes each one onto the network layer. At the receiver's end, transport layer rebuilds packets into the original message, and to ensure that the packets arrive correctly, the receiving transport layer sends acknowledgements to the sender's end.
5. **Session Layer:** The session layer comes into play primarily at the beginning and end of transmission. At the beginning of the transmission, it lets the receiver know its intent to start transmission. At the end of the transmission, it determines whether or not the transmission was successful. This layer also manages errors that occur in the upper layers such as a shortage of memory or disk space necessary to complete an operation or printer errors. Some services provided by the session layer are *dialog control*, *synchronization* and *token management*. **Dialog control** service allows traffic to flow in both directions or in single direction at a time and also keeps track of whose turn it is to transmit data. **Synchronization** helps to insert checkpoints in data streams, so that if connection breaks during a long transmission then only the data which have not passed the checkpoint yet need to be retransmitted. **Token management** prevents two nodes to execute the same operation at the same time.
6. **Presentation Layer:** The function of this layer is to ensure that information sent from the application layer of one system would be readable by the application layer of another system. Therefore,

presentation layer concerns with the syntax and semantics of the information transmitted. This is the place where application data is packed or unpacked and is made ready to use by the running application. This layer also manages security issues by providing services such as data encryption and compression, so that fewer bits need to be transferred on the network.

7. **Application Layer:** This layer is the entrance point that programs use to access the OSI model and utilize network resources. This layer represents the services that directly support applications. This OSI layer is closest to the end users. Application layer includes network software that directly serves the end users of the network by providing them user interface and application features such as electronic mail.

7. Explain the terms interfaces and services? Discuss protocol data unit (PDU).

Ans: Each layer contains some active elements called **entities**, such as process. Entities are named as **peer entities** when they are in the same layer on different systems. Between two adjacent layers is an **interface** which defines the operations and services of the lower layer that are available to its immediate upper layer. A well-defined interface in a layered network helps to minimize the amount of traffic passed between layers. The set of operations provided by a layer to the layer above it is called **service**. The service is not concerned about the implementations of operations but defines what operations the layer can perform for its users. Thus, lower layer implements services that can be used by its immediate upper layer with the help of an interface. The lower layer is called a **service provider** and the upper layer is called a **service user**.

A layer can request for the services of the lower layer, which is present below it, through a specific location known as **service access point** (**SAP**). SAP has a unique address associated with it. For example, in a fax machine system, SAP is the socket in which a fax machine can be plugged and SAP addresses are the fax numbers which are unique for every user. Therefore, to send a fax, the destination SAP address (fax number) must be known (Figure 2.3).

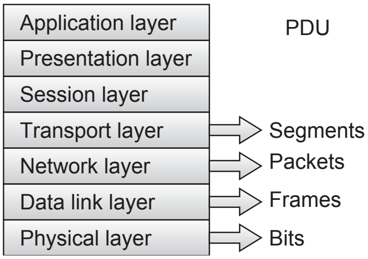


Figure 2.3 Layers and Their PDU

For communication and information sharing, each layer makes use of PDUs. PDU can be attached in front (header) or end (trailer) of the data and contains control information which is encapsulated with data at each layer. Depending on the information provided in the header, each PDU is given a specific name. For example, at transport layer, data plus PDU is called a **segment**; at network layer, segment and PDU (added by network layer) is given the name **packet** or **datagram** and at data link layer, packet with data link PDU is called a **frame**. The PDU information attached by a specific layer at the sender's end can only be read by the peer layer at the receiver's end. After reading the information, the peer layer strips off the PDU and passes the remaining package to its immediate upper layer.

8. Write the functions of data link layer in OSI model.

Ans: Data link layer is responsible for the transmission of frames between two nodes and provides error notificatio to ensure that data is delivered to the intended node. To achieve this, it performs the following functions:

❑ **Framing:** The data link layer takes the raw stream of bits from the physical layer and divides it into manageable units called frames. To indicate the start and end of each frame to the receiver, several methods including character count, bit stuffing and byte stuffing are use

- **Physical Addressing:** The data link layer adds physical address of the sender and/or receiver by attaching header to each frame.
- **Flow Control:** The data link layer provides flow control mechanism, which prohibits a slow receiver from being flooded by the fast sender. If the sender's transmission speed is faster as compared to the receiving capability of receiver, it is quite probable that some frames are lost. To avoid such undesirable events, the data link layer must provide a means to control the flow of data between sender and receiver.
- **Error Control:** The data link layer is responsible for ensuring that all frames are finally delivered to the desired destination. To achieve this, the error control mechanism of data link layer makes the receiver to send positive or negative acknowledgement to the sender. Positive acknowledgement gives surety to the sender that frame has been received without any errors and negative acknowledgement indicates that frame has not been received or has been damaged or lost during transmission. It is the responsibilty of data link layer to ensure the retransmission of damaged and lost frames.
- **Access Control:** When two or more devices are connected to each other via same link then data link layer protocol detects which device has control over the link at a point of time. The Institute of Electrical and Electronis Engineers (IEEE) has divided the data link layer into two sublayers**.**
    - **Logical Link Control (LLC) Sublayer:** This sublayer establishes and maintains links between the communicating devices. It also provides SAPs, so that hosts can transfer information from LLC to the network layer.
    - **Media Access Control (MAC) Sublayer:** This sublayer determines which device to access the channel next in case the channel is being shared by multiple devices. It communicates directly with the network interface card (NIC) of hosts. NIC has MAC address of 48 bits that is unique for each card.

9. Discuss some functions of the session layer and presentation layer.

Ans: Session layer is responsible for the establishing and maintaining session between processes running on different machines as well as synchronizing the communication between them. Some other functions of this layer are as follows:

- It allows the processes to communicate in either half duplex or full duplex mode. That is, information can be transmitted between the processes either only in one direction at a time or in both directions at same time.
- It makes use of checkpoints for synchronization that helps in identifying which data to retransmit.

The presentation layer is concerned with the syntax and semantics of the information being transmitted between communicating devices. Other functions of presentation layer are as follows:

- It converts the representation of information used within the computer to network standard representation and vice versa.
- It encrypts and decrypts data at the sender's and receiver's end respectively. It also compresses the data for reducing the traffic on the communication channel

10. Compare the functionalities of network layer with transport layer.

Ans: Both network and transport layers are responsible for end-to-end communication but still there are certain differences in the set of services they provide. These differences are listed in Table 2.1.

Table 2.1 Comparison Between Network and Transport Layer

Network layer	Transport layer
• It performs routing and makes the routing decisions based on the priority of packets.	• It ensures that the entire message is delivered to destination machine's transport layer without any error.
• It is a connection-oriented layer. That is, it requires connection to be established between source and destination before delivering the packets.	• It provides both connection-oriented and connectionless services.
• It performs packet sequencing, flow control and error control.	• It provides end-to-end data transport service.

11. Explain in brief the transmission control protocol/Internet protocol (TCP/IP) reference model.

Ans: TCP/IP model was developed by the U.S. **Department of Defense** (**DoD**) to connect multiple networks and preserve data integrity. TCP/IP protocol model came after the OSI model and the numbers of layers in TCP/IP differ from that of the OSI model. TCP/IP model comprises of four layers, namely, *network access* (also called host-to-network layer), *Internet*, *transport* and *application* layers (see Figure 2.4).

The network access layer of TCP/IP model corresponds to the combination of physical and data link layers of OSI model. The Internet layer corresponds to the network layer of OSI model and the application layer performs tasks of session, presentation and application layers of OSI model with the transport layer of TCP/IP performing a part of responsibilities of session layer of OSI model.

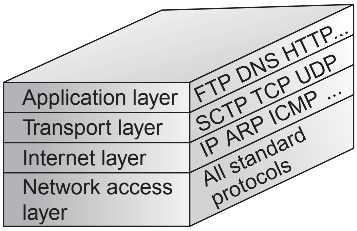


Figure 2.4 TCP/IP Model

TCP/IP protocol suite contains a group of protocols forming a hierarchy such that the lower layer protocols support upper layer protocols.

1. **Network Access Layer:** This layer does not rely on specific protocol hence supports all standard protocols. It connects two nodes to the network with the help of some protocol and move data across two nodes which are connected via same link. The nodes after connection can transfer IP packets to each other. This layer is also referred to as **host-to-network layer**.
2. **Internet Layer:** The main function of this layer is to enable the hosts to transmit packets to different networks by taking any of the routes available for reaching the destination. This layer strengthens the whole architecture and defines the format of packet. The rules to be followed while delivering the packets are transparent to the users. Internet layer supports many protocols such as IP, address resolution protocol (ARP), reverse ARP (RARP), Internet control message protocol (ICMP) and Internet group message protocol (IGMP). **IP** is an unreliable and connectionless protocol that transmits data in the form of packets called datagrams. Each datagram is transmitted independently and can travel through a different route. Moreover, the datagrams may reach the destination not necessarily in the order in which they were sent or may be duplicated. IP neither keeps track of the routes followed by the datagrams nor does it perform any error checking. It tries its best to deliver the datagrams at their intended destinations; however, it does not ensure the delivery. **ARP** is used to identify the physical address of a node whose logical address is known. **RARP** performs just the reverse of ARP, that is, it enables a host whose physical address is known to identify its logical address. This protocol is used when a new node is connected to the

network or when an already connected node is formatted. **ICMP** is used to send error messages to the sender in case the datagram does not reach its destination. **IGMP** is used to deliver the same message to a number of recipients at the same time.

3. **Transport Layer:** The main function of this layer is to deliver a message from a process on the source machine to a process on the destination machine. This layer is designed to allow end-to-end conversation between peer entities. It uses three protocols, namely, *TCP*, *user datagram protocol* (*UDP*) and *stream control message protocol* (*SCMP*) to accomplish its responsibilities. **TCP** is a connection-oriented protocol which means a connection must be established between the source and the destination before any transmission begins. It is also a reliable protocol, as it ensures error-free delivery of data to the destination. **UDP** is an unreliable and a connectionless protocol that performs very limited error checking. **SCTP** is the combination of UDP and TCP and it supports advanced features such as voice over the Internet.
4. **Application Layer:** This layer contains all the high-level protocols such as file transfer protocol (FTP) and virtual terminal (TELNET). Some more protocols which were added later include domain name service (DNS), hyper text transfer protocol (HTTP) and many more. With the help of various protocols, this layer integrates many activities and responsibilities for effective communication.

12. Describe various types of addresses associated with the layers of TCP/IP model.

Ans: Each layer in the TCP/IP model uses an address for the efficient delivery of data between communicating nodes. The host-to-network layer (physical plus data link layer) relates to *physical address*, network layer relates to *logical address*, transport layer concerns with *port address* and application layer defines *specific address*. The description of these addresses is as follows:

- **Physical Address:** It is the address assigned to a node by the network (LAN or WAN) in which it is connected. It is the lowest-level address that is included in the frames at the data link layer to identify the destination node. The size and format of physical address is highly dependent on the underlying physical network. That is, different networks can have different address formats. Physical address is also known by other names including **link address**, **MAC address** and **hardware address**.
- **Logical Address:** In an inter-networked environment connecting different networks having different address formats, the physical addresses are inadequate for communication. Thus, a universal addressing system is used that assigns each host in the network a unique address called logical address (also referred to as **IP address** or **software address**) which is independent of the underlying physical network. For example, in Internet, each host connected to the Internet is assigned a 32-bit IP address and no two hosts connected to the Internet can have the same IP address. It is the responsibility of the network layer to translate the logical addresses into physical addresses.
- **Port Address:** The data link layer (using physical address) and network layer (using IP address) ensure end-to-end delivery of data, that is, data is reached the destination host. Now, since multiple processes may be running simultaneously on the host machine, there should be some means to identify the process to which data is to be communicated. To enable this, each running process on the host machine is assigned with a label what is known as port address. Using the port address, the transport layer ensures process-to-process delivery. In TCP/IP architecture, port address is of 16 bits.
- **Specific Address:** Some applications such as e-mail and World Wide Web (WWW) provide user-friendly addresses designed for that specific address. Some examples of specific address include an e-mail address that helps to identify the recipient of that e-mail and URL of a website that helps to search a document on the web.

13. Compare OSI model with TCP/IP model.

Ans: OSI and TCP/IP are layered models that allow the computer systems to communicate with each other. The OSI reference model was developed by ISO in order to standardize the protocols being used in various layers and the TCP/IP model was developed by DoD to connect multiple networks. Both models have some similarities which are as follows:

❑ Both OSI and TCP/IP models use set of independent protocols for enabling communication between users.

❑ In both the models, upper layers focus on application such as web browser and lower layers focus on end-to-end delivery of data.

The differences between OSI and TCP/IP models are listed in Table 2.2.

Table 2.2 Differences Between OSI and TCP/IP Models

OSI model	TCP/IP model
• It is a seven-layer model.	• It is a four-layer model.
• It was unable to connect to radio and satellite network.	• It had the ability to connect to radio and satellite network.
• It supports only connection-oriented communication in transport layer while both connection-oriented and connectionless communication in network layer.	• It supports both connection-oriented and connectionless communication in transport layer while only connectionless communication in network layer.
• It clearly distinguishes services, interfaces and protocols.	• It does not clearly distinguish services, interfaces and protocols.
• It was defined before the invention of the Internet.	• It was defined after the invention of Internet.
• The model was developed before the corresponding protocols came into existence.	• The model was developed after the protocols came into existence.

14. Explain where the following fit in the OSI eference model.
(a) A 4-kHz analog connection across the telephone network.
(b) A 33.6-kbps modem connection across the telephone network.
(c) A 64-kbps digital connection across the telephone network.

Ans: **(a)** The actual 4-kHz analog signal exists only in the physical layer of the OSI reference model.

(b) A 33.6-kbps modem is used for connecting a user to the switch across the telephone network and a modem also performs error checking, framing and flow control. Therefore, data link layer will be used for performing such functionality.

(c) A 64-kbps digital signal carries user information and is similar to the 4-kHz analog connection which makes use of twisted pair cable. Therefore, physical layer will be used for performing such functionality.

15. Discuss in brief the Novell Netware network model.

Ans: Novell Netware is the popular network system which was designed for replacing mainframes with a network of PCs thereby reducing the cost of companies. In this network, each user is assigned a desktop PC operating as **client** that uses services (database, file etc) provided by some powerful PCs operating as **servers**. Novell network is the modification of old Xerox network system (XNS) and it uses a protocol stack (see Figure 2.5). It was developed prior to OSI and looks like TCP/IP model.

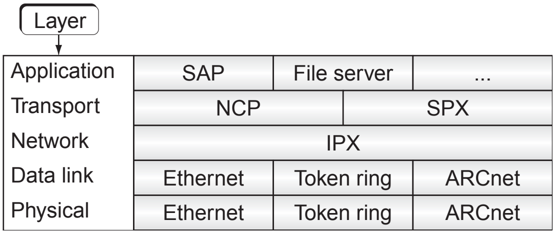


Figure 2.5 Novell Netware Model

The physical and data link layers of Novell Netware network can use any standard protocols including Ethernet, IBM token ring and ARCnet. The network layer uses Internet packet exchange (IPX) protocol, which is an unreliable and connectionless inter-network protocol. IPX transmits packets from the source to destination transparently regardless of whether the source and destination are on the same or on the different networks. It provides the same functionality as that of IP. However, the only difference between the two is that IPX uses 12-byte address while IP uses 4-byte address. The transport layer uses network core protocol (NCP) which is a connection-oriented protocol. It provides many services in addition to transporting data. Another protocol which works on transport layer is sequenced packet exchange (SPX) that provides only data transport service. The application can choose from a variety of protocols such as SAP and file serve .

16. Explain various network devices.

Ans: Networks are becoming more complicated and more pervasive everyday. Therefore, to reduce complication, some network devices were developed. Network devices help nodes to get connected in a network for efficient communication. Network devices include *NIC*, *switch*, *router*, *bridge* and *gateway*.

Network Interface Card

It is a hardware device that connects clients, servers and peripherals to the network through a port. Most network interfaces come as small circuit board that can be inserted onto one of the computer motherboard's slots. Alternatively, modern computers sometimes include the network interface as part of their main circuit boards (motherboards). Each network interface is associated with a unique address called its MAC address. The MAC address helps in sending information to the intended destination. NICs are the major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation one is using (Figure 2.6).

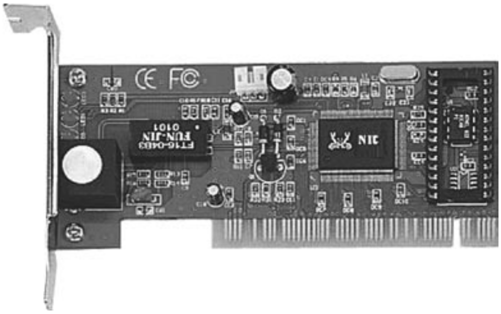


Figure 2.6 Network Interface Card

Repeater

It is the most basic device on a network. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater installed on the link receives signal, regenerates it and sends the refreshed copy back to the link. Doing this means that the new signal is clean and free from any background noise introduced while travelling down the wire. In Figure 2.7, two sections in a network are connected by the repeater.

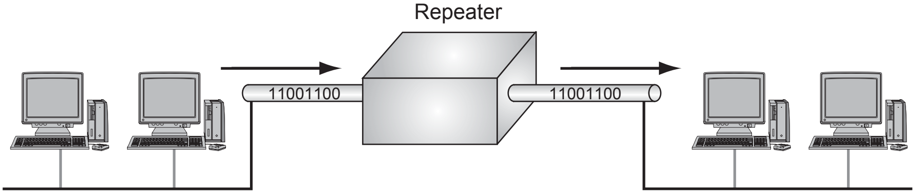


Figure 2.7 Repeater

Repeaters are most commonly used to extend a network. All network cable standards have maximum cable length specification. If the distance between two network devices is longer than this specification, a repeater is needed to regenerate the signal. Without the repeater, the signal will be too weak for the computers on each end to reliably understand. A good example of the use of repeaters would be in a LAN using a star topology with unshielded twisted pair cabling. The length limit for unshielded twisted pair cable is 100 m. The repeater amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 m limit. Nonetheless, the repeaters have no in-built intelligence and they do not look at the contents of the packet while regenerating the signal. Thus, there is no processing overhead in sending a packet through a repeater. However, a repeater will repeat any errors in the original signal.

Hub

It is a small box that connects individual devices on a network, so that they can communicate with one another. The hub operates by gathering the signals from individual network devices, optionally amplifying the signals, and then sending them onto all other connected devices. Amplification of the signal ensures that devices on the network receive reliable information. A hub can be thought of as the centre of a bicycle wheel, where the spokes (individual computers) meet.

Nowadays, the terms repeater and hub are used synonymously, but actually they are not same. Although at its very basic level, a hub can be thought of as a multi-port repeater. Typically, hubs have anywhere from 4 to over 400 ports. When a signal is received on one port of the hub, it is regenerated out to all the other ports. It is most commonly used to connect multiple machines to the same LAN. Administrators connect a computer to each port on the hub, leaving one port free to connect to another hub or to a higher-level device such as a bridge or router.

Bridge

This device allows the division of a large network into two or more smaller and efficient networks. It monitors the information traffic on both sides of the network, so that it can pass packets of information to the correct location. Most bridges can 'listen' to the network and automatically figure out the address of each computer on both sides of the bridge. A bridge examines each packet as it enters though one of the ports. It first looks at the MAC address of the sender and creates a mapping between the port and the sender's MAC address. It then looks at the address of the recipient, comparing the MAC address to the list of all learned MAC addresses. If the address is in the list, the bridge looks up the port number and forwards the packet to the port where it thinks the recipient is connected. If the recipient's MAC address is not in the list, the bridge then does a flood; it sends the signal to all the ports except the one from where it was received. As a result, a bridge reduces the amount of traffic on a LAN by dividing it into two segments. It inspects incoming traffic and decides whether to forward or discard it (Figure 2.8).

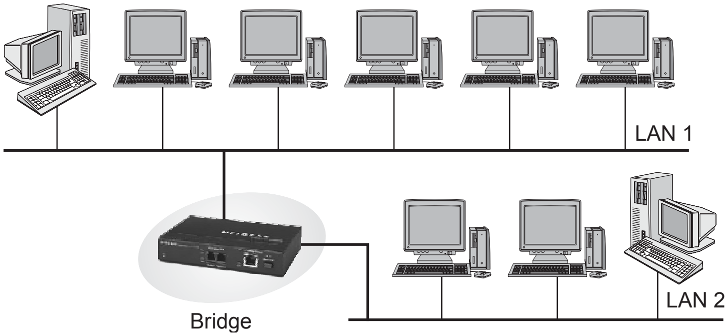


Figure 2.8 Bridge

Bridges can be used to connect networks with different types of cabling or physical topologies. They must, however, be used between networks employing the same protocol. Since a bridge examines the packet to record the sender and looks up the recipient, there is overhead in sending a packet through a bridge. On a modern bridge, this overhead is miniscule and does not affect network performance.

Switch

It is a multi-port bridge. It connects all the devices on a network, so that they can communicate with one another. The behaviour of a switch is same as that of a bridge. It is capable of inspecting the data packets as they are received, determining the source and destination device of that packet, and forwarding that packet appropriately. The difference is that most switches implement these functions in hardware using a dedicated processor. This makes them much faster than traditional software-based bridges.

Router

It is an essential network device for interconnecting two or more networks. The router's sole aim is to trace the best route for information to travel. As network traffic changes during the day, routers can redirect information to take less congested routes. A router creates and/or maintains a table, called a routing table that stores the best routes to certain network destinations. While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges and other routers on the network. Routers can even 'listen' to the entire network to determine which sections are the busiest. They can then redirect data around those sections until they clear up (Figure 2.9).

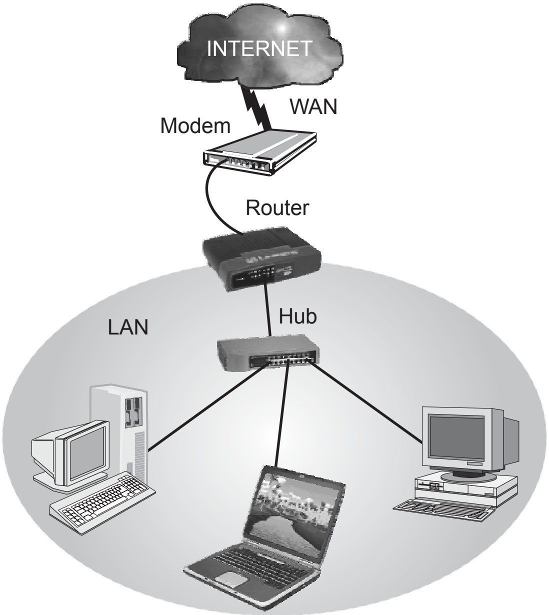


Figure 2.9 Router

Routers are generally expensive and difficult to configure and maintain. They are critical components of a network and if they fail, the network services will be significantly impaired. Most routers operate by examining incoming or outgoing signals for information at the network layer. In addition, they can permit or deny network communications with a particular network.

Gateway

It is an internetworking device, which joins networks operating on different protocols together. It is also known as protocol converter. A gateway accepts the packet formatted for one protocol and converts the formatted packet into another protocol. For example, a gateway can receive e-mail message in one format and convert it into another format. A gateway can be implemented completely in software, hardware, or as a combination of both. One can connect systems with different protocols, languages and architecture using a gateway (Figure 2.10).

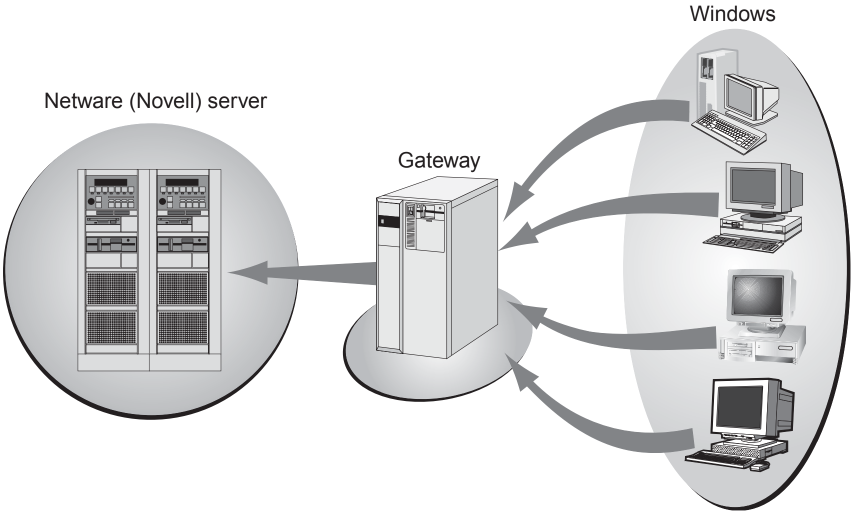


Figure 2.10 Gateway

17. What are the different types of bridges?

Ans: A bridge is a network device that allows division of a large network into two or more similar networks. It connects two segments of LANs and monitors the traffic on both sides of the network, so that it can pass packets of information to the correct location. It maintains a forwarding table that links addresses of all stations connected through it and, thus, helps to forward frames from one station to another. Different types of bridges are as follows.

Transparent Bridge

As the name implies, the existence of bridge is transparent to the stations connected through it. The transparent bridge is also called learning bridge, as its forwarding table is made automatically by learning the movement of frames in the network. Initially, the forwarding table contains no entries; however, as the frame move across the networks, the bridge uses the source addresses to make or update entries to the forwarding table and the destination address to make forwarding decisions. Figure 2.11 shows a transparent bridge connecting two networks LAN1 and LAN2 via ports 1 and 2, respectively.

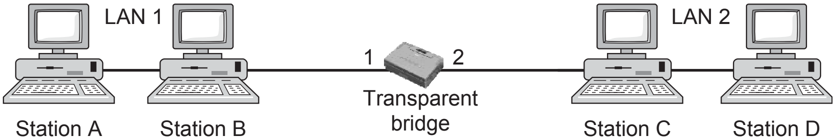


Figure 2.11 Transparent Bridge

To understand how transparent bridge works, suppose station A wishes to send frame to station D. Since there is no entry corresponding to A or D in the forwarding table, the bridge broadcasts the frames to both the ports (that is, ports 1 and 2). However, at the same time, it learns from the source address A that the frame has come through port 1 and, thus, adds an entry (the source address A and port 1) to the forwarding table. Next time, whenever a frame from a station (say, C) destined for A comes to the bridge, it is forwarded only to port 1 and not elsewhere. In addition, an entry (source address C and port 2) is added to the forwarding table. Thus, as the frames are forwarded, the learning process of bridge continues.

An important advantage of transparent bridge is that since stations are not aware of the presence of bridge, the stations need not be reconfigured in case the bridge is added or deleted

Source Routing Bridge

This bridge is used to connect two or more token ring LANs. In addition to the source and destination address, each frame includes the address of the all the bridges to be visited as specified by the source station. Thus, the path of a frame is already defined by the source station and intermediate nodes cannot take any decision on the routes. The source station acquires the addresses of bridges by exchanging some special frames with the destination station before the transmission of data frame begins. Figure 2.12 shows a source routing bridge.

Remote Bridge

It is used to connect two bridges at remote locations using dedicated links. Remote bridge configuration is shown in Figure 2.13 in which two bridges are interconnected using WAN.

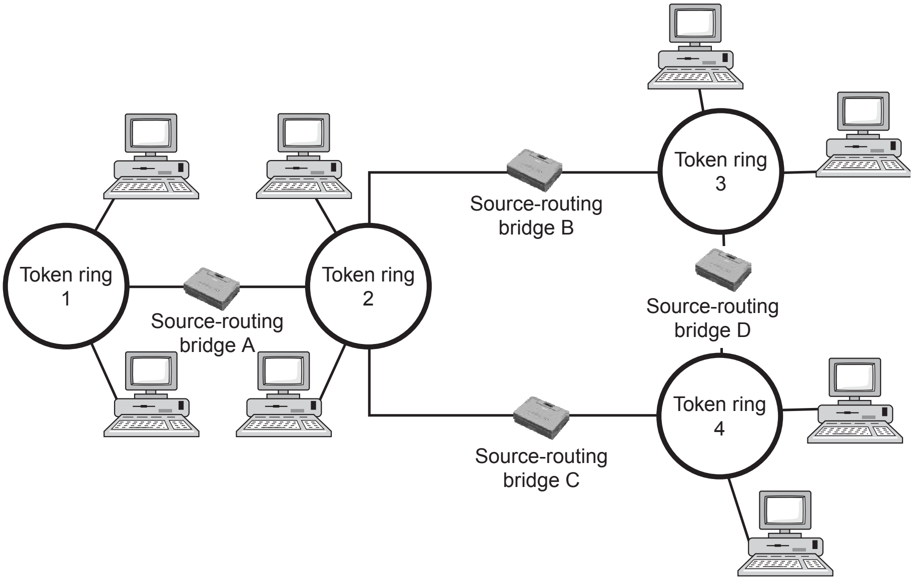


Figure 2.12 Source Routing Bridge

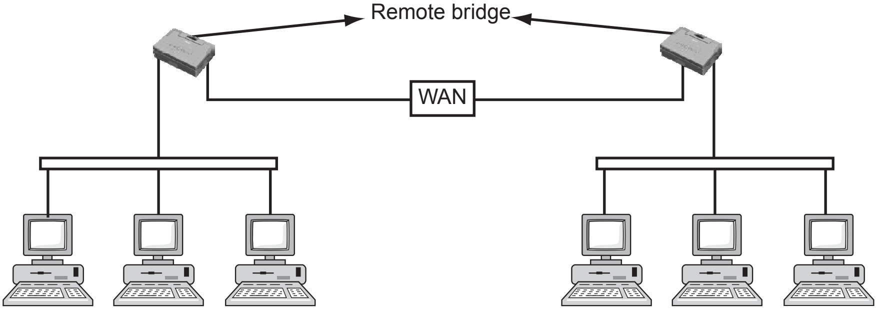


Figure 2.13 Remote Bridge

18. Differentiate bridge, router and repeater.

Ans: Some differences among bridge, router and repeater are listed in Table 2.3.

Table 2.3 Comparison Among Bridges, Routers and Repeaters

Bridge	Router	Repeater
• It operates at the data link layer of OSI model.	• It operates at the network layer of OSI model.	• It operates at the physical layer of OSI model.
• It is mostly used in LANs.	• It is mostly used in internetworking.	• It is used to extend the physical length of a network.
• It transmits the frames in similar network.	• It transmits the packets using similar protocols in different networks.	• It is an analog device connected to two cable segments which regenerates the signals.

19. Differentiate switch and hub.

Ans: The differences between switch and hub are listed in Table 2.4.

Table 2.4 Differences Between Switch and Hub

Switch	Hub
A switch operates at the data link layer.	A hub operates at the physical layer.
It is a complex device and more expensive than a hub.	It is a simple device and cheaper than switch.
It is a full-duplex device and more secured.	It is a half-duplex device and less secured.
Each port of switch has its own collision domain, that is, each port has buffer space for storing frame; therefore, when two frames arrive at the same time, frames will not be lost.	The entire hub forms a single-collision domain, that is, when two frames arrive at the same time, they will always collide and hence frame will be lost.
It is an intelligent device, as it maintains a table to transmit the frame to the intended recipient.	It is a non-intelligent device, as each time frame is broadcast to all the connected nodes.
It utilizes the bandwidth effectively.	Wastage of bandwidth is more in the case of hub.

20. Differentiate router and switch.

Ans: Some of differences between the router and switch are listed in Table 2.5.

Table 2.5 Differences Between Router and Switch

Router	Switch
• It connects nodes on different networks.	• It connects nodes within a same network.
• It operates in network layer.	• It operates in data link layer.
• It uses IP address for transmission of packets.	• It uses MAC address for transmission of frames.
• It is more intelligent and complex device than switch.	• It is less intelligent and simpler device than router.
• Various algorithms are used to forward packets along their best path.	• No such algorithms are used by switch.
• It needs to be configured before using.	• Most switches are ready to use and need not be configured.

Multiple Choice Questions

1. The correct order of corresponding OSI layers for having the functionalities of packet priortization, shared access resolution, end-to-end flow and error control and socket-based inter process communication are _______________.
   (a) network, physical, transport and application
   (b) network, data link, presentation and application
   (c) network, presentation, data link and transport
   (d) network, data link, application, presentation

2. The main function of transport layer is _______________.
   (a) synchronization
   (b) node-to-node delivery

(c) process-to-process delivery
(d) updating routing tables

3. IP is responsible for __________ communication while TCP is resposible for __________ communication.
(a) process-to-process, host-to-host
(b) host-to-host, process-to-process
(c) process-to-process, node-to-node
(d) node-to-node, host-to-host

4. Which of the following is/are an application layer service?
(a) File transfer and access
(b) Domain name service
(c) Remote login
(d) All of these

5. To interconnect two homogeneous WANs, we need a ___________.
(a) bridge (b) gateway
(c) router (d) hub

6. A bridge recognizes the addresses of __________.
(a) physical layer
(b) data link layer
(c) network layer
(d) application layer

7. Which of the following internetworking device uses the greatest number of layers in the OSI model?
(a) Bridge
(b) Gateway
(c) Router
(d) None of these

8. In Novell Netware, IPX is a/an _________ byte address.
(a) 8 (b) 12
(c) 4 (d) 48

9. Which type of bridge builds and updates its tables from address information of packets?
(a) Tranparent
(b) Source routing
(c) Remote
(d) None of these

10. Which of the following address(es) is needed for the effective communication?
(a) MAC (b) IP
(c) Port address (d) All of these

Answers

1. (b) 2. (c) 3. (b) 4. (d) 5. (c) 6. (b) 7. (b) 8. (b) 9. (a) 10. (d)

3

Analog and Digital Transmission

1. What do you mean by data and signal?

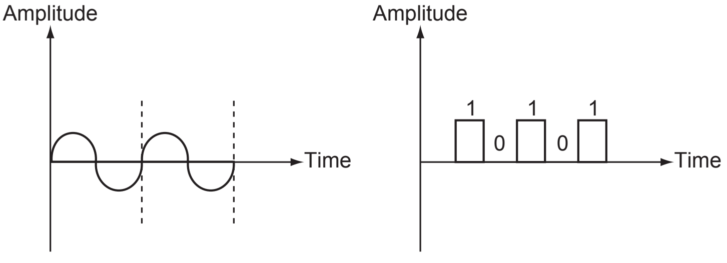
Ans: **Data** refers to an entity that expresses some meaning based on rules which are agreed upon by the sender and the receiver. It can be available in various forms such as text, graphics, audio and video. **Signal** refers to the representation of the data in a form (such as electrical, electronic or optical) suitable for transmission over a transmission medium.

2. Defin analog and digital data.

Ans: **Analog data** is defined as the data having continuous states. For example, sounds produced while speaking take continuous values. **Digital data** is defined as the data having discrete states. For example, data to be stored in the memory of computer is in the form of 0s and 1s.

3. Distinguish analog and digital signals?

Ans: Data is transmitted across a transmission medium in the form of electromagnetic signals. An electromagnetic signal can be either *analog* or *digital*. A signal that passes through and includes a wide range of varying values of intensity over a period of time is referred to as **analog signal** [Figure 3.1(a)].



(a) Analog signal

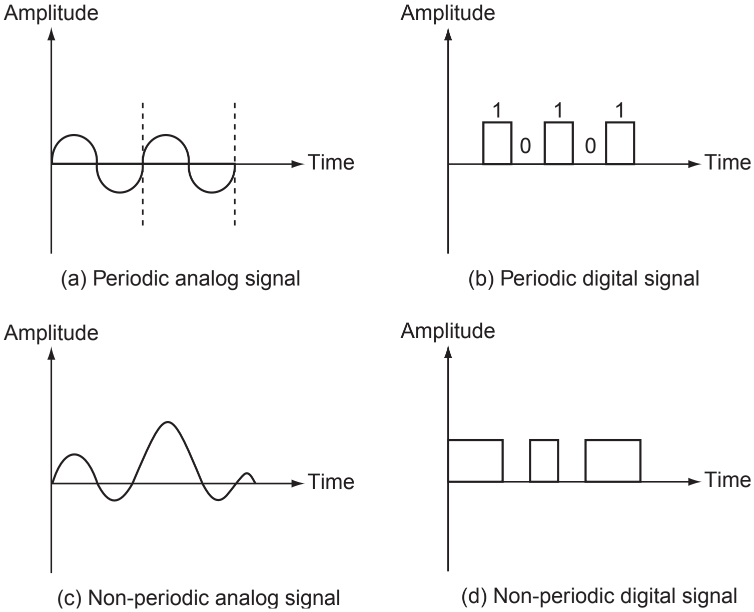
(b) Digital signal

Figure 3.1 Analog and Digital Signals

In contrast, a signal that has only a finite range of values (generally 0 and 1) is referred to as **digital signal** [Figure 3.1(b)]. Either of the analog or digital signals can be used to transmit either analog or digital data.

4. What do you understand by periodic and non-periodic signals?

Ans: Both analog and digital signals can be either *periodic* or *non-periodic*. A **periodic signal** exhibits a specific signal pattern that repeats over time [Figures 3.2(a) and 3.2(b)]. Sine waves and square waves are the most common examples of periodic analog and digital signals, respectively. On the other hand, a **non-periodic** (or **aperiodic**) signal does not repeat any specific signal pattern over time [Figures 3.2(c) and 3.2(d)]. Usually, in data communications, periodic analog and non-periodic digital signals are used.



(a) Periodic analog signal

(b) Periodic digital signal

(c) Non-periodic analog signal

(d) Non-periodic digital signal

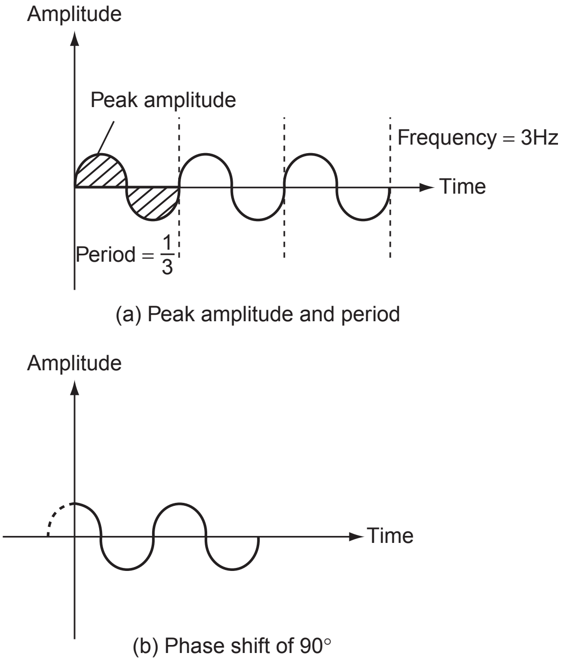
Figure 3.2 Periodic and Non-periodic Signal

5. Describe the parameters that characterize the sine waves.

Ans: The sine wave is the most fundamental form of periodic analog signal. It is characterized by the following three parameters.

- **Peak Amplitude:** It is the highest value or strength of the signal at any point of time [Figure 3.3(a)]. The unit for amplitude depends on the type of the signal. For example, in case of electrical signals, the unit of amplitude is normally volts and amperes.
- **Frequency:** It refers to the number of cycles a signal completes in 1 s. It is measured in cycles per second or Hertz (Hz). Another parameter equivalent to frequency is the **period** which is defined as the time taken by a signal to complete one cycle [Figure 3.3(a)]. Thus, we can say that frequency is equal to the number of periods per second. Both frequency (f) and period (T) are related to each other by the following formula.

$$f = 1/T$$



(a) Peak amplitude and period

(b) Phase shift of 90°

Figure 3.3 Sine Wave

For example, if a signal wave completes one period in 1 s, its frequency is 1 Hz.

- **Phase:** It refers to the measure of shift in the position of a signal with respect to time 0. Figure 3.3(b) shows a shift of 90° in the sine wave shown in Figure 3.3(a). Phase is measured in degree (°) or radians (rad) where 1° = 2π/360 rad.

6. Defin wavelength. What is the relation between wavelength and frequency?

Ans: Wavelength refers to the distance covered by the signal in one cycle. In other words, it is the distance between two similar points in corresponding phases of two adjacent cycles of a signal (Figure 3.4). It is usually denoted by λ.

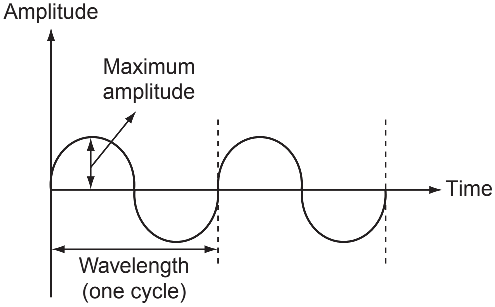


Figure 3.4 Wavelength of a Signal

Wavelength relates the frequency (f) of a signal with the speed of propagation of the medium through which the signal is being transmitted. The relation between frequency and wavelength is expressed using the following formula.

$$\lambda = \text{propagation speed}/f$$

$$\Rightarrow \lambda = \text{propagation speed} \times \text{period}$$

For example, in vacuum, the signal propagates with speed of light (c), which is equal to 3×10^8 m/s. Thus,

$$\lambda = c/f$$

7. Distinguish time-domain and frequency-domain representations.

Ans: A signal can be represented in two ways: *time-domain* and *frequency-domain*. In **time-domain** representation, the signal is represented as a function of time. The time-domain plot of a signal depicts the changes in the amplitude of a signal with time. Figure 3.5 represents the sine wave using time-domain plot. The horizontal axis represents the time and the vertical axis represents the amplitude.

In **frequency-domain** representation, a signal is represented as a function of frequency. Unlike time-domain plot, the frequency-domain plot does not depict the changes in amplitude; rather it depicts only the peak amplitude of the signal and frequency. In addition, the complete sine wave is represented just by a spike. Figure 3.6 shows the frequency domain plot for the sine wave shown in Figure 3.5.

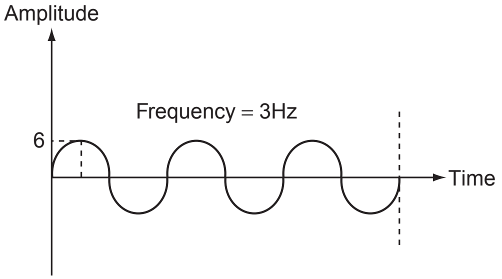


Figure 3.5 Time-domain Representation of a Sine Wave

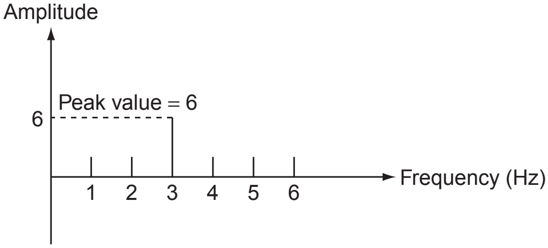


Figure 3.6 Frequency-domain Representation of a Sine Wave

8. What do you understand by composite signal?

Ans: In data communications, single frequency sine waves are not used to communicate data, rather composite signals are used. A **composite signal** is a collection of one or more signals having different frequencies, amplitude and phases (Figure 3.7). It can be periodic or non-periodic. The decomposition of a periodic composite signal produces a series of signals with discrete frequencies, whereas the decomposition of a non-periodic composite signal produces a combination of signals with continuous frequencies in the range of zero to infinit .

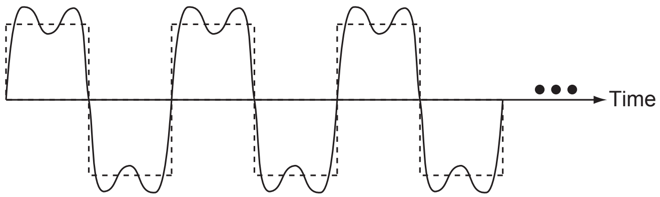


Figure 3.7 Composite Signal

9. Why digital transmission is preferred over analog transmission?

Ans: Analog transmission is a means of transmitting analog signals (representing either analog or digital data) while the **digital transmission** is a means of transmitting digital signals (representing either analog or digital data). Digital transmission offers certain advantages due to which it is preferred over analog transmission. These advantages are as follows:

- To achieve long-distance analog transmission, amplifiers are to be used for boosting up the signal energy. However, the amplifiers boost up the noise too, thereby resulting in more distorted signal. In contrast, repeaters used in digital transmission do not contribute to noise and other impairments. As a result, the data can be transmitted to longer distances while maintaining the data integrity.
- The digital data as well as the digitized analog data can be easily encrypted using encryption techniques.
- With the advent of large-scale integration (LSI) and very large-scale integration (VLSI) technologies, the size and cost of digital equipments have reduced to a greater extent as compared to analog equipments.
- To utilize the large channel capacity effectively, multiplexing is required and it is quite easier and economical to accomplish this using digital techniques than analog techniques.
- All data including voice, video and digital data can be integrated and passed through digital circuits conveniently.

10. How Fourier analysis is important in data communication?

Ans: Fourier analysis is a tool that is used to convert a time domain signal to a frequency domain signal and vice versa. According to this analysis, a composite periodic signal with a period T can be decomposed into a series called **Fourier series** of sine and cosine functions with each function being an integral harmonic of the fundamental frequency f of the composite signal as shown here.

$$S(t) = A_0 + \sum_{n=1}^{\infty} A_n \sin(2\pi nft) + \sum_{n=1}^{\infty} B_n \cos(2\pi nft),$$

where

$$A_0 = \frac{1}{T}\int_0^T s(t)\,dt, \text{ the average value of a signal over a period}$$

$$A_n = \frac{2}{T}\int_0^T s(t)\cos(2\pi nft)\,dt, \text{ the coefficient of } n\text{th cosine component}$$

$$B_n = \frac{2}{T}\int_0^T s(t)\sin(2\pi nft)\,dt, \text{ the coefficient of } n\text{th sine component.}$$

Fourier series converts time domain of a periodic signal to discrete frequency domain. To convert time domain of a non-periodic signal to continuous frequency domain, **Fourier transform** is used as expressed below:

$$S(f) = \int_{-\infty}^{\infty} s(t)e^{j2\Pi ft}\,dt$$

Inverse Fourier transform is expressed by the following formula:

$$s(t) = \int_{-\infty}^{\infty} S(f)e^{-j2\Pi ft}\ dt$$

11. Defin bit interval, bit rate and bit length of a digital signal.

Ans:

- **Bit Interval:** It is the time required to transmit one bit.
- **Bit Rate:** The number of bits transmitted per second is known as bit rate. It can also be defined as the number of bit intervals per second. Its unit is **bits per second** (**bps**). The bit rate for a bit having bit interval `t` will be `1/t`.
- **Bit Length:** The distance occupied by a single bit while transmission on a transmission medium is known as bit length. It is related to bit interval as per the formula given below:

  `Bit length = bit interval × speed of propagation`

12. Differentiate baseband and broadband transmissions?

Ans: Though both baseband and broadband transmissions are the approaches used to transmit digital signals, there are certain differences between the two. These differences are listed in Table 3.1.

Table 3.1 Differences Between Baseband and Broadband Transmissions

Baseband transmission	Broadband transmission
• The digital signal is sent over a channel without converting it into an analog signal.	• The digital signal is first converted into analog signal and then sent over the channel.
• The entire bandwidth of the cable is consumed by a single signal.	• Signals are sent on multiple frequencies, allowing multiple signals to be sent simultaneously.
• It requires a **low-pass channel**—a channel whose bandwidth starts from zero.	• It requires a **bandpass channel**—a channel whose bandwidth does not start from zero.

13. Discuss different types of transmission impairments.

Ans: Sometimes, when a signal passes through a transmission medium, it gets deteriorated due to imperfections in the transmission medium. As a result, the signal received at the receiver's end differs from the one being sent. For example, while transmitting digital signals, bit errors may occur such that in the received signal, some binary 1 is transformed to binary 0 or vice versa. The types of impairments that may occur during transmission are as follows:

- **Attenuation:** While a signal passes through a transmission medium, it loses some of its strength (or weakens) to get over the resistance of transmission medium. This loss of strength or energy is termed as attenuation. In case the signal strength becomes very low, it cannot be detected and interpreted properly at the receiver's end. To compensate the loss of strength, amplifiers or repeaters can be used. The extent of attenuation of a signal depends greatly on its frequency; the effect of attenuation is different for different frequency components. For example, during the transmission of a composite signal, some frequency components bypass without any attenuation, some lose little bit strength while others get blocked. This dependence of attenuation upon frequency leads to a distortion what is called **attenuation distortion**, which is more prevalent in analog signals than digital signals. However, its effect can be reduced by using a suitable equalizer between the channel and the receiver.

- **Delay Distortion:** This is another type of distortion that results because of difference in the delays experienced by different frequency components while passing through the transmission medium. Since the speed of propagation of a signal varies with frequency, different frequency components of a composite signal arrive at the receiver at different times leading to delay distortion. As a result, the shape of received signal changes or gets distorted. Like attenuation distortion, the effect of delay distortion can be neutralized with the use of equalizers. However, unlike attenuation distortion, delay distortion is predominant in digital signals.
- **Noise:** When a signal transits through a transmission medium, some types of undesired signals may mix with it such as intermodulation noise and crosstalk. Intermodulation noise occurs in the cases where signals with different frequencies pass through the same transmission medium. In such cases, the frequencies of some signals may combine (add or subtract) to generate new frequency components which may interfere with the signals of same frequency sent by the transmitter. This leads to distortion in the signal what is known as **intermodulation noise**. **Crosstalk** results when the electromagnetic signals passing through one wire are induced on other wires due to the close proximity of wires.

14. What does the signal-to-noise ratio (SNR) determine?

Ans: The **SNR** is used to determine the effect of noise on the signal. Formally, it is defined as the ratio of the average power of a signal to the average noise power, as shown here.

$$\mathrm{SNR} = \mathrm{avg}(P_S)/\mathrm{avg}(P_N)$$

More the value of SNR is, the less is the signal distorted due to noise and vice versa. SNR is usually expressed in decibel (dB) units. SNR_{dB} is defined as

$$\mathrm{SNR}_{dB} = 10 \log_{10} \mathrm{SNR}$$

15. Write down the theoretical formula to calculate data rate for a noiseless channel and a noisy channel.

Ans: Data rate for a noiseless channel can be determined by using the **Nyquist bit rate** formula as given below.

$$\text{Bit rate} = 2 \times B \times \log_2 L,$$

where B = bandwidth of channel and L = the number of signal levels used to represent data.
Data rate for a noisy channel can be determined by **Shannon capacity**, as given below.

$$C = B \times \log_2(1 + \mathrm{SNR}),$$

where C = data rate and B = bandwidth of channel.

16. Describe the factors used to measure the performance of a network?

Ans: The performance of a network is one of the most important issues in networking. Some major factors that measure the performance of a network are as follows.

- **Bandwidth:** It is one of the main characteristics that measure the performance of a network. It can be used in two different contexts. First is the **bandwidth in hertz** which refers to the range of frequencies in a composite signal and second is the **bandwidth in bps** which refers to the number of bits that can be transmitted by a channel or network in 1 s. An increase in bandwidth in hertz implies the increase in bandwidth in bps.

- ❑ **Throughput:** It is the measure of how much data can be transmitted through a network in 1 s. Though from the definitions throughput sounds similar to bandwidth, it can be less than bandwidth. For example, a network may have bandwidth of 10 Mbps but only 2 Mbps can be transmitted through it.
- ❑ **Latency (Delay):** It refers to the time elapsed between the first bit transmitted from the source and the complete message arrived at the destination. It is the sum of propagation time, transmission time, queuing time and processing delay of a frame.

  The time taken by a bit to travel from the source to destination is referred to as the **propagation time**. It can be calculated using the following formula.

  ```
  Propagation time = distance/propagation speed
  ```

  As the propagation speed increases, propagation time decreases.

  The **transmission time** measures the time between the transmission of first bit from the sender's end and the arrival of last bit of the message at the destination.

  ```
  Transmission time = message size/bandwidth
  ```

  Greater is the message size is, the more will be the transmission time.

  Whenever a message being transmitted arrives at some intermediate device, such as router, it is kept in a queue (if device is not free) maintained by the device. The device processes the queued messages one by one. The time a message spends in the queue of some intermediate or end device before being processed is referred to as the **queuing time**. It depends on the traffic load in the network. More the load of traffic is, the more is the queuing time
- ❑ **Bandwidth-Delay Product:** It refers to the product of bandwidth and delay of a network which specifies the maximum number of bits that can be at any time on the link. For example, if a link has a bandwidth of 8 bps and delay is 5 s, then the maximum number of bits that can fill the link is 40 bits.
- ❑ **Jitter:** It refers to a problem that occurs when the inter-arrival time between packets is not constant and the application using the data is time sensitive.

17. Defin line coding. List some common characteristics of line coding schemes.

Ans: Line Coding is defined as the process of converting digital data or sequence of bits to digital signals. **Encoder** is used at the sender's end to create a digital signal from digital data and **decoder** is used at the receiver's end to recreate digital data from digital signal (Figure 3.8).

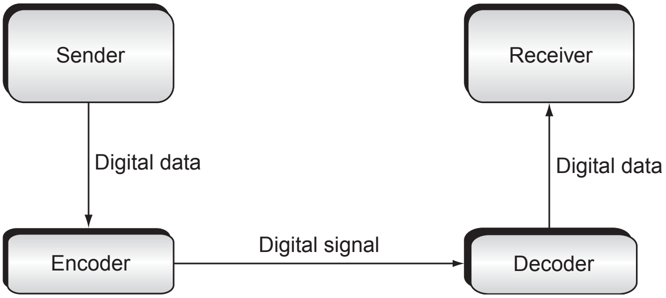


Figure 3.8 Line Coding

Some common characteristics of line coding schemes are as follows:

- **Data Element:** It refers to the smallest entity (that is, bit) that expresses some information. It describes what is to be sent.
- **Signal Element:** It refers to the shortest unit of digital signal. Each signal element carries one or more data elements. The ratio (r) of number of data elements to number of signal element indicates the number of data elements carried by a signal element.
- **Data Rate:** Data rate, also called **bit rate**, refers to the number of data elements that can be transmitted per second. It is usually expressed in bps. The speed of transmission increases with the increase in data rate.
- **Signal Rate:** Signal rate, also called **baud rate** or **modulation rate** or **pulse rate**, refers to the number of signal elements transmitted per second. It is expressed in baud. An increase in signal rate increases the demand of bandwidth. The relationship between data rate and signal rate can be expressed as:

  $$S = CF \times d \times (1/r),$$

  where S = the number of signal elements; CF= case factor; D = data rate and r = the number of data elements carried by a signal element.
- **Bandwidth:** Bandwidth refers to the maximum volume of data that can be transferred over any communication medium at a given point of time. More the data needed to be transmitted in a given period is, the more is the bandwidth required. On digital circuits, bandwidth is measured in bps. The bandwidth is related to signal rate (S) as per the formula shown below.

  $$B_{min} = S$$
  $$\Rightarrow B_{min} = CF \times d \times (1/r)$$

  Similarly, if we are given the bandwidth (B) of channel, we can find out the maximum data rate (d_{max}) using the following formula.

  $$d_{max} = B \times r \times (1/CF)$$
- **DC Components:** A signal may include very low frequency component in its spectrum. These components with frequencies around zero (called DC components) are undesirable, as some systems do not allow such components to pass through them. Thus, for these systems, the line coding with no DC component is required.
- **Baseline Wandering: Baseline** refers to the average of the received signal power calculated by the receiver while decoding a digital signal. Baseline wandering refers to the movement or drift in the baseline. Due to baseline wandering, the process of decoding at the receiver's end becomes difficult. Thus, a good line coding scheme must prevent baseline wandering.
- **Error Detection:** Line coding scheme should have built-in capability to detect some or all the errors that occur during transmission.
- **Self-Synchronization:** Bit intervals of the receiver should match with bit intervals of the sender to interpret correctly the signal at the receiver's end. For this, the digital signal must include timing information (that is, self-synchronized) which means the transitions in the digital signal alert the receiver at different points of the pulse. This information is used to readjust or reset a clock if the receiver's clock is not synchronized.
- **Resistance to Noise:** Line coding scheme should have ability to create a code that is unsusceptible to noise or other inferences in the transmission medium.
- **Complexity:** Line coding scheme should be simple, as it is quite expensive to implement a complex coding scheme as compared to a simple scheme.

18. Can the bit rate be less than the pulse rate? Why or why not?

Ans: Bit rate is always greater than or equal to the pulse rate because the relationship between pulse rate and bit rate is defined by the following formula

$$\texttt{Bit rate = pulse rate} \times \texttt{log}_2\texttt{L,}$$

where L denotes the number of data levels of the signal and $\texttt{log}_2\texttt{L}$ denotes the number of bits per level.

If a pulse carries only 1 bit (that is, $\texttt{log}_2\texttt{L=1}$), the pulse rate and the bit rate are the same. However, if the pulse carries more than 1 bit, then the bit rate is greater than the pulse rate.

19. Discuss various line coding schemes.

Ans: There are various line coding schemes that can be classified into three basic categories namely, *unipolar*, *polar* and *bipolar*.

Unipolar Scheme

This scheme uses two voltage levels of a signal and both of these voltage levels are on one side of the time axis (above or below). In this scheme, bit rate and baud rate are equal. However, the encoded signal includes DC components and there is lack of synchronization in case of long series of 0s and 1s. The only coding scheme that falls under this category is non-return-to-zero (NRZ).

- ❑ **NRZ:** In this scheme, bit 1 is used to define positive voltage while bit 0 is used to define zero voltage of a signal. The name NRZ comes from the fact that the signal does not return to zero during the middle of a bit rather only between two bits (Figure 3.9). The unipolar NRZ scheme is not generally used for data communication.

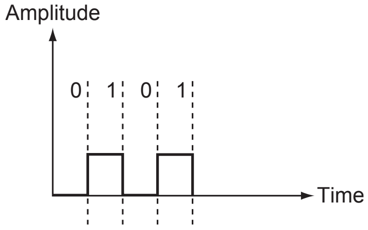


Figure 3.9 Unipolar NRZ Scheme

Polar scheme

This scheme uses two voltage levels of a signal, positive and negative, that can be on both sides of the time axis. The positive voltage may represent 0 while negative voltage may represent 1 or vice versa. Four different schemes fall under this category, which are discussed as follows.

- ❑ **NRZ:** It is the most common type of polar coding scheme. In this scheme, positive voltage is used to represent one binary value and negative voltage is used to represent another. There are two types of polar NRZ schemes namely, *NRZ-level* (*NRZ-L*) and *NRZ-invert* (*NRZ-I*). In **NRZ-L**, the value of bit is determined by the signal level which remains constant during bit duration (Figure 3.10). In **NRZ-I**, the value of bit is determined by inversion or lack of inversion in the signal level. If there is change in the signal level, the value of bit will be 0, whereas if there is lack of change in the signal level, the value of bit will be 1 (Figure 3.11). Both NRZ-L and NRZ-I suffer from synchronization problem in case of long sequence of 0s. However, NRZ-I suffers in case of long sequence of 1s also. In addition, both NRZ-L and NRZ-I have DC component problem.
- ❑ **Return-to-Zero (RZ):** This scheme solves the synchronization problem of NRZ scheme. It uses three values of voltage namely, *zero*, *positive* and *negative*. Unlike NRZ, the signal changes during the middle of a bit but not between the bits. Once it changes during the bit, it remains there until

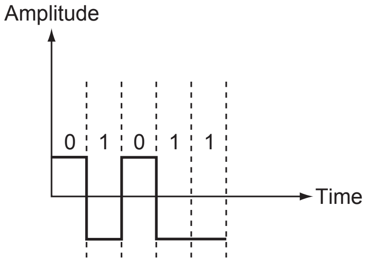


Figure 3.10 Polar NRZ-L Scheme

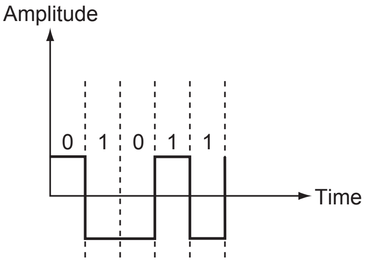


Figure 3.11 Polar NRZ-I Scheme

the next bit starts. Thus, to encode a single bit, two signal changes are required (Figure 3.12). There is no DC component problem in RZ coding scheme. However, it is complex as it requires three levels of voltage.

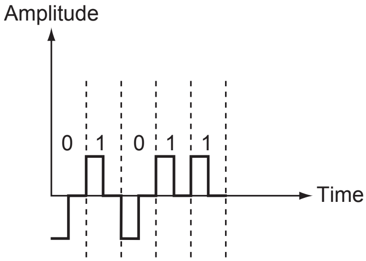


Figure 3.12 RZ Scheme

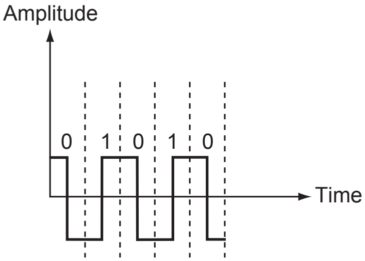


Figure 3.13 Manchester Scheme

- ❑ **Manchester Scheme:** This is a biphase scheme that combines the idea of RZ and NRZ-L schemes. In this scheme, the level of voltage changes at the middle of bit to provide synchronization (Figure 3.13). The low-to-high transition in the middle of a bit indicates 1 while the high-to-low indicates 0. This scheme overcomes the disadvantages of NRZ-L scheme.
- ❑ **Differential Manchester:** This is also a biphase scheme. It combines the idea of RZ and NRZ-I schemes. It is similar to the manchester scheme in the sense that it changes during the middle of a bit but the only difference is that the bit values are determined at the starting of bit. Transition occurs when the next bit is 0; otherwise, no transition occurs (Figure 3.14). This scheme overcomes all the disadvantages of NRZ-I scheme.

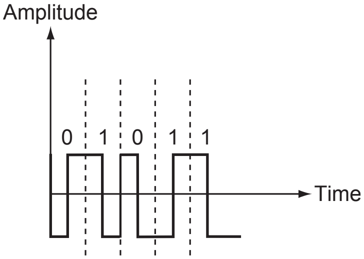


Figure 3.14 Differential Manchester Scheme

Bipolar Scheme

This scheme is similar to RZ encoding scheme and has three levels of voltage. The only difference is that bit 0 is represented by zero level and bit 1 is represented by positive and negative levels of voltage. In bipolar encoding, a stream of bits containing long sequence of binary 0s creates a constant zero voltage. Therefore, bipolar encoding schemes does not have DC component. This scheme is available in two forms, which are as follows:

- **Alternate Mark Inversion (AMI):** This is the most commonly used bipolar coding scheme. It is so called because it involves representation of binary 1s by alternate positive and negative levels of voltages. Here, bit 0 is represented using zero level of voltage (Figure 3.15). This scheme is used for communication between devices placed at a large distance from each other. However, it is difficult to achieve synchronization in this scheme when a continuous stream of bit 0 is present in the data.
- **Pseudoternary:** This scheme is a modification of AMI encoding scheme. In this scheme, binary 1 is represented using zero level of voltage while binary 0s are represented by alternate positive and negative voltages (Figure 3.16).

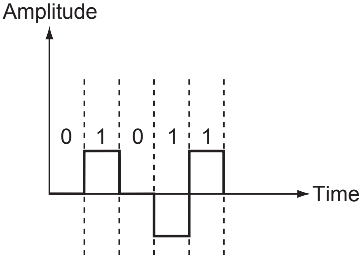


Figure 3.15 AMI Scheme

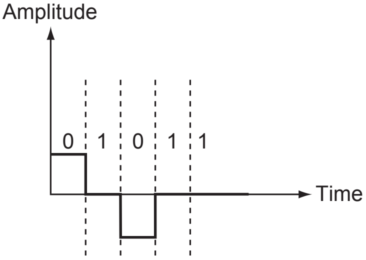


Figure 3.16 Psedoternary Scheme

20. Explain the concept of block coding.

Ans: **Block Coding** is an alternative to line coding scheme that is also used to convert digital data to digital signals. However, it is much better than line coding, as it ensures synchronization and has built-in error detecting capability, which results in better performance than line coding. In this scheme, a three-step process (Figure 3.17) is used to code the digital data.

1. **Division:** The original sequence of bits is divided into blocks or groups of n bits each.
2. **Substitution:** Each n-bit group is replaced with m bits where $m>n$.
3. **Line Coding:** An appropriate line coding scheme is used to combine the m-bit groups to form a stream.

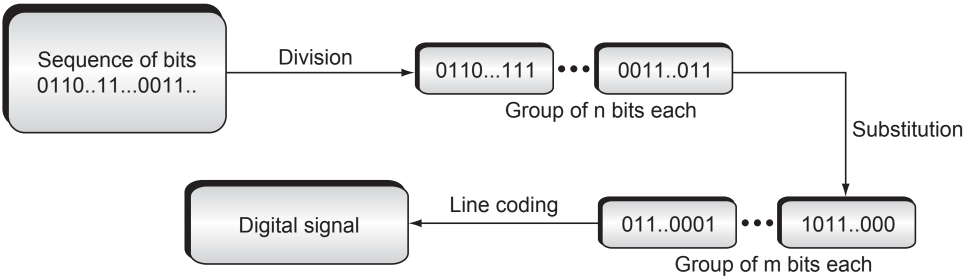


Figure 3.17 Block Coding

The block coding is usually represented as $n\text{B}/m\text{B}$ (n binary/m binary) such as 4B/5B and 5B/6B. For example, in 4B/5B coding, original bit sequence is divided into 4-bit codes and each 4-bit code is replaced with a 5-bit block and then NRZ-I line coding is used to convert 5-bit groups into digital signal.

21. Explain pulse code modulation (PCM) and delta modulation (DM).

Ans: Both PCM and DM are the techniques used to convert analog signal to digital data.

Pulse Code Modulation

This technique involves PCM encoder which encodes analog signal using three steps, namely, *sampling*, *quantization* and *encoding* (Figure 3.18).

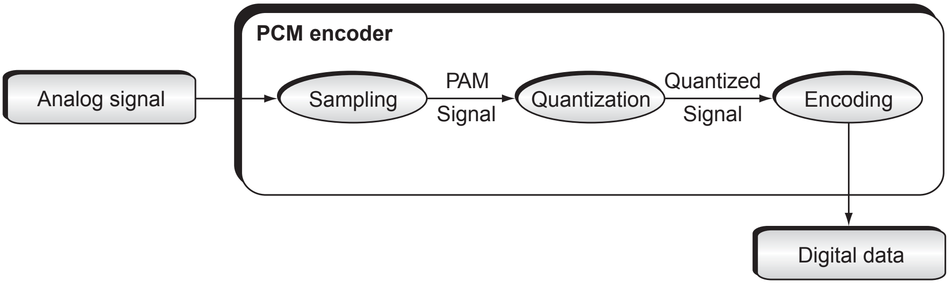


Figure 3.18 PCM Encoding

1. **Sampling:** In this process, the numbers of samples of the original analog signal are taken at regular intervals of time (called **sampling period**). The inverse of sampling period is referred to as **sampling rate**. According to Nyquist theorem**,** the sampling rate should be at least two times of the highest frequency contained in the signal to regenerate the original analog signal at the receiver's end. For example, during the sampling of voice data, with frequency in the range of 400–5,000 Hz, 10,000 samples per second are sufficient for the coding. The sampling process is also termed as **pulse amplitude modulation** (**PAM**) because it produces a **PAM signal**—a series of pulses having amplitude between the highest and the lowest amplitudes of the original analog signal. Sample and hold is the most common sampling method used today for creating flat-top samples.
2. **Quantization:** The sampled PAM pulses may have non-integral values of amplitude which cannot be encoded directly. Thus, the sampled pulses need to be quantized and approximated to integral values using analog-to-digital converter. Considering the original analog signal has amplitudes between $\mathrm{V}_{\mathrm{maximum}}$ and $\mathrm{V}_{\mathrm{minimum}}$, the following steps are used for quantizing the signal.

   i) The range of amplitudes of analog signal is partitioned into L levels or zones each of height h, where

   $$h = (\mathrm{V}_{\mathrm{maximum}} - \mathrm{V}_{\mathrm{minimum}})/\mathrm{L}.$$

   The value of L is chosen depending on the range of amplitudes of the original analog signal as well as the extent of accuracy required in the recovered signal. The signal having more amplitude values require more number of quantization levels.

   ii) The quantized values of 0 to L-1 are assigned at the midpoint of each zone.

   iii) The value of the sample amplitude is approximated to the quantized value.

   Since the output values of the quantization process are only the approximated values, an error known as **quantization error** may occur due to which it may not be possible to recover the original signal exactly. The quantization error also affects the signal-to-noise ratio $(\mathrm{SNR}_{\mathrm{dB}})$ of the signal and the amount of effect depends on the value of L or the number of bits per sample (n_b) as shown in the following formula.

   $$\mathrm{SNR}_{\mathrm{dB}} = 6.02\, n_b + 1.76\ \mathrm{dB}.$$

The effect of quantization error can be minimized by using a process called *companding* and *expanding*. This process uses a compressor before encoding and uses an expander after decoding. **Companding** refers to decreasing the instantaneous voltage amplitude for larger values while **expanding** refers to increasing the instantaneous voltage amplitude for smaller values. This helps to improve the $\mathtt{SNR}_{\mathtt{dB}}$ of the signal.

3. **Encoding:** After quantization, encoding is done in which each sample is converted to m-bit codeword where m is equal to number of bits per sample (n_b). The value of n_b depends on the value of L as shown in the following formula.

$$m = n_b = \log_2 L$$

The relationship between bit rate and the number of bits per sample (n_b) can be expressed as:

$$\text{Bit rate} = n_b \times \text{sampling rate}$$

At the receiver's side, original signal is recovered using PCM decoder which converts the codeword into a staircase signal. The staircase signal is formed by changing the codeword into a pulse that maintains the amplitude till the next pulse. Then, a low-pass filter is used to smoothen the staircase signal into an analog signal. Figure 3.19 depicts this process.

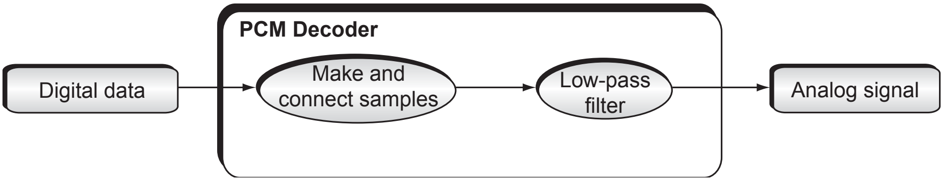


Figure 3.19 PCM Decoding

Delta Modulation

This is an alternative to PCM technique with much reduced quantization error. In this technique, a modulator is used at the sender's side that produces the bits from an analog signal and these bits are sent one after another; only one bit is sent per sample. The modulator generates a staircase signal against which analog signal is compared. At each sampling interval, the amplitude value of analog signal is compared with last amplitude of staircase signal to determine the bit in the digital data. If amplitude of analog signal is smaller, the next bit will be 0. However, if the amplitude of analog signal is greater, the next bit will be 1. Figure 3.20 shows the components of DM.

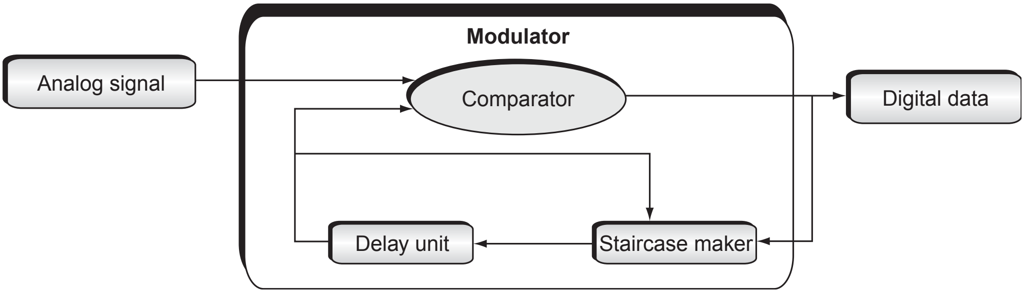


Figure 3.20 Delta Modulation Components

To reproduce analog signal from digital data, **demodulator** is used at the receiver's end. The demodulator uses staircase maker and delay unit to generate analog signal which is then passed through a low-pass filter for smoothing. Figure 3.21 depicts the delta demodulation process

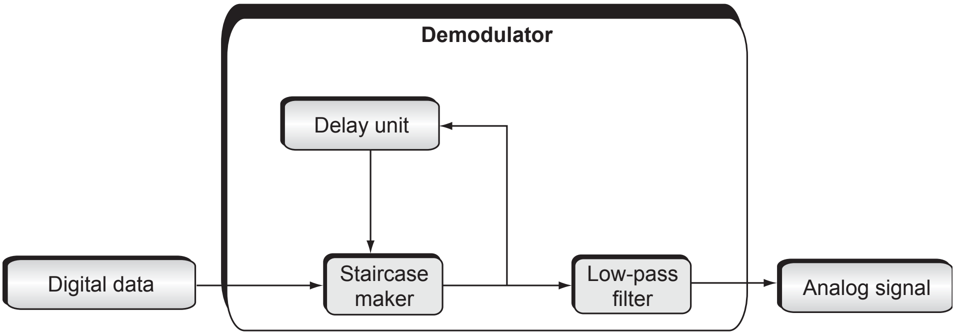


Figure 3.21 Delta Demodulation

22. What are the differences between serial and parallel transmissions?

Ans: The transmission of binary data across a link connecting two or more digital devices can be performed in either of two modes: *serial* and *parallel* (Figure 3.22). There are certain differences between these modes which are listed in Table 3.2.

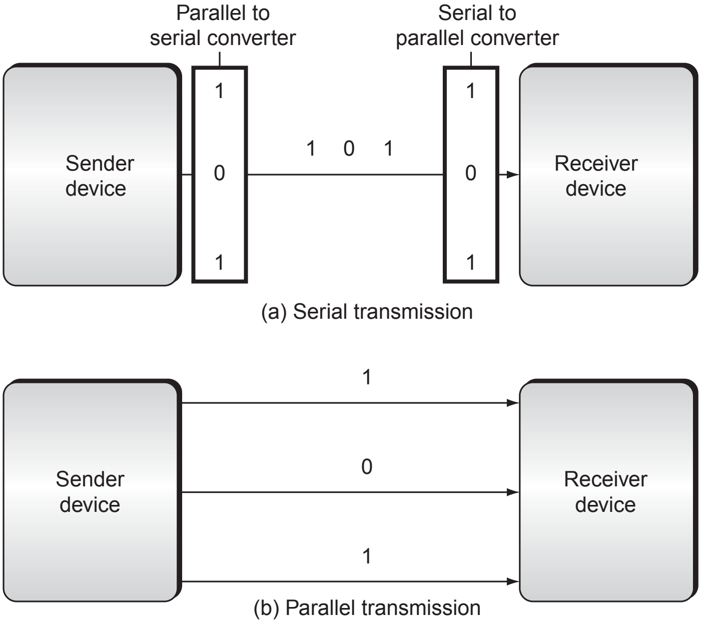


Figure 3.22 Serial and Parallel Transmissions

Table 3.2 Serial and Parallel Transmissions

Serial transmission	Parallel transmission
• The data is transmitted by sending one bit per each clock pulse [see Figure 3.21(a)].	• The stream of bits is divided into groups and one group is sent per each clock pulse [see Figure 3.21(b)].
• It is a slower mode of transmission, as only one bit can be transmitted at a time.	• It is a faster mode of transmission, as several bits can be transmitted at a time.
• It requires only one communication channel between communicating devices; thus, it is a cheaper mode of transmission.	• To send n bits at a time, it requires n communication channel between communicating devices. As a result, cost is increased by a factor of n as compared to serial transmission.
• As communication within devices is parallel, both sender and receiver require converter at the interface between the device and the communication channel. The converter at the interface between sender device and communication channel converts parallel transmission to serial transmission while the converter at the interface between communication channel and receiver device converts serial transmission to parallel transmission.	• No such converters are required.

23. Discuss the three types of serial mode transmissions.

Ans: Serial mode transmission can be classified into three types, namely, *synchronous*, *asynchronous* and *isochronous*.

- **Asynchronous Transmission:** In this transmission, the entire bit stream is divided into groups of 8 bits (that is, one byte) each (Figure 3.23). Each byte is treated independently and transmitted whenever ready regardless of the timer. To let the receiver know about the arrival of a byte, a **start bit**

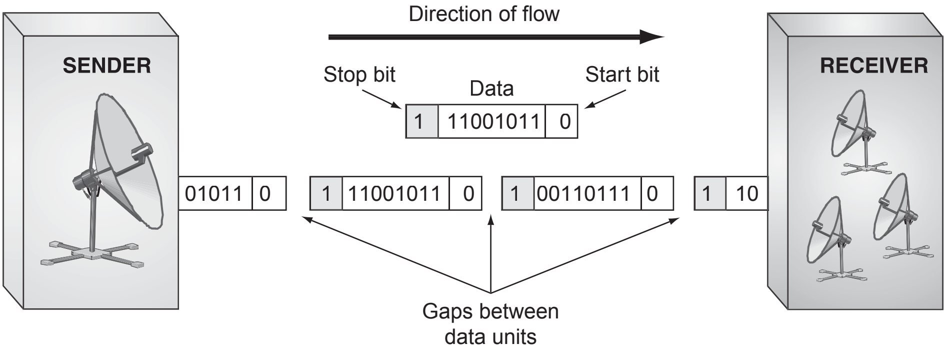


Figure 3.23 Asynchronous Transmission

(usually represented by 0) is added to the starting of each byte. Similarly, one or more **stop bits** (usually represented by 1) are added to indicate the end of each byte. Though the transmission is asynchronous at the byte level, still some synchronization is needed during the transmission of bits within a byte. To achieve this synchronization, the receiver starts the timer after finding the start bit and counts the number of bits until it finds the stop bit. There may be gap between the transmission of two bytes which is filled with a series of stop bits or idle channel. Asynchronous transmission is slow as it adds control information such as start bits, stop bits, and gap between bytes. However, it is a cheaper and effective mode of transmission and thus is suitable for communication between devices which do not demand fast speed.

- **Synchronous Transmission:** In this transmission, timing source is used for synchronization, so that the receiver can receive the information in the order in which it is sent. Multiple bytes are combined together to form **frames**. Data is transmitted as a continuous sequence of 1s and 0s with no gap in between. However, if there is any gap, that gap is filled with a special sequence of 0s and 1s called **idle** (Figure 3.24). At the receiver's end, the receiver keeps counting the bit and separates them into byte groups for decoding. Synchronous transmission is fast as compared to asynchronous transmission, as it does not use any extra bits such as start bits and stop bits. Thus, it is best suitable for applications requiring high speed. However, this transmission cannot be used for real-time applications such as television broadcasting, as there can be uneven delays between the arrival of adjacent frames at the receiver's end which in turn results in poor quality of video.

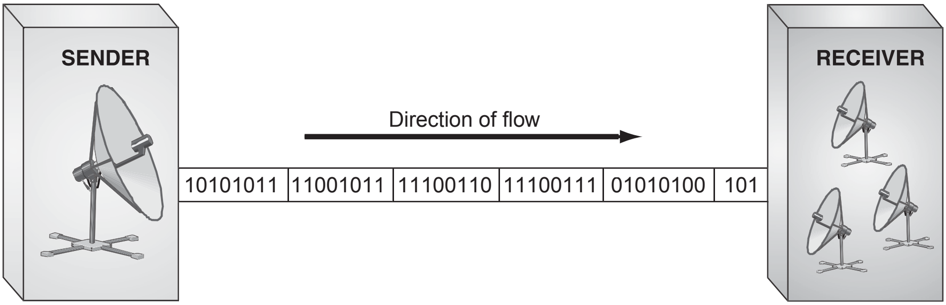


Figure 3.24 Synchronous Transmission

- **Isochronous Transmission:** This transmission provides synchronization in the entire stream of bits and not only at the byte level thereby ensuring the fixed arrival rate of data. This characteristic makes this transmission suitable for real-time applications for which synchronous transmission is not suitable.

24. What do you mean by carrier signal?

Ans: Carrier Signal, also called **carrier frequency**, refers to the high-frequency signal produced by the sender device to which receiver device is tuned and is used as a base for the information signal.

25. Defin digital-to-analog conversion. Discuss various techniques for digital-to-analog conversion.

Ans: The process of changing one or more of the attributes of analog signal based on information in digital data is referred to as **digital-to-analog conversion**. It is also called the **modulation** of a digital signal. Depending on whether the amplitude, frequency or phase of the carrier signal is modified, there are three basic techniques for digital-to-analog conversion, which include *amplitude shift keying* (*ASK*), *frequency shift keying* (*FSK*) and *phase shift keying* (*PSK*). In addition, one more efficient technique for digital-to-analog conversion is *quadrature amplitude modulation* (*QAM*) (explained in **Q27**) that involves changing of both amplitude and phase of the carrier signal.

Amplitude Shift Keying

It involves changing the amplitude of the carrier signal without changing its frequency and phase. The amplitude of a carrier signal is multiplied by binary 0 or 1. A special case of ASK is **binary ASK** (**BASK**), also known as **on-off keying** (**OOK**), where peak amplitude for one binary digit is taken as 0 while the other binary digit has amplitude equal to the peak amplitude of carrier frequency (Figure 3.25). Another variation of ASK is the **multilevel ASK (MFSK)** which involves more than two levels of amplitude.

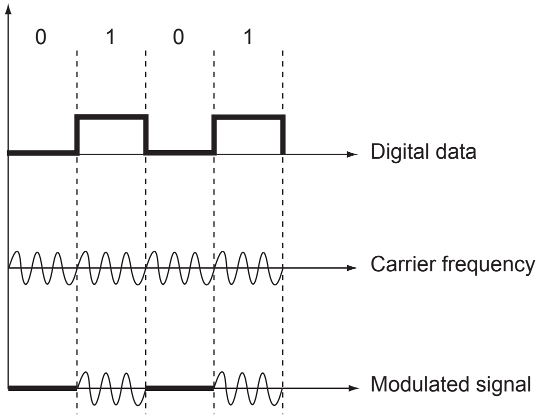


Figure 3.25 Amplitude Shift Keying

The bandwidth (B) for ASK is directly proportional to signal rate (S) as shown in the formula given below:

$$B = (1 + f_c) \times S$$

Here, f_c is the factor whose value lies between 0 and 1 and it depends on the modulation and filtering process

It is clear from the above formula that $B_{min} = S$ (when $f_c = 0$) and $B_{max} = 2 \times S$ (when $f_c = 1$).

Though ASK is the simplest technique, it is highly susceptible to noise and thus is an inefficient modulation technique

Frequency Shift Keying

In this technique, the frequency of the carrier signal is changed without changing its amplitude and phase. The simplest form of FSK is **binary FSK** (**BFSK**) in which two different frequencies (say f_1 and f_2) close to the carrier frequency are taken to represent two binary values in digital data (Figure 3.26).

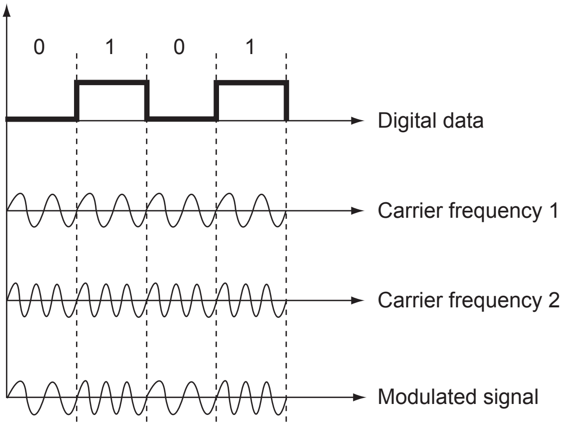


Figure 3.26 Binary Frequency Shift Keying

The bandwidth for BFSK is calculated by the following given formula:

$$B = (1 + f_c) \times S + (f_1 - f_2),$$

where, $f_1 - f_2 = 2\Delta f$

Another variation of FSK is **multilevel FSK (MFSK)** which involves using more than two carrier frequencies. For example, four frequencies can be used to transmit two bits, eight frequencies to transmit three bits and so on. The only requirement is that the distance between any two carrier frequencies should be $2\Delta f$. FSK is less susceptible to noise than ASK and thus is suitable for high-frequency radio transmission.

Phase Shift Keying

In this technique, the phase of the carrier signal is changed without changing its amplitude and frequency. There are two forms of PSK techniques; namely, *binary PSK* (*BPSK*) and *quadrature PSK* (*QPSK*). **BPSK,** also called as **two-level PSK**, uses two phase values. To represent one binary value, the signal is sent with the same phase as that of its predecessor and to represent another binary value; the signal is sent with opposite phase from its predecessor (Figure 3.27). The bandwidth of BPSK is equal to BASK, but less than that for BFSK.

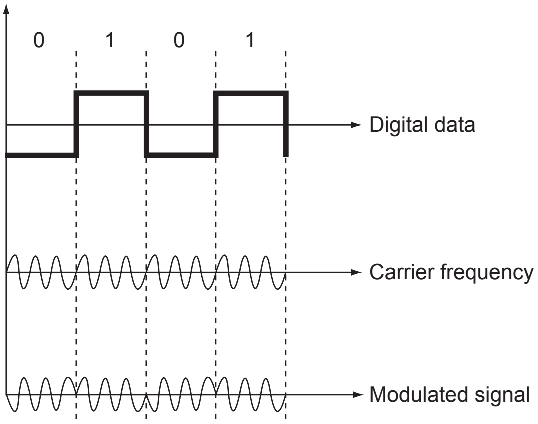


Figure 3.27 Binary Phase Shift Keying

QPSK, also called as **four-level PSK**, offers an efficient use of bandwidth by using two bits at a time in each signal element. It is so called, because it involves two BPSK modulations of which one is in-phase and another is out-of-phase (quadrature). In this technique, the stream of bits is first passed through a converter which converts serial transmission into parallel transmission and then, one bit is transmitted to in-phase modulator and other bit is transmitted to out-of-phase modulator. Both modulators produce composite signals which have the same frequency but different phases. When these signals are combined, the resultant signal may involve one of four different phases: 45°, –45°, 135° and –135°.

PSK is more commonly used than ASK and FSK. It is less susceptible to noise than ASK as phase is not likely to be affected easily by the noise. Moreover, it does not require two carriers as required in FSK.

26. What is constellation diagram? Explain with a suitable example.

Ans: Constellation Diagram is a 2D diagram used to define the amplitude and phase of a signal element especially in the cases where two carrier signals (one in-phase and other quadrature) are being used. The horizontal axis of the diagram represents the in-phase carrier while the vertical axis represents the quadrature carrier signal (Figure 3.28). Each signal element is represented by a point (black dot) with bit or combinations of bits written next to it. The projection of the point on the horizontal axis defines the peak amplitude of in-phase component while the projection of point on the vertical axis defines the peak amplitude of the quadrature component. The line joining the point to origin indicates the peak amplitude of signal element and the angle that this line makes with the horizontal axis indicates the phase of the signal element.

For example, the constellation diagram for QPSK as discussed in previous question may involve four phases as shown in Figure 3.29.

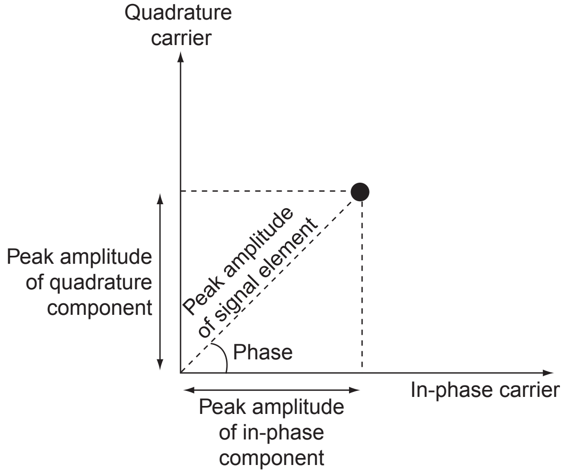

Quadrature carrier
Peak amplitude of quadrature component
Peak amplitude of signal element
Phase
In-phase carrier
Peak amplitude of in-phase component

Figure 3.28 Constellation Diagram

Bits	Phase
00	45°
01	135°
10	–135°
11	–45°

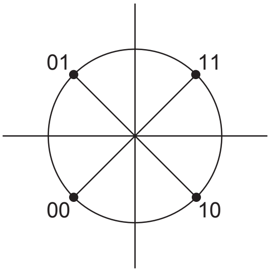


Figure 3.29 Constellation Diagram for QPSK Signal

27. Write a short note on quadrature amplitude modulation (QAM).

Ans: QAM technique combines the idea of ASK and PSK. That is, instead of changing only one attribute of a carrier, two attributes including amplitude and phase of the carrier signal are changed. Like QPSK, it uses two carriers (one is in-phase and the other is quadrature) with different amplitude levels. Figure 3.30 shows the constellation diagram of a QAM signal with two amplitude levels and four phases.

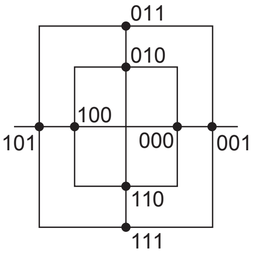


Figure 3.30 Constellation Diagram for QAM Signal

The minimum bandwidth required by QAM is equal to that for ASK and PSK. It is less susceptible to noise than ASK as well as does not require two carriers as required in FSK.

28. Define analog-to-analog conversion. Discuss various techniques for analog-to-analog conversion.

Ans: The process of representing analog data by analog signal is known as **analog-to-analog conversion** (also called **analog modulation**). The techniques used for analog-to-analog conversion include *amplitude modulation* (*AM*), *frequency modulation* (*FM*) and *phase modulation* (*PM*).

Amplitude Modulation

In this modulation, the amplitude of a carrier wave is varied in accordance with the characteristic of the modulating signal. The frequency of the carrier remains the same, only the amplitude changes to follow variations in the signal. In simpler words, the two discrete binary digits (0 and 1) are represented by two different amplitudes of the carrier signal. Figure 3.31 depicts how the modulating signal is superimposed over the carrier signal that results in an amplitude-modulated signal.

The bandwidth of the amplitude-modulated signal is twice of that of modulating signal. That is,

$$B_{AM} = 2B,$$

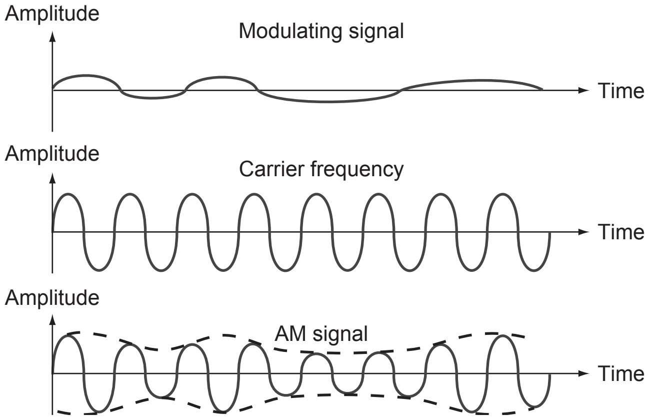


Figure 3.31 Amplitude Modulation

where B = bandwidth of modulating signal.

Frequency Modulation

In this modulation, the instantaneous frequency of carrier wave is caused to depart from the centre frequency by an amount proportional to the instantaneous value of the modulating signal. In simple words, FM is the method of impressing modulating signal onto a carrier signal wave by varying its instantaneous frequency rather than its amplitude (Figure 3.32).

The total bandwidth that is needed for the frequency-modulated signal can be calculated from the below-given formula.

$$B_{FM} = 2\ (1 + \beta)\ B,$$

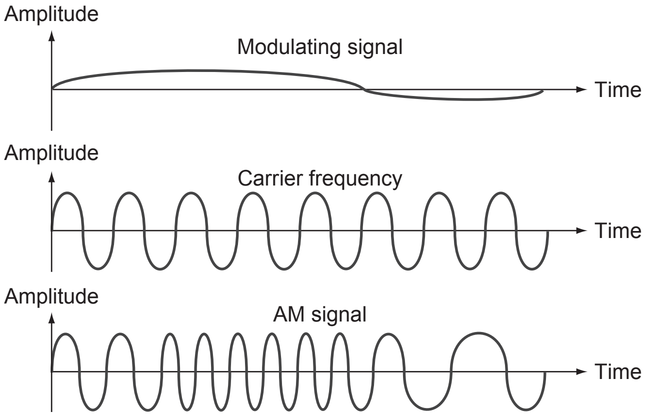


Figure 3.32 Frequency Modulation

where β is a factor whose value depends on the modulation technique with a common value of 4 and β is the bandwidth of modulating signal.

Phase Modulation

This is the encoding of information into a carrier wave by variation of its phase in accordance with an input signal. In this modulation technique, the phase of sine wave carrier is modified according to the amplitude of the message to be transmitted (Figure 3.33).

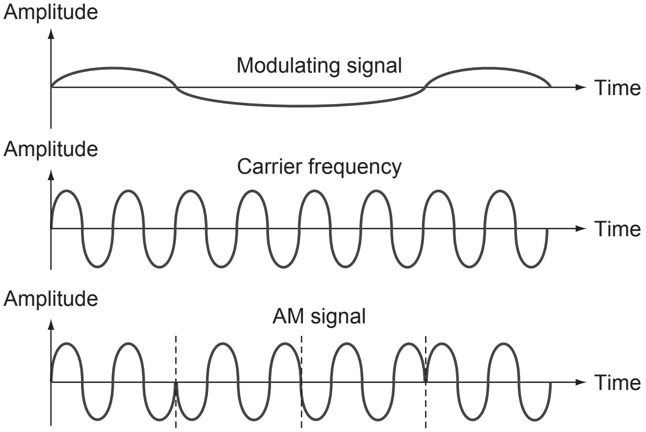


Figure 3.33 Phase Modulation

The total bandwidth that is needed by a PM signal can be calculated from the bandwidth and maximum amplitude of the modulating signal as shown here.

$$B_{PM} = 2\ (1 + \beta)\ B,$$

where β is a factor whose value is lower in PM than FM. For narrowband, its value is 1 and for wideband, its value is 3. B is the bandwidth of modulating signal.

29. What does a decibel (dB) measure? Give example.

Ans: Decibel (dB) is a measure of comparative strength of two signals or one signal at two different points. It is used by engineers to determine whether the signal has lost or gained strength.

The positive value of a signal indicates gain in strength while negative value indicates that the signal is attenuated.

$$dB = 10\ \log_{10}(P_2/P_1),$$

where P_1 and P_2 are the powers of signal at two different points or the powers of two different signals.

30. For the following frequencies, calculate the corresponding periods. Write the result in seconds (s), milliseconds (ms) and microseconds (μs): 24 Hz; 8 MHz.

Ans: As frequency = 1/period. Thus, for frequency 24 Hz, period = 1/24 s = 0.041 s

$$\text{As } 1\text{ s} = 10^3\text{ ms} \Rightarrow 0.041\text{ s} = 0.041 \times 10^3 = 41\text{ ms}$$
$$\text{As } 1\text{ s} = 10^6\ \mu\text{s} \Rightarrow 0.041\text{ s} = 0.041 \times 10^6 = 41000\ \mu\text{s}.$$

Similarly, for frequency 8 MHz, period = 1/8000000 s = 0.000000125 s

$$0.000000125 \times 10^3 \text{ ms} = 0.000125 \text{ ms}$$
$$0.000000125 \times 10^6 \ \mu\text{s} = 0.125 \ \mu\text{s}.$$

31. A sine wave completes one cycle in 25 microseconds. What is its frequency? Express the frequency in hertz.

Ans: Frequency = 1/period. Here, period = 25 µs = 25 × 10^{-6} s.
Therefore, frequency = $10^6/25$ = 40000 Hz.

32. A digital signal has a bit interval of 40 microseconds. What is the bit rate? Express the bit rate in kbps.

Ans: Bit rate = number of bit intervals per second. Therefore, bit rate = 1/(40 × 10^{-6}) = 25000 bps.
⇒ Bit rate = 25 kbps.

33. A signal has a bandwidth of 30 Hz. The highest frequency is 80 Hz. What is its lowest frequency? Draw the spectrum if the signal contains all the frequency of same amplitude.

Ans: Bandwidth = the highest frequency – the lowest frequency. Bandwidth = 30 Hz (given). The highest frequency = 80 Hz. Thus, the lowest frequency = 80–30 = 50 Hz. The spectrum of the signal containing all the frequencies of same amplitude is shown in Figure 3.34.

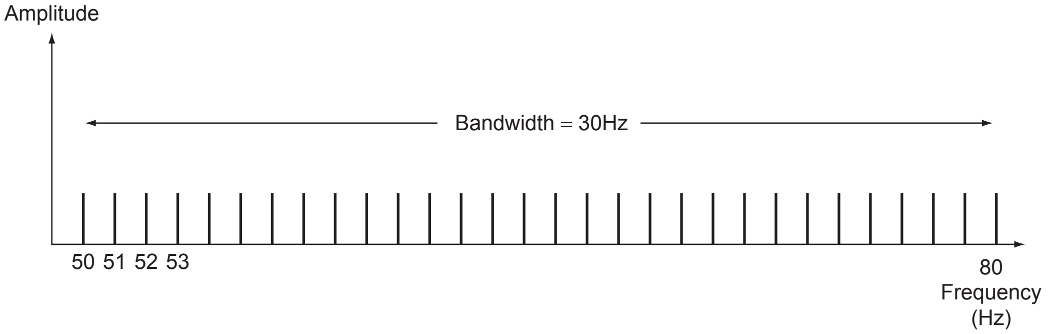


Figure 3.34 Spectrum of a Signal

34. An image has the size of 1024 × 786 pixel with 256 colours. Assume the image is uncompressed. How does it take over a 56-kbps modem channel?

Ans: To represent 256 colours, we need $\log_2 256$ = 8 bits. Therefore, the total number of bits that are to be transmitted will be equal to 1024 × 786 × 8 = 6438912 bits. Thus, bit rate = 6438912/(56 × 1000) = 115 bps.

35. An analog signal carries four bits in each signal element. If 1000 signal elements are sent per second, fin the baud rate and bit rate.

Ans: Baud rate = the number of signal elements per second = 1000. As we know that baud rate = bit rate × (1/number of data elements carried in one signal element). Bit rate = 1000 × 4 = 4000 bps.

36. The power of a signal is 10 mW and the power of the noise is 1 μW. What is the value of SNR in dB?

Ans: SNR = signal power/noise power. Thus, SNR = $(10 \times 10^{-3})/(1 \times 10^{-6})$ = 10,000.

$SNR_{dB} = 10 \log_{10} SNR = 10 \log_{10} 10000 = 10 \times 4 = 40$.

37. Calculate the highest bit rate for a telephone channel, given the bandwidth of a line to be 3000 Hz and the SNR being 35 dB.

Ans: As $SNR_{dB} = 10 \log_{10} SNR$. SNR = $10^{(SNR_{dB}/10)} = 10^{3.5}$ = 3162 (rounded off). According to Shannon's capacity, The highest bit rate = bandwidth × $\log_2 (1 + SNR)$. Therefore, the highest bit rate = $3000 \log_2 (1 + 3162) = 3000 \times \log_2 3163 = 3000 \times 11.6 = 34800$ bps.

38. What is the Nyquist minimum sampling rate for the following?

(a) A complex low-pass signal with a bandwidth of 300 kHz.

Ans: According to Nyquist theorem, the sampling rate is two times of the highest frequency in the signal. As the frequency of a low-pass signal starts from zero, the highest frequency in the signal = bandwidth; that is, 300 kHz. Thus, sampling rate = 2 × 300 kHz = 600000 samples per second.

(b) A complex bandpass signal with a bandwidth of 300 kHz.

Ans: The sampling rate cannot be found in this case because we do not know the maximum frequency of the signal.

(c) A complex bandpass signal with bandwidth of 300 kHz and the lowest frequency of 100 Hz.

Ans: The highest frequency = 100 +300 = 400 kHz. Thus, sampling rate = 2 × 400 kHz = 800000 samples per second.

39. What is the maximum bit rate for a noiseless channel with a bandwidth of 6000 Hz transmitting a signal with four signal levels?

Ans: Bit rate = 2 × channel bandwidth × $\log_2$ (number of signal levels). Therefore, bit rate = $2 \times 6000 \times \log_2 4$ = 24000 bps.

40. What is the total delay (latency) for a frame size of 10 million bits that is being set up on a link with 15 routers, each having a queuing time of 2 μs and a processing time of 1 μs? The length of link is 3000 km. The speed of light inside the link is 2×10^8 m/s. The link has bandwidth of 6 Mbps.

Ans: Here, propagation time = distance / propagation speed

$$\Rightarrow (3000 \times 1000)/(2 \times 10^8) = 1.5 \times 10^{-2} \text{ s.}$$

Transmission time = message size / bandwidth

$$\Rightarrow (10 \times 10^6)/(6 \times 10^6) = 1.7 \text{ s (approx).}$$

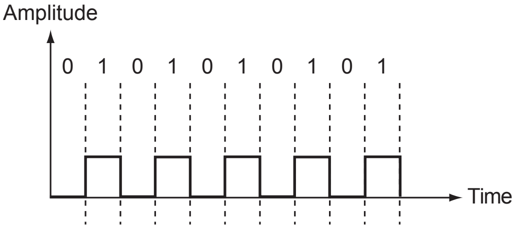
As there are 15 routers, total queuing time = $15 \times 2 \times 10^{-6} = 30 \times 10^{-6}$ s.
Processing time = $15 \times 1 \times 10^{-6} = 15 \times 10^{-6}$ s. Now, latency = propagation time + transmission time + queuing time + processing time

$$\Rightarrow 1.5 \times 10^{-2} + 1.7 + 30 \times 10^{-6} \text{ s} + 15 \times 10^{-6} \text{ s} = 1.715045 \text{ s.}$$

41. A data stream is made of 10 alternating 0s and 1s. Encode this stream using the following encoding schemes.

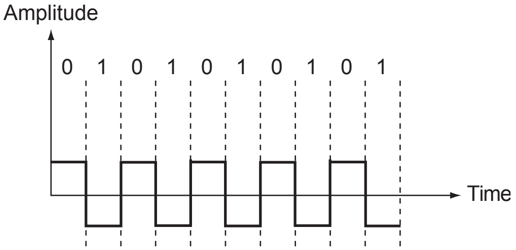
(a) Unipolar

Ans:



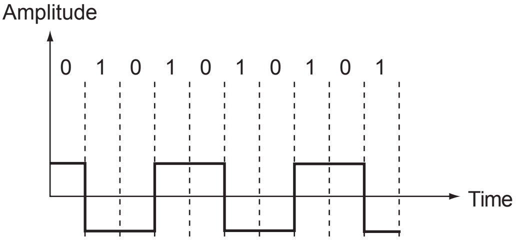
(b) Polar NRZ-L

Ans:



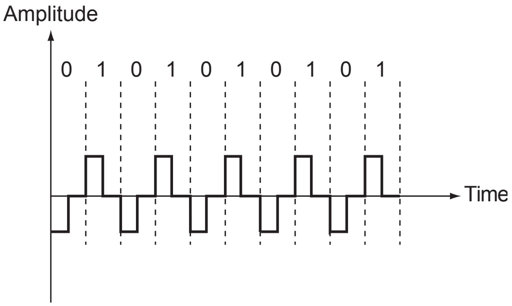
(c) NRZ-I

Ans:



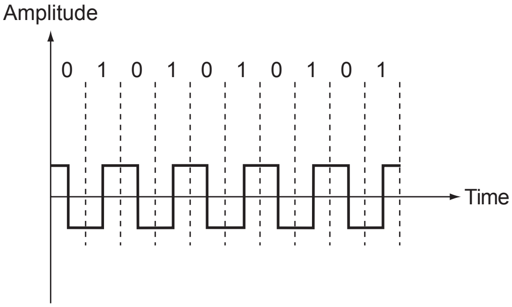
(d) RZ

Ans:



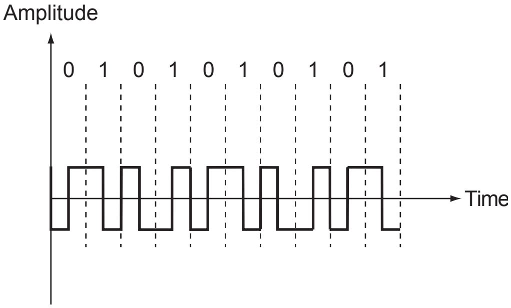
(e) **Manchester**

Ans:

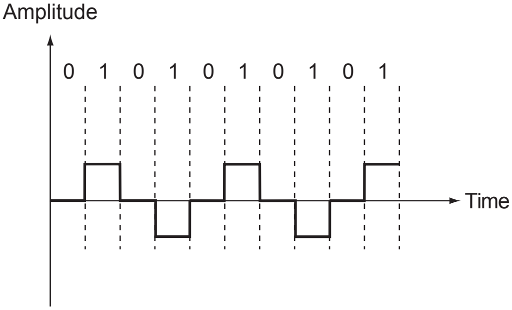


(f) **Differential Manchester**

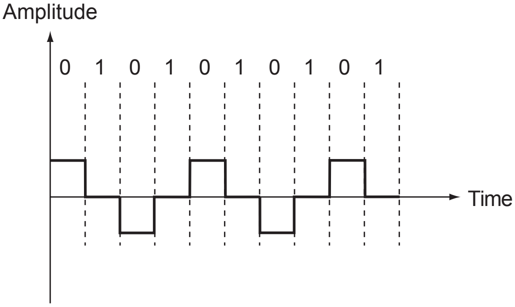
Ans:



(g) **AMI**



(h) **Pseudoternary**



42. A signal is quantized using 10-bit PCM. Find the SNR in dB.

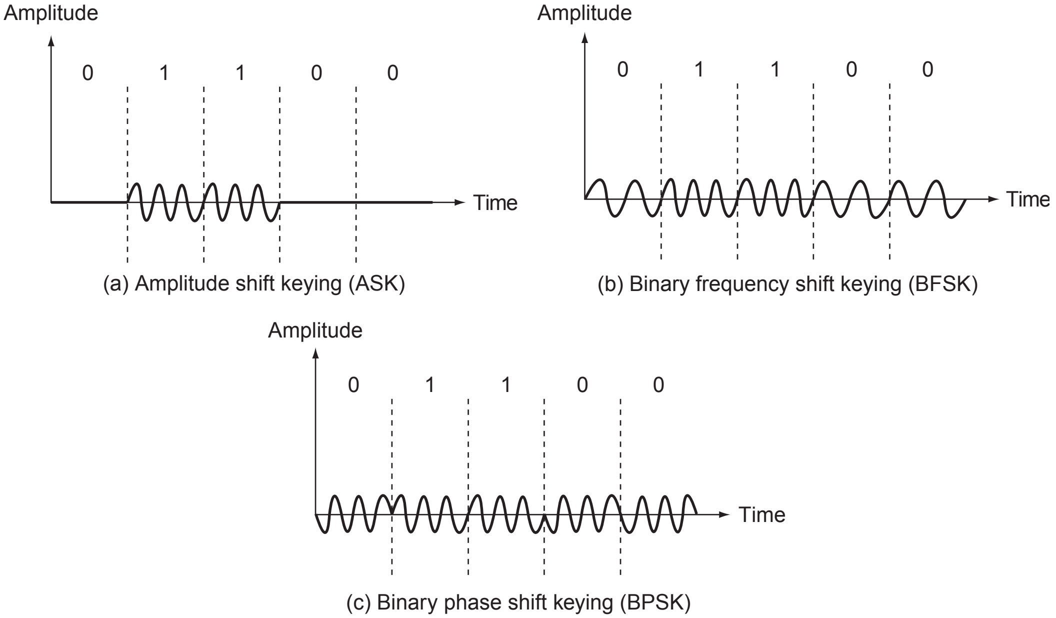
Ans: $SNR_{dB} = 6.02\ n_b + 1.76$. Here, n_b is the number of bits used for quantization = 10. Thus, $SNR_{dB} = 6.02 \times 10 + 1.76 = 61.96$ dB.

43. A system is designed to sample analog signals, convert them to digital form with a 4-bit converter, and transmit them. What bit rate is required if the analog signal consists of frequencies between 400 Hz and 3400 Hz.

Ans: Bandwidth = 3400 – 400 = 3000 Hz. Bit rate = $2 \times \text{bandwidth} \times \log_2 L = 2 \times 3000 \times \log_2 4$
$\Rightarrow 2 \times 2 \times 3000 = 12000$ bps = 12 kbps.

44. Given the bit pattern 01100, encode this data using ASK, BFSK, and BPSK.

Ans: Bit pattern 01100 can be encoded using ASK, BFSK and BPSK as shown in Figure 3.35(a), 3.35 (b) and 3.35 (c), respectively.



(a) Amplitude shift keying (ASK)

(b) Binary frequency shift keying (BFSK)

(c) Binary phase shift keying (BPSK)

Figure 3.35 Encoding of Bit Pattern Using ASK, BFSK and BPSK

45. Find the maximum bit rate for an FSK signal if the bandwidth of the medium is 12,000 Hz and the difference between the two carriers must be at 2000 Hz. Transmission is in full-duplex mode.

Ans: As we know that in FSK, bandwidth = $(1 + f_c)$ × signal rate + difference between carrier frequencies.

$$\Rightarrow 12000 = (1 + 1) \times \text{signal rate} + 2000$$
$$\Rightarrow \text{Signal rate} = 5000 \text{ baud.}$$

Now, as we know that signal rate = bit rate × (1/r). For FSK, one data element is carried by one signal element, that is, r = 1

$$\Rightarrow \text{Bit rate} = 4000 \text{ kbps.}$$

46. Find the bandwidth for the following situations if we need to modulate a 5-kHz voice.

(a) AM

Ans: $B_{AM} = 2 \times B = 2 \times 5 = 10$ kHz.

(b) PM (set $\beta = 5$)

Ans: $B_{FM} = 2 \times (1 + \beta) \times B = 2 \times (1 + 5) \times 5 = 60$ kHz.

(c) PM (set $\beta =1$)

Ans: $B_{PM} = 2 \times (1 + \beta) \times B = 2 \times (1 + 1) \times 5 = 20$ kHz.

Multiple Choice Questions

1. Which of the following is a characteristic of an analog quantity?
   (a) Changes in quantity are represented by discrete values.
   (b) Its values follow a logarithmic response curve.
   (c) It can be described with a finite number of steps.
   (d) It has a continuous set of values over a given range.

2. In which of the following form data has to be transformed so that it can be transmitted.
   (a) Electromagnetic signals
   (b) Aperiodic signals
   (c) Low-frequency sine waves
   (d) None of these

3. A sine wave is
   (a) Periodic and continuous
   (b) Aperiodic and continuous
   (c) Periodic and discrete
   (d) Aperiodic and discrete

4. What is the bandwidth of a signal that ranges from 200 MHz to 500 MHz?
   (a) 400 MHz (b) 100 MHz
   (c) 300 MHz (d) None of these

5. A sine wave has a frequency of 8 kHz. What is its period?
   (a) 124 microseconds
   (b) 150 microseconds
   (c) 125 microseconds
   (d) 156 microseconds

6. Shannon's noisy channel capacity theorem states that $C = B \log_2 (1+ SNR)$ bps. In this equation, B stands for
   (a) Bandwidth of the signal
   (b) Bandwidth of the channel
   (c) Strength of the signal
   (d) None of these

7. In which of the following encoding schemes three levels of voltage are used?
   (a) Unipolar (b) Polar
   (c) Bipolar (d) None of these

8. In differential manchester encoding, transition at the middle of the bit is used for
   (a) Bit transfer (b) Synchronization
   (c) Baud transfer (d) None of these

9. In which of the following schemes change or lack of change in the value of voltage determines the value of bit
   (a) NRZ-I (b) NRZ-L
   (c) Both (a) and (b) (d) None of these

10. A 6-MHz analog video signal can be sampled and later reconstructed if it was sampled at a rate of at least (in *M* samples/s)?
    (a) 3 (b) 6
    (c) 12 (d) 9

11. One factor in the accuracy of a reconstructed PCM signal is the
    (a) Signal bandwidth
    (b) Carrier frequency
    (c) Number of bits used for quantization
    (d) Baud rate

12. Amplitude modulation is a technique used for
    (a) Analog-to-digital conversion
    (b) Digital-to-analog conversion
    (c) Analog-to-analog conversion
    (d) Digital-to-digital conversion

13. Which of the following factors of a carrier frequency is varied in QAM?
    (a) Frequency (b) Amplitude
    (c) Phase (d) Both (b) and (c)

14. How many carrier frequencies are used in BFSK?
    (a) 2 (b) 1
    (c) 0 (d) None of these

15. How many dots are present in the constellation diagram of 8-QAM?
    (a) 4
    (b) 8
    (c) 16
    (d) None of these

Answers

1. (d) 2. (a) 3. (a) 4. (c) 5. (c) 6. (b) 7. (c) 8. (b) 9. (b) 10. (c)
11. (c) 12. (c) 13. (d) 14. (a) 15. (b)

4

Transmission Media

1. What are transmission media? What are the different categories of transmission media?

Ans: Transmission media refer to the media through which data can be carried from a source to a destination. Data is transmitted from one device to another through electromagnetic signals. Transmission media are located under and controlled by the physical layer as shown in Figure 4.1.

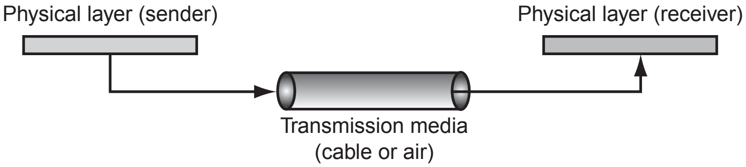


Figure 4.1 Transmission Media and Physical Layer

The different categories of transmission media include *guided* (or *wired*) and *unguided* (or *wireless*) media as shown in Figure 4.2. **Guided transmission media** use a cabling system that guides the data signals along a specific path. It consists of a cable composed of metals such as copper, tin or silver. The data signal in guided medium is bound by the cabling system; hence, the guided medium is also known as **bound medium**. There are three basic types of guided transmission media: twisted-pair cable, coaxial cable and fibre-optic cable

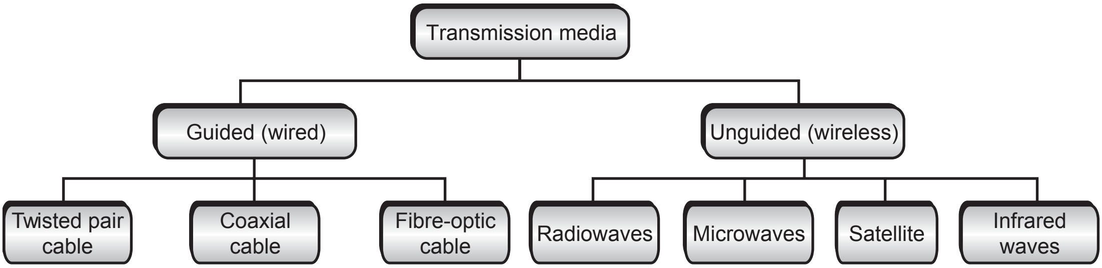


Figure 4.2 Categories of Transmission Media

Unguided transmission media facilitate data transmission without the use of a physical conduit. The electromagnetic signals are transmitted through earth's atmosphere (air, water or vacuum) at a much faster rate covering a wide area. The electromagnetic waves are not guided or bound to a fixed channel to follow. There are basically four types of unguided transmission media including radio waves, microwaves, satellite transmission and infrared waves.

2. Differentiate guided and unguided transmission media.

Ans. In order to transmit a message or data from a source to a destination, we need a transmission medium. Transmission medium can be broadly classified into two categories, which are guided and unguided media. The differences between these two transmission media are listed in Table 4.1.

Table 4.1 Differences Between Guided and Unguided Media

Guided media	Unguided media
• Signal is transmitted by establishing a physical path between the source and destination.	• No physical path is established between the source and destination; signals are propagated through air.
• Signals propagate in the form of current or voltage.	• Signals propagate in the form of electromagnetic waves.
• Guided media are well suited for point-to-point communication.	• Unguided media are well suited for broadcast communication.
• Examples of guided media are twisted-pair cables, coaxial cables and fibre-optic cables.	• Examples of unguided media are microwave satellites, infrared waves and radio waves.

3. Write in short the design factors for a data transmission system.

Ans: The major concerns during the design of a data transmission system are achieving a higher data rate and covering maximum transmission distance. The key design factors that affect the data rate and transmission distance are as follows:

❑ **Bandwidth:** The greater the bandwidth of the signal is, the higher will be the data rate.

❑ **Transmission Impairments:** Impairments such as attenuation, limit the transmission distance and hence, they are undesirable.

❑ **Interference:** Different signals in overlapping frequency bands result in interference which can distort or cancel out a signal. Interference is a major issue with unguided media but it also affects the guided media.

❑ **Number of Receivers:** In a guided medium, as the number of receivers on a shared link increases, more attenuation and distortion are introduced which limit the distance and/or data rate.

4. Explain in detail the various types of guided transmission media.

Ans: There are three basic types of guided media—*twisted-pair cable*, *coaxial cable* and *fibre-optic cable*.

Twisted-pair Cable

It is one of the most common and least expensive transmission media. A twisted-pair cable consists of two insulated copper conductors that are twisted together forming a spiral pattern. A number of such pairs are bundled together into a cable by wrapping them in a protective shield. One of the wires in each twisted pair is used for receiving data signal and another for transmitting data signal. Twisted pairs are used in short-distance communication (less than 100 metres). The biggest network in the world, the telephone network, originally used only twisted-pair cabling and still does for most local connections. A twisted-pair cable has the capability of passing a wide range of frequencies. However, with the increase in frequency, attenuation also increases sharply. As a result, the performance of a twisted-pair cable decreases with the increase in frequency. A twisted-pair cable comes in two forms: unshielded and shielded with a metal sheath or braid around it. Accordingly, they are known as *unshielded twisted-pair* (*UTP*) and *shielded twisted-pair* (*STP*) cables.

- **UTP Cable:** This cable has four pairs of wires inside the jacket (Figure 4.3). Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting is, the higher will be the supported transmission rate and greater will be the cost per foot. Each twisted pair consists of two metal conductors (usually copper) that are insulated separately with their own coloured plastic insulation. UTP cables are well suited for both data and voice transmissions; hence, they are commonly used in telephone systems. They are also widely used in DSL lines, 10Base-T and 100Base-T local area networks.

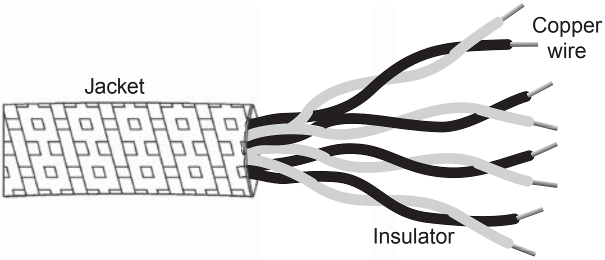


Figure 4.3 UTP Cable

- **STP Cable:** This cable has a metal foil or braided-mesh covering that covers each pair of insulated conductors (Figure 4.4). The metal foil is used to prevent infiltration of electromagnetic noise. This shield also helps to eliminate crosstalk. An advantage of STP cables over UTP cables is that they are suitable for the environments with electrical interference. In addition, they provide better performance at higher data rates. However, the extra shielding makes the STP cables quite bulky and more expensive than UTP cables.

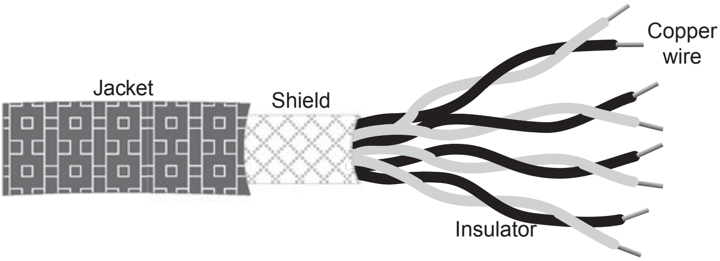


Figure 4.4 STP Cable

Coaxial Cable

Coaxial cables (or **coax**) have a single central conductor, which is made up of solid wire (usually, copper) (Figure 4.5). This conductor is surrounded by an insulator over which a sleeve of metal mesh is woven to block any outside interference. This metal mesh is again shielded by an outer covering of a thick material (usually PVC) known as **jacket**.

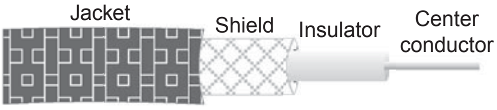


Figure 4.5 Coaxial Cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. It can support greater cable lengths between network devices and can offer greater bandwidth than twisted-pair cable. However, attenuation in coaxial cables is much higher as compared to twisted-pair cables due to which the signal weakens rapidly. As a result, repeaters are to be used frequently to boost up the signals. Coaxial cables are capable of transmitting data at a fast rate of 10Mbps. Some of the applications that use coaxial cables include analog and digital telephone networks, cable TV networks, Ethernet LANs, and short range connections.

Fibre-optic Cable

Fibre-optic cable or **optical fib e** consists of thin glass fibres that can carry information in the form of visible light. The typical optical fibre consists of a very narrow strand of glass or plastic called the **core**. Around the core is a concentric layer of less dense glass or plastic called the **cladding**. The core diameter is in the range of 8–50 microns (1 micron = 10^{-6} metres) while cladding generally has a diameter of 125 microns. The cladding is covered by a protective coating of plastic, known as **jacket** (see Figure 4.6).

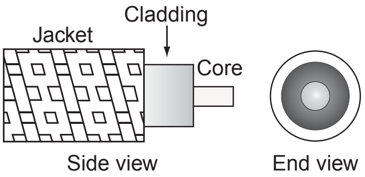


Figure 4.6 Optical Fibre

Optical fibres transmit a beam of light by means of **total internal reflectio** . When a light beam from a source enters the core, the core refracts the light and guides the light along its path. The cladding reflects the light back into the core and prevents it from escaping through the medium (see Figure 4.7). These light pulses, which can be carried over long distances via optical fibre cable at a very high speed, carry all the information

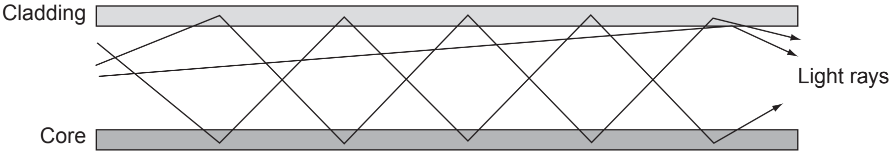


Figure 4.7 Signals Carried over an Optical Fibre

Optical fibre has the capability to carry information at greater speeds, higher bandwidth and data rate. A single optical fibre can pack hundreds of fibres, where each fibre has the capacity equivalent to that of thousands of twisted-pair wires. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. In addition, fibre optic cables offer lower attenuation and superior performance and require fewer repeaters as compared to coaxial and twisted-pair cables. The major applications of the fibre-optic cables are cable TV, military applications, long-haul trunks, subscriber loops, local area networks, metropolitan trunks and rural trunks.

5. Why twisting of wires is necessary in twisted-pair cables?

Ans: Twisting is done in twisted-pair cables because it tends to minimize the interference (noise) between the adjacent pair of wires in cable thereby reducing the crosstalk. In case the two wires are parallel, they may not get affected equally by the electromagnetic interferences (noise and crosstalk) from nearby sources due to their different locations relative to the source. As a result, the receiver would receive some unwanted signals. On the other hand, if the wires are twisted, both wires are probable to be get affected equally by the external interferences thereby maintaining a balance at the receiver. To understand, suppose in one twist, one of the twisted wires is closer to noise source and the other is farther, then in the next twist, the opposite will be true. As a result, the unwanted signals of both the wires cancel out each other and the receiver does not receive any unwanted signal. Thus, crosstalk is reduced.

6. What are the different categories and connectors of UTP cables?

Ans: As per the standards developed by the Electronic Industries Association (EIA), UTP cables have been classified into seven categories, from 1 to 7. Each category is based on the quality of the cable and the higher number denotes higher quality. Table 4.2 lists the categories of UTP cables along with their specification and data rate

To connect UTP cables to network devices, UTP connectors are required. The most common connector for the UTP cables is RJ45 (RJ stands for **registered jack**) as shown in Figure 4.8. Being a keyed connector, the RJ45 can be inserted in only one way.

Table 4.2 Categories of UTP Cables

Category (CAT)	Specification	Data rate (in Mbps)
1	UTP cables used in telephones	<0.1
2	UTP cables used in T-lines	2
3	Improved CAT2 used in LANs	10
4	Improved CAT3 used in token ring network	20
5	Cable wire is normally 24AWG with a jacket and outside sheath; used in LANs	100
5E	Extension to category 5 that reduces crosstalk and interference; used in LANs.	125
6	A new category with matched components coming from the same manufacturer. This cable must be tested at a data rate of 200 Mbps. This is used in LANs.	200
7	This is the shielded screen twisted-pair cable (SSTP). Shielding increases data rate and reduces crosstalk effect. This cable is used in LANs.	600

7. What are the different categories and connectors of coaxial cables?

Ans: According to the ratings provided by radio government (RG), the coaxial cables have been divided into three categories. Each category has a specific RG number that indicates a unique set of physical specifications. These specifications include the wire gauge of inner conductor, shield, type and size of outer casing and type and thickness of inner insulator. Different categories of the coaxial cables are listed in Table 4.3.

To connect coaxial cables to other devices, coaxial connectors are required. The three most popular coaxial connectors include the *BNC connector*, *BNC*

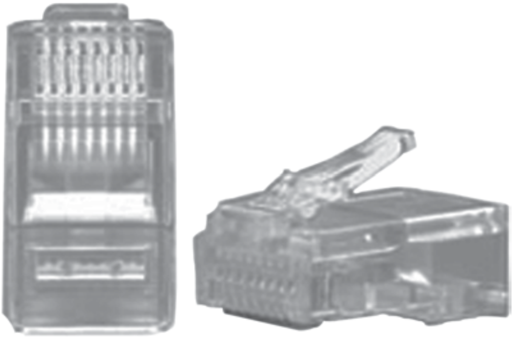
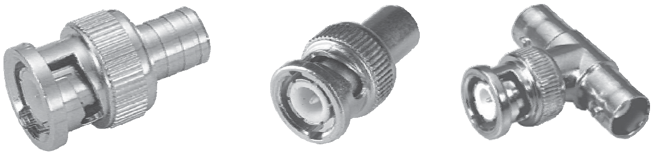


Figure 4.8 RJ45 UTP Connector

Table 4.3 Categories of Coaxial Cables

Category	Use	Impedance
RG-59	Cable TV	75 Ω
RG-58	Thin Ethernet	50 Ω
RG-11	Thick Ethernet	50 Ω

terminator and *BNC T connector* as shown in Figure 4.9. The **Bayone-Neill-Concelman** (**BNC**) connector is the most commonly used connector that connects the coaxial cable to a device such as an amplifier or television set. The **BNC terminator** is used at the end of the cable to prevent the reflection of the signal and the **BNC T** connector is often used in Ethernet networks for branching out connections to other devices.



BNC connector BNC terminator BNC T

Figure 4.9 Coaxial Cable Connectors

8. Explain the different fibre-optic propagation modes.

Ans: Fibre-optic cables support two modes for propagating light, which are *multimode* and *single mode*. Each mode requires fibre with different physical characteristics.

Multimode Propagation

In this mode, many beams from a light source traverse the fibre along multiple paths and at multiple angles as shown in Figure 4.10(a). Depending upon the structure of core inside the cable, multimode can be implemented in two forms: *step-index* and *graded-index*. In **multimode step-index fibre**, the core's density is constant from the centre to the edges. A light beam moves through the core in a straight path until it meets the interface of the core and cladding. As the interface has a lower density than the core, there comes a sudden change in the angle of the beam's motion further adding to distortion of the signal as it moves on. The **multimode graded-index fibre** reduces such distortion of signal through the cable. As the density is high at the centre of the core, the refractive index at the centre is high which causes the light beams at the centre to move slower than the rays that are near the cladding. The light beams curve in a helical manner [see Figure 4.10(b)], thus, reducing the distance travelled as compared to zigzag movement. The reduction in path and higher speed allows light to arrive at the destination in almost the same time as straight lines.

Single-mode Propagation

This mode employs step-index fibre of relatively small diameter and less density than that of multimode fibre and a much focused light source. Because of the focused light source, the beams spread out to a small range of angles and propagate almost horizontally. Since all beams propagate through the fibre along a single path, distortion does not occur. Moreover, all beams reaching at the destination together can be recombined to form the signal. The single-mode propagation is well suited for long-distance applications such as cable television and telephones.

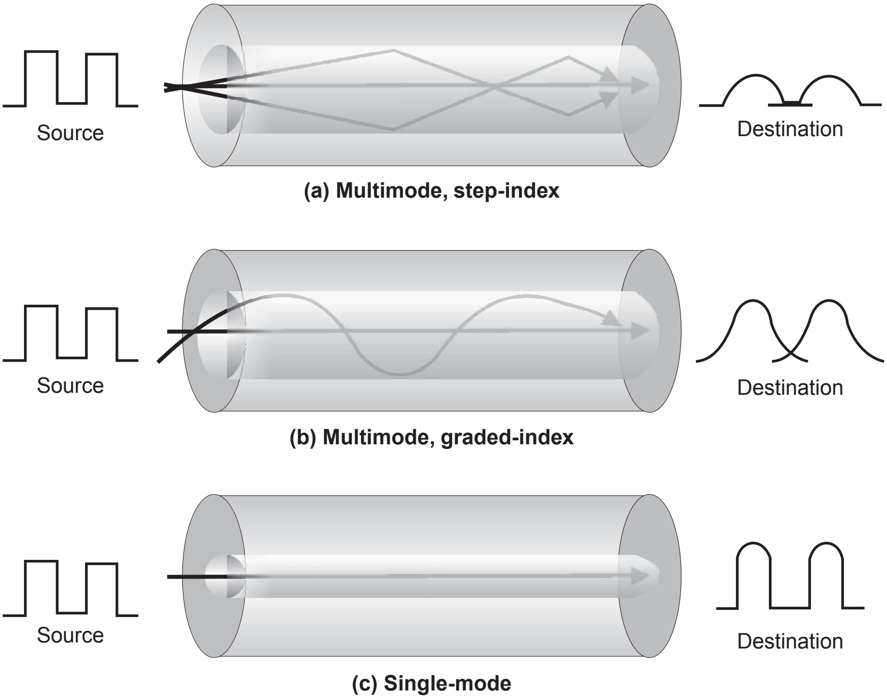


Figure 4.10 Propagation Modes for Fibre-optic Cable

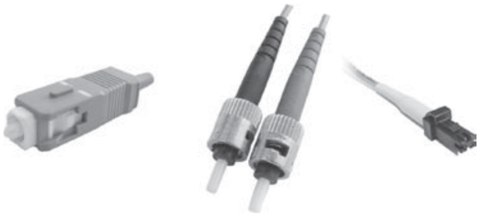
9. What are the different fib e sizes and connectors available?

Ans: The type of optical fibre is specified by the ratio of the diameter of its core to the diameter of its cladding. The commonly available fibre sizes are listed below in Table 4.4.

Fibre-optic cables use three types of connectors, which are *SC connector*, *ST connector* and *MT-RJ connector* as shown in Figure 4.11. **SC** (**subscriber channel**) **connector** uses a push–pull locking mechanism and is primarily used to connect fibre-optic cables for cable television. The **ST** (**straight tip**) **connector** is used to connect fibre-optic cables to network devices. This connector is more reliable than SC connector. **MT-RJ** (**mechanical transfer-registered jack**) **connector** is a small size connector which looks similar to RJ-45 connector. It is widely used for networking applications.

Table 4.4 Fibre Types

Type (core/cladding)	Mode
50/125	Multimode, graded index
62.5/125	Multimode, graded index
100/125	Multimode, graded index
7/125	Single mode



SC connector ST connector MT-RJ connector

Figure 4.11 Fibre-optic Cable Connectors

10. What are the advantages and disadvantages of fibre optic cables?

Ans: Fibre-optic cables are widely used in many domains such as telephone network and cable television network. Some advantages of fibre-optic cables are as follows

- ❑ Since transmission is light-based rather than electricity, it is immune to noise interference.
- ❑ Transmission distance is greater than other guided media because of less signal attenuation (degradation in quality over distance).
- ❑ It is extremely hard to tap into, making it desirable from the security viewpoint.
- ❑ They are smaller and lighter than copper wire and are free from corrosion as well.
- ❑ Fibre optic offers, by far, the greatest bandwidth of any transmission system.
- ❑ Transmission through fibre optic cable requires lesser number of repeaters for covering larger transmission distances.

The disadvantages of fibre-optic cables are as follows

- ❑ The installation and maintenance of fibre-optic cables are quite expensive
- ❑ The propagation of light is unidirectional and often requires precise alignment.
- ❑ Extending the fibre-optic cables by joining them together is a tough task
- ❑ It is more fragile when compared to copper wires.

11. What are the two kinds of light sources used in fibre-optic cables?

Ans: In fibre-optic cables, the light sources generate a pulse of light that is carried through the fibre medium. The two kinds of light sources used with the fibre-optic cables include *light-emitting diodes* (*LEDs*) and *semiconductor laser diodes*. These light sources are used to perform signalling and can be tuned in wavelengths by inserting Mach–Zehnder or Fabry–Pérot interferometers between the source and the fibre media. Table 4.5 lists the comparison between these two light sources.

Table 4.5 Comparison Between LEDs and Semiconductor Diodes

Characteristics	LED	Semiconductor laser diode
Data rate	Low	High
Cost	Low cost	Expensive
Fibre type	Multimode	Multimode/single mode
Lifetime	Long life	Short life
Temperature sensitivity	Minor	Substantial
Distance	Short	Long

12. Explain the use of electromagnetic spectrum for communication.

Ans: Electromagnetic signals include power, voice, radio waves, infrared light, visible light, ultraviolet light, X-rays and gamma rays. Each of these forms a portion of the electromagnetic spectrum (see Figure 4.12). The portions of the electromagnetic spectrum that can be used for transmitting information include radio wave, microwave, infrared light and visible light. Information can be transmitted using these portions by modulating the frequency, amplitude or phase of the electromagnetic waves. Though using UV, X-rays and gamma rays for transmitting information is a better choice due to their high frequency (HF), they are not generally used. This is because it is difficult to produce and modulate these rays as well as they cannot penetrate obstacles such as buildings. Moreover, they are dangerous for the living beings.

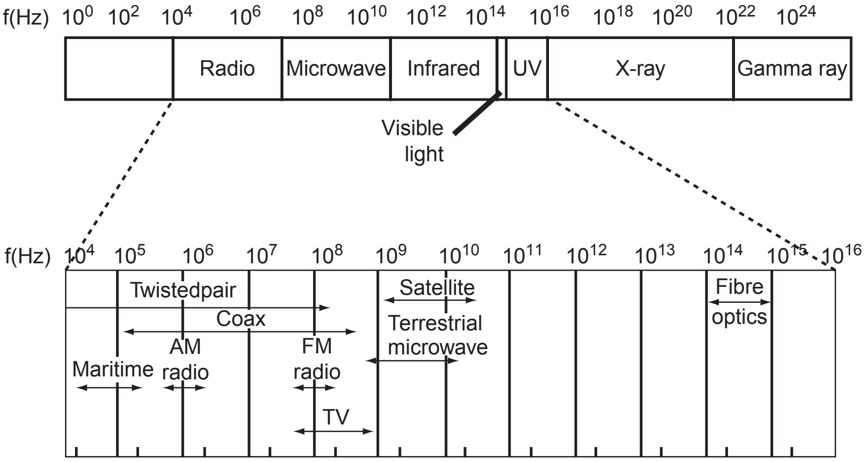

f(Hz) 10^0 10^2 10^4 10^6 10^8 10^10 10^12 10^14 10^16 10^18 10^20 10^22 10^24
Radio
Microwave
Infrared
UV
X-ray
Gamma ray
Visible light
f(Hz) 10^4 10^5 10^6 10^7 10^8 10^9 10^10 10^11 10^12 10^13 10^14 10^15 10^16
Twistedpair
Coax
AM radio
Maritime
FM radio
TV
Satellite
Terrestrial microwave
Fibre optics

Figure 4.12 Electromagnetic Spectrum and Its Uses for Communication

The portion of the electromagnetic spectrum that can be used for transmitting information is parted into eight different ranges. These ranges are regulated by the government authorities and are known as **bands.** Some of the properties of bands are listed in Table 4.6.

Table 4.6 Properties of Bands

Band	Use	Range	Propagation
VLF (very low frequency)	Long-range radio navigation	3–30 kHz	Ground wave
LF (low frequency)	Locators, radio beacons	30–300 kHz	Ground wave
MF (middle frequency)	AM radio	300 kHz–3 MHz	Sky
HF (high frequency)	Citizens band, ship/aircraft communication	3–30 MHz	Sky
VHF (very high frequency)	FM radio, VHF TV	30–300 MHz	Sky and line-of-sight
UHF (ultra high frequency)	Cell phones, satellite, UHF TV, paging	300 MHz–3 GHz	Line-of-sight
SHF (super high frequency)	Satellites	3–30 GHz	Line-of-sight
EHF (extremely high frequency)	Satellite, radars	30–300 GHz	Line-of-sight

13. Explain the different propagation methods for unguided signals.

Ans: Unguided signals can propagate in three ways, which are *ground wave*, *ionosphere* and *line-of-sight*.

- **Ground Wave Propagation:** In this propagation method, the radio waves pass through the lowest portion of the atmosphere, that is, the curvature of the earth (Figure 4.13). These low frequency radio waves when transmitted by an antenna disperse in all directions following the curvature of earth. The distance travelled is directly proportional to the power of the signal. That is, greater the amount of power in the signal is, the more will be the distance covered.

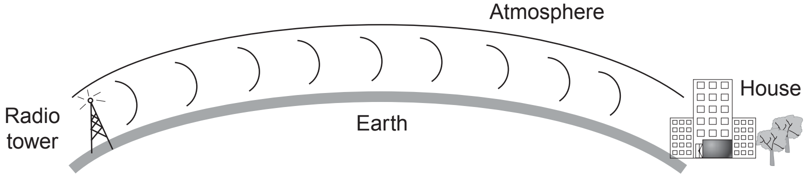


Figure 4.13 Ground Wave Propagation

- **Ionospheric Propagation:** In this propagation method, the higher frequency radio waves transmitted by antenna travel upwards into ionosphere layer in the upper portion of atmosphere and bounced off by the layer towards earth; a low power signal can travel a greater distance (Figure 4.14). It operates in the frequency range of 2–30 MHz. As this type of propagation depends on the earth's ionosphere, it changes with the day timings and weather. This method of propagation is also known as **sky wave propagation**.

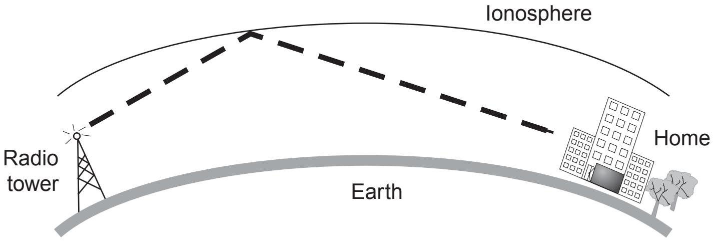


Figure 4.14 Ionosphere Propagation

- **Line-of-Sight Propagation:** In this propagation method, very high frequency signals are transmitted which travel exactly in straight line (Figure 4.15). This method demands both transmitting and receiving antennas to be in line of sight of each other, that is, the receiving antenna must be in view of the transmitting antenna. It is sometimes called **space waves** or **tropospheric propagation**. It is limited by the curvature of the earth for ground-based stations (50 km).

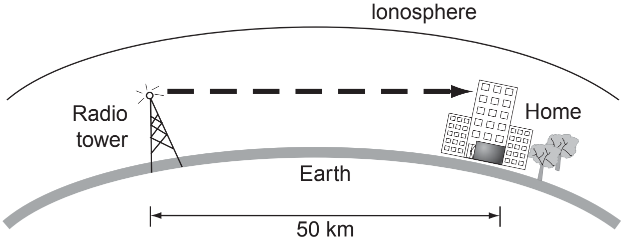


Figure 4.15 Line-of-Sight Propagation

14. Explain in detail the different types of unguided media.

Ans: Unguided media are used in those cases when transmission of data through guided media is difficult. The three main types of unguided media are discussed in the following sections:

Radio Waves

The electromagnetic waves with frequency in the range of 3 kHz to 1 GHz are generally known as **radio waves**. These waves are omnidirectional, that is they are propagated in all directions when transmitted by an antenna. Thus, the antennas that send and receive the signals need not be aligned. However, the radio waves transmitted by two antennas using the same band or frequency may interfere with each other.

Radio waves present different characteristics at different frequencies. At low (VLF, LF) and medium (MF) frequencies, they follow the curvature of earth and can penetrate walls easily. Thus, a device such as a portable radio inside a building can receive the signal. At high frequencies (HF and VHF bands), as the earth absorbs the radio waves, they are propagated in sky mode. The higher frequency radio waves can be transmitted up to greater distances and thus are best suited for long-distance broadcasting. However, at all frequencies, radio waves are susceptible to interference from electrical equipments.

An omnidirectional antenna is used to transmit radio waves in all directions (see Figure 4.16). Due to their omnidirectional characteristics, radio waves are useful for multicast (one sender, many receivers) communication. Examples of multicasting are cordless phones, AM and FM radios, paging and maritime radio.

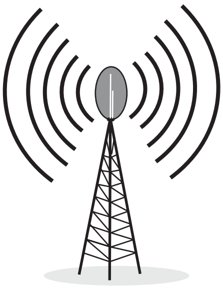


Figure 4.16 Omnidirectional Antenna

Microwaves

The electromagnetic waves with frequency in the range of 1–300 GHz are known as **microwaves**. Unlike radio waves, microwaves are unidirectional. The advantage of the unidirectional property is that multiple transmitters can transmit waves to multiple receivers without any interference. Since microwaves are transmitted using line-of-sight propagation method, the towers with mounted antennas used for sending and receiving the signal must be in direct sight of each other (Figure 4.17). In case, the antenna towers are located far away from each other, the towers should be quite tall so that the signals do not get block off due to curvature of earth as well as other obstacles. Moreover, repeaters should be often used to amplify the signal strength. Microwaves at lower frequencies cannot penetrate buildings and also, during propagation, refraction or delays can occur due to divergence of beams in space. These

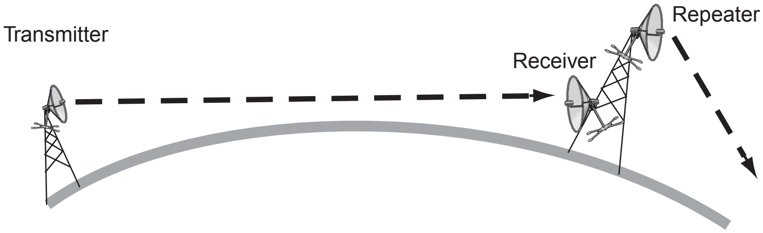
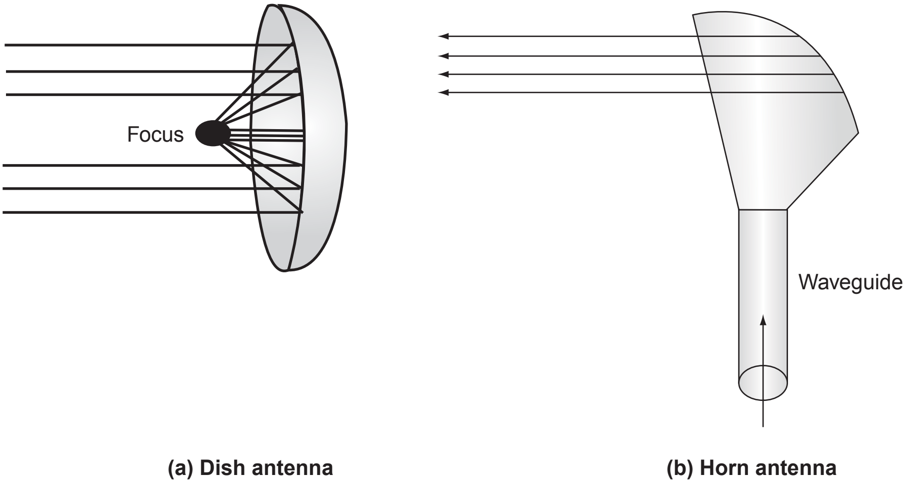


Figure 4.17 Microwave Transmission

delayed waves can come out of phase with the direct wave leading to cancellation of the signal. This phenomenon is known as the **multipath fading effect**.

Microwaves require unidirectional antennas that transmit signal only in one direction. Two such antennas are *dish antenna* and *horn antenna* (see Figure 4.18). A **dish antenna** works based on the geometry of a parabola. All the lines parallel to the line of sight when hit the parabola, they are reflected by the parabola curve at angles such that they converge at a common point called the **focus**. The dish parabola catches many waves and directs them on the focus. As a result, the receiver receives more of the signal. In a **horn antenna**, outgoing transmission is sent through a stem and as it hits the curved head, the transmission is deflect d outward as a series of parallel beams. The received transmissions are collected by a horn similar to the parabolic dish, which deflects them back into the stem

Since microwaves are unidirectional, they are best suited for unicast communication such as in cellular networks, wireless local area networks and satellite networks.



(a) Dish antenna

(b) Horn antenna

Figure 4.18 Unidirectional Antennas

Infrared Waves

The electromagnetic waves with frequency in the range of 300 GHz to 400 THz are known as **infrared waves**. These waves are widely used for indoor wireless LANs and for short-range communication; for example, for connecting a PC with a wireless peripheral device, in remote controls used with stereos, VCRs, TVs, etc. (Figure 4.19). Infrared waves at high frequencies are propagated using line-of-sight method and cannot penetrate solid objects. Therefore, a short range infrared system in a room will not be interfered by such a system present in an adjacent room. Furthermore, infrared waves cannot be used outside a building because the infrared rays coming from the sun may interfere with it and distort the signal.

The use of infrared waves has been sponsored by an association, known as **Infrared Data Association (IrDA)**. This association has also established standards for the usage of infrared signals for communication between devices such as keyboards, printers, PCs and mouses. For example, some wireless keyboards are attached with an infrared port that enables the keyboard to communicate with

Figure 4.19 Infrared Waves

the PC. Since infrared signals transmit through line-of-sight mode, the infrared port must be pointed towards the PC for communication.

Communication Satellites

A communication satellite can be referred to as a **microwave relay station**. A satellite links two or more ground-based (earth) stations that transmit/receive microwaves. Once a satellite receives any signal on a frequency (**uplink**), it repeats or amplifies that signal and sends it back to earth on a separate frequency (**downlink**). The area shadowed by the satellite (see Figure 4.20) in which the information or data can be transmitted and received is called the **footprint**.

Satellites are generally set in geostationary orbits directly over the equator, which rotates in synchronization with the earth and hence looks stationary from any point on the earth. These geostationary orbits are placed approximately 36,000 km above the earth's surface and satellites placed in this orbit are known as **geostationary satellites**.

Satellite transmission is also a kind of line-of-sight transmission and the best frequency for it is in the range of 1–10 GHz. The major applications for satellites are long-distance telephone transmission, weather forecasting, global positioning, television, and many more.

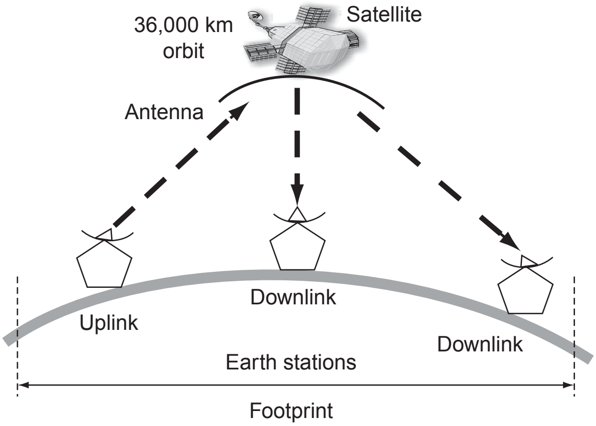


Figure 4.20 Satellite Transmission

Multiple Choice Questions

1. A transmission medium is located under and controlled by the
   (a) transport layer (b) application layer
   (c) physical layer (d) session layer

2. Guided transmission media include
   (a) coaxial cable (b) fibre-optic cabl
   (c) twisted-pair cable (d) All of these

3. Which of the following is not a type of twisted-pair cable?
   (a) UTP (b) FTP
   (c) STP (d) None of these

4. BNC connectors are used with
   (a) satellites (b) fibre-optic cable
   (c) coaxial cables (d) twisted-pair cables

5. The transmission medium with maximum error rate is
   (a) coaxial cable (b) twisted-pair cable
   (c) satellite link (d) optical fibr

6. Optical fibres transmit a beam of light by means of
   (a) total internal reflection
   (b) total internal refraction
   (c) Both (a) and (b)
   (d) None of these

7. In multimode step-index fibre, the density of the core ______ from the centre to the edges.
   (a) increases (b) decreases
   (c) remains constant (d) None of these

8. Which of the following is not a band?
   (a) VHF (b) UHF
   (c) VLF (d) SLF

9. Unguided signals can propagate in ______ ways.
   (a) two (b) eight
   (c) three (d) four

10. The frequency at which a signal is received by a satellite is known as its ______ frequency.
    (a) downlink (b) microwave
    (c) terrestrial (d) uplink

Answers

1. (c) 2. (d) 3. (b) 4. (c) 5. (b) 6. (a) 7. (c) 8. (d) 9. (c) 10. (d)

5

Multiplexing and Switching

1. What is meant by bandwidth utilization?

Ans: Bandwidth utilization refers to the wise use of the available bandwidth in order to achieve the utmost efficiency, privacy and anti-jamming. Bandwidth can be used optimally using two techniques, namely, *multiplexing* and *spreading*. **Multiplexing** allows sharing the available bandwidth of a communication link among a number of communicating stations, thus achieving efficiency. On the other hand, **spreading** allows expanding the bandwidth of link for achieving privacy and anti-jamming.

2. What is multiplexing? In what situations, it can be used?

Ans: Multiplexing is a technique used for transmitting several signals simultaneously over a single communication link. An analogy of multiplexing can be made with a multilane highway. Just as a multilane highway can carry increased volumes of traffic in multiple lanes at higher speeds and at relatively low incremental cost per lane, the higher-capacity circuit can carry multiple conversations in multiple channels at relatively low incremental cost per channel. Multiplexing is done to utilize the available bandwidth properly and to improve the efficiency during a transmission. In a multiplexed system (Figure 5.1), several devices share a communication link called **common medium**. Each part of the communication link being used for carrying transmission between an individual pair of input and an output line is referred to as a **channel**.

At the sender's end, the N input lines are combined into a single stream by a communication device, called **multiplexer** (**MUX**). At the receiver's end, another communication device, called **demultiplexer** (**DEMUX**), completes the communication process by separating multiplexed signals from a communication link and distributing them to corresponding N output lines.

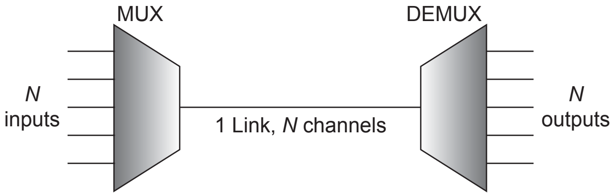


Figure 5.1 A Multiplexed System

Multiplexing can be used in situations where the signals to be transmitted through the transmission medium have lower bandwidth than that of the medium. This is because in such situations, it is possible to combine the several low-bandwidth signals and transmitting them simultaneously through the transmission medium of larger bandwidth.

3. Why we need multiplexing in a communication channel?

Ans: Multiplexing is needed in a communication channel because of the following reasons:

- To send several signals simultaneously over a single communication channel.
- To reduce the cost of transmission.
- To effectively utilize the available bandwidth of the communication channel.

4. Explain the different multiplexing techniques.

Ans: Multiplexing can be done using three techniques: frequency-division multiplexing (FDM), wavelength-division multiplexing (WDM) and time-division multiplexing (TDM).

Frequency-Division Multiplexing

FDM is used when the bandwidth of the transmission medium is greater than the total bandwidth requirement of the signals to be transmitted. It is often used for baseband analog signals. At the sender's end, the signals generated by each sending device are of similar frequency range. Within the multiplexer, these similar signals modulate carrier waves of different frequencies and then the modulated signals are merged into a single composite signal, which is sent over the transmission medium. The carrier frequencies are kept well separated by assigning a different range of bandwidth (channel) that is sufficient to hold the modulated signal. There may also be some unused bandwidth between successive channels called **guard bands**, in order to avoid interference of signals between those channels.

At the receiver's end, the multiplexed signal is applied to a series of bandpass filters which breaks it into component signals. These component signals are then passed to a demodulator that separates the signals from their carriers and distributes them to different output lines (Figure 5.2).

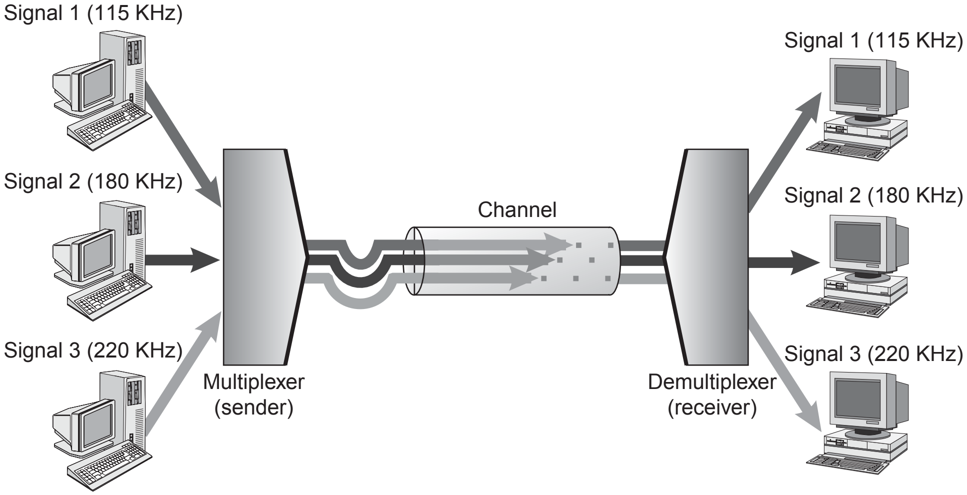


Figure 5.2 Frequency-division Multiplexing

Though FDM is an analog multiplexing technique, it can also be used to multiplex the digital signals. However, before multiplexing, the digital signals must be converted to analog signals. Some common applications of FDM include radio broadcasting and TV networks.

Wavelength-Division Multiplexing

WDM is an analog multiplexing technique designed to utilize the high data rate capability of fibre-optic cables. A fibre-optic cable has a much higher data rate than coaxial and twisted-pair cables and using it as a single link wastes a lot of precious bandwidth. Using WDM, we can merge many signals into a single one and hence, utilize the available bandwidth efficientl . Conceptually, FDM and WDM are same; that is, both combine several signals of different frequencies into one, but the major difference is that the latter involves fibre-optic cables and optical signals as well as the signals are of very high frequency.

In WDM, the multiplexing and demultiplexing are done with the help of a prism (Figure 5.3), which bends the light beams by different amounts depending on their angle of incidence and wavelength. The prism used at the sender's end combines the multiple light beams with narrow frequency bands from different sources to form a single wider band of light which is then passed through fibre-optic cable. At the receiver's end, the prism splits the composite signal into individual signals. An application of WDM is the SONET network.

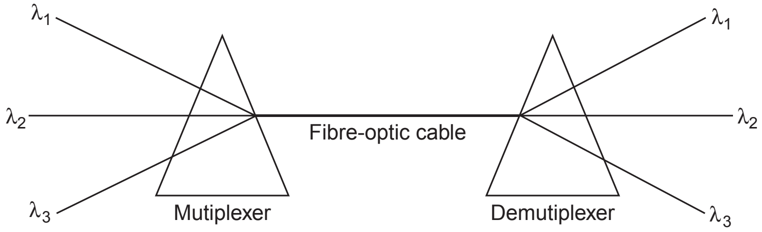


Figure 5.3 Wavelength-division Multiplexing

Time-Division Multiplexing

TDM is a digital multiplexing technique that allows the high bandwidth of a link to be shared amongst several signals. Unlike FDM and WDM, in which signals operate at the same time but with different frequencies, in TDM, signals operate at the same frequency but at different times. In other words, the link is time-shared instead of sharing parts of bandwidth among several signals.

Figure 5.4 gives a conceptual view of TDM. At the sender's end, the time-division multiplexer allocates each input signal a period of time or time slot. Each sending device is assigned the transmission path for a predefined time slot. Three sending signals, Signals 1, 2 and 3, occupy the transmission sequentially. As shown in the figure, time slots `A`, `B`, `P`, `Q`, `X` and `Y` follow one after the other to carry signals from the three sources, which upon reaching the demultiplexer, are sent to the intended receiver.

Though TDM is a digital multiplexing technique, it can also multiplex analog signals. However, before multiplexing, analog signals must be converted to DSs.

5. Explain different schemes of TDM.

Ans: TDM can be divided into two different schemes, namely, *synchronous TDM* and *statistical TDM*.

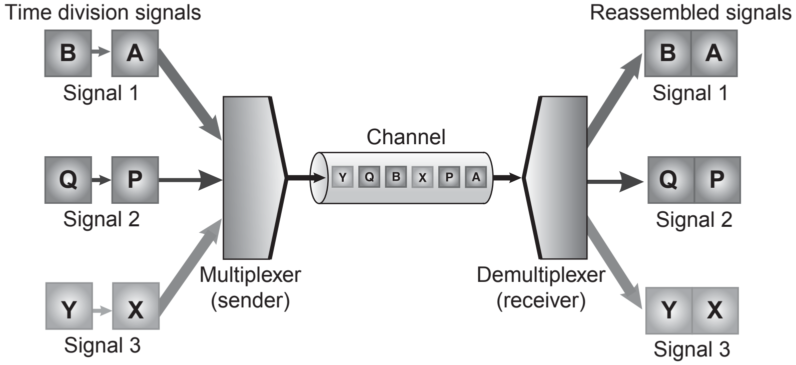


Figure 5.4 Time-division Multiplexing

Synchronous TDM

In this technique, data flow of each input source is divided into units where a unit can be a bit, byte or a combination of bytes. Each input unit is allotted one input time slot. A cycle of input units from each input source is grouped into a **frame**. Each frame is divided into time slots and one slot is dedicated for a unit from each input source. That is, for n connections, we have n time slots in a frame and every slot has its own respective sender. The duration of input unit and the duration of each frame are same unless some other information is carried by the frame. However, the duration of each slot is n times shorter where n is the number of input lines. For example, if duration of input unit is t seconds, then the duration of each slot will be t/n seconds for *n* input lines. The data transmission rate for the output link must be n times the data transmission rate of an input line to ensure the transmission of data. In addition, one or more synchronization bits are to be included in the beginning of each frame to ensure the data synchronization between the multiplexer and the demultiplexer.

Figure 5.5 shows a conceptual view of synchronous TDM in which data from the three input sources has been divided into units (P1, P2, P3), (Q1, Q2) and (R1, R2, R3). As the total number of input lines is three, each frame also has three time slots. Now, if the duration of an input unit is t seconds, then after every t seconds, a unit is collected from each source and kept into the corresponding time slot in the frame. For example, Frame 1 contains (P1, Q1, R1). In our example, the data rate for the transmission link must be three times the connection rate to ensure the flow of data. In addition, the duration of each frame is three time slots whereas the duration of each time slot is t/3.

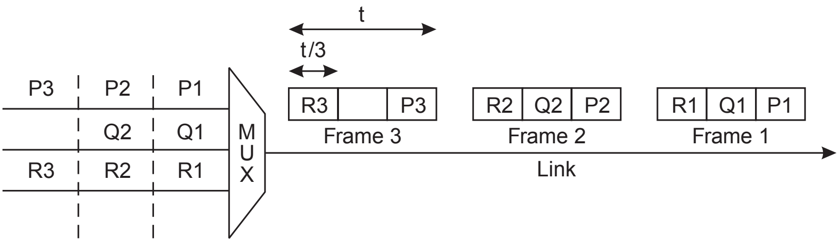


Figure 5.5 Synchronous TDM

A major drawback of synchronous TDM is that it is not highly efficient. Since each slot in the frame is pre-assigned to a fixed source, the empty slots are transmitted in case one or more sources do not have any data to send. As a result, the capacity of a channel is wasted. For example, in Figure 5.5, an empty slot is transmitted in Frame 3 because the corresponding input line has no data to send during that time period.

Statistical TDM

Statistical TDM, also called **asynchronous TDM** or **intelligent TDM**, overcomes the disadvantage of synchronous TDM by assigning the slots in a frame dynamically to input sources. A slot is assigned to an input source only when the source has some data to send. Thus, no empty slots are transmitted which in turn result in an efficient utilization of bandwidth. In statistical TDM, generally each frame has less number of slots than the number of input lines and the capacity of link is also less than the combined capacity of channels.

Figure 5.6 shows a conceptual view of statistical TDM. At the sender's end, the multiplexer scans the input sources one by one in a circular manner and assigns a slot if the source has some data to send; otherwise, it moves on to the next input source. Hence, slots are filled up as long as an input source has some data to send. At the receiver's end, the demultiplexer receives the frame and distributes data in slots of frame to appropriate output lines.

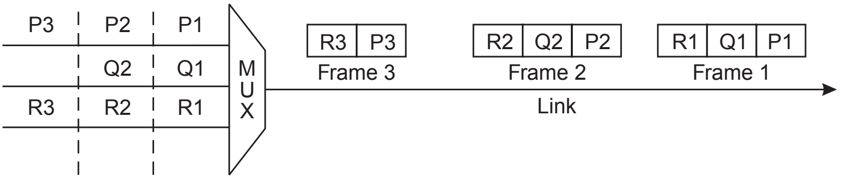


Figure 5.6 Statistical TDM

Unlike synchronous TDM, there is no fixed relationship between the inputs and the outputs in statistical TDM because here slots in a frame are not pre-assigned or reserved. Thus, to ensure the delivery of data to appropriate output lines, each slot in the frame stores the destination address along with data to indicate where the data has to be delivered. For n output lines, an m-bit address is required to define each output line where $m = \log_2 n$. Though the inclusion of address information in a slot ensures the proper delivery, it incurs more overhead per slot. Another difference between synchronous and statistical TDMs is that the latter technique does not require the synchronization among the frames thereby eliminating the need of including synchronization bits within each frame.

6. Distinguish multilevel, multiple-slot and pulse-stuffed TDMs.

Ans: Multilevel multiplexing, multiple-slot allocation and pulse stuffing are the strategies used in TDM to handle the different input data rates of the input lines.

Multilevel Multiplexing

Multiple multiplexing is used in situations where the data rate of an input line is an integral multiple of other input lines. As the name suggests, several levels of multiplexing are used in this technique. To understand, consider Figure 5.7 where we have three input lines; the first two input lines have a data rate of 80 kbps each and the last input line has a data rate of 160 kbps. As the data rate of third input line (160 kbps) is a multiple of that of other two (80 kbps), the first two input lines can be multiplexed to produce a data rate of 160 kbps that is equal to that of the third input line. Then, another level of multiplexing can be used to combine the output of first two input lines and the third input line thereby generating an output line with a data rate of 320 kbps.

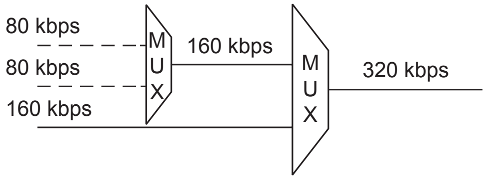


Figure 5.7 Multilevel Multiplexing

Multiple-Slot Allocation

Like multilevel multiplexing, multiple-slot allocation technique is also used in situations where the data rate of an input line is an integral multiple of other input lines. Generally, one slot per each input source is reserved in the frame being transmitted. However, sometimes, it is more useful to allocate multiple slots corresponding to a single input line in the frame. For example, again consider Figure 5.7 where we can divide one 160-kbps input line into two (each of 80 kbps) with the help of serial-to-parallel converter and then multiplex the four input lines of 80 kbps each to create an output line of 320 kbps. However, now there will be total four slots in the transmitting frame with two slots corresponding to input line with originally 160 kbps data rate (Figure 5.8).

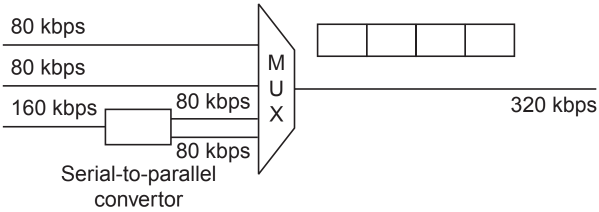


Figure 5.8 Multiple-slot Allocation

Pulse Stuffing

Pulse stuffing, also known as **bit padding** or **bit stuffing**, technique is used in situations where the data rates of input lines are not the integral multiples of each other. In this technique, the highest input data rate is determined and then dummy bits are added to input lines with lower data rates to make the data rate of all the lines equal. For example, consider Figure 5.9 where the first input line has the highest data rate equal to 80 kbps and other two input lines have data rate of 60 and 70 kbps, respectively. Hence, the data rates of second and third input lines are pulse-stuffed to increase the rate to 80 kbps.

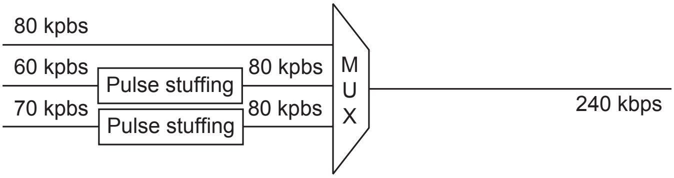


Figure 5.9 Pulse Stuffing

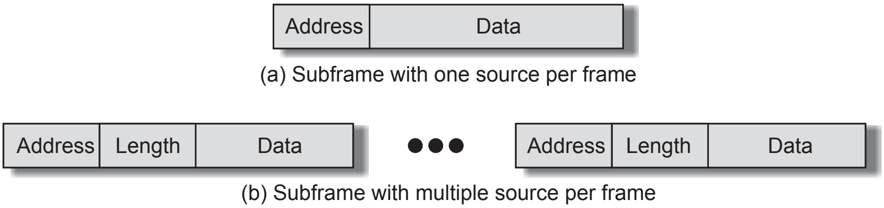
7. What is the purpose of framing bit? Is it used in FDM or TDM?

Ans: Framing bits are used in TDM to ensure the synchronization between multiplexer and demultiplexer. Without synchronization, there may be some error in delivery of bits; that is, a bit may be delivered to the wrong output line. Thus, one or more synchronization bits, called **framing bits**, are generally added at the beginning of each transmitting frame. The framing bits follow a specific pattern in each frame, which allows the demultiplexer to get in synchronization with the input data and divide the time slots with accuracy.

8. What is the frame format in statistical TDM?

Ans: In statistical TDM, there are two possible frame structures that a multiplexer can use. These structures are described as follows:

- **One Data Source Per Frame:** This frame structure permits to include data from one source per each frame. The frame consists of two parts: **address**, which is used to identify the source, and **data**, which is of variable length [Figure 5.10(a)]. The end of data field is indicated by the end of overall frame. This type of frame structure is suitable in environments where the load is less. However, as the load increases, this frame structure becomes inefficient
- **Multiple Data Sources Per Frame:** This frame structure permits to include data from multiple sources in a single frame. For each source, the frame contains **address** to identify the source, **length** of data field and **data** [see Figure 5.10(b)]. This frame structure helps to improve efficienc .



(a) Subframe with one source per frame

(b) Subframe with multiple source per frame

Figure 5.10 Statistical TDM Frame Structures

9. Describe the DS hierarchy.

Ans: The DS hierarchy, also called **digital signal service**, is a hierarchy of digital signals which the telephone companies use for implementing TDM. This hierarchy consists of several levels with each level supporting a different data rate. The digital signals at lower levels in hierarchy are multiplexed into signals at higher levels in hierarchy (Figure 5.11). Various levels of DS hierarchy are described as follows:

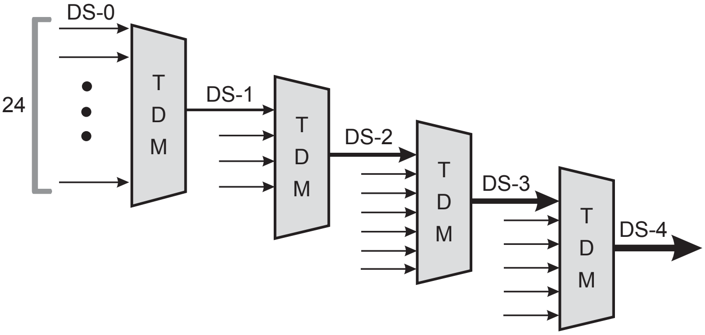


Figure 5.11 DS Hierarchy

- ❑ **DS-0:** This service is at the lowest level of hierarchy. It is a single digital channel of just 64 kbps.
- ❑ **DS-1:** This service has a capacity of 1.544 Mbps which is 24 times of a DS-0 channel with an additional overhead of 8 kbps. It can be utilized for multiplexing 24 DS-0 channels, as a single service for transmissions of 1.544 Mbps or can even be used in different combinations to utilize capacity up to 1.544 Mbps.
- ❑ **DS-2:** This service has a capacity of 6.312 Mbps which is 96 times of DS-0 with an additional overhead of 168 kbps. It can be utilized for multiplexing 96 DS-0 channels, four DS-1 channels or can also be utilized as a single service for transmission up to 6.312 Mbps.
- ❑ **DS-3:** This service has a capacity of 44.376 Mbps which is seven times the data rate of DS-2 channels with an additional overhead of 1.368 Mbps. It can be utilized for multiplexing 672 DS-0 channels, 28 DS-1 channels or seven DS-2 channels. In addition, DS-3 can be utilized as a single transmission line or as a combination of its previous hierarchies.
- ❑ **DS-4:** This service is at the highest level of the DS hierarchy and has a capacity of 274.176 Mbps. It can be utilized for multiplexing six DS-3 channels, 42 DS-2 channels, 168 DS-1 channels or 4,032 DS-0 channels. It can also be used as a combination of service types at lower levels of hierarchy.

10. Explain the analog hierarchy used by telephone networks with an example.

Ans: Analog hierarchy is used by telephone companies for maximizing the efficiency of their infrastructure such as switches and other transmission equipments. In analog hierarchy, the analog signals from the lower bandwidth channels are multiplexed onto the higher bandwidth lines at different levels. For multiplexing of analog signals at all levels of hierarchy, the FDM technique is used. The standards for multiplexing vary in countries but the basic principle remains the same. One of such analog hierarchies is used by AT&T in the United States. This analog hierarchy comprises *voice channels*, *groups*, *super groups*, *master groups* and *jumbo groups* (Figure 5.12).

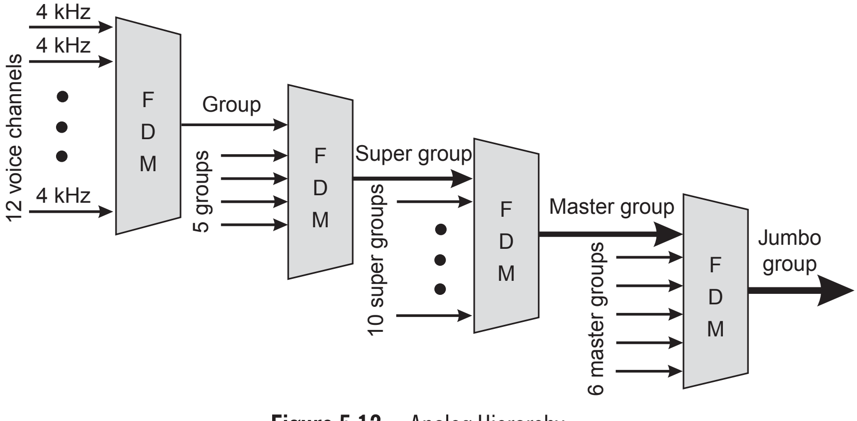


Figure 5.12 Analog Hierarchy

At the lowest level of hierarchy, 12 **voice channels**, each having a bandwidth of 4 kHz, are multiplexed onto a higher bandwidth line thereby forming a **group** of 48 kHz (12 × 4 kHz). At the next level of hierarchy, five groups (that is, 60 voice channels) are multiplexed to form a **super group** that has a bandwidth of 240 kHz (5 × 48 kHz). Further, 10 super groups (that is, 600 voice channels) are multiplexed to form a **master group**. A master group must have a bandwidth of 2.4 MHz (10 × 240 kHz). However, to avoid interference between the multiplexed signals, the requirement of guard bands increases the total bandwidth of a master group to 2.52 MHz. Finally, six master groups are multiplexed to form a **jumbo**

group that must have a bandwidth of 15.12 MHz (6 × 2.52 MHz). However, the requirement of guard bands to separate the master groups increases the total bandwidth of a jumbo group to 16.984 MHz.

11. What is inverse multiplexing?

Ans: Inverse multiplexing is the opposite of the multiplexing technique. In this technique, the data from a single high-speed line or source is split into chunks of data that can be transmitted over low-speed lines at the same time and without any data loss in the combined data rate.

12. What do you understand by spread spectrum?

Ans: Spread spectrum is a technique used to expand the available bandwidth of a communication link in order to achieve goals such as privacy and anti-jamming. For achieving these goals, the spread spectrum techniques expand the original bandwidth required for every system (adding redundancy) such that the signals from different sources can together fit into larger bandwidth. For example, if the bandwidth requirement of each system is B, then the spread spectrum techniques increase it to B´ such that B´ >> B. To spread the bandwidth, a **spreading process** is used which is independent of the original signal. The spreading process uses a **spreading code**—a series of numbers following the specific pattern—and results in expanded bandwidth.

The spread spectrum technique is generally used in wireless LANs and WANs where the systems sharing the air transmission medium must be able to communicate without any interception from intruders, blocking of message during transmission and so on.

13. List the principles to be followed by the spread spectrum technique?

Ans: The spread spectrum technique uses the following principles to achieve its goals.

- ❑ The spreading process must be independent of the original signal. This implies that spreading process is used after the source has generated the signal.
- ❑ Each source station is assigned a bandwidth much greater than what it actually needs thereby allowing redundancy.

14. Compare frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) technique?

Ans: FHSS and DSSS are the techniques to expand the bandwidth of the digital signal. However, both techniques follow a different process to achieve their goal.

Frequency Hopping Spread Spectrum

In this technique, a number of different carrier frequencies (say, N) are used. The input signal modulates one of N carrier frequencies in each hopping period (T_{hop}). As shown in Figure 5.13, FHSS uses a pseudorandom code generator, also known as **pseudorandom noise** (**PN**), which generates an m-bit pattern (where $m = \log_2 N$) for every hopping period T_{hop}. For example, if an application uses 16 hopping frequencies, then the pseudorandom code generator creates 16 different four-bit patterns one per each hopping period. During each hopping period, the m-bit pattern generated by pseudorandom code generator is used by the frequency table to determine the hopping frequency to be used for that hopping period. The frequency selected from the frequency table is passed to the frequency synthesizer which generates a carrier signal of the selected frequency. The input signal modulates the carrier signal generated by the frequency synthesizer and as a result, spread signal with bandwidth (B_{FHSS}) much greater than the original bandwidth (B) is produced.

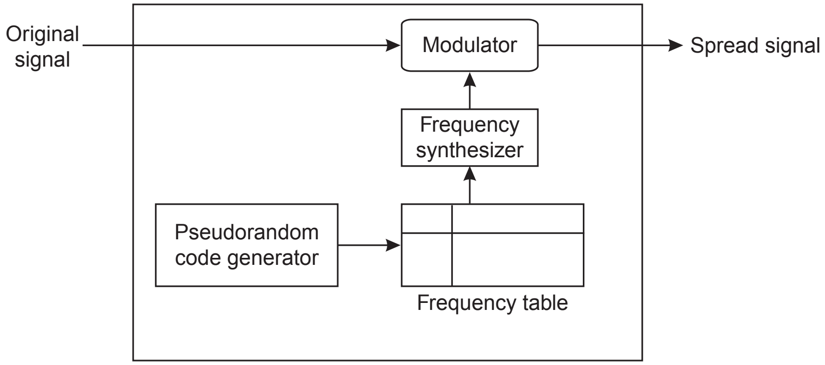


Figure 5.13 Frequency Hopping Spread Spectrum

Since one out of N hopping frequencies is used by a source station in each hopping period, the remaining N-1 frequencies can be used by other N-1 stations. Thus, N hopping frequencies (N channels) can be multiplexed into one using the same bandwidth B_{FHSS}. That is, N source stations can share the same bandwidth B_{FHSS}. In addition, due to randomization in the frequency and the frequent frequency hops, the intruders may be able to intercept the signal or send noise to jam the signal possibly for one hopping period but not for the entire period thus, achieving privacy and anti-jamming.

Direct Sequence Spread Spectrum

In this technique, each bit of the original signal is replaced by *n* bits using a spreading code. As shown in Figure 5.14, DSSS uses a chip generator that generates a spreading code of *n* bits (called **chips**) for each signal bit. To expand the bandwidth of the original signal, each bit of the original signal is multiplied by the code generated by the chip generator. After multiplication, the resultant spread signal with a bandwidth *n* times of that of the original signal is produced. DSSS provides privacy between the sender and the receiver if the intruder does not know the spreading code. It also prevents interference if a different spreading code is used for each source station.

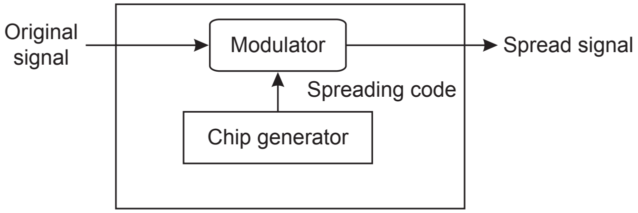


Figure 5.14 DSSS Process

Figure 5.15 illustrates the DSSS process. The spreading code used in this example is eight chips with the pattern 10110100. Each bit of the original signal is multiplied by the eight-bit spreading code to obtain the new spread signal. Now, if the original signal rate is S, then the new spread signal rate will be 8S. This implies that the required bandwidth for the spread signal would be eight times of the original bandwidth.

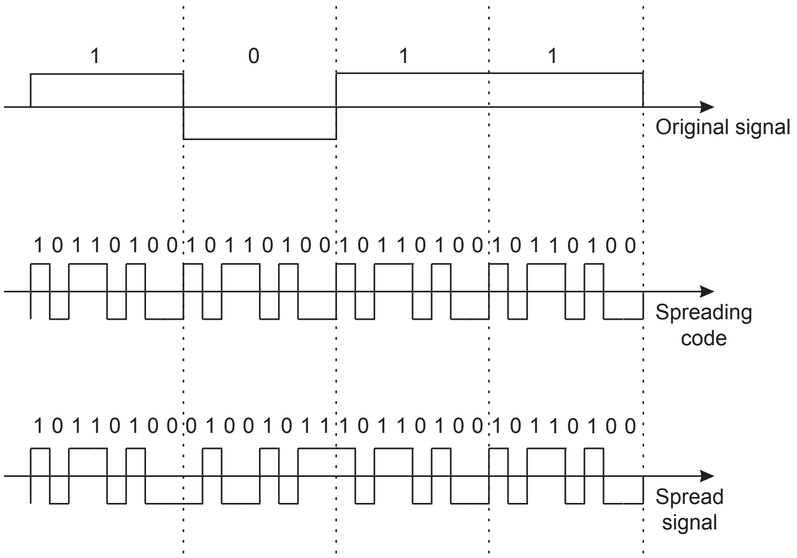


Figure 5.15 DSSS Example

15. What is meant by the term switching?

Ans: On a network, **switching** means routing traffic by setting up temporary connections between two or more network points. This is done by devices located at different locations on the network, called **switches** (or **exchanges**). Switches create temporary connections amongst two or more devices connected to them. In a switched network, some switches are directly connected to the communicating devices, while others are used for routing or forwarding information.

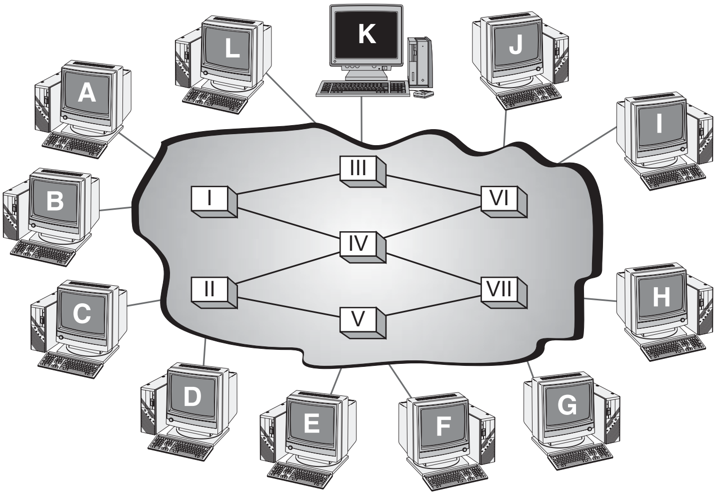


Figure 5.16 Switched Network

Figure 5.16 depicts a switched network in which communicating devices are labelled `A, B, C` and so on and switches are labelled `I, II, III, IV` and so on. Each switch is connected either to a communicating device or to any other switch for forwarding information. Notice that multiple switches are used to complete the connection between any two communicating devices at a time, hence saving the extra links required in case of a point-to-point connection.

16. Explain different types of switching techniques along with their advantages and disadvantages.

Ans: There are three different types of switching techniques; namely, *circuit switching*, *message switching* and *packet switching*.

Circuit Switching

When a device wants to communicate with another device, circuit switching technique creates a fixed bandwidth channel, called a **circuit**, between the source and the destination. This circuit is a physical path that is reserved exclusively for a particular information flow, and no other flow can use it. Other circuits are isolated from each other, and thus their environment is well controlled. For example, in Figure 5.17, if device A wants to communicate with device D, sets of resources (switches I, II and III) are allocated which act as a circuit for the communication to take place. The path taken by data between its source and destination is determined by the circuit on which it is flowing, and does not change during the lifetime of the connection. The circuit is terminated when the connection is closed. Therefore, this method is called **circuit switching**.

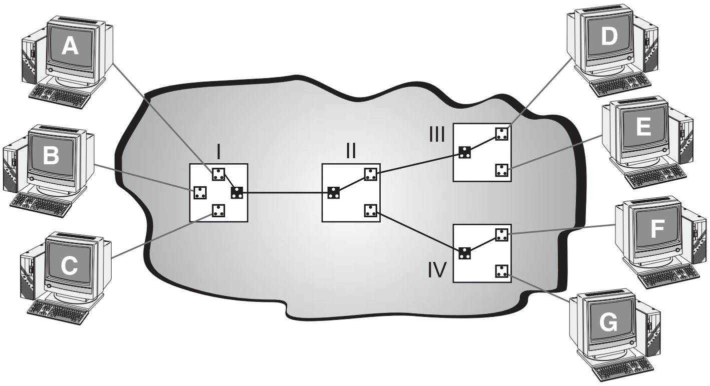


Figure 5.17 Circuit Switching

Some advantages of circuit switching are as follows:

- ❑ It is a simple method and does not require the use of any special facilities.
- ❑ After a circuit is determined and established, data is transmitted with just a minimal propagation delay and without congestion.
- ❑ It is the preferred choice for the transmission of real-time data and voice.

Some disadvantages of circuit switching are as follows:

- ❑ The time required to establish a dedicated circuit between two stations is 10 s approximately and this time duration increases more depending upon the distance between the stations. For many applications, this is unsuitable and undesirable.

- ❑ The resources are not efficiently utilized during circuit switching in a computer network
- ❑ For communication amongst stations that use costly and high-speed transmission lines, circuit switching is not cost effective and economical, as communication between stations occurs generally in fast and small time gaps.

Packet Switching

Packet switching introduces the idea of breaking data into packets, which are discrete units of potentially variable length blocks of data. Apart from data, these packets also contain a header with control information such as the destination address and the priority of the message. These packets are passed by the source point to their local packet switching exchange (PSE). When the PSE receives a packet, it inspects the destination address contained in the packet. Each PSE contains a navigation directory specifying the outgoing links to be used for each network address. On receipt of each packet, the PSE examines the packet header information and then either removes the header or forwards the packet to another system. If the communication channel is not free, then the packet is placed in a queue until the channel becomes free. As each packet is received at each transitional PSE along the route, it is forwarded on the appropriate link mixed with other packets. At the destination PSE, the packet is finally passed to its destination. Note that not all packets of the same message, travelling between the same two points, will necessarily follow the same route. Therefore, after reaching their destination, each packet is put into order by a packet assembler and disassembler (PAD).

For example, in Figure 5.18, four packets (1, 2, 3 and 4) once divided on machine A are transmitted via various routes, which arrive on the destination machine D in an unordered manner. The destination machine then assembles the arrived packets in order and retrieves the information.

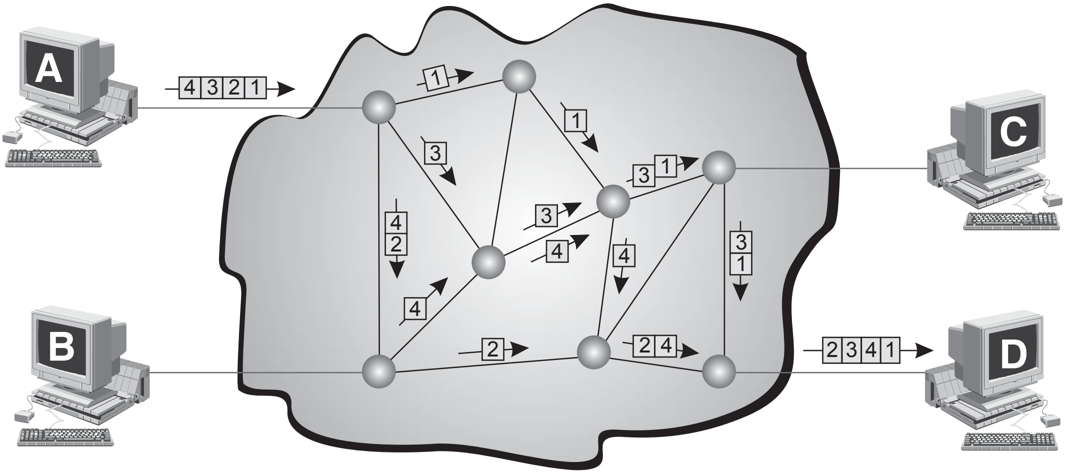


Figure 5.18 Packet Switching

Some advantages of packet switching are as follows:

- ❑ It is a fault-tolerant technique.
- ❑ It provides a much fairer and cost-efficient sharing of the resources. In addition, if no data is available to the sender at some point during a communication, then no packet is transmitted over the network and no resources are wasted.

- ❑ It requires lesser storage capacity for stations.
- ❑ The transmission rate in packet switching is fast.

Some disadvantages of packet switching are as follows:

- ❑ As packets do not follow a specific path, they may arrive out of order at the destination
- ❑ The cost incurred per packet is large.

Message Switching

A message is a unit of information which can be of varying length. Message switching is one of the earliest types of switching techniques, which was common in the 1960s and 1970s. This switching technique employs two mechanisms; they are *store-and-forward mechanism* and *broadcast mechanism*. In **store-and-forward mechanism** (Figure 5.19), a special device (usually, a computer system with large storage capacity) in the network receives the message from a communicating device and stores it into its memory. Then, it finds a free route and sends the stored information to the intended receiver. In such kind of switching, a message is always delivered to one intermediate device where it is stored and then rerouted to its final destination

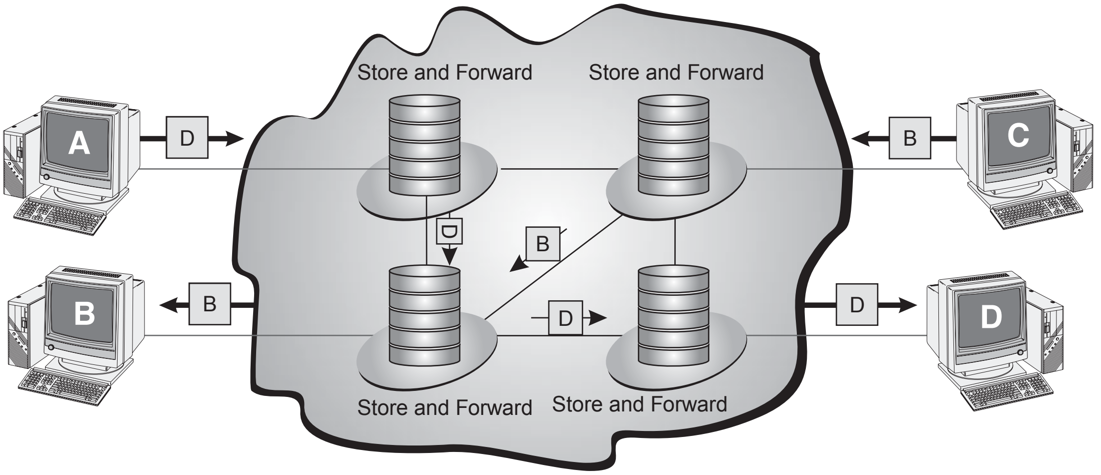


Figure 5.19 Store-and-Forward Mechanism of Message Switching

In **broadcast switching mechanism**, the message is broadcasted over a broadcast channel as shown in Figure 5.20. As the messages pass by the broadcast channel, every station connected to the channel checks the destination address of each message. A station accepts only the message that is addressed to it.

Some advantages of message switching are as follows:

- ❑ In message switching technique, no physical path is established in advance.
- ❑ The transmission channels are used very effectively in message switching, as they are allotted only when they are required.

Some disadvantages of message switching are as follows:

- ❑ It is a slow process.

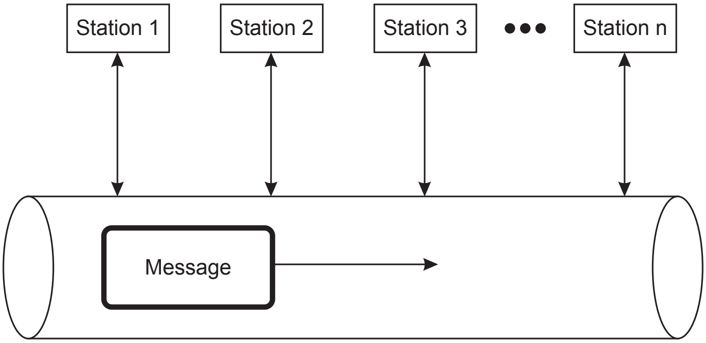


Figure 5.20 Broadcast Mechanism of Message Switching

- It involves propagation and queuing delay; in addition, a large capacity of data storage is required.
- With unlimited message length, the switching nodes needed to have a larger storage space to buffer the message.

17. Compare circuit switching, packet switching and message switching techniques.

Ans: The comparison of circuit switching, packet switching and message switching is summarized in Table 5.1.

Table 5.1 Comparison of Circuit Switching, Packet Switching and Message Switching

Circuit switching	Packet switching	Message switching
• A physical circuit is established before transmission begins.	• No physical circuit is established before transmission.	• No physical circuit is established before transmission.
• Message to be transmitted is in the form of packets.	• Message to be transmitted is in the form of packets.	• Message to be transmitted is in the form of blocks.
• Store-and-forward technique is not used.	• Store-and-forward technique is used.	• Store-and-forward technique is used.
• It can be used with real-time applications.	• It can be used with real-time applications.	• It cannot be used with real-time applications.
• It is used in telephone network for bi-directional, fast and real-time data transfer.	• It is used for the Internet.	• It was used in the transmission of voice signals and messages.

18. Describe the major components of a telephone network?

Ans: The traditional telephone network, referred to as **plain old telephone system** (**POTS**), was purely an analog system used to transmit voice. However, with advancement in computing technologies, they were used to transmit other data along with voice. Three major components of a telephone network are *local loops*, *trunks* and *switching office* (Figure 5.21). These components are described as follows:

- **Local Loops:** A twisted-pair cable connection between each subscriber's telephone and the nearest end office of telephone company (also called **local central office**) is referred to as a local loop. Generally, the distance between the subscribers' telephone and the nearest end office is 1–10 km.

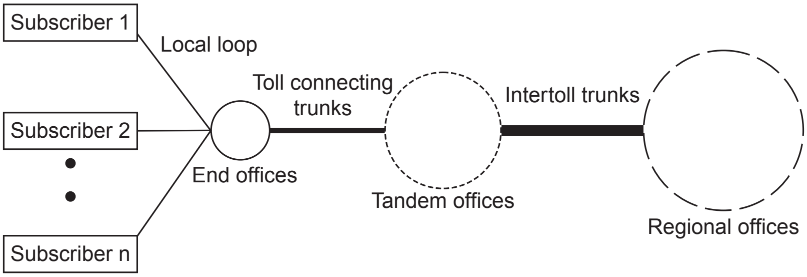


Figure 5.21 Components of a Telephone Network

Also referred to as the **last mile**, the local loops follow analog technology and can extend up to several miles. When a local loop utilized for voice, its bandwidth is 4 kHz. Earlier, uninsulated copper wires were commonly used for local loops. However, these days, category 3 twisted pairs are used for local loops.

- ❑ **Trunks:** The transmission media used for communication between switching offices is referred to as trunk. Generally, fibre-optic cable or satellite transmission is used for trunks. A single trunk can carry multiple conversations over a single path by using a multiplexing technique.
- ❑ **Switching Offices:** In telephone network, no two subscribers are connected by a permanent physical link. Instead, switches are used to provide a connection between the different subscribers. These switches are located in the switching offices of the telephone company and connect many local loops or trunks. In telephone network, there are several levels of switching offices including end offices, toll offices, tandem offices and regional offi

When a subscriber calls to another subscriber connected to same end office, a direct electrical connection is established between the local loops with the help of switching mechanism within the end office. However, if the called subscriber's telephone is connected to a different end office, the connection is established by the toll offices or tandem offices. Several end offices are connected to their nearby switching centre called toll office or tandem office (if end offices are in the same local area) through **toll connecting trunks**. If the caller and called subscriber do not have a common toll office, the connection between them is established by regional offices to which toll offices are co ected via high bandwidth **intertoll trunks**.

19. Explain dial-up modems along with their standards in detail.

Ans: The word **modem** is an acronym for ***mo*dulator-*dem*odulator**. The **modulator** converts digital data into analog signals (that is, **modulation**) and the **demodulator** converts the analog signal back into digital data (that is, **demodulation**). A dial-up modem uses the traditional telephone line as the transmission media and enables to send digital data over analog telephone lines.

Figure 5.22 depicts the modulation/demodulation process during communication between machines A and B. At the sender' side (that is, machine A), the digital signals from machine A are sent to the modem, which converts them into analog signals. These analog signals are transmitted over the telephone lines and received by the modem at the receiver's end (that is, machine B). The modem at machine B converts analog signals back into digital signals and sends them to computer B.

ITU-T gave V-series standards for effective working of modems. Some modems of this series are as follows:

- ❑ **V.22:** This modem transmits data at 1,200 bps and works over two-wire leased line. It provides full-duplex synchronous transmission.

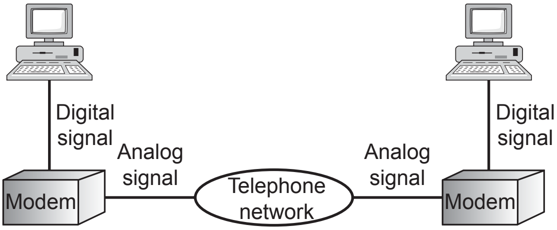


Figure 5.22 Modulation/Demodulation Process

- **V.32:** This modem transmits data at 9,600 bps and designed for full-duplex synchronous transmission. This modem works on two-wire leased line or telephone network. This standard uses the technique called **trellis coding** that detects error which gets introduced during transmission. In this coding, data stream is divided into four-bit sections and one extra bit is added to each quadbit (four-bit pattern) during data transmission for error detection.
- **V.32bis:** This modem transmits data at 14,400 bps and is the enhancement of V.32 standard. V.32bis includes feature of fall-back and fall-forward which help the modem to adjust upstream and downstream speed automatically. This adjustment of speed depends on the quality of the signal.
- **V.34:** This modem transmits data up to 33.6 kbps and works on a two-wire leased line. It is designed for full-duplex synchronous and asynchronous transmissions and also supports error correcting feature.
- **V.90:** This modem is designed for full-duplex synchronous and asynchronous transmission over two-wire connection. The V.90 series modems are also called **56-K modems** because their data transmission rate is 56 kbps. They are asymmetric in nature as the speed of upstream and downstream varies. They support downloading data rate up to 56 kbps and uploading up to 33.6 kbps. The main reason for the difference in the speed between uploading and downloading is that in uploading, signal gets sampled at various switching stations and gets affected by noise which is introduced here but in downloading, there is no such sampling of signals.
- **V.92:** This modem has the capability to upload the data at the rate of 48 kbps while its downloading data rate is same as that of V.90 standard, that is, 56 kbps. This modem has the advanced feature of call-waiting service.

20. Write a short note on DSL and its different technologies.

Ans: DSL (stands for **digital subscriber line)** was developed by the telephone companies to fulfil the requirement of high-speed data access and the efficient utilization of the bandwidth of the local loops. DSL is a very promising technology, as it provides the customers with a telephone connection and high-speed Internet access simultaneously over the existing local loops. To provide a simultaneous telephone connection and Internet access, DSL systems are installed between the telephone exchange and the customers' site.

The DSL technology comprises many different technologies including *ADSL*, *VDSL*, *HDSL* and *SDSL*. Often, this group of technologies is referred to as *x*DSL where *x* represents A, V, H or S. These technologies are described as follows:

- **ADSL:** It stands for **asymmetric digital subscriber line**, also called **asymmetric DSL**. ADSL uses the existing local loops and provides a higher downstream rate from the telephone exchange to the subscriber than in the reverse direction. This asymmetry in data rates is suitable for the applications such as video-on-demand and Internet surfing, as the users of these applications need to download more data in comparison to uploading and that too at a higher speed. Along with the Internet service, ADSL also provides simultaneous telephone connection over the same copper cable. By using FDM, the voice signals are separated from data signals (upstream and downstream). ADSL technology is useful for residential customers and not for the business customers, as business customers often require larger bandwidth for both downloading and uploading.

- **ADSL Lite:** It is a newer version of the ADSL technology. Also known as the **spliterless ADSL**, this technology can provide a maximum upstream data rate of 512 kbps and a maximum downstream data rate of 1.5 Mbps. This technology differs from ADSL technology in the sense that ADSL technology requires installing a splitter at the subscribers' home or business location to split voice and data, while if ADSL Lite modem is used, no such splitter is required at the premises of the subscriber and all the splitting is done at the telephone exchange. The ADSL Lite modem is directly plugged into the telephone's jack at the subscribers' premises and connected to the computer.
- **HDSL:** It stands for **high-bit-rate digital subscriber line**, also called **high-bit-rate DSL**. It was developed by Bellcore as a substitute for the T-1 (1.544 Mbps) line. In T-1 lines, alternate mark inversion (AMI) encoding is used. This encoding is subject to attenuation at high frequencies and repeaters are to be used for covering longer distance. Thus, it was quite expensive. On the other hand, in HDSL, 2B1Q encoding is used which is less susceptible to attenuation at higher frequencies. Also, a very high data rate of 1.544 Mbps can be achieved without using repeaters to a distance of approximately 4 km. To achieve full-duplex transmission, HDSL uses two twisted pairs with one pair for each direction. HDSL2, a variant of HDSL, uses single pair of twisted cables and is under development.
- **SDSL:** It stands for **symmetric digital subscriber line**, also called **symmetric DSL**. It was developed as a single copper pair version of HDSL. SDSL uses 2B1Q line coding and provides full-duplex transmission on a single pair of wires. It provides same data rate of 768 kbps for both upstream and downstream, as it supports symmetric communication.
- **VDSL:** It stands for **very high-bit-rate digital subscriber line**, also called **very high-bit-rate DSL**. It is similar to ADSL and offers very high data transfer rates over small distances using coaxial, fibre-optic and twisted-pair cables. The downstream data rate for VDSL is 25–55 Mbps and the upstream data rate is generally 3.2 Mbps.

Table 5.2 summarizes all the DSL technologies along with their characteristics.

Table 5.2 Summary of the DSL Technologies

Technology	Upstream rate	Downstream rate	Distance in thousands feet	Simultaneous voice capacity	Number of twisted pairs
ADSL	16–640 kbps	1.5–6.1 Mbps	12	Yes	1
ADSL Lite	500 kbps	1.5	18	Yes	1
HDSL	1.5–2.0 Mbps	1.5–2.0 Mbps	12	No	2
SDSL	768 kbps	768 kbps	12	Yes	1
VDSL	3.2 Mbps	25–55 Mbps	3–10	Yes	1

21. What are the two types of switch technologies used in circuit switching? Compare them.

Ans: In circuit switching, two types of switch technologies are used, namely, *space-division switch* and *time-division switch*.

Space-Division Switch

In space-division switching, many different connections in the circuit that are active at the same time use different switching paths which are separated spatially. Initially, this technology was developed for the analog signals; however, presently, it is being used for both analog signals and DSs. Space-division switches may be *cross-bar switches* or *multistage switches*.

- **Cross-bar Switch:** This switch connects `p` input lines with `q` output lines in the form of a matrix of the order `p×q`; the value of `p` and `q` may be equal. Each input line is connected to output line with the help of a transistor at each **cross-point**—the intersection point of input and output lines. Each cross-point is basically an electric switch that can be opened or closed by a control unit depending on whether or not communication is required between the connecting input and output lines. Figure 5.23 shows a schematic diagram of a 4 × 4 cross-bar switch.

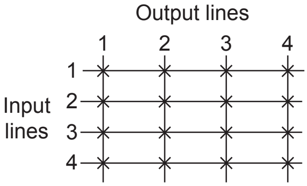


Figure 5.23 A 4 × 4 Cross-bar Switch

A cross-bar switch has certain limitations, which are as follows:

- To connect `m` inputs with `m` outputs, m^2 number of cross-points is required. In addition, the number of cross-points required increases with the increase in number of lines to be connected. This makes the cross-bar switches expensive and more complex.
- The cross-points are not utilized properly. Even when all the devices are connected, only a few cross-points are active.
- If a cross-point fails, the devices connected via that cross-point cannot connect to each other.

- **Multistage Switch:** This switch overcomes the limitations of the cross-bar switch. A multistage space-division switch consists of several stages, each containing `(p×q)` cross-bar switches. These switches can be connected in several ways to build a large multistage network (usually, three-stage network). In general, for `n` inputs and `n` outputs, $m = \log_2 n$ stages are required. Figure 5.24 shows a three-stage space-division switch. Here, each cross-point in the middle stage can be accessed through several cross-points in the first or third stage

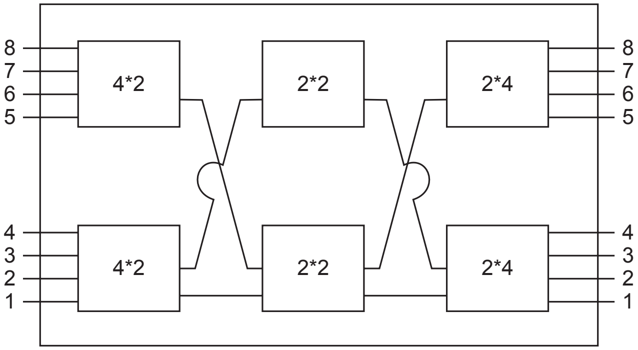


Figure 5.24 A Three-stage Space-division Switch

The main advantage of multistage switches is that the cost of having an m × m multistage network is much lower than that of an m × m cross-bar switch because the former network requires a lesser number of cross-points as compared to the latter network. However, in case of heavy traffic, it suffers from **blocking** problem due to which it cannot process every set of requests simultaneously.

Time-division Switch

In time-division switch, TDM is implemented inside a switch. Various active connections inside the switch can utilize the same switching path in an interleaved manner. One of the commonly used methods of time-division switching is **time slot interchange** (**TSI**), which alters the sequencing of slots depending on the connection desired. TSI has a random access memory (RAM) and a control unit. The data is stored in RAM sequentially, however, retrieved selectively based on the information in control unit. The control unit stores the control information such as which input line to connect to which output.

Figure 5.25 depicts the operation of TSI. Suppose the input lines want to send data to output lines in the order 1 to 4, 2 to 3, 3 to 2 and 4 to 1. This information is stored in control unit. At the sender's end, the input unit from each of the four input lines is put serially into time slots to build a frame. The data in the time slots is stored on the RAM in the exact order in which it is received, that is, A, B, C and D. The data is retrieved from RAM and then filled up in the time slots of the output frame in the order as determined by the control unit, that is, D, C, B and A.

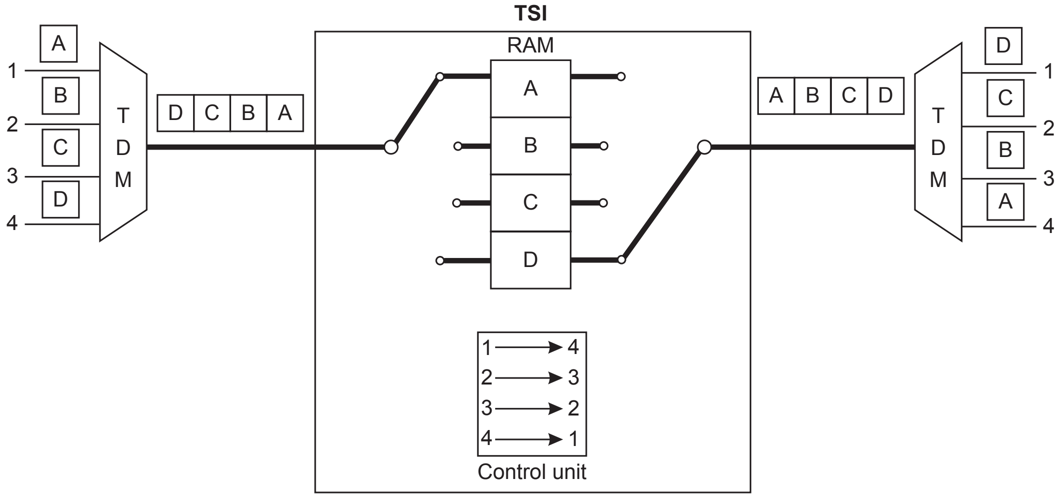


Figure 5.25 Time-division Switch

A disadvantage of time-division switching is that it requires a sufficient amount of RAM always to be able to store and forward data from the incoming frames to the outgoing frames.

22. Explain in brief about the generations of cable TV networks.

Ans: Cable TV networks provide a wide variety of services ranging from distributing video signals to Internet access. There are mainly two generations of cable networks: *traditional cable networks* and *hybrid-fib e-coaxial networks.*

Traditional Cable Networks

Cable TV network started providing video services in the late 1940s. An antenna mounted on the top of a building or tower was used to receive the signals from the TV stations and to distribute them to subscribers with the help of coaxial cables. That's why it was also referred to as **community antenna TV** (**CATV**).

Figure 5.26 shows a conceptual view of traditional cable networks. The broadcasting stations send video signals to cable TV office called **head end**. The head end transmits these video signals to subscribers' houses with the help of coaxial cable. To deal with the attenuation problem, amplifiers were used. At the subscribers' end, splitters were used to split the cable and taps and drop cables were used to make the connection to the subscriber's houses. Communication in these cable networks was unidirectional; signals could be transmitted only in one direction from cable TV office to subscribe 's premises.

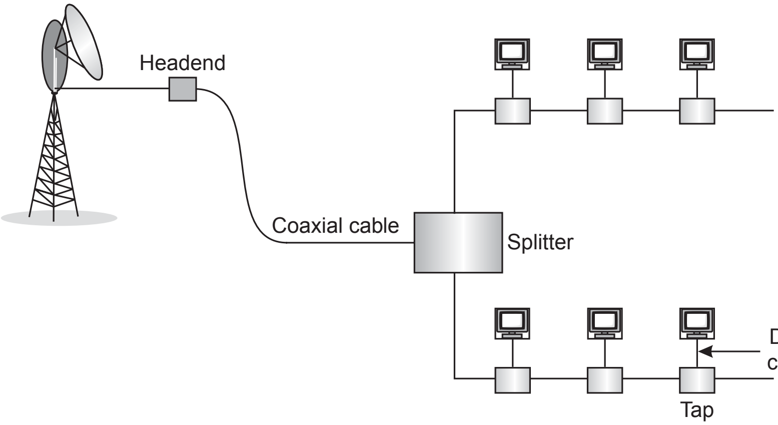


Figure 5.26 Traditional Cable TV Network

Hybrid Fibre-coaxial (HFC) Network

In this generation of cable TV network, cable operators decided to provide Internet services. This cable network is so called because it uses both the fibre-optic cable and the coaxial cable, the fibre-optic cable for long haul runs while coaxial cable to the houses. The interface between the electrical and the optical parts of the system is provided through electro-optical converters known as **fib e nodes**.

Figure 5.27 shows an HFC network. The signals transmitted from cable TV office, referred to as **regional cable head** (**RCH**), are passed to the distribution hubs that act as subordinate to RCH.

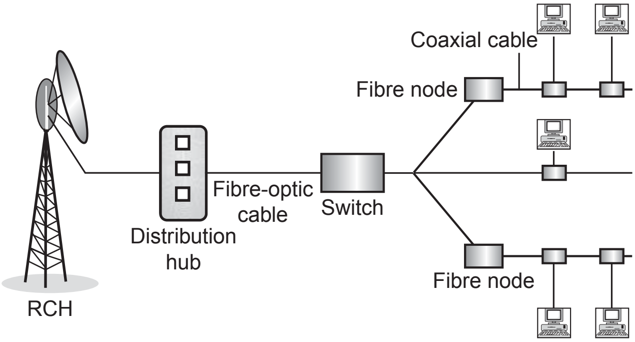


Figure 5.27 HFC Network

The distribution hubs perform modulation of signals and distribute them to fibre nodes over the fibre-optic cable. The fibre nodes split the signal to send same signal to each coaxial cable

In comparison to traditional cable TV network, HFC network requires less number of amplifiers as well as offers bidirectional communication.

23. Which devices are needed for using cable networks for data transmission?

Ans: Traditional cable TV network was used only for providing video signals but nowadays, HFC network—an extension of traditional cable TV network—is being used to provide high-speed access to the Internet. However, to use cable TV network for data transmission, two devices are needed, namely, *cable modem* (*CM*) and *CM transmission system* (*CMTS*).

Cable Modem

This is an external device that is installed at the end user's premises where the Internet has to be accessed. It is connected to the user's home PC via Ethernet port and it works similar to an ADSL modem. CM divides the HFC network into two channels, upstream and downstream channels, with downstream channel having a higher data transmission rate than the upstream channel. The upstream channel is used for transmission from the home PC to the head end and the downstream channel is used to handle transmission in the opposite direction. Since HFC is a shared broadcast network, each packet from the head end is broadcasted on every link to every home; however, vice versa does not happen. As a result, when several users are downloading contents simultaneously through the downstream channel, the transmission rate received by each user is much lesser than the actual rate of downstream channel. In contrast, when only some users are surfing the web, each user will receive a full downstream rate because it is very rare that two users request the same page at the same time.

Cable Modem Transmission System

This device is installed inside the distribution hub of HFC network by the cable company. The data is received by the CMTS from both the Internet and the user. When CMTS receives data from Internet, it passes the data to the combiner. The combiner combines the data with the video signals received from head end and passes the resultant information to the intended user. On the other hand, the data received by the CMTS from the end user is simply forwarded to the Internet.

24. Write a short note on ISDN.

Ans: **ISDN** (stands for **integrated services digital network**) was developed by ITU-T in 1976. The idea behind ISDN is to digitize the telephone network, so that all the data including audio, video and text could be transmitted over existing telephone lines. The main objective of ISDN is to create a wide area network (WAN) for providing global end-to-end connectivity over digital media. For this, it integrates different transmission services with no addition of new links or subscriber lines. ISDN provides higher data rates usually 2 Mbps on a local link and 64 kbps or 128 kbps on a wide area link.

ISDN caters to the need of both voice and non-voice applications of the same network. It also supports a variety of applications which involve switched (circuit switched or packet switched) as well as non-switched connections. The new services can be added to ISDN provided they are compatible with 64 kbps switched digital connections. ISDN can use X.25 standards and can be used as local access link in frame relay and X.25 networks.

Though ISDN is a digital service and offers much more bandwidth than standard telephone service, still like telephone service, the ISDN users also need to dial an ISDN number (different from standard telephone number) for establishing a connection and connecting to other sites. A user can establish a digital connection by dialling another ISDN number from his/her own ISDN number. However, unlike leased lines which provide permanent connection, the ISDN users can disconnect ISDN WAN link whenever desired.

25. What are the two types of ISDN?

Ans: Based on the transmission and switching capabilities, there are two types of ISDN, namely, *narrowband ISDN* and *broadband ISDN*.

- **Narrowband ISDN (N-ISDN):** This is the first generation of ISDN and uses circuit-switching technique. It has smaller bandwidth and supports low bit rates (usually up to 64 kbps). Due to lower bit rates, N-ISDN cannot cater to the needs of certain applications such as multimedia applications. Four-wire twisted pairs are used for transmission in N-ISDN thereby resulting in poor quality of service. N-ISDN follows the concept of frame relay.
- **Broadband ISDN (B-ISDN):** This is the second generation of ISDN and uses packet-switching technology. It supports high-resolution video and multimedia applications. It can support data rates of hundreds of Mbps (usually up to 622 Mbps) and thus, is suitable to be used for high-resolution video and multimedia applications. Optical fibre is used as the transmission media for B-ISDN thereby resulting in better quality of service as compared to N-ISDN. B-ISDN follows the concept of cell relay.

26. What are the services provided by ISDN?

Ans: ISDN provides various services including data applications, existing voice applications, facsimile, videotext and teletext services. These services are grouped under the following three categories.

- **Bearer or Carrier Services:** These services allow the sender and the receiver to exchange information such as video, voice and text in real time. A message from the sender can be communicated to the receiver without any modification in the original content of the message. Bearer services are provided by ISDN using packet switching, circuit switching, cell relay and frame relay. These services correspond to the physical, data link and network layers of the OSI model.
- **Teleservices:** These services not only permit to transport information but include information-processing function also. To transport information, teleservices make use of bearer services while to process the information, a set of higher-level functions that correspond to the transport, session, presentation and application layers of the OSI model are used. Some examples of teleservices are videotex, teletex and telefax.
- **Supplementary Services:** These services are used in combination with at least one teleservice or bearer service but cannot be used alone. For example, reverse charging, call waiting and message handling are some of the supplementary services that are provided with the bearer and teleservices.

27. Describe the type of channels provided by ISDN along with their purpose.

Ans: The ISDN standard has defined three types of channels, namely, *bearer* (*B*) *channel*, *data* (*D*) *channel* and *hybrid* (*H*) *channel*, with each channel having a specific data rate

- **B Channel:** This is the basic channel used to carry only the user traffic in digital form such as digitized voice and digital data at the rate of 64 kbps. The transmission through B channel is full-duplex as long as the required data transmission rate is up to 64 kbps. Multiple conversations destined for a single receiver can be carried over a single B channel with the use of multiplexing. Since a B channel provides end-to-end transmission, signals can be demultiplexed only at the receiver's end and not in the mid way.

- **D Channel:** This channel is mainly used to carry the control information that is required for establishing and terminating the switched connections on the B channels. For example, the dialled digits while establishing a telephone connection are passed over the D channel. Under certain circumstances, the D channel can be used to carry user data also. The D channel provides data rates of 16 or 64 kbps depending on the requirements of the user.
- **H Channel:** This channel is used for applications having higher data requirements such as video-conferencing and teleconferencing. There are certain types of H channels including H0 channel with a data rate of 384 kbps, H11 channel with a data rate of 1,536 kbps and H12 channel with a data rate of 1,920 kbps.

28. Distinguish BRI and PRI in ISDN.

Ans: In ISDN network, each user is connected to the central office via digital pipes called **digital subscriber loops**. The digital subscriber loops are of two types, namely, *basic rate interface* (*BRI*) and *primary rate interface* (*PRI*), with each type catering to a different level of customers' needs. Table 5.3 lists some differences between these two types.

Table 5.3 Differences Between BRI and PRI

BRI	PRI
• It comprises two B channels and one D channel, thus, referred to as **2B + D** channel.	• It comprises up to 23 B channels and one D channel in North America and Japan. In countries such as Europe, Australia and other parts of the world, it comprises 30 B channels and one D channel.
• The BRI-D channel operates at 16 kbps.	• The PRI-D channel operates at 64 kbps.
• It provides total bit rate of 192 kbps.	• In North America and Japan, it provides total bit rate of 1.544 Mbps and in other parts of the world, it provides total bit rate of 2.048 Mbps.
• It is primarily used at home for connecting to Internet or business networks.	• It is primarily used in business replacing the leased lines that can provide the same bandwidth and signal quality but with more flexibility.

29. Explain the architecture of ISDN.

Ans: In ISDN network, to enable the users to access the services of BRI and PRI, certain devices are used. The main devices used in the architecture of ISDN (Figure 5.28) include terminal equipment (types 1 and 2), network termination devices (types 1 and 2) and terminal adapters. All these devices are used in the subscriber's premises. In addition, several reference points are used to determine the interfaces between any two elements of ISDN installation. The description of these equipments is as follows:

- **Terminal Equipment 1 (TE1):** It refers to a device that supports ISDN standards. For example, computer or ISDN telephone. To connect TE1s to the ISDN network, a four-wire twisted-pair cable is used.
- **Terminal Equipment 2 (TE2):** It refers to a device that is non-specialized ISDN. For example, the standard telephone is a non-ISDN device.

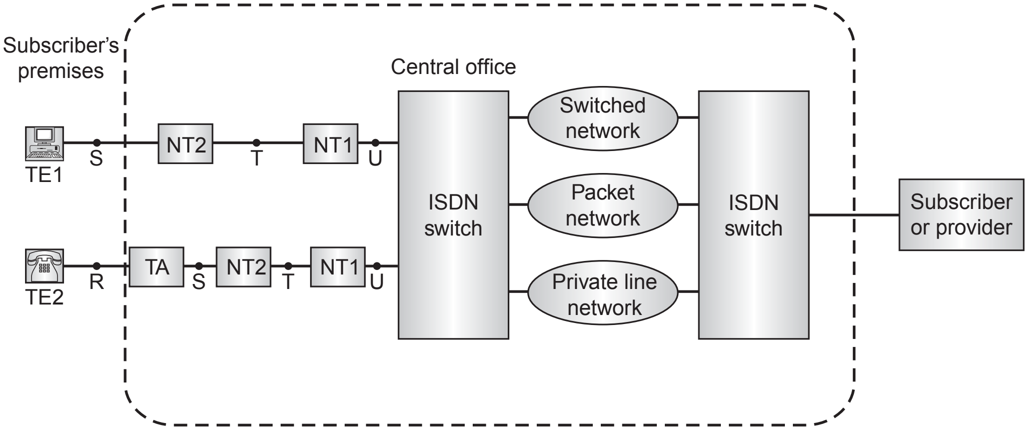


Figure 5.28 Architecture of ISDN

- **Terminal Adapters:** It refers to a device that translates the information in a non-ISDN format into a form usable by an ISDN device. It is generally used with TE2s devices.
- **Network Termination 1 (NT1):** It refers to a device that connects the internal system at the subscriber's end to digital subscriber loop. It organizes the data received from the subscriber's end into frames that are to be sent over the network. It also translates the frames received from the network into a format which can be understood by the subscriber's devices. It interleaves the bytes of data from subscriber's devices but is not a multiplexer; the multiplexing occurs automatically, as NTI provides synchronization between the data stream and the process of creating a frame.
- **Network Termination 2 (NT2):** It refers to a device that performs multiplexing, flow control and packetizing at the physical, data link and network layers of OSI model, respectively. It acts as an intermediate device between data-producing devices and NT1. An example of NT2 is private branch exchange (PBX) that coordinates transmissions from telephone lines and multiplexes them, so that they can be transmitted by NT1.
- **Reference Points:** It refers to a tag that is used to define logical interfaces between various termination devices. The reference points used in ISDN architecture include R, S, T and U. **Reference point R** specifies the link between TE1 and TA. **Reference point S** specifies the link between TE1 or TA and NT1 or NT2. **Reference point T** specifies the link between NT1 and NT2. **Reference point U** specifies the link between NT1 and ISDN offic

To exchange the control information between end user and the network, protocols are used. ISDN uses more than one twisted pair to provide the full-duplex communication link between the end user and the central office. The operation performed by central office includes accommodating multiplexed access to provide high-speed interface using digital PBX and LAN. With the help of central office, subscriber can access circuit switched network and packet switched network.

30. Five 1-kbps connections are multiplexed together and each unit represents 1 bit. Find:

(a) the duration of 1 bit before multiplexing,

(b) the transmission rate of the link,

(c) the duration of a time slot and

(d) the duration of a frame.

Ans: (a) The duration of one bit before multiplexing is 1/1 kbps, that is, 0.001 s or 1 ms.

(b) The transmission rate of the link will be five times the data r te of the connection, that is, 5 kbps.

(c) The duration of a time slot will be one-fifth of the duration of each bit before multiplexing, that is, 1/5 ms or 200 µs.

(d) Since there are five slots in a frame, the duration of a frame will be equal to five times the duration of a time slot, that is, 5 × 200 µs or 1 ms.

31. Five channels, each with a 100-KHz bandwidth, are to be multiplexed together. What is the minimum bandwidth of the link if there is a need for a guard band of 10 KHz between the channels to prevent interference?

Ans: To multiplex five channels, four guard bands are needed. Thus, the minimum bandwidth (B) required will be calculated as follows:

$$B = 5 \times (100\text{ KHz}) + 4 \times (10\text{ KHz}) = 540\text{ KHz}$$

Multiple Choice Questions

1. A device that combines *n* input lines into a single stream is known as ________.
   (a) Demultiplexer
   (b) Serial to parallel convertor
   (c) Prism
   (d) Multiplexer

2. Multiplexing can be used in situations where the signals to be transmitted through the transmission medium have ________ bandwidth than that of the medium.
   (a) Higher (b) Lower
   (c) Equal (d) None of these

3. Which of the following multiplexing techniques involves signals composed of light beams?
   (a) FDM (b) TDM
   (c) WDM (d) All of these

4. Multilevel multiplexing and multiple-slot allocation are the strategies used in
   (a) TDM (b) WDM
   (c) Both (a) and (b) (d) FDM

5. The digital signal service has ________ levels.
   (a) Five (b) Seven
   (c) Six (d) Eight

6. Which of the following is not a group in the analog hierarchy?
   (a) Voice channels
   (b) Master groups
   (c) Slave groups
   (d) Jumbo groups

7. A technique used to expand the bandwidth of a communication link to achieve goals such as privacy and anti-jamming is called _________.
   (a) Spread spectrum
   (b) Multiplexing
   (c) Switching
   (d) Pulse stuffin

8. Which of the following is not a switching technique?
   (a) Circuit switching
   (b) Data switching
   (c) Message switching
   (d) Packet switching

9. Store-and-forward technique is used in
   (a) Message switching
   (b) Packet switching
   (c) Time-division multiplexing
   (d) Both (a) and (b)

10. The transmission media used for communication between switching offices is referred to a
    (a) Switch
    (b) Local loop
    (c) Trunk
    (d) None of these

11. Which of the following is a DSL technology?
    (a) ADSL Lite
    (b) VDSL
    (c) SDSL
    (d) All of these

12. The broadcasting stations send video signals to cable TV office, called ______
    (a) Fibre node
    (b) Head end
    (c) Toll offic
    (d) CATV

13. Narrow band ISDN supports bandwidth up to
    (a) 128 kbps
    (b) 112 kbps
    (c) 96 kbps
    (d) 64 kbps

Answers

1. (d) 2. (b) 3. (c) 4. (a) 5. (a) 6. (c) 7. (a) 8. (b) 9. (d) 10. (c)
11. (d) 12. (b) 13. (d)

6

Error Detection and Correction

1. Explain various design issues of the data link layer.

Ans: Data link layer is responsible for efficient and reliable transmission of frames between two adjacent nodes connected via a single communication channel. However, sometime, the efficiency of data transfer is significantly affected due to finite data rate of communication circuits, non-zero propagation delay between the sending and the receiving times of a bit, and errors in connection. Thus, to achieve efficient data transmission, all these factors must be kept in mind. Some of the important design issues of data link layer are as follows:

- **Reliable Delivery:** Frames sent by a sender must reach the receiver reliably and in the same order as sent by the sender. For effective transmission, a receiver must let the sender to know which frames have been received and which frames need to be retransmitted.
- **Flow Control:** Each node connected on a link has its own limited frame-buffering capacity. Without a flow control mechanism, if a sender sends frames at a rate that is higher than the receiver can receive, then some frames may be lost. Therefore, the data link layer should provide flow control in such a way that sender should not send frames at a rate that is faster than the receiver can process it.
- **Acknowledged Delivery:** A receiver must send an acknowledgement frame to indicate the sender that a frame has been received properly. For this, each frame transmitted from the sender is given a unique sequence number, so that unacknowledged frames that have got damaged or lost during transmission can be known and the sender can retransmit those frames.
- **Error Detection and Correction:** Bit errors may introduce during the transmission of a frame because of the signal attenuation and electromagnetic noise. For example, bit 1 may be replaced with bit 0 or vice versa. Therefore, the sender must add certain error-detection bits in the frame, so that the receiver can check whether a frame contains some errors or not. The receiver should not only be able to detect errors but also be able to determine the location of the errors in the frame and then correct the errors as well.
- **Addressing:** The media access control (MAC) address of the sender and receiver must be specified in the frames that are transmitted by the data link layer. This would ensure the delivery of frames to the appropriate receiver.

2. What are the different types of services provided by the data link layer to the network layer?

Ans: The data link layer offers various services to the network layer; however, some of the basic types are as follows.

- □ **Unacknowledged Connectionless Service:** As the name suggests, this is a connectionless service, that is, no logical connection between the sender and the receiver needs to be established or released before or after the transmission respectively. In addition, the receiver does not send acknowledgement frame to the sender on receiving a data frame. If a frame is lost or damaged during the transmission, no attempt is made to discover the loss and recover from it. This type of service is suitable for applications with low error rate and for real-time traffi such as voice.
- □ **Acknowledged Connectionless Service:** In this service also, no logical connection is established between the communicating nodes; however, each frame received by the receiver is acknowledged in order to indicate the sender that the data frame has been received properly. Thus, the frames for which the sender does not receive any acknowledgement within a stipulated time can be retransmitted. This service is suitable for wireless systems.
- □ **Acknowledged Connection-oriented Service:** In this type of service, a connection is established between the communicating nodes before starting data transmission. The data link layer ensures that each frame is received exactly once by the receiver and all the frames are received in the correct order. For this, each frame is numbered before the transmission and the receiver sends back an acknowledgement frame on receiving a data frame. In a connection-oriented service, the data transfer takes place by following three phases, namely, *connection establishment*, *data transmission* and *connection release*. During the first phase, a connection is made between the sender and the receiver. For establishing a connection, both sender and receiver initialize some variables and counters to identify the frames that have been received and that have not. After the connection has been established, the second phase commences during which the actual transmission of frames is carried out between the sender and the receiver. After the frames have been transmitted, the third phase begins in which the connection is released by freeing up the used variables, counters and buffers.

3. What is framing? Discuss various framing methods.

Ans: The data link layer accepts the bit stream from the physical layer and breaks it into discrete frames. This process is known as **framing**. For ensuring that the bit stream is free of errors, the data link layer computes the checksum of each transmitting frame at the sender's side. After the frame has been received, the data link layer on the receiver's side re-computes the checksum. If the new value of checksum differs from the checksum contained in the frame, then the data link layer comes to know that an error has occurred and takes appropriate measures to deal with errors. For example, some bad frames can be discarded and the request for their retransmission can be made.

In order to make the receiver to detect the frame boundaries, several framing methods have been developed. These methods are described as follows.

Character Count

This framing method uses a field in the header of each frame which specifies the total number of characters in that frame. This field helps the data link layer at the destination node in knowing the number of characters that follow and detecting the end of each frame. The disadvantage of this method is that while transmitting a frame, the count of total characters in it may alter due to errors, thereby making the destination node go out of synchronization. Furthermore, the destination node will not be able to locate the correct start of the new frame and, therefore, asking sender for the retransmission of the frame, as the destination node does not know the exact count of characters that should be skipped to get to the start of the retransmission.

Byte Stuffing

This framing method uses a byte called the **flag byte** at the starting and the ending of each frame. This helps the destination node to find the end of the current frame even if the destination goes out of synchronization. The presence of two successive flag bytes marks the ending of one frame and the beginning of the next one. However, a problem occurs when binary data such as object programs or floating-point numbers are transmitted. In such cases, the bit pattern of the flag byte may also appear in the data and thus, may cause interference with the framing. To solve this problem, the data link layer at the sender's side can insert a special **escape byte** (**ESC**) before each flag byte appearing in the data. At the destination node, the data link layer stripes off the escape byte and passes the data to the network layer.

Now, it may also happen that the escape byte appears in the data. To prevent the escape byte from being mixed with the data, each escape byte appearing in data is stuffed with another escape byte. Thus, a single escape byte in the data indicates that it is a part of escape sequence while the occurrence of two consecutive escape bytes in the data indicates that one escape byte is the part of data. The disadvantage of this framing method is that it can only be used for eight-bit characters; therefore, this method cannot be used for the character codes that use more than eight bits. Byte stuffing is also referred to as **character stuffing**.

Bit Stuffing

This framing method overcomes the limitation of byte stuffing and can be used with any number of bits per character and allows a data frame to comprise an arbitrary number of bits. In bit-stuffing method, a special bit pattern, 01111110, called **flag byte** is inserted at the start and end of each frame. In order to prevent the occurrence of flag byte in data to get misunderstood as start or end of frame, when a sender's data link layer finds five consecutive 1s in the data, it automatically stuffs a 0 bit at the end of these 1s (refer **Q13**). The data link layer at the destination de-stuffs or deletes a 0 bit followed by five consecutive 1s and then passes de-stuffed bits onto the network layer. An advantage of bit stuffing is that the boundary between two consecutive frames can be clearly identified by the flag byte. Therefore, in a case where receiver misses its track, it can scan the incoming bits for the flag byte, since a flag byte can be present only at the boundaries of a frame.

Physical Layer Coding Violations

This method can only be used in a network where encoding on physical medium comprises some redundancy. For example, in some LANs, one bit of data is encoded using two physical bits, with bit 1 is represented as a high-low pair and bit 0 is represented as a low-high pair. Every bit undergoes a transition during encoding and makes it easier for a receiver to accurately locate the bit boundaries.

4. Explain two types of errors with the help of a diagram.

Ans: During data transmission, one or more bits of data being transmitted may get corrupted. Depending on the number of bits in data that have been corrupted, there exist two types of errors: *single-bit error* and *burst error*.

- **Single-bit Error:** In this type of error, only one bit of the data is altered during transmission, that is, bit 1 may be received as 0 or bit 0 may be received as 1 (Figure 6.1).

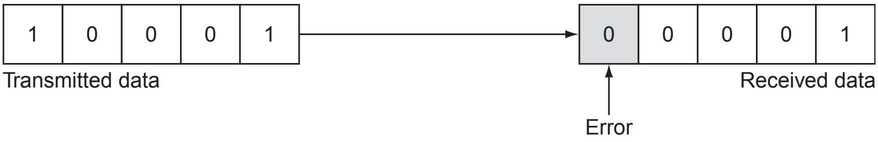


Figure 6.1 Single-bit Error

- **Burst Error:** A burst error occurs when two or more bits (consecutive or non-consecutive) are altered during the transmission (Figure 6.2). The length of burst is measured from the firs altered bit to the last altered bit. However, it does not necessarily mean that all bits comprising the burst length have been altered.

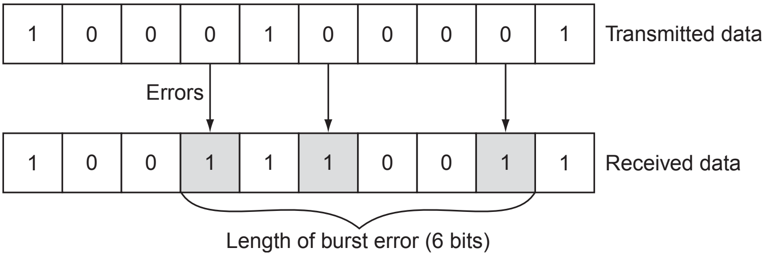


Figure 6.2 Burst Error

5. Discuss the concept of redundancy in error detection and correction.

Ans: During data transmission, errors may occur because of certain transmission impairments such as attenuation and electromagnetic noise. Usually, the burst errors are more likely to occur instead of single-bit errors. For the detection and correction of these errors, some extra bits (called **redundant bits**) are required to be sent along the data. Redundancy is the central concept in both error detection and error correction.

At the sender's end, the redundant bits are added to the data bits using a process that establishes a relationship between the data bits and the redundant bits. At the receiver's end, this relationship is examined by the receiver to detect or correct the errors in the received data. After detecting or correcting the errors, the receiver removes the redundant bits and keeps only the data bits.

6. Compare error detection and error correction.

Ans: In error detection, the emphasis is on findin whether or not there is an error(s) in the received data irrespective of the number of errors. The sender adds only enough extra (redundant) bits to the data being transmitted that enables the receiver to infer that some error has occurred. Thus, whether there is a single-bit error or burst error, it does not make any difference. Some of the commonly error-detecting codes include simple parity check, two-dimensional (2D) parity check, checksum and cyclic redundancy check (CRC).

Contrastive to error detection, in error correction, the emphasis is on not only to detect the errors but also to correct them. For this, it becomes important to know the exact number of bits that have been corrupted as well as their positions in the received data unit. In error correction, the sender adds enough redundant bits to the data being transmitted that enable the receiver to infer what the original data was. This helps the receiver to detect as well as correct the errors in the received data. Error correction is more difficult than error detection. Hamming code is one of the commonly used categories of error-correcting codes.

Generally, for highly reliable channels such as fibres error-detecting codes are used; however, for wireless links, the use of error-correcting codes is preferred.

7. Define the following

(a) Codeword

(b) Code Rate

(c) Hamming Weight of a Codeword

Ans: **(a) Codeword:** While transmitting a block of data (referred to as **dataword**) containing d bits, a few parity or redundancy bits (say, r) are added to form an n-bit (where n = d + r) encoded block of data what is referred to as codeword. In other words, codeword is formed by appending redundancy bits to the dataword.

(b) Code Rate: It refers to the ratio of the number of data bits in the codeword to the total number of bits. That is,

$$\text{Code rate} = d/n$$

(c) Hamming Weight of a Codeword: It refers to the number of non-zero elements in the codeword. It can be obtained by performing an XOR operation on the given codeword and a codeword containing all zeros.

8. What do you understand by Hamming distance? Describe the role of minimum Hamming distance in error detection and error correction.

Ans: Given a pair of codewords, say X and Y, containing same number of bits. The **Hamming distance** between X and Y, denoted as d(X, Y), is define as the number of positions in which the corresponding bits of X and Y differ. For example, if X = 10010010 and Y = 11011001, then the Hamming distance between X and Y is four, as the bits in X and Y differ in four positions, namely, 1, 2, 4 and 7.

The Hamming distance between two codewords can be calculated by firs performing XOR operation on them and then checking for the number of 1s in the resulting bit string; the Hamming distance will be equal to the number of 1s in the result string. For example, the result of XOR operation on X and Y is 01001011. Since there are four 1s in the resulting bit string, the Hamming distance is four.

Generally, during transmission, a large number of binary words are transmitted in a continuous sequence from sender to receiver. Accordingly, a block of codewords are received at the receiver; as a result, many values of Hamming distances can be calculated between each possible pair of codewords. Therefore, the Hamming distance is not of much significance instead minimum Hamming distance (d_{min}) is used for designing a code. The **minimum Hamming distance** (d_{min}) of a linear block of code is define as the smallest of the Hamming distances calculated between each possible pair of codewords.

The minimum Hamming distance (d_{min}) plays a significant role in error detection and error correction. It is always possible to detect the errors in a received codeword if the total number of errors in the codeword is less than d_{min}; otherwise, errors cannot be detected. This is because if the number of errors in a codeword is equal to or greater than d_{min}, the codeword may correspond to another valid codeword; as a result, the receiver may not be able to detect errors. The error-detection and error-correction capabilities of any coding technique largely depend on the minimum Hamming distance as explained below.

- To enable the receiver to only detect up to n errors in the codeword, d_{min} must be greater than or equal to $n + 1$. For example, for $d_{min} = 5$, up to four errors can be detected in a codeword, as $5 > = n + 1$, that is, $n < = 4$.
- To enable the receiver to correct up to m errors in the codeword, d_{min} must be greater than or equal to $2m+1$. For example, for $d_{min}= 5$, up to two errors can be corrected in a codeword, as $5 > = 2m + 1$, that is, $m < = 2$.
- To enable the receiver to correct up to m errors and detect up to n errors (where $n>m$) in the codeword, d_{min} must be greater than or equal to $m+n+1$.

In case, the value of d_{min} is even, this scheme is partially ineffective. For instance, if $d_{min} = 4$, the value of m (the number of errors that can be corrected) comes out to be 1.5 that is rounded off to 1. This means only one error can be corrected for $d_{min} = 4$ and thus, efficienc is wasted.

9. Explain various error-detection methods with the help of suitable examples.

Ans: To perform error detection, a few redundant bits must be added to the data. Redundant bits are also called **check bits**, as they do not carry any useful information; however, their presence in data block lets the receiver to detect errors that have occurred during transmission. Some of the commonly used error-detection methods are discussed here.

Parity Checking

This is the simplest method for detecting errors in the data. An extra bit known as **parity bit** is added to each word that is being transmitted. In a word, the parity bit is generally the MSB and remaining bits are used as data bits. Parity of a word can be either even or odd depending on the total number of 1s in it. If the total number of 1s in a word including parity bit is even, then it is called **even parity** while if the total number of 1s in a word including parity bit is odd, then it is called **odd parity**.

Depending on the type of parity required, the parity bit can be set to either 0 or 1. For example, if data is to be sent with odd parity, then the parity bit is set to 0 or 1, such that the number of 1s becomes odd. Similarly, to obtain even parity, the parity bit is set to 0 or 1, such that the total number of 1s in the whole word is even. The receiver can detect an error when it receives data in parity different from the expected parity, that is, if receiver knew that the data will be in even parity but it receives data with an odd parity. If the receiver detects an error, it discards the received data and requests the sender to retransmit the same byte. Examples given in **Q14** and **Q15** illustrate the use of simple parity checking method.

The detection of errors by the parity checking method depends on the number of errors that have occurred. If the total number of errors in the received data is odd, then the parity of received data will be different from that of transmitted data; therefore, error will be detected. However, if the number of errors in the received data is even, the parity of received data will be the same as that of the transmitted data and hence, the receiver will not be able to detect any errors. The main advantage of parity method is that no additional storage or computational overhead is needed for generating parity. The parity checking method has certain disadvantages too, which are listed below:

- Parity checking cannot correct error.
- Even number of errors cannot be detected.
- It is not possible to fin the location of the erroneous bit.

Two-dimensional Parity Check

An improvement over simple parity check is 2D parity check. As the name implies, this technique organizes a number of binary words being transmitted or received in succession along two dimensions, that is, in the form of rows and columns. At the sender's end, the parity bits are computed for each row and each column using the simple parity check method. In this way, two sets of parity bits are generated: one is associated with the rows of data block, referred to as **longitudinal redundancy check** (**LRC**), and the other is associated with the columns of the data block, referred to as **vertical redundancy check** (**VRC**). Each LRC and VRC bits are set such that the parity of corresponding row and column is even. After generating the parity bits, the parity bits along with data are sent to the receiver. Example given in **Q16** illustrates the generation of LRC and VRC parity bits.

At the receiver's end, each row and column (including LRC and VRC bits) of the received block of data are checked to verify whether its parity is still even. If so, the receiver knows that there is no error in the data block. Otherwise, for any single-bit error in the block of data, one of the LRC bits and one of the VRC bits are incorrect. The intersection of row and column corresponding to incorrect LRC and VRC bits respectively determines the position of erroneous bit. Example given in **Q17** illustrates the error detection using 2D parity checking method.

The 2D parity check is also referred to as **block parity**, as more than one parity bit are used for error detection. Using 2D parity check, burst errors are more likely to be detected.

Checksum

To overcome the limitation of detecting multiple errors in parity checking, checksum was introduced. Checksum method can be used for detecting multiple errors within the same word. With the transmission of a word in a block of data bytes, its contents are added bit by bit to that of its predecessor and the sum is maintained at the sender's side. Similarly, the contents of each successive word are added to the previous sum. After all, the words of a block of data bytes have been transmitted and the total sum (called **checksum byte**) up to that time is transmitted. While computing the checksum byte, the carries of the MSB are discarded. The example described in **Q18** illustrates how to compute the checksum byte.

At the receiver's end, the checksum is again computed by adding the bits of received bytes. The newly computed checksum is compared with the checksum transmitted by the sender. If both are found to be same, then it implies no error; otherwise, errors are present in the received block of data. Sometimes, the 2's compliment of the checksum is transmitted instead of the checksum. In such a case, the receiver adds the data block of received bytes with 2's complement of the checksum obtained bit by bit from the sender. If the sum is zero, then there is no error in data; otherwise, the errors are present. The advantage of checksum method is that it can detect burst errors.

The performance of checksum detection method is better than simple parity checking, as it can detect all odd number of errors and most of the even number of errors.

Cyclic Redundancy Check (CRC)

This is one of most widely used and most powerful error-detecting techniques developed by IBM. The CRC code is also referred to as **polynomial code**, as it treats the bit string to be transmitted as a polynomial (say, `M(x)`) whose coefficient are the 0 and 1 values in the bit string and operations on bit string interpreted as polynomial arithmetic. To generate CRC code, the sender and receiver must firs agree on a predetermined pattern of bits known as **generator polynomial**, denoted by G(x). Notice that the high- and low-order bits of the generator should always be 1.

CRC is based on binary division. Initially, at the sender's end, n 0s are appended to the bit string (say, d bits) to be transmitted where n is one less than the number of bits in the generator (say, m bits) or we can say equal to the degree of the generator polynomial. Then, the resultant bit string of d + n bits is divided by the generator using modulo-2 arithmetic with ignoring the carries and borrows in the addition and subtraction, respectively. Here, it is important to note that whenever during division, the leftmost bit of the dividend becomes zero, the regular divisor is not used for division; instead, a divisor containing all zeros is used. After performing the division, the remainder bits (say, r bits), called **redundant bits** or **CRC**, are added to the dividend to form the codeword of d + r bits. Notice that the number of bits in CRC must be exactly one less than the number of bits in generator, that is, r = m−1. Finally, the codeword of d + r bits is transmitted to the receiver. The example described in **Q19** illustrates how to generate the CRC code.

At the receiver's end, the received codeword of d + r bits is again divided by the same generator as used by the sender. If the remainder obtained after this division is non-zero, the receiver comes to know that an error has occurred and thus, rejects the received data unit; otherwise, the receiver knows that there is no error in the received data and thus, accepts the same. The example described in **Q20** illustrates how to detect errors using CRC method.

10. Reliability of CRC is better than that of simple parity and LRC. Justify this statement.

Ans: CRC is more reliable than simple parity and LRC, because it can detect single-bit errors, burst errors, double errors and an odd number of errors. On the other hand, simple parity can detect only an odd number of errors and is considered only 50% efficien as compared to CRC, whereas LRC can detect only up to three errors. Therefore, both simple parity and LRC are considered less reliable than CRC and cannot be implemented in all networks.

11. Write a short note on error correction.

Ans: In error correction, the receiver that has received corrupt data needs to discover the original data, the exact number of error bits and their location. To enable error correction, encoder and decoder are used at the sender's and receiver's ends, respectively. Figure 6.3 shows the structure of encoder and decoder in error correction. Each m-bit dataword at the sender's end is converted into an n-bit codeword (n > m) with the help of a generator that applies some encoding on the dataword thereby adding r redundant bits to the dataword. Thus, an n-bit codeword contains m bit of data and r redundant bits, that is, n = m + r. The codeword is then transmitted to the receiver. At the receiver's end, the checker examines the redundant bits to detect and correct errors in the data. After this, the dataword (without redundant bits) is passed to the receiver.

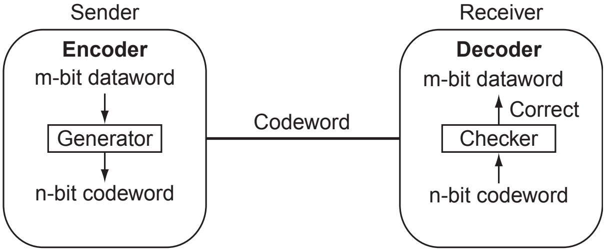


Figure 6.3 Structure of Encoder and Decoder in Error Correction

The two main methods for error correction are *forward error correction* (*FEC*) and *retransmission*. **FEC** is the technique in which the receiver makes guesses to find out the actual message using the redundant bits. In this technique, no request can be made for the retransmission of the message and thus, is useful only when the number of errors is small. In **retransmission** technique, whenever a receiver detects that there is some error in the received data, it rejects the received data and asks the sender to retransmit the data. The receiver continues to do so until it receives the data that it considers free of errors.

12. Explain Hamming codes in detail.

Ans: Hamming code is a linear block code that was developed by a scientist named R.W. Hamming. It is a single-bit error-correction technique. The basic idea is to insert parity bits in between the data bits to be transmitted. The parity bits are placed at each 2^n bit position where n = 0, 1, 2, and so on. That is, firs parity bit is placed at firs ($2^0 = 1$) position, second parity is placed at second ($2^1=2$) position, third parity bit is placed at fourth ($2^2 = 4$) position and so on.

There can be any number of bits (say, n) in the Hamming code including data bits (d) and parity bits (r). For finding the total number of parity bits in the dataword so as to form Hamming code, the condition, $2^r >= n + 1$, that is, $2^r >= d + r + 1$ must be satisfied. For example, if the dataword is of four bits, then three parity bits will be required as r = 3 satisfie the condition $2^3 >= (4 + 3 + 1)$. A seven-bit Hamming code is commonly used that comprises four data bits and three parity bits. Figure 6.4 shows the structure of seven-bit Hamming code.

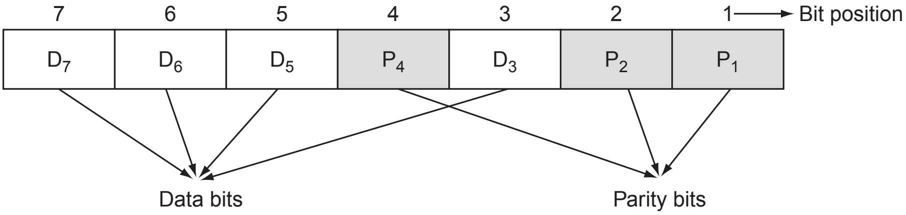


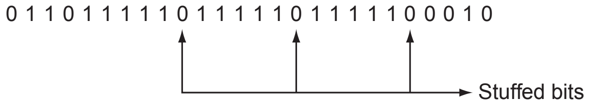
Figure 6.4 Structure of Seven-bit Hamming Code

The value of parity bits can be set to either 1 or 0. The value of P_1 is set to 0 or 1, such that the bits at positions 1, 3, 5 and 7, that is, P_1, D_3, D_5 and D_7, make an even parity. The value of P_2 is set to 0 or 1, such that the bits at positions 2, 3, 6 and 7, that is, P_2, D_3, D_6 and D_7, together make an even parity. Similarly, the value of P_4 is set to 0 or 1, such that the bits at positions 4, 5, 6 and 7, that is, P_4, D_5, D_6 and D_7, together make an even parity.

After Hamming code has been generated at the sender's side, the code is transmitted to the receiver. At the receiver's end, it is decoded back into the original data. The bits at positions (1, 3, 5 and 7), (2, 3, 6 and 7) and (4, 5, 6 and 7) are again checked for even parity. If each group of bits makes an even parity, then the received codeword is free from errors; otherwise, the error exists. In case of an error, a three-bit number is made from three parity bits ($P_4P_2P_1$) and its decimal equivalent is determined, which gives the position of erroneous bit. After detecting the position of error bit, it is corrected by inverting the error bit (refer **Q21**).

13. Apply bit stuffing to the given bit st eam 0110111111111111110010.

Ans: In bit stuffing the data link layer stuffs one zero after each group of fiv consecutive 1s. Thus, the outgoing bit stream after bit stuffin will be:



14. Given a dataword 1010011. What codeword will be transmitted if:

(a) an even parity is used.

(b) an odd parity is used.

Ans: (a) As the number of 1s in the given dataword is four (that is, even), the parity bit is zero. Thus, the codeword that will be transmitted is 01010011 (parity bit is at MSB position).

(b) As the number of 1s in the given dataword is four (that is, even), the parity bit is one. Thus, the codeword that will be transmitted is 11010011.

15. If the transmitted codeword is 11010011 and the received codeword is 10111011, detect the error (if any) in following cases.

(a) An even parity is used.

(b) An odd parity is used.

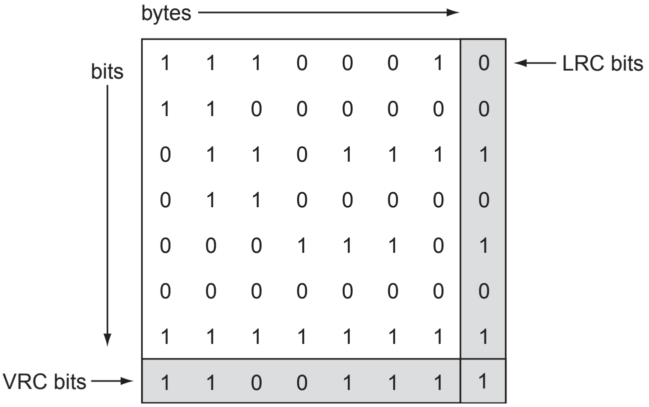
Ans: (a) It is clear from the transmitted and the received codewords that there are three errors in the received codeword. However, in case of even parity, since the number of 1s in the received codeword is six (that is, even), the receiver will not be able to detect errors. The received codeword will be assumed as the correct word.

(b) Since the number of 1s in the received codeword is six (that is, even), there is some error in the received codeword in case of odd parity.

16. Consider the following bit stream that is to be encoded using VRC, LRC and even parity. What will be the transmitted data?

1100001 1111001 1011001 0000101 0010101 0010101 1010001

Ans: The given bit stream is organized into rows and columns to compute the LRC and VRC bits, as shown below:



1	1	1	0	0	0	1	0
1	1	0	0	0	0	0	0
0	1	1	0	1	1	1	1
0	1	1	0	0	0	0	0
0	0	0	1	1	1	0	1
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1

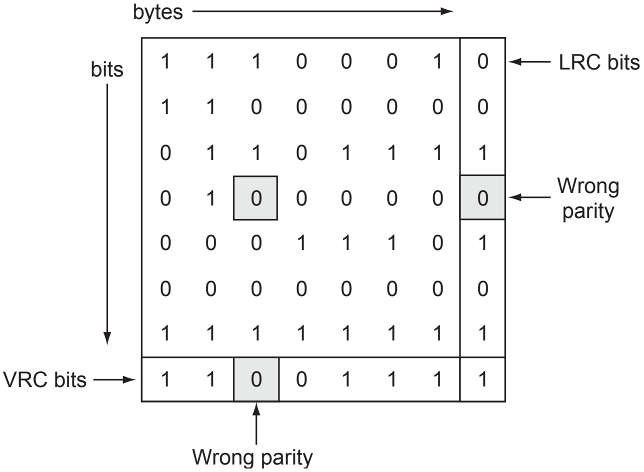
Thus, the bytes that will be transmitted are:

11000011 11110011 10110010 00001010 00101011 00101011 10100011 00101011

17. Consider the following bit stream that has been encoded using VRC, LRC and even parity. Locate the error if present.

11000011 11110011 10100010 00001010 00101011 00101011 10100011 00101011

Ans: To locate the error, the received byte stream is organized into rows and columns as shown below:



bytes
bits
LRC bits
Wrong parity
VRC bits
Wrong parity

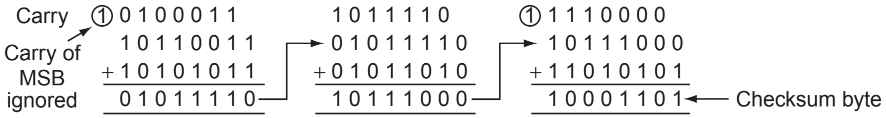
1	1	1	0	0	0	1	0
1	1	0	0	0	0	0	0
0	1	1	0	1	1	1	1
0	1	0	0	0	0	0	0
0	0	0	1	1	1	0	1
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1

Since fourth LRC and third VRC bits make the parity of its respective row and column even, there is an error in the received data stream. The erroneous bit will be present at the intersecting position of fourth row and third column, that is, the fourth bit of third byte is incorrect.

18. Compute the checksum byte for the following datawords.

10110011 10101011 01011010 11010101

Ans: The checksum of the given datawords will be computed as shown below:

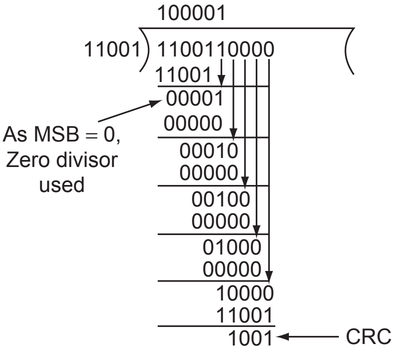


19. Given message is M(X) = X^5 + X^4 + X + 1 and the generator is G(X) = X^4 + X^3 + 1. Compute CRC code.

Ans: Given dataword = 110011

divisor = 11001

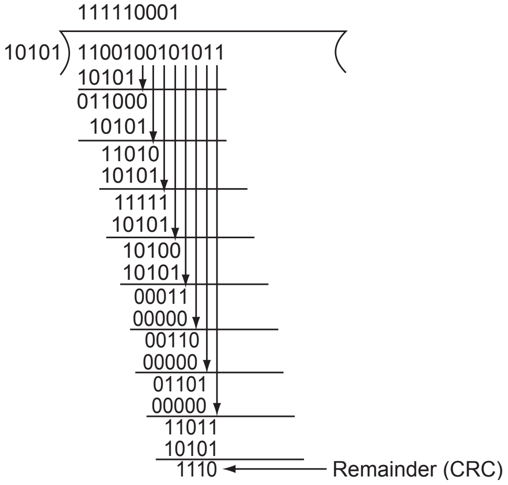
Since the degree of generator polynomial is four, four zeros will be appended to the given dataword. Thus, the dividend will be 1100110000. Now, the CRC will be computed as shown below:



The CRC code is obtained by appending CRC (that is, 1001) to the given dataword (that is, 110011). Thus, the CRC code is 1100111001.

20. The codeword is received as 1100100101011. Check whether or not there are errors in the received codeword, if the divisor is 10101.

Ans: To check codeword for errors, the received codeword is divided by the given divisor, that is, 10101 as shown below.



Since the remainder obtained (CRC) is non-zero, the received codeword contains errors.

21. For the bit sequence 1001110:

(a) Calculate the number of parity bits that will be required to construct Hamming code.

(b) Construct the Hamming code.

Ans: **(a)** To calculate the number of parity bits, the following condition must be satisfied

$$2^r >= d + r + 1$$

As the number of data bits (d) is 7, so putting $d = 7$ in above equation, we get

$$2^r >= 7 + r + 1$$

$$\Rightarrow 2^r >= 8 + r \qquad (I)$$

Putting $r = 4$ satisfie the equation (I) since $2^4 > 12$. Thus, four parity bits are required with seven data bits to construct the Hamming code and these parity bits will be inserted at first second, fourth and eighth positions.

(b) The structure for Hamming code for the data 1001110 is shown below.

D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	0	---	1	1	1	---	0	---	---

To be decided

As the bits $D_3D_5D_7D_9D_{11}$ are 01101, thus, $P_1 = 1$ to establish the even parity.
As the bits $D_3D_6D_7D_{10}D_{11}$ are 01101, thus, $P_2 = 1$ to establish the even parity.
As the bits $D_5D_6D_7$ are 111, thus, $P_4 = 1$ to establish the even parity.
As the bits $D_9D_{10}D_{11}$ are 001, thus, $P_8 = 1$ to establish the even parity.
Therefore, the Hamming code which will be transmitted to the receiver is:

D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	0	1	1	1	1	1	0	1	1

Complete codeword

22. A seven-bit Hamming code is received as 1100101. What is the correct code?

Ans: The received codeword is:

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	1	0	0	1	0	1

Received codeword

As the bits $P_1D_3D_5D_7$ (that is, 1101) together make an odd parity, there is an error. Thus, $P_1 = 1$.
As the bits $P_2D_3D_6D_7$ (that is, 0111) together make an odd parity, there is an error. Thus, $P_2 = 1$.
As the bits $P_4D_5D_6D_7$ (that is, 0011) together make an even parity, there is no error. Thus, $P_4 = 0$.
The erroneous bit position can be determined as follows:

P_4	P_2	P_1
0	1	1

3-bit number, that is, error word

The decimal equivalent of ($P_4P_2P_1$), that is, (011) is 3. Hence, third bit in the received codeword contains the error, so by inverting the third bit, the correct code can be obtained as shown below.

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	1	0	0	0	0	1

Correct codeword

Inverted bit

Multiple Choice Questions

1. Which of the following service is not provided by the data link layer?
   (a) Unacknowledged connectionless
   (b) Unacknowledged connection-oriented
   (c) Acknowledged connectionless
   (d) Acknowledged connection-oriented

2. The process of breaking stream of bits into frames is known as __________.
   (a) Bit stuffin
   (b) Byte stuffin
   (c) Framing
   (d) Character count

3. What is the process of adding one extra 0 whenever there are fiv consecutive 1s in the data, so that the receiver does not mistake the data about a flag
   (a) Bit stuffing (b) Bit padding
   (c) Byte stuffing (d) Byte padding

4. In single-bit error, _____ bit is altered during the transmission.
   (a) Zero (b) One
   (c) Two (d) None of these

5. CRC computation is based on
   (a) OR operation
   (b) AND operation
   (c) XOR operation
   (d) NOR operation

6. Which of the following error-detection method involves the use of parity bits?
   (a) LRC
   (b) VRC
   (c) Checksum
   (d) Both (a) and (b)

7. VRC parity bit is associated with ________.
   (a) Rows
   (b) Columns
   (c) Both (a) and (b)
   (d) None of these

8. What is the formula to calculate the number of parity bits (*r*) required to be inserted in dataword (*d* bits) to construct the Hamming code?
   (a) $2^r >= d + r$
   (b) $2^r >= d$
   (c) $2^d >= d + r$
   (d) $2^r >= d + r + 1$

9. Hamming code can detect up to ________ if minimum Hamming distance is 3.
   (a) 2 (b) 3
   (c) 4 (d) 5

10. If a codeword in Hamming code is of seven bits, then how many parity bits it contains?
   (a) 2 (b) 3
   (c) 7 (d) 9

Answers

1. (b) 2. (c) 3. (a) 4. (b) 5. (c) 6. (d) 7. (b) 8. (d) 9. (a) 10. (b)

7

Flow and Error Control

1. Differentiate between flo control and error control.

Ans: Flow control and error control are the most important functions of data link layer. **Flow control** refers to a set of procedures that allows the communicating devices having different speed and memory characteristics to communicate with each other in an efficient manner. It ensures that a slow receiver is not being flooded by the fast sender. Thus, flow control restricts the amount of data that can be sent from the sender before waiting to receive an acknowledgement (ACK) from the receiver. Each receiver has a block of memory known as buffer for reserving the incoming data before they can get processed. The flow control mechanism can be achieved in two ways. First, if the receiver's end buffer begins to fill up, then the receiver should tell the sender either to stop the transmission completely or send fewer frames. Second, the receiver must acknowledge the received frames by sending ACK frame to the sender. For the frames, which are damaged or lost during transmission, the receiver should send negative acknowledgement (NACK) to the sender by transmitting NACK frame. Two basic protocols that can be used to control the flow of data include stop-and-wait and sliding window protocol

Error control, on the other hand, refers to a set of procedures that ensure that all the frames have eventually been received at the destination. If any frames are lost or damaged during transmission, the error control mechanism allows the receiver to inform the sender about it and coordinates the retransmission of those frames by the sender. In data link layer, the error control is based on an automatic repeat request (ARQ) in which whenever any error is detected, the lost or damaged frames are retransmitted. The basic protocols that can be used for error control include stop-and-wait ARQ, Go-back-N ARQ and selective-reject ARQ.

2. Explain the working of stop-and-wait flo control protocol.

Ans: **Stop-and-Wait** is the simplest protocol used to control the flow of data between a sender and a receiver. As the name implies, the sender sends one frame, then stops and waits for the ACK frame from the receiver to confirm the receipt of the frame. Only after getting an ACK frame from the receiver, the sender sends the next frame (Figure 7.1). In stop-and-wait flow control, the receiver can stop the flow of the data by not sending the ACK frame, thereby keeping the sender in waiting state.

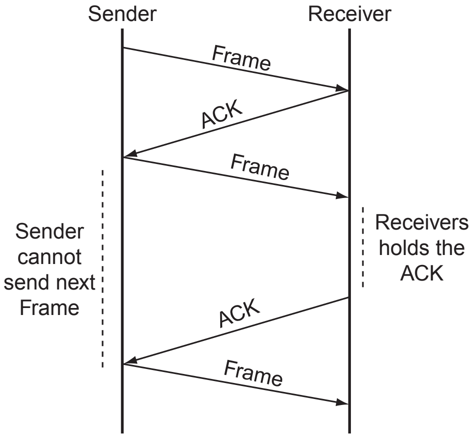


Figure 7.1 Stop-and-Wait Flow Control

Mostly, the sender breaks the large block of data into smaller blocks called frames because sending the message in the larger blocks may increase the transmission time and errors are more likely to occur. In contrast, when message is transmitted in smaller frames, errors may be detected earlier and a smaller amount of data needs to be transmitted. Another reason of breaking into frames may be the limited buffer size of the receiver due to which entire large frame cannot be processed at a single time, thus causing long delays. But the disadvantage of sending small frames for a single message is that stop-and-wait method cannot be used effectively because in this protocol only one frame can be sent at a time (either from sender to receiver or vice versa) which results in underutilization of the communication link.

Link Utilization

To understand the link utilization in stop-and-wait flow control, consider t_{frame} that denotes the time taken in transmitting all bits of a frame and t_{prop} denotes the propagation time from the sender to receiver. Now, the propagation delay (a) which is defined as the time taken by one bit to reach from the sender to receiver can be expressed as

$$a = t_{prop}/t_{frame}$$

If $a < 1$ then $t_{prop} < t_{frame}$, which implies that the frame is longer enough such that the leading bits of frame reach the receiver before the entire frame is transmitted. That is, link is inefficiently utilized. On the other hand, if $a > 1$, then $t_{prop} > t_{frame}$, which implies that the sender has transmitted the entire frame and the leading bits of that frame have still not arrived at the receiver. This results in underutilization of the link.

3. Derive the expression for the maximum possible utilization of link in stop-and-wait flo control.

Ans: Suppose a long message is to be transmitted between two stations. The message is divided into a number of frames $F_1, F_2, F_3, \ldots, F_n$. The communication between stations proceeds in such a manner that the frames (from station 1) and the ACKs (from station 2) are sent alternatively. That is, initially sender (station 1) sends F_1, then receiver (station 2) sends an ACK and then sender sends F_2 then receiver sends an ACK and so on.

Now, if T_f denotes the time taken in sending one frame and receiving an ACK, then the total time (T) taken to send the message can be expressed as

$$T = nT_F$$

where n is the total number of frames and T_F can be expressed as

$$T_f = t_{prop} + t_{frame} + t_{proc} + t_{prop} + t_{ack} + t_{proc}$$

where

t_{prop} is the propagation time from station 1 to station 2.
t_{frame} is the time taken in transmitting all bits of the frame.
t_{proc} is the processing time by each station to respond to an incoming event.
t_{ack} is the time to transmit an ACK.

$t_{prop} + t_{frame} + t_{proc}$ is the total time taken by the station 1 to send the frame and getting it processed at the receiver's end and $t_{prop} + t_{ack} + t_{proc}$ is the total time taken by the station 2 to send the ACK frame and getting it processed by the sender.

Therefore, $$T = n(t_{prop} + t_{frame} + t_{proc} + t_{prop} + t_{ack} + t_{proc})$$

Assuming that the processing time is negligible and the ACK frame is very small as compared to the data frame, we can neglect t_{proc} and t_{ack}. Thus, T can be written as

$$T = n(2t_{prop} + t_{frame})$$

As $n*t_{frame}$ is the time that is actually involved in sending the frames and rest is considered as overhead, the link utilization (U) may be given as

$$U = \frac{n*t_{frame}}{n*(2t_{prop}+t_{frame})} = \frac{t_{frame}}{(2t_{prop}+t_{frame})}$$

$$\Rightarrow U = 1/(1 + 2a)$$

where $a = t_{prop}/t_{frame}$ = propagation delay.

This is the maximum utilization of the link, which can be achieved in situations where propagation delay (a) is constant and fixed-length frames are often sent. However, due to overhead bits contained in a frame, the actual utilization of the link is usually lower than this.

4. Derive the expression for the propagation delay showing that it is proportional to the bit length of the channel.

Ans: We know, propagation delay (a) = propagation time/transmission time.

Now, propagation time $= d/V$

where d is the distance of the link and V is velocity of propagation. For guided media, $V = 3*10^8$ m/s and for unguided transmission, $V = 0.67 *3*10^8$ (approximately).

Transmission time $= L/R$

where L is the length of the frame in bits and R is the data rate of transmission. Therefore,

$$a = \frac{d/V}{L/R} = \frac{Rd}{VL}$$

Since, we know that the bit length of channel (B) = Rd/V

$$\Rightarrow a = B/L$$

Hence, $$a \propto B$$

5. Explain the mechanism of sliding window flo control.

Ans: The sliding window flow control technique was introduced to remove the disadvantage of the stop-and-wait protocol in which only one frame can be transmitted at a time, thus, reducing the efficiency of the link. The efficiency can be greatly improved by using the sliding window flow control protocol as in this technique multiple frames can be sent at the same time.

The mechanism of sliding window protocol is as follows. Let there be two stations, `A` and `B`, connected to each other via a full-duplex link. Station `B` (destination) has buffer space that can accommodate `N` frames, that is, `B` can accept `N` frames at a time, and station `A` (source) is allowed to send `N` frames to station `B` without waiting for any ACKs from `B`. Each frame is assigned a sequence number that helps to keep track of the frames which have been acknowledged and which have not yet been received. Station `B` acknowledges each frame by sending a **receive-ready** (**RR**) frame that contains the sequence number of the next expected frame. An RR frame from station `B` indicates to the station `A` that `B` is ready to receive next `N` frames starting with the frame having the sequence number specified within the RR frame. Instead of sending ACK to each frame, the station `B` can also acknowledge many frames at the same time by sending a single RR frame, that is, acknowledgements are cumulative. For example as shown in Figure 7.2, after receiving frame 3 (F3), station `B` can hold to send the ACK of the frames 0, 1, 2 and 3 until frame 4 arrives. After frame 3 has arrived, `B` can send an ACK with the sequence number 4 indicating to `A` that frames 0, 1, 2 and 3 have been received and now it is expecting to receive frame 4.

At any instant, `B` can also ask `A` to stop the flow of frames by sending a **receive-not-ready** (**RNR**) message which acknowledges the former frames and indicates the sender not to transmit more frames. For example, an RNR 3 message from `B` means that it has received all frames up to number 2 and cannot accept any further frames. Later, `B` must send a normal ACK to `A` to restart the transmission process.

To keep track of the frames to be sent or received, the sender and receiver maintain a list of sequence numbers called the **sender's window** and **receiver's window** (indicated by the boxes in Figure 7.2), respectively. The sender's window indicates the sequence numbers of the frames that the sender can send while the receiver's window indicates the sequence numbers of the frames that the receiver is expecting to receive. For example, in Figure 7.2, the initial window of `A` and `B` indicates that `A` can transmit frames

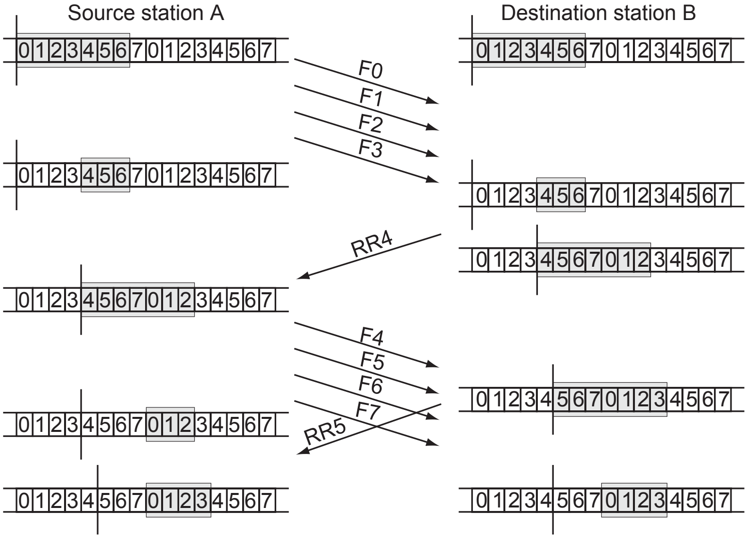


Figure 7.2 Sliding Window Flow Control

numbered from 0 to 6 without having to wait for any ACK from B and B can receive frames numbered from 0 to 6 from A, respectively. As the frames are sent or received at the sender's and receiver's end respectively, the window size shrinks. For example, after transmitting frames F0, F1, F2 and F3, the size of A's window shrinks to three frames and after receiving frames F0, F1, F2 and F3, the size of B's window shrinks to three frames (Figure 7.2). Similarly, the window size expands as the ACKs are received or sent by the sender and receiver, respectively. Therefore, the scheme is named as sliding window flow control.

Notice that at A's end in Figure 7.2, the frames between the vertical line and the box indicate those frames that have been sent but not yet acknowledged by B. Similarly, at B's end, the frames between the vertical line and the box indicate those frames which have been received but not yet acknowledged.

As each sequence number used occupies some field in the frame, the range of sequence number that can be used gets limited. In general, for a k-bit field, the range of sequence number will be from 0 to $2^k - 1$ and frames will be numbered as modulo 2^k. That is, after sequence number $2^k - 1$, the next number again will be 0. For example, for a 3-bit sequence number, the frames will be numbered sequentially from 0 to 7 and the maximum window size will be 7 ($2^3 – 1$). Thus, seven frames can be accommodated in the sender's window and the receiver can also receive a maximum of seven frames at a time.

Link Utilization

In sliding window flow control, the link utilization (U) depends on the window size (N) and propagation delay (a) and is expressed as

$$U = \begin{cases} 1, \text{ if } N > = 2a + 1 \\ N/(2a + 1), \text{ if } N < 2a + 1 \end{cases}$$

6. Defin piggybacking. What is its usefulness?

Ans: Usually, the link used between the communicating devices is full duplex and both the sender and receiver need to exchange data. In addition to data, both sender and receiver send ACK for the received data to each other. To improve the efficiency in a two-way transmission, a technique called **piggybacking** can be employed, which permits an ACK from either device (sender or receiver) to be assembled with the next outgoing data frame from that device instead of sending a separate ACK frame. In case a device has only ACK but no data to send, it needs to use a separate ACK frame. However, if the device has to send the ACK followed by data, it can temporarily withhold the ACK and later, include the ACK in the outgoing data frame.

By temporarily delaying the outgoing ACKs and sending them along with data frames, piggybacking results in better use of the available channel bandwidth. Moreover, by using piggybacking technique, less number of frames needs to be sent which further implies less number of interrupts as well as less number of buffers required at the receiver's end.

7. What is meant by lost frame and damaged frame? List the common techniques of error control method.

Ans: A frame that fails to arrive at the destination node due to noise burst is called **lost frame**. In this case, the receiver does not know that the frame has been transmitted by the sender. A **damaged frame** is the frame in which some bits have been changed or altered during the transmission. In case of lost frame, no frame is received by the receiver while in case of damaged frame, a frame is received but not in the exact order.

8. Explain the mechanism of stop-and-wait ARQ.

Ans: Stop-and-Wait ARQ is the extended form of stop-and-wait flow control technique where data frames are retransmitted if the sender does not receive any ACK for the frame. In this method, the sender transmits a single frame and waits for the ACK from the receiver before sending the next frame. The sender cannot transmit a new frame until the ACK is received from the other side. Since either the frame or the ACK can be transmitted at a time, this technique is also known as **one-bit sliding window protocol**.

Notice that the ACK will not be received by the sender if the frame has been lost during the transmission, that is, it has not been received by the receiver or if the receiver has received the frame free of errors but its ACK has been lost or delayed during the transmission. In both cases, the sender needs to retransmit the frame. For this, the sender maintains a copy of sent data frame in its buffer so that they can be retransmitted whenever required.

To identify the frames to be retransmitted, sequence numbers are attached to the consecutive data frames and ACKs. As only one frame or one ACK can be on the transmission link at a given time, only two numbers 0 and 1 are needed to address the data frames and ACK. Data frames are alternatively numbered 0 and 1, that is, first data frame will be marked as `F0`, second will be `F1`, third again will be marked as `F0` and so on. The numbers that are attached with ACK indicates the sender to send that numbered data frame. For example, if ACK1 is sent by the receiver, then the sender comes to know that `F0` has been received successfully and now, it has to send `F1` to the receiver. This process helps the receiver to discard the duplicate frames; however, ACKs need to be sent by the receiver for the duplicate frames also so as to keep the sender in synchronization.

Lost or Damaged Frames

To handle the problem of lost or damaged frames, the sender maintains a timer. Whenever the sender sends a frame, the timer starts. In case the frame is lost during the transmission, the receiver does not send any ACK to that frame. If the sender does not receive any ACK before the time-out (timer expires), it retransmits the same frame after the time-out. On the other hand, if the frame is received by the receiver with errors in it, then the receiver simply discards the frame and sends NACK to the sender indicating the sender to retransmit the same frame.

Lost or Delayed ACKs

Now, consider the case where the receiver receives the frame with no errors and therefore, sends an ACK to the sender but the ACK frame is lost or delayed. In both scenarios, the sender retransmits the same frame after the time-out. This results in the duplication of frames at the receiver's end. To identify the duplicate frames, the receiver maintains a buffer at its end hold those frames for which ACK has been sent.

Link Utilization

The link utilization (U) in the stop-and-wait ARQ is given as

$$U = (1 - p)/(1 + 2a)$$

where

p is the probability of receiving a bit in error

a is the propagation delay which is also equal to $(t_{prop}*R)/L$ where t_{prop}, R and L denotes propagation time, data rate of the link and number of bits in the frame, respectively.

9. What are the two types of sliding window ARQ error control?

Ans: To provide the efficient utilization of the link, the sliding window error control technique is adopted. The sliding window ARQ is also known as **continuous ARQ** because it allows the sender to send many frames continuously without waiting for an ACK. There are two techniques, namely, *Go-back-N ARQ* and *selective-reject ARQ* that are based on the concept of sliding window.

10. Explain the mechanism of Go-back-N ARQ technique.

Ans: **Go-back-N ARQ** is the most commonly used form of error control that is based on the sliding window flow control. In this technique, the sender sends the data frames depending on its window size but at the receiving end window size is always one. That is, the sender can send many frames without waiting for an ACK from the receiver but the receiver can receive only one frame at a time. For each frame that is received without any error, the receiver acknowledges the frames by sending RR message. However, when it detects error in the frame, it discards that frame and sends a negative acknowledgment **reject** (**REJ**) to the sender. The receiver continues to discard the further transmitted frames until the frame in error is received correctly. When the sender receives an REJ, it retransmits the frame in error plus all the succeeding frames that it has sent already.

Figure 7.3 shows the mechanism of Go-back-N ARQ where the sender's window size is seven. That is, the sender can transmit frames `F0-F6` to the receiver without waiting for an ACK.

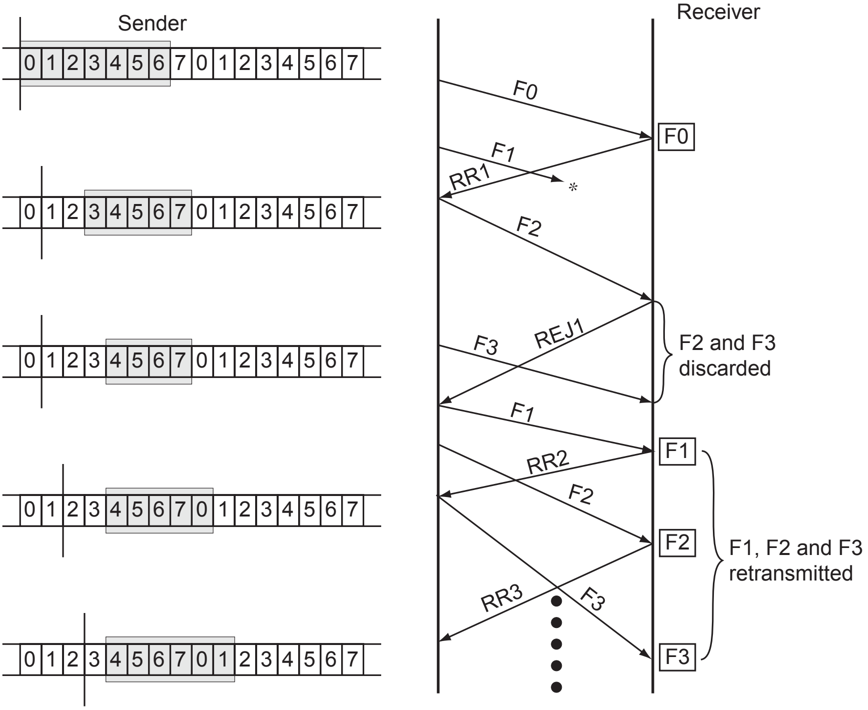


Figure 7.3 Go-Back-N ARQ Mechanism

Lost or Damaged Frames

As shown in Figure 7.4, initially, the sender sends `F0`, which is received by the receiver. In response the receiver sends RR1 frame to the sender and slides its window to `F1–F7`. By the time the sender receives RR1, it has transmitted `F1` which is either lost or damaged during the transmission. On receiving RR1, the sender transmits `F2` and shrinks its window to `F3–F7`. Though `F1` and `F2` have been transmitted,

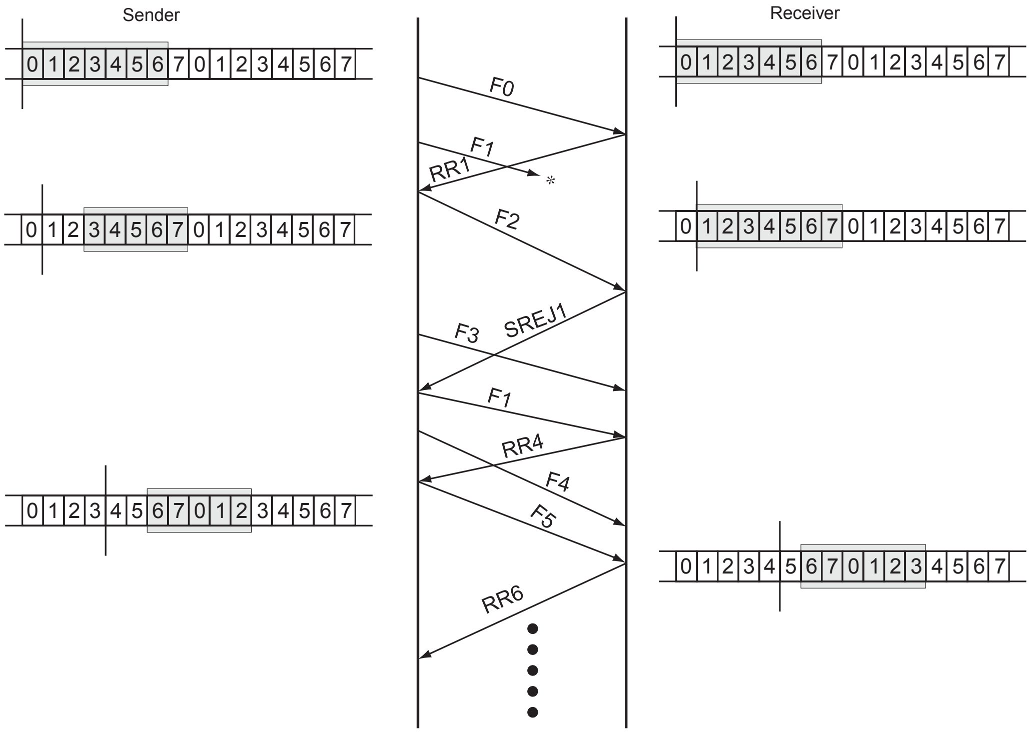


Figure 7.4 Selective-reject ARQ Mechanism

the sender stores them in the buffer until they are acknowledged by the receiver. When the receiver receives `F2`, it accepts `F2` and stores in its buffer. It also comes to know that `F1` has not arrived. Thus, it sends SREJ1 to the sender to indicate the retransmission of `F1`. Now, the receiver cannot send RR frame until it receives `F1` because sending RR3 would indicate that all frames up to `F2` have been received. By the time the sender receives SREJ1, it has transmitted `F3` which is accepted by the receiver and kept in the buffer. When sender receives SREJ1, it retransmits frame `F1`. On receiving `F1`, the receiver replies with RR4 indicating to the sender that all frames up to `F3` have been received successfully. This procedure continues until all the frames have been transmitted.

Lost or Delayed RR or REJ

To understand how lost or delayed RR frame is handled, suppose that the receiver receives `F2` frame error free and thus, responds to sender with RR3 which is either lost or delayed. As the sender does not receive any acknowledgement before the time-out, it retransmits `F2` after the timer expires. Now, as the receiver has already received `F2`, it simply ignores `F2` thus, avoiding the duplication. However, as the acknowledgements in the Go-back-N method are cumulative, it might be possible that before the timer associated with frame `F2` expires, the sender receives next RR frame (that is, RR4) which acknowledges all the previous data frames. In such a case, the sender remains unaware of the fact that RR3 has lost in the network and the operation remain unaffected.

To understand how lost or delayed REJ is handled, suppose that the receiver receives `F4` frame with some errors in it. Thus, the receiver discards `F4` and transmits REJ4 to the sender, which is either lost or delayed. In both cases, the sender does not receive any further acknowledgements because the receiver will deny accepting any frame other than F4. Thus, the sender has to retransmit F4.

Link Utilization

The link utilization (U) in Go-back-N ARQ method can be considered in the following two situations:

1. When N > 2a + 1, U = (1 - p)/(1 + 2ap) and
2. When N < 2a + 1, U = N(1 - p)/((2a + 1)*(1 – p + Np)).

11. Explain the mechanism of selective-reject ARQ technique.

Ans: **Selective-reject ARQ** (also known as **selective-repeat ARQ**) method offers an improvement over Go-back-N by retransmitting only the lost or damaged frame but not all the frames succeeding it. In this method, usually the size of receiver's window is same as that of sender's window and the damaged frames are acknowledged by the receiver by transmitting **selective reject** (**SREJ**) frame to the sender. As this method retransmits only lost or SREJ frames, a large buffer needs to be maintained at the receiver's end so that if some frame is not received in proper order then the receiver can accept the rest incoming frames and buffer them until that valid frame has been received. When all the data frames are reached, the receiver arranges all frames in proper sequence and sends them to the next upper layer.

Figure 7.4 shows the selective-reject ARQ mechanism where the window size of both sender and receiver is seven. That is, the sender can transmit frames F0-F6 to the receiver without waiting for an acknowledgement and the receiver can also receive frames F0-F6.

Lost or Damaged Frame

As shown in Figure 7.3, initially, the sender sends F0. As the receiver's window size is 1, the receiver accepts F0 and replies with RR1 to the sender and slides its window to F1. By the time the sender receives RR1, it has transmitted F1 which gets lost in the transmission. At the time the sender receives RR1, it transmits F2 and slides its window from F3 to F7. Though F1 and F2 have been transmitted, the sender stores them in the buffer until they are acknowledged by the receiver. On receiving F2, the receiver finds that F1 is still not received. Therefore, the receiver discards F2 and sends REJ1 to the sender. Before the sender receives REJ1, it transmits F3 which is also discarded by the receiver. When the sender receives REJ1, it needs to retransmit F1, F2 and F3. First it sends F1, which is accepted by the receiver and the receiver responds with RR2 to the sender. This procedure continues until all the frames have been transmitted.

In case the receiver receives a damaged frame, it simply discards the frame and sends REJ to the sender indicating the retransmission of that frame.

Lost or Delayed RR

To understand how lost or delayed RR is handled, suppose that the receiver receives frame F2 and in response sends RR3 which either gets lost or gets delayed. In both cases, when RR4 reaches the sender, the sender assumes it as a cumulative ACK of frames up to F3 and thus, the operation remains unaffected.

Lost or Delayed SREJ

To understand how lost or delayed SREJ is handled, suppose that the receiver receives F4 frame with some errors and thus, sends SREJ4 to the sender, which either gets lost or delayed. To handle this, the receiver maintains a timer at its end, which is started at the time the receiver sends a SREJ frame. If the receiver does not receive the frame F4 before the time-out, it retransmits SREJ4 to the sender after the timer expires. Thus, eventually, the sender receives SREJ4 and retransmits F4.

Link Utilization

The link utilization (U) in selective-reject ARQ can be considered in the following two situations:

1. when $N \geq 2a + 1$, $U = 1 - p$ and
2. when $N < 2a + 1$, $U = (N*(1 - p))/(2a + 1)$.

12. What do you mean by a bit-oriented and byte-oriented protocol?

Ans: In a **bit-oriented protocol**, the data received from the upper layers whether text, images, audio or video is carried in the form of bits; the data field of each frame comprises a sequence of bits. To distinguish between the consecutive frames, a special eight-bit pattern flag 01111110 is used in the beginning and at the end of each frame. In case the flag bit pattern appears in the data field of frame, **bit stuffing** is used at the sender's end. After each five consecutive 1s in data, an extra bit 0 (a single bit) is inserted to prevent the bit pattern from looking like a flag. The extra bit stuffed by the sender is then destuffed at the receiver's end. An example of bit-oriented protocol is high-level data link control (HDLC) protocol.

On the other hand, in a **byte-oriented** (also called **character-oriented**) **protocol**, the data received from upper layers is carried in the form of eight-bit characters (that is, bytes) from a coding system such as ASCII. Each frame comprises a sequence of bytes. To distinguish between the consecutive frames, a 1-byte (instead of single bit) flag is used in the beginning and at the end of each frame; the flag is usually composed of special characters depending on the protocol being used. In case the flag byte appears in the data field of frame, **byte stuffing** (also called **character stuffing**) is used at the sender's end. An extra byte, called **escape character** (**ESC**), is stuffed in the data when there appears a character with the same pattern as flag. The extra byte stuffed by the sender is then destuffed at the receiver's end. An example of byte-oriented protocol is point-to-point (PPP) protocol.

13. Explain in brief HDLC protocol.

Ans: The HDLC is the most commonly used data link protocol developed by ISO. It supports both half-duplex and full-duplex communication lines and switched or non-switched channels. That is why it has been widely implemented throughout the world. It is a bit-oriented protocol that is used to provide communication in point-to-point and multipoint networks. Further, HDLC protocol implements the ARQ mechanism and satisfies a variety of applications. In addition, HDLC defines three types of stations, two types of link configuration and three modes of data transfer to work in various possible network configurations

Types of stations

Three types of stations defined by HDLC are as follows:

- **Primary Station:** This station has the responsibility of controlling the operation of the link. The frames that are sent by a primary station are called commands.
- **Secondary Station:** This station works under the control of the primary station and the frames that are sent by a secondary station are called responses. Each secondary station on the line is linked with the primary station via a separate logical link. During communication between primary and secondary stations, the primary station is responsible for establishing, managing and terminating the link.
- **Combined Station:** This station can act as both a primary and a secondary station and thus, can send both commands and responses. It does not rely on any other stations on the network and thus, no other station can control a combined station.

Types of Link Configurations

For three stations, two link configurations supported by HDLC are as follows

- **Unbalanced Configuration** This type of configuration consists of one primary and one or more secondary stations. Both full-duplex and half-duplex transmissions are possible in unbalanced configuration and the primary station polls each secondary station for input
- **Balanced Configuration** This type of configuration consists of two or more combined stations and supports both full-duplex and half-duplex transmissions.

Modes of Data Transfer

Three types of data transfer modes defined by HDLC are as follows

- **Normal Response Mode (NRM):** This mode of transfer is used with an unbalanced configur - tion. In this mode, the data transfer is initiated by the primary station to a secondary station. The secondary station is allowed to transmit only in a response to a command from primary station and not by itself. In other words, the secondary station must get an explicit permission from the primary station to send responses.
- **Asynchronous Balanced Mode (ABM):** This mode of transfer is used with a balanced configuration. In this mode, any of the combined stations can start data transmission without the need of any permission from other combined stations. This mode is used widely as it results in an efficient utilization of full-duplex point-to-point link
- **Asynchronous Response Mode (ARM):** This mode of transfer is used with an unbalanced confi - uration. In this mode, secondary station may initiate data transfer without needing the permission from the primary station. Despite of this, the primary station is still responsible for link establishment, link disconnection and error recovery. This mode helps to reduce overhead on the link, as no frames need to be sent to provide explicit permission to secondary stations. However, this mode is used only in rare situations where it is necessary for a secondary station to initiate transfer.

14. Explain the frame structure of HDLC.

Ans: The HDLC defines three types of frames, namely, *information frames* (*I-frames*), *supervisory frames* (*S-frames*) and *unnumbered frames* (*U-frames*) to support all modes of data transfer and link configurations. The **I-frames** are used to carry user data. The ACK of the received frames can also be piggybacked on I-frames. The **S-frames** do not carry any user data and are used to transport only control information, which cannot be piggybacked on I-frames such as RR, REJ, RNR and SREJ frames. The **U-frames** are reserved for carrying information regarding management of the link, mode setting or other control information.

Frame Structure

The frame structure of I-frames and U-frames is exactly similar (Figure 7.5) and consists of six fields: starting flag field, an address field, a control field, an information field, a frame check sequence (FCS) field and an ending flag. Since S-frame cannot carry user data, it consists of rest of the five fields excluding the user information field. When multiple frames are transmitted between the communicating stations, then the ending flag field of one frame may act as the starting flag field of the next frame and each frame is transmitted from left to right.

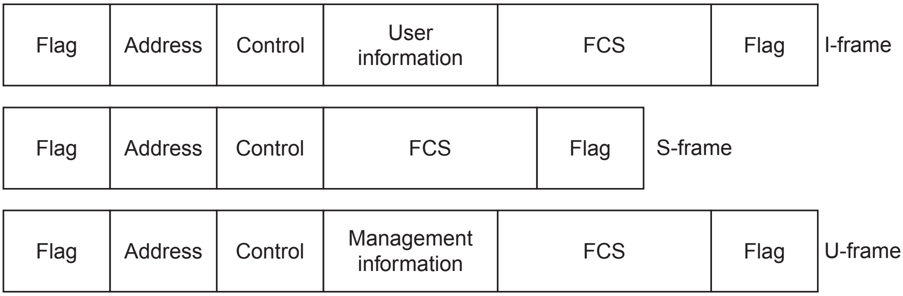


Figure 7.5 Frame Structures in HDLC

The description of the fields in different types of frames in HDLC is as follows:

- **Flag:** It is an eight-bit long field having the unique bit pattern of 01111110. This pattern is used to identify the starting and ending of a frame and the pattern can also be inserted whenever there is some idle time between the consecutive frames. This field serves as a synchronization pattern for the secondary station.
- **Address:** It is usually an eight-bit (1 byte) long field but can be extended up to several bytes depending on the need of the network. This field contains the address of the secondary station irrespective of whether the frame is transmitted by the primary station or the secondary station. If the frame is transmitted by the primary station, then the address field contains a *to* address and thus, indicates that the frame is a command. If the frame is transmitted by the secondary station then the address field contains a *from* address and thus, indicates that frame is a response. The last bit of address field always ends with one whether the address field is of one byte or of many bytes. However, if the address field is of more than one byte then the last bit of every intermediate byte ends with a zero indicating to the receiver that there are more address bytes to come.
- **Control:** It is an eight-bit long field that can be extended up to 16 bits. This field identifies the type of HDLC frame and is used for carrying the sequence number, acknowledgements request for retransmission and other control information. The implementation of bits in control field depends on the frame type (discussed in **Q15**).
- **Information:** It is a variable-length field that contains the user's data bits in I-frame. However, in U-frames, the information field is used to carry system management information.
- **FCS:** It is a 16-bit long field that contains cyclic redundancy check (CRC) for detecting errors in the address, control and information fields. This field can be extended up to 32 bits

15. Explain the format of control fiel in all types of frames in HDLC.

Ans: The HDLC defines three types of the frames I, S and U and the control field of each frames differs from each other. This field comprises various subfields (Figure 7.6) that define the functions associated with the frame.

Control Field for I-frame

The first bit of the control field specifies the type of the frame. For an I-frame, this bit is always set to zero. The next three bits comprise **N(S)** subfield that defines the sequence number of the frame. As three bits are defined for sequence number, the frames can be numbered from 0 to 7. However, if the

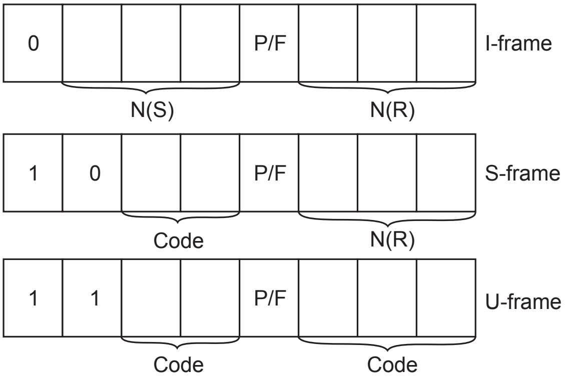


Figure 7.6 Control Field Format for HDLC Frame Types

extended frame format in which the control field is of 16-bits is used then N(S) field becomes larger. The next single bit after N(S) is the **P/F** bit where **P** stands for **poll** and **F** stands for **fina** . If P/F bit is set to one, it means poll, that is, frame has been sent by a primary station to a secondary station. On the other hand, if P/F bit is zero, it means final, that is, frame has been sent by a secondary station to the primary station. The last three bits in control field comprise the **N(R)** subfield that defines an ACK number corresponding to received frame, which has been piggybacked on the I-frame.

Control Field for S-frame

In an S-frame, the first two bits of the control field define the type of the frame. For an S-frame, these bits are always set to 10. Since an S-frame carries control information, the next two bits of the control field, called **code**, indicate the type of control information being carried in an S-frame. There can be four possible combinations of two bits and accordingly, four types of ACKs that an S-frame may carry. These types are as follows:

- **Receive Ready (RR):** If the value of code is 00, then the frame is an RR S-frame. This kind of frame sends the ACK to the sender for a frame or a group of frames that have been received.
- **Receive not Ready (RNR):** If the value of code is 10, then the frame is an RNR S-frame. This kind of frame is similar to RR frame, however, includes some additional features. In addition to acknowledging the frames, it also asks the sender to slow down or not to send any more frames as the receiver is busy.
- **Reject (REJ):** If the value of the code is 01, then the frame is an REJ S-frame. This kind of frame is used in Go-back-N ARQ to inform the sender about the loss or damage of the received frame before the sender's timer expires.
- **Selective-Reject (SREJ):** If the value of the code is 11, then the frame is an SREJ S-frame. This kind of frame is used in selective-repeat ARQ to inform the sender about the loss or damage of a specified frame before the sende 's timer expires.

The next single bit after code bits is **P/F** bit having the same purpose as in I-frame and the last three bits comprise **N(R)** subfield that defines positive ACK number or NACK depending on the type of S-frame.

Control Field for U-Frame

In U-frame, the first two bits specify the type of the frame. For a U-frame, these bits are always set to 11. The next two bits before the **P/F** bit and the last three bits following the P/F bit correspond to the **code** bits in the control field. These five code bits together can create up to 32 different types of U-frames.

16. Describe the frame structure of SDLC. How HDLC frame format is superior to SDLC frame format?

Ans: **Synchronous Data Link Control** (**SDLC**) is a data link layer protocol that is widely used by IBM. It is a subset of HDLC protocol with some minor additional features. The frame structure of SDLC (Figure 7.7) is somewhat similar when compared with the HDLC frame structure. The description of various fields used in SDLC is as follows:

- **Flag:** It is an eight-bit long field having the unique bit pattern of 01111110. The same bit pattern is also used for the last field in the frame. The flag field in the beginning of the frame is used for synchronization while the flag field at the end is used to indicate the end of fram
- **Address:** It is an eight-bit long field that is used to carry the address of the secondary station
- **Control:** It is an eight-bit long field that is used to carry the sequence number of frames. The implementation of control field depends on the frame type and can be extended up to 32 bits
- **Data:** It is a variable-length field that is used to carry use ’s data.
- **Error Checking Field (ECF):** It is a 16-bit long field that is used for the error control

The HDLC frame format is superior to SDLC frame format because in HDLC, FCS field can be of 32-bits but in SDLC, it is limited to 16-bit only.

Flag	Address	Control	User’s data	ECF	Flag

Figure 7.7 SDLC Frame Format

17. Describe the services provided by the PPP protocol. Also, list some services which PPP does not provide.

Ans: The **PPP protocol** operates over a link, which directly connects two nodes, one on each end of the link. Thus, PPP is the most commonly used data link layer protocol for PPP access. This protocol is used by several users who need to connect their home computers with the server of ISP. The PPP protocol can control and manage the transfer of the data, which a modem was unable to provide. That is why PPP has become the popular choice among users accessing Internet over a dial-up connection.

PPP provides a wide variety of services, some of which are as follows:

- It can operate over various types of links such as serial/parallel, synchronous/asynchronous, etc.
- It defines the format of frames that are exchanged between the communicating nodes
- It defines how link should be established between two nodes and how data should be exchanged
- It defines authentication mechanism to be used by the communicating devices to authenticate each other.
- It provides a mechanism for the communicating nodes to learn the network layer address of each other.
- It supports many network layer protocols such as IP and DECnet.
- It can detect the errors in the received frames.

In order to keep PPP simple, some services have not been implemented in PPP. These services are as follows:

- It does not concern about flow control. However, it provides error control to some extent. It enables to detect errors; however, the errors cannot be corrected.
- It operates only where there is single sender and single receiver. Thus, cannot be used over multipoint links.
- It does not support frame sequencing, thus, frames are delivered to the destination not necessarily in the same order in which they were sent by the sender.

18. Explain the frame format of the PPP.

Ans: The PPP is a byte-oriented protocol and uses an HDLC like frame format (Figure 7.8). The description of each field in PP frame is as follows:

- **Flag:** It is a one-byte long field having the unique pattern of 01111110. This unique pattern is inserted at the start and end of each PPP frame. Though the flag field in PPP uses the same bit pattern as that of HDLC, the flag is treated as a byte in PP .
- **Address:** It is a one-byte long field that is set to a constant value of 11111111, which means a broadcast address. This byte can be omitted upon an agreement between two parties during negotiation.
- **Control:** It is a one-byte long field that is set to a constant value of 00000011, which indicates an unnumbered frame. This implies that PPP does not use sequence numbers and ACKs and thus, does not provide reliable transmission. Though PPP does not provide flow control and error control is also limited to error detection only, the control field can also be omitted if both parties agree to do so during negotiation.
- **Protocol:** It is a two-byte long field that defines what is being carried in the payload field, that is, user data or some other information. Only one byte of this field can be used if both parties agree during negotiation.
- **Payload:** It is a variable-length field containing either the user data or other information in the form of sequence of bytes. The default maximum length of payload field is 1,500 bytes; however, two parties can negotiate on this maximum length. If the flag byte appears in the data in payload field, the data is byte stuffed. In case the size of payload field is less than 1,500 bytes or the maximum negotiated value, padding is required.
- **FCS:** It is a two-byte or four-byte long field that is used to detect errors in the transmitted frame. This two- or four byte is simply a CRC.

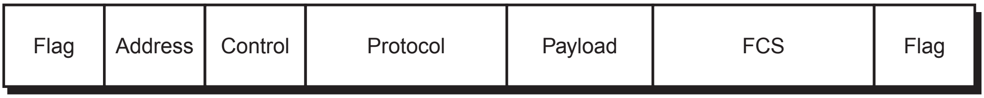


Figure 7.8 PPP Frame Format

19. Explain all the transition phases of PPP.

Ans: A PPP connection transits through various phases while configuring, maintaining, and terminating the PPP link (Figure 7.9). These phases are described as follows:

- **Dead:** This is the initial phase of protocol, which means the line is quiet and no physical layer connection exists. When an event such as a physical carrier detection occurs, the connection goes into establishment phase. The PPP protocol always begins and ends with this phase.

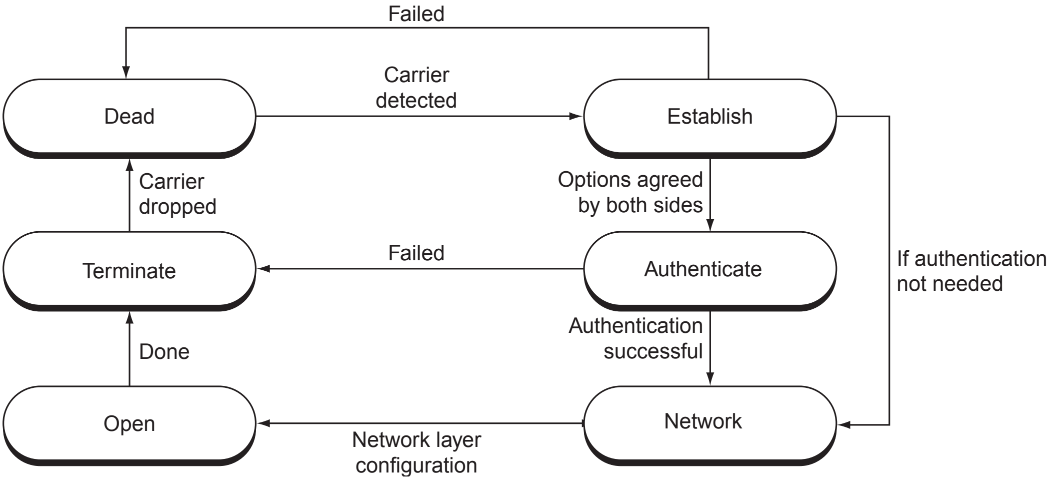

Failed
Dead
Carrier detected
Establish
Carrier dropped
Options agreed by both sides
Terminate
Failed
Authenticate
If authentication not needed
Done
Authentication successful
Open
Network
Network layer configuration

Figure 7.9 Transition Phases of PPP

- **Establish:** In this phase, one of the nodes starts the communication and negotiations are made between the communicating nodes. The link control protocol (LCP) packets and several other packets are exchanged between the nodes if the negotiation is successful. With this, the connection transits to authenticate phase. Notice that if authentication is not required, the connection directly switches to network phase.
- **Authenticate:** This is an optional phase that can be skipped upon an agreement between both nodes during the negotiation in the establishment phase. If both parties agree to undergo this phase then several authenticate protocols are used by the communicating nodes to verify each other's identity. If the authentication becomes successful, then the connection moves to the network phase else it goes to the terminate phase.
- **Network:** In this phase, two nodes negotiate on the network layer protocol that should be used so that the data can be received. As PPP supports multiple protocols and many protocols may run simultaneously at the network layer, the receiver node should negotiate with the sender node on a common protocol to be used for exchanging the data at the network layer. After the protocol has been decided, the connection switches to open phase.
- **Open:** In this phase, data packets are exchanged between the communicating nodes. The connection remains in this phase until one of the nodes wants to close the connection.
- **Terminate:** In this phase, the connection link is closed and the nodes now cannot transfer any data packets between themselves. Certain packets are exchanged between two nodes for house cleaning the connection and then the link is terminated. After this, the connection goes to dead phase.

20. Write a short note on LCP and NCP.

Ans: The **link control protocol** (**LCP**) and **network control protocol** (**NCP**) are the PPP protocols that are used to establish the link, authenticate the communicating nodes and move the network layer data.

Link Control Protocol

This protocol has the responsibility of establishing, configuring, maintaining and terminating the link. The link can be established when both the communicating nodes agree on certain options. For this, LCP provides the negotiation mechanism. Each LCP packet is encapsulated in the payload field of PPP frame and a value 0xC021 (hexadecimal) is placed in the protocol field of PPP frame to indicate that PPP is carrying an LCP frame (Figure 7.10).

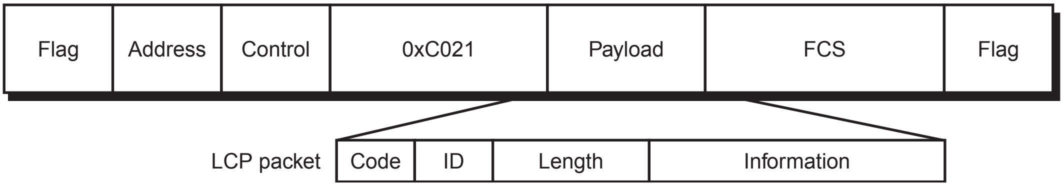


Figure 7.10 LCP Packet Encapsulated into PPP Frame

The frame structure of LCP consists of various subfields, which are described as follows

- **Code:** It is a one-byte long field that defines the type of LCP packet. There are 11 types of LCP packets that are divided into three categories. The first category includes four packets and is used to configure the link during the establishment phase. The second category includes two packets that are used to terminate the connection. The third category includes five packets that are used to debug and monitor the link.
- **ID:** It is a one-byte long field that contains a value to match a request with a reply. When one node sends the data to another node then the sender node inserts a value in the ID field, which is then copied by the receiver and placed into the reply packet to be transmitted.
- **Length:** It is a two-byte long field that defines the length of the whole L packet.
- **Information:** It is a variable length field, which carries options like authentication protocol, payload field size, etc. These options can be negotiated between the two communicating nodes.

Network Control Protocol

PPP supports multiple network layer protocols defined by OSI, Novel, DECnet and Xerox. To carry a network layer data packet from these protocols, PPP has defined an NCP for each network layer protocol. The NCP consists of a set of protocols that encapsulate the data received from the network layer protocols into the PPP frame. The NCP also configures the link at the network layer. Like LCP, each NCP packet is also included in the payload field of PPP frame and the protocol field of PPP is set to a value 0x8021 (hexadecimal) which indicates that PPP frame is carrying the NCP packet.

21. Explain two authentication protocols that are used in PPP.

Ans: As PPP is used over point-to-point link, authentication is important between the communicating nodes for the effective transmission of resources. The PPP uses two protocols, namely, *password authentication protocol* (*PAP*) and *challenge handshake authentication protocol* (*CHAP*) for the verification of user identity during the authentication phase.

Password Authentication Protocol

PAP uses three types of packets for authentication, namely, *authenticate-request*, *authenticate-ack* and *authenticate-nak*. A node that wishes to access the system uses **authentication-request packet** to send its username and password to the system. After receiving authentication-request packets, the system checks the validity of username and password. If the requesting node is validated, the system sends an **authenticate-ack packet** to the node indicating that access is allowed. However, if the node is not validated, then the system sends an **authenticate-nak packet** indicating that access is denied. Whenever a PAP packet is being carried in a PPP frame, the protocol field of PPP frame is set to a value 0xC023 (hexadecimal).

Challenge Handshake Authentication Protocol

This is a three-way handshaking authentication protocol. It uses four packets, namely, *challenge*, *response*, *success* and *failure*. The system sends a **challenge packet** containing a challenge value to the user needing access to the system. The user retrieves the challenge value from the challenge packet and inputs this value along with its password to a predefined function to generate an output. The user encapsulates the output obtained in the **response packet** and sends it to the system. The system also applies the same function on the challenge value and the user's password. If the output obtained is same as the output received in the response packet, the user is validated. The system sends a **success packet** to the user indicating that the access is granted. Otherwise, the system sends a **failure packet** indicating that the access is denied. Whenever a CHAP packet is being carried in a PPP frame, the protocol field of PPP frame is set to a value 0xC233 (hexadecimal).

Further, CHAP provides more security as compared to PAP as it prevents the need of sending the password online. In case an intruder gets access to the challenge value and the output in the response packet, he/she cannot know the password. That is, password always remains secret.

22. Why CRC is always added in trailer and not in the header of all data link protocols?

Ans: All data link protocols comprise a CRC field that stores the checksum for error detection and correction. The CRC is calculated over all the bits that are needed to be transmitted to the destination node and added to the trailer of the outgoing data stream as soon as the last bit is transmitted. If CRC is to be attached in the header part of the data stream, then CRC has to be calculated before the transmission of the frame. This would result in more overhead as each byte of frame needs to be handled twice, once for computing CRC and then for transmission. On the other hand, when CRC is put in the trailer, each byte of frame needs to be handled only once, resulting in less overhead. That is why CRC is added in the trailer and not in the header of data link protocols.

23. A channel has a bit rate of 4 kbps and propagation delay of 20 msec. For what frame size does stop and wait gives an efficienc of at least 50%.

Ans: Given, propagation delay, $a = 20$ msec

Bit rate, $R = 4$ kbps $= 4 \times 10^3$ s

Let L denotes the size of frame, then transmission time of a frame (t_{frame}) can be given as

$$\begin{aligned} t_{\text{frame}} &= L/R \\ &= L/(4 \times 10^3) \\ \text{As } a &= t_{\text{prop}}/t_{\text{frame}} \\ &= 20 \times 10^{-3}/(L/(4 \times 10^3)) \\ &= (20 \times 10^{-3} \times 4 \times 10^3)/L \\ &= 80/\text{L} \end{aligned}$$

The maximum link utilization (U) can be given as

$$\begin{aligned} U &= 1/(1 + 2a) \\ &= 1/(1 + 160/L) \qquad \ldots (1) \end{aligned}$$

Given $U \geq 50\%$

$$\Rightarrow U \geq 0.5 \qquad \ldots (2)$$

From Eqs (1) and (2), we have

$$
\begin{aligned}
&1/(1 + 160/L) \geq 0.5\\
\Rightarrow\ &1/0.5 \geq 1 + 160/L\\
\Rightarrow\ &2 \geq 1 + 160/L\\
\Rightarrow\ &L \geq 160
\end{aligned}
$$

Thus, for achieving at least 50% efficienc , the frame size should be at least 160 bits.

24. If the window size is 15, give the sequence number of frames in Go-back-N ARQ and selective-repeat ARQ.

Ans: In Go-back-N ARQ, the maximum window size is equal to $2^m - 1$ where m is the number of bits in the frame sequence number and the frame sequence numbers range from 0 to $2^m - 1$. Here, given that

$$
\begin{aligned}
&2^m - 1 = 15\\
\Rightarrow &2^m = 16
\end{aligned}
$$

Thus, the sequence numbers range from 0 to 15.

In selective repeat ARQ, the maximum window size is equal to 2^{m-1} and the frame sequence numbers range from 0 to $2^m - 1$. Here, given that

$$
\begin{aligned}
&2^{m-1} = 15\\
\Rightarrow &2^m = 30
\end{aligned}
$$

Thus, the sequence numbers range from 0 to 29.

25. A channel has a bit rate of 20 kbps. The stop-and-wait protocol with a frame size of 4,500 bits is used. The delay for error detection and sending ACK by the receiver is 0.25 seconds because of a fault. Find the maximum efficiency of the channel if the destination is 30,000 km away and the speed of the propagation of the signal is 2.8×10^8 m/s. Find the decrease in efficienc due to the fault.

Ans: Given, bit rate (R) = 20 kbps = 20×10^3 bps
Frame size (L) = 4,500 bits
Distance between sender and receiver (d) = 30,000 km = $30{,}000 \times 10^3$ m
Propagation speed (V) = 2.8×10^8 m/s
Now, the frame transmission time (t_{frame}) can be computed as

$$
\begin{aligned}
t_{\text{frame}} &= L/R\\
&= 4{,}500/(20 \times 10^3) = 0.225 \text{ s}
\end{aligned}
$$

The propagation delay (a) can be computed as

$$
\begin{aligned}
a &= Rd/VL\\
&= (20 \times 10^3 \times 30{,}000 \times 10^3) / (2.8 \times 10^8 \times 4500)\\
&= 0.4761
\end{aligned}
$$

Now, the maximum utilization (with ignoring the fault) can be computed as

$$
\begin{aligned}
U_{\max} &= 1/(1 + 2a)\\
&= 1/(1 + 2 \times 0.4761)\\
&= 0.512 = 51.2\%
\end{aligned}
$$

If we consider the fault, the time taken in sending each frame and receiving its ACK will be increased by 0.25 s. Thus, the total time spent in sending all the frames (say, n) can be given as

$$T = n^*(2t_{\text{prop}} + t_{\text{frame}} + 0.25)$$

The link utilization (in case of fault) can be given as

$$\begin{aligned} U_{\text{fault}} &= (n^* t_{\text{frame}})/(n^*(2t_{\text{prop}} + t_{\text{frame}} + 0.25)) \\ &= t_{\text{frame}}/(2t_{\text{prop}} + t_{\text{frame}} + 0.25) \\ &= 1/(1 + 2a + 0.25/t_{\text{frame}}) \\ &= 1/(1 + 0.9522 + 1.1111) \\ &= 0.326 = 32.6\% \end{aligned}$$

The decrease in efficiency (in %) due to fault $= ((U_{\text{max}} - U_{\text{fault}})/U_{\text{max}})^*100$

$$\begin{aligned} &= ((0.512 - 0.326)/0.512)^*100 \\ &= 36.3\% \end{aligned}$$

Multiple Choice Questions

1. Propagation delay is inversely proportional to ________.
   (a) distance of the link
   (b) data rate of transmission
   (c) length of the frame
   (d) none of these

2. When data and ACK are sent on the same frame, this is called ________.
   (a) piggybacking
   (b) backpacking
   (c) piggypacking
   (d) forwarding and backing

3. A frame that fails to arrive at the destination node due to noise burst is called ___________.
   (a) damaged frame
   (b) transmission frame
   (c) undamaged frame
   (d) lost frame

4. The link utilization (U) in stop-and-wait ARQ is expressed as
   (a) (1 + P)/(1 + a) (b) (1 + P)/(1 + 2a)
   (c) (1 – P)/(1 + 2a) (d) (1 – P)/(1 + a)

5. In Go-back-N ARQ, if frames 3, 4 and 5 are received successfully, which ACK number may be sent to the sender?
   (a) 5 (b) 6
   (c) 7 (d) 8

6. ABM in HDLC stands for _______.
   (a) asynchronous balanced mode
   (b) asynchronous balanced modem
   (c) asynchronous bisync mode
   (d) asynchronous bus modem

7. The shortest frame in HDLC protocol is usually the _________.
   (a) information frame
   (b) supervisory frame
   (c) unnumbered frame
   (d) control frame

8. The maximum number of unconfirmed frames that can be outstanding at any one time with SDLC is ___________.
   (a) 4 (b) 7
   (c) 8 (d) 14

9. PPP is a ______ -oriented protocol.
   (a) bit
   (b) byte
   (c) both (a) and (b)
   (d) none of these

10. If you connect to the Internet from your home computer, chances are that you are using: _________.
    (a) PPP (b) NCP
    (c) DAP (d) FTAM

Answers

1. (c) 2. (a) 3. (d) 4. (c) 5. (b) 6. (a) 7. (b) 8. (a) 9. (b) 10. (a)

8

Media Access Control

1. Write a short note on channel allocation.

Ans: In a broadcast (or multipoint) network, multiple users (stations) use a single broadcast channel to communicate with each other. In case more than one user wish to access the shared channel at the same time, the channel is allocated to one of the competing users at one time. This is called channel allocation. The decision to allocate the channel among the competing users can be made using any of the two schemes, namely, *static channel allocation* and *dynamic channel allocation*.

Static Channel Allocation

In this scheme, a single channel can be shared among multiple users using either frequency division multiplexing (FDM) or time division multiplexing (TDM) technique. In FDM, for n users, the bandwidth of a channel is divided into n parts of equal sizes and each part is kept fixed for use by a specific user. With a separate frequency band for each user, there is no interference between competing users. Though FDM is simple and efficient, it does have some drawbacks. For example, if at a specific point of time, less than n users communicate through the channel, there will be wastage of frequency spectrum and if more than n users want to communicate through the channel, some of them will not be permitted due to bandwidth deficienc . Moreover, when some users are inactive, it results into loss of precious bandwidth as no one else is allowed to use the bandwidth allocated to those users.

On the other hand, in TDM, time is divided into n slots for n users and every n^{th} time slot is statically allocated to each user during which it can transmit the frames. However, if at any instance, the user does not use the allotted slot, it goes wasted.

Dynamic Channel Allocation

The drawbacks of static channel allocation can be overcome by dynamic allocation method. In this method, neither a fixed frequency nor a fixed slot is allocated to the user in advance; rather, each user is allocated the channel dynamically at the time it needs using many protocols. Dynamic channel allocation can be used when bursty traffic is present in the network. To implement this method, certain assumptions are followed.

- **Station Model:** The model consists of n stations (sometimes, called **terminals**) such as computers and telephones that can work independently on a network. Each terminal has the capability to produce frames for transmission. After a frame has been generated, the station remains idle or is blocked until the entire frame has been transmitted.
- **Single Channel:** A single communication channel is shared by all the stations for transmission.
- **Collision:** When two stations transmit frames simultaneously, the reception of frames may overlap in time resulting in a garbled signal. This phenomenon is known as **collision**. The collided frames must be retransmitted by their respective stations.
- **Continuous Time and Slotted Time:** Some systems follow continuous time assumption while others follow slotted time assumption. If continuous time assumption is followed in a network, then a station can transmit a frame at any time. However, if slotted time assumption is followed then time is partitioned into discrete intervals and a frame can be transmitted only at the beginning of a slot. Thus, for synchronization, some mechanism such as a clock is required.
- **Carrier Sense and no Carrier Sense:** A network can have either carrier sensing or not. A station with a carrier sense can determine whether a channel is in use before attempting to use it. If a channel is busy, no station attempts to use it until it gets free. However, if the network has no carrier sense then a station cannot sense the channel before starting the transmission. If the station needs to send a frame, it just transmits it.

2. What is the need of multiple-access protocol? List the categories of multiple-access protocols.

Ans: When multiple stations or nodes connected via a network use a common link or channel (multipoint or broadcast) to send or receive data, some means is required to coordinate access to the link. This is what a multiple-access protocol does. It decides which of the stations is going to access the shared channel next. A number of multiple-access protocols have been devised to handle access to shared link. All these protocols belong to a sublayer of data link layer called **medium access control** (**MAC**) sublayer. These protocols have been classified into three categories, namely, *random access*, *controlled access* and *channelization* protocols.

3. What is meant by random access method? Give examples of random access protocols.

Ans: The method, which allows the stations to access the transmission medium (channel) randomly at any time, is known as random access method. No station is under the control of any other station and there is no specific time for stations to start transmission. Moreover, there are no rules to be followed for deciding which station should be allowed access to the channel. If multiple users need to access the channel at the same time, they have to compete with each other. Hence, this method is also known as **contention method**. Examples of random access protocols are ALOHA, carrier sense multiple access (CSMA), CSMA/collision detection (CD) and CSMA/collision avoidance (CA).

4. Explain pure ALOHA and slotted ALOHA.

Ans: Pure ALOHA and slotted ALOHA are the versions of ALOHA protocol, the earliest contention-based method that was invented in 1970 at the University of Hawaii.

Pure ALOHA

Pure ALOHA is a simple protocol. It was originally developed for packet radio networks but can be applied to any system where a single shared channel is being used among multiple competing users. The basic idea is that each station can send a frame whenever it needs to transmit. When two frames are sent at the same time, they may collide with each other fully or partially and get corrupted (Figure 8.1). The sender, therefore, must retransmit the corrupted frames.

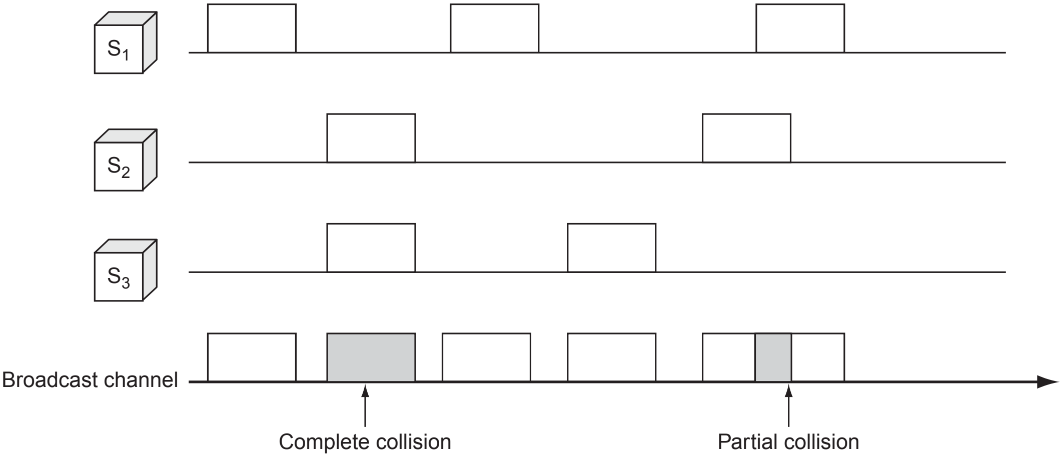


Figure 8.1 Collisions in Pure ALOHA

Detection of collision is easy in pure ALOHA. A station can detect the destruction of a frame by listening to the channel. However, if listening is not possible, the receiving station must send an acknowledgement to the sender after receiving a frame. The sending station, after sending a frame, waits for a random amount of time computed using binary exponential back-off algorithm (discussed in **Q7**). If it receives the acknowledgement until that period, it knows that the frame has been received successfully. Otherwise, it assumes that collision has happened and thus, retransmits the frame.

In pure ALOHA system, the throughput (S), which is defined as the average number of successful transmissions, is given as

$$S = Ge^{-2G}$$

where G = the average number of frames generated by the system during one frame transmission time, that is, the offered traffic and e = a mathematical constant with the value 2.718.

The offered traffic G) can also be expressed as

$$G = N_s \times N_f \times t$$

where

N_s = total number of stations in the system.

N_f = the number of frames that can be transmitted by a station in one second.

t = frame transmission time.

As shown in Figure 8.2, the maximum throughput (S_{max}) of pure ALOHA is obtained at G = 0.5 (50% ordered traffic) and is equal to 1/2e, that is, 0.184 or we can say 18.4%. At lower offered traffic ($G < 0.5$), the channel's capacity is underutilized while on higher-offered traffic ($G > 0.5$), the throughput starts decreasing due to increase in number of collisions.

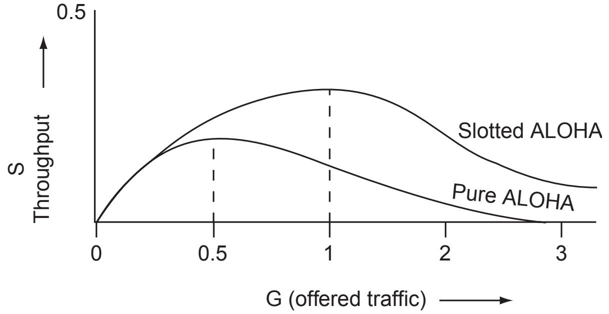


Figure 8.2 Throughput of Pure ALOHA and Slotted ALOHA

Slotted ALOHA

Slotted ALOHA is a modification of ALOHA that has been developed to improve the efficienc . This is a discrete time system in which time is partitioned into intervals or slots with each slot corresponding to a frame. Slotted ALOHA demands for the stations to agree on the boundaries of slots and a clock are needed to synchronize the stations. In this method, a station can begin the transmission of a frame only at the beginning of a slot. If a station is unable to start the transmission at the beginning of a slot, then it has to wait until the next slot, thereby reducing the chances of collisions. However, collisions may still occur when two stations are ready for transmission in same slot resulting in garbled frames, which have to be retransmitted by the sender (Fig. 8.3).

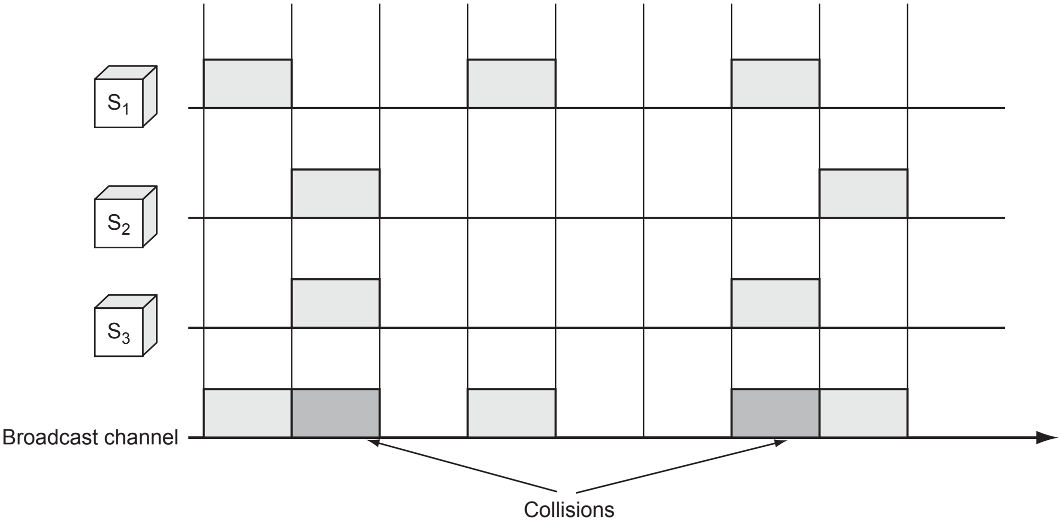


Figure 8.3 Collisions in Slotted ALOHA

The throughput (S) of slotted ALOHA is given as

$$S = Ge^{-G}$$

As shown in Figure 8.2, the maximum throughput (S_{max}) of slotted ALOHA is obtained at $G = 1$ (100% ordered traffic) and is equal to $1/e$, that is, 0.368 or we can say 36.8%. Thus, it is clear that the throughput of slotted ALOHA is twice that of pure ALOHA.

5. List some limitations of ALOHA protocol.

Ans: The ALOHA protocol suffers from certain limitations, which are as follows:

- ❑ If any station transmits a frame but the propagation delay between stations is very large in comparison to transmission time of a frame, then it will be harder for the stations to know about it. During that time, another station can transmit a frame, which can result in a collision.
- ❑ It is not possible for stations to sense a channel before utilizing it for transmission. They can only detect the channel after transmission of a frame.
- ❑ The system needs to maintain queuing buffers to store the transmitted frames until the receiver receives them successfully. This is required to enable the retransmission of frames in case of a collision.

6. What is the vulnerable period? Show that the vulnerable time period of slotted ALOHA is half of that of pure ALOHA.

Ans: Consider a system consisting of several stations that share a common link to transmit and receive frames. The time interval during which collision may occur in the frame transmission is referred to as the **vulnerable period** of the system. To determine the vulnerable period of pure ALOHA and slotted ALOHA, consider three stations S_1, S_2 and S_3 which are transmitting frames and the time taken in transmitting a complete frame by any station is t.

Consider the pure ALOHA protocol. Let station S_1 transmits a frame F_1 at time t_0. This frame will be completely transmitted by the time $t_0 + t$. Now, suppose station S_2 has already transmitted a frame F_2 between the time $t_0 - t$ and t_0. This will result in a collision as the ending part of frame F_2 may collide with the leading part of frame F_1 (Figure 8.4). Further, suppose that station S_3 transmits a frame F_3 between the time t_0 and $t_0 + t$. This will again result in a collision as the ending part of frame F_1 may collide with the leading part of frame F_3. Thus, it is clear that if a station transmits a frame at t_0, a collision may occur if any other station transmits frame between the time $t_0 - t$ and $t_0 + t$. This implies that the vulnerable period of pure ALOHA is $2t$, that is, twice of the frame transmission time.

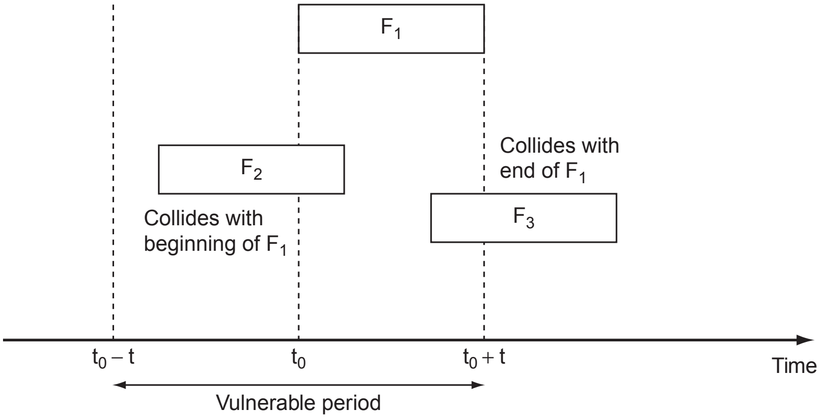


Figure 8.4 Vulnerable Period in Pure ALOHA Protocol

In slotted ALOHA, the stations are allowed to transmit frames only in the beginning of each time slot. If any station misses the chance in one time slot, it must wait for the beginning of next time slot. This implies that a station, which has started at the beginning of this time slot, has already transmitted its frame completely. However, a collision may still occur if two stations attempt to transmit in the beginning of same time slot (Figure 8.3). Hence, the vulnerable period of slotted ALOHA is t, which is half of that of pure ALOHA.

7. Explain the binary exponential back-off algorithm with the help of an example.

Ans: In case of a collision, the stations whose frames have collided are required to retransmit the frames. However, before attempting to retransmit the frames, each station that was involved in the collision waits for some random amount of time (**random delay**) to ensure that the collision is not likely to occur at the time of retransmission. The random delay increases with each repeated collision.

Binary exponential back-off algorithm specifies the random amount of time a station has to wait for retransmission of a frame after a collision occurs. After a collision occurs, this algorithm works as follows:

1. Time is divided into discrete slots. For the $\texttt{k}^{\texttt{th}}$ attempt of retransmission, a random number `r` between 0 and $\texttt{2}^{\texttt{k}}\ \texttt{- 1}$ is selected. The value of `k` is incremented by one with every retransmission attempt and thus, the range of random numbers also increases.
2. A station waits for `r` number of slots before making an attempt to retransmit the frames.
3. If number of collision or number of attempts is more than 15, transmission is aborted and failure is reported to the station.

For example, after two collisions, that is, two attempts of retransmission, a station will wait for random number chosen between 0 and 3 (that is, $2^2 - 1$) of slots. If more than one station selects the same random number, then collision occurs again. As the number of collisions increases, the range of random number increases thereby reducing the chances of collision among stations. However, the increase in range of random numbers also implies increase in average wait time, which results in increased delay.

8. Explain the working of carrier sense multiple-access protocol.

Ans: Carrier Sense Multiple Access (**CSMA**) is a contention-based protocol that was developed to overcome the drawbacks of ALOHA system. This protocol tends to reduce the chances of collisions and thus, improving the performance of the network. This protocol operates on the principle of **carrier sensing** which states that any station, before attempting to use the channel, must sense (listen to) it to check whether any other station is using the channel or not. A station sends the data only if it finds the channel free, that is, when there is no other carrier.

There are three variations of CSMA protocol, which are as follows:

- **1-persistent CSMA:** In this method, when a station needs to transmit a frame, it monitors the channel, and transmits the frame as soon as it finds the channel idle. However, if it finds the channel busy, it continuously senses the channel until it becomes free. Despite of the fact that carrier sensing is used, collisions may still occur if two or more stations find the channel idle at the same time and thus, transmit frames simultaneously. The performance of this protocol is greatly affected by the propagation delay. To understand, consider that a station sends a frame and the propagation delay is greater than the transmission time of a frame. It takes some time for the first bit of the transmitted frame to reach and be sensed by other stations. In the mean time, any other station that becomes ready to send, may sense the channel idle and thus, transmits the frame. This leads to a collision. This protocol is so named as a station transmits with probability one on finding the channel idle
- **Non-persistent CSMA:** In this method, when a station needs to send a frame, it first senses the channel. If the channel is idle, the station transmits the frame instantly. However, if the station finds the channel busy, it waits for a random amount of time before sensing the channel again. This method reduces the chances of collision as it is rare that two stations will wait for same amount of time and then will retry to transmit at the same time. Due to fewer collisions, the utilization of network is also improved.
- **P-persistent CSMA:** This method is applicable and used with the channel that has time slots with each slot being greater than or equal to maximum propagation time. In this method, if the channel

is found idle, a station is allowed to transmit with a probability p. With probability q (which is equal to 1 – p), the station waits for the beginning of the next time slot and senses the line again. If the channel is idle in the next time slot also, the above method is repeated; the station either transmits or waits with probabilities p and q, respectively. This process continues and eventually, either that station transmits the frame or some other station starts transmitting the frame. In the latter case, the station assumes that a collision has occurred and thus, it waits for a random period (computed using back-off algorithm) and then starts again.

9. Compare the performance of non-persistent and 1-persistent CSMA protocols.

Ans: The performance of non-persistent and 1-persistent CSMA protocols can be compared with respect to two parameters: delay and channel utilization. In case of fewer load on the network, 1-persistent has shorter delay than non-persistent because 1-persistent method permits a station to begin sending a frame as soon as the channel is sensed idle. Due to less delay, the channel utilization of 1-persistent method is better than that of non-persistent method. On the other hand, in case of heavy load on the network, non-persistent method has shorter delay than 1-persistent method because the number of collisions in 1-persistent method is higher than that of non-persistent method. Due to less probability of collisions, the channel utilization of non-persistent method is better than that of 1-persistent method. Thus, it can be concluded that at low loads, 1-persistent method is preferable over non-persistent method while at heavy loads, non-persistent method is preferable over 1-persistent method.

10. What is CSMA/CD? Explain its working.

Ans: **Carrier Sense Multiple Access/Collision Detection** (**CSMA/CD**) is the refinement of CSMA protocol. It was developed to overcome the inefficiency of CSMA protocol where the stations involved in the collision do no stop transmitting bits of frames even though the collision is detected. This leads to inefficient channel utilization. Further, CSMA/CD improves the channel utilization by making the stations to sense the channel not only before starting the transmission but during the frame transmission also (referred to as **collision detection**). This implies that in CSMA/CD, both transmission and collision detection are continuous processes. Once a station starts transmitting bits of a frame, it continuously senses the channel to detect the collision. As soon as the station detects a collision, it aborts the frame transmission immediately rather than finishing the transmission. Collision can be detected by comparing the power of the received signal with that of transmitted signal.

The CSMA/CD can be in any of the three states, namely, *contention*, *transmission* or *idle*. **Contention** refers to the state in which more than one station is ready to transmit and competing to get the channel. **Transmission** refers to the state in which data are transmitted. **Idle** refers to the state in which channel is idle and no station is transmitting data.

Figure 8.5 depicts the working of CSMA/CD. When a station has a frame to send, a variable k denoting the number of retransmission attempts is initialized with zero. The station applies one of the persistence methods to sense the channel. When the channel is found idle, the station starts transmitting bits of frame and detecting for collision as well. If collision does not occur during the entire transmission period, the station assumes that the frame has been received successfully. However, if a collision takes place during the transmission, the station aborts the transmission and a jam signal is sent to inform all other stations on the network about the collision. If the station has not crossed the limit of maximum retransmission attempts (k_{max}), the back-off time is computed for the station using the binary exponential algorithm (explained in **Q7**). The station is made to wait for the back-off period and then restart the process.

To better understand CSMA/CD, consider two stations S_1 and S_2. Suppose when contention period starts at time t_1, station S_1 starts transmitting a frame F_1. After some time, station S_2 senses the channel

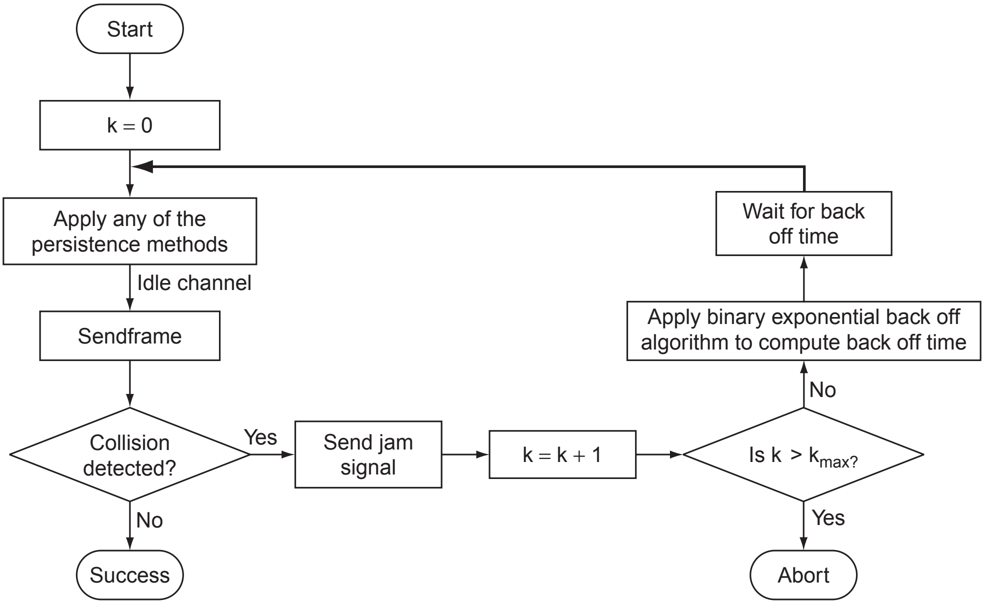


Figure 8.5 Working of CSMA/CD

and finds it idle as the first bit of frame F_1 sent by station S_1 has not yet reached. Therefore, station S_2 starts transmitting the bits of frame F_2 at time t_2; the bits are propagated in both forward and backward direction. Collision occurs between frames F_1 and F_2, which is detected by the station S_2 at time t_3. As soon as the station S_2 detects the collision, it discontinues sending further bits of frame F_2. Now, let at time t_4, station S_1 detects a collision. It also aborts the transmission of frame F_1. After detecting a collision, stations S_1 and S_2 immediately abort the transmission rather than finishing the transmission of frames, which will be garbled anyway (Figure 8.6).

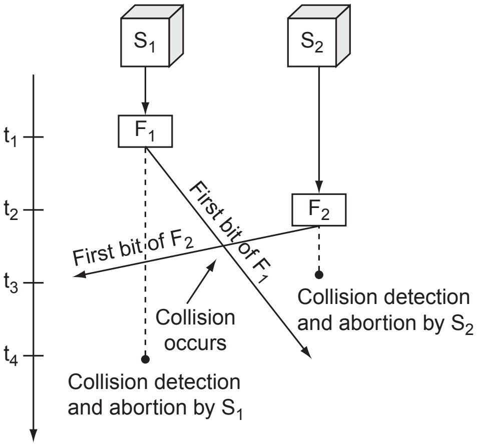


Figure 8.6 CSMA/CD

The advantage of this protocol over CSMA is that it saves time and bandwidth as it aborts the transmission of a frame as soon as the collision is detected. Thus, it offers better performance than CSMA. It is widely used on LANs in MAC sublayer.

11. Describe CSMA/CA protocol.

Ans: In wireless networks, it is difficult to effectively detect the collision using CSMA/CD. This is because in wireless networks, most energy of the signal is lost during transmission and as a result, the signal received by a station is of very less energy. That is why in wireless networks, a need arises to avoid the collision rather than detect the collision. The CSMA/CA is a protocol developed for wireless networks to help in avoiding collisions.

Figure 8.7 shows the working of CSMA/CA protocol. When a station is ready to transmit the frames, a variable k denoting the number of retransmission attempts is initialized with zero. The station uses any of the persistent methods to sense the channel. If the channel is busy, it again senses the channel. The station continues to do so until it finds the station idle. After the station has found the channel idle, it does not send the frame immediately rather it waits for a random amount of time known as **interframe space** (**IFS**). The station is required to wait for IFS time because it may happen that some other distant station has already started the transmission of a frame but the leading bits of the frame have not reached here until yet.

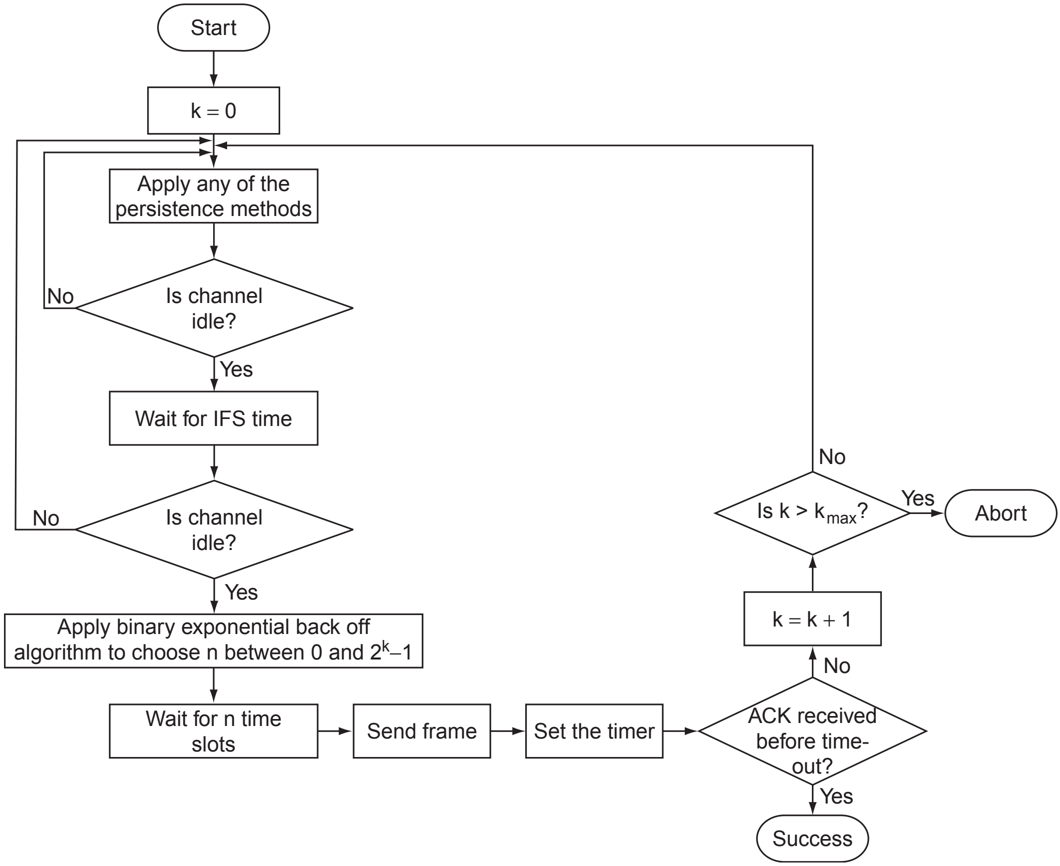


Figure 8.7 Working of CSMA/CA

After waiting for IFS amount of time, the station again senses the channel. If it finds the channel still idle, it waits for a random amount of time partitioned into slots. This time is referred to as the contention time and it is computed using the binary exponential back-off algorithm; a random number n is chosen between 0 and $2^k - 1$ and the station is made to wait for n time slots. After each time slot, the station senses the channel. If the channel is busy, the timer is stopped and it is not restarted until the channel is found idle.

After waiting for n time slots, the station sends the frame and starts waiting for its acknowledgement. If the station receives the positive acknowledgement before the time-out, it knows that the frame has been received successfully. However, if acknowledgement is not received before the time-out, the station needs to retransmit the frame. To check whether the station is eligible for retransmission, the value of k is increased by one and compared with k_{max}—the maximum number of retransmissions allowed. If the value of k is less than k_{max}, the whole process is repeated. Otherwise, the station aborts the transmission.

12. Write a short note on the collision-free protocols.

Ans: Generally, when CSMA/CD protocol is used, collisions do not occur. Still, there are some chances of occurrence of collisions during the contention period. To resolve the contention problem along with avoiding the collisions, collision-free protocols were developed. *Bit-map* and *binary countdown* are the two commonly used collision-free protocols, which are discussed here.

Bit-Map Protocol

This protocol involves the division of contention period into n number of slots for n number of stations in the network with one slot corresponding to each station. Both stations and slots are numbered from 0 to n – 1. If a station needs to transmit a frame, it will transmit a 1 bit in its respective slot; no other station can transmit in this time slot. At the end of n-bit contention period, each station knows which stations wish to transmit. Then, the stations begin transmitting frames in the numerical order. After the last ready station has transmitted the frame, the next n-bit contention period starts. In case a station is ready to send but its slot has passed by, then it must wait for its turn. Since, every station knows which station has to transmit next, collisions cannot occur.

To understand the bit-map protocol, consider a network with five stations numbered from 0 to 4. If stations 0, 2 and 3 want to transmit frames, they insert 1 bit into their corresponding slots and they are transmitted in the order 0, 2 and 3 only (Figure 8.8).

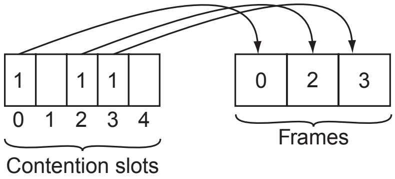


Figure 8.8 Bit-map Protocol

To analyze the performance of channel in bit-map protocol, let the total number of stations is n and the quantity of data per each frame is d bits. At low loads, the bit-map will be repeated over and over lacking of frames, creating an overhead of n bits per frame. Thus, the performance of channel at low loads can be given as

$$S_{low} = d/(N + d)$$

On the other hand, at high loads, almost every station has some data to send. As a result, each n-bit contention period will have bits per each frame, creating an overhead of one bit per frame. Thus, the performance of channel at high loads can be given as

$$S_{high} = d/(1 + d)$$

Binary Countdown Protocol

When a large number of stations are present, the bit-map protocol does not prove efficient because of the overhead of one bit per each station. To overcome this problem, a more efficient protocol named binary countdown can be used. In this protocol, each station has a binary address that identifies it and the one out of many competing stations that has the highest binary address is allowed to use the channel at a given time.

Every station that wants to use the channel, broadcasts its binary address starting with the most significant bit. During each bit time, the higher-order bits from the competing stations are ORed together. If the result comes out to be one, then stations with zero high-order bit quit as they come to know that some station with higher binary address is contending to use the channel. On the other hand, stations with high-order bit 1 still continue. This process continues until a station with the highest binary address is determined and thus, allowed access to channel.

To better understand the process, consider three stations S_1, S_2 and S_3 with binary addresses 0011, 1000 and 1011, respectively are trying to use the channel. Each station transmits its higher-order bit in the bit time slot and these bits (0, 1, 1) from all the stations are ORed together, which results in 1. Now, station S_1 knows that stations S_2 and S_3 with a higher address are contending for the channel, hence, it quits. Again, the next high-order bits (0, 0) from stations S_2 and S_3 are ORed together and the result comes out to be zero. Both stations continue to transmit next higher-order bit, that is, (0, 1) which are ORed together and result obtained is one. The station S_2 sees this result and quits. Thus, S_3 gets the channel to transmit data. Figure 8.9 depicts the whole process.

The main limitation of this protocol is that the station with higher address will always get the higher priority. The efficiency of channel in this protocol is equal to $d/(d + \log_2 n)$.

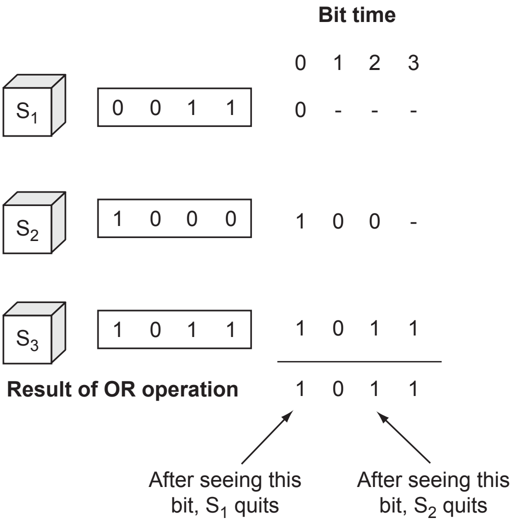


Figure 8.9 Binary Countdown Protocol

13. **Explain limited-contention protocol.**

Ans: Limited-contention protocol is the combination of contention and collision-free protocols. At high loads, it uses collision-free protocol to achieve better efficiency of network and at low loads, it uses contention protocols to achieve shorter delay for transmission. Further, limited-contention protocol is asymmetric in nature; different stations attempt to seize the channel with different probabilities.

The basic idea behind the limited-contention protocol is that chances of some station acquiring the channel can be increased by reducing the number of stations competing for the channel. Thus, in limited-contention protocol, stations are divided into groups. For slot 0, stations under group 0 are allowed to compete for the channel. If any of the group 0 stations succeeds, it gets the channel and transmits the frame. However, if some collision occurs then stations under group 1 compete for the channel in slot 1. This process continues, reducing the amount of competition for each slot.

To appropriately divide the stations into groups, **adaptive tree-walk algorithm** is used, which considers all the stations in the network as the leaves of a binary tree as shown in Figure 8.10. The process starts at the root of the tree (node 1). Initially, in the first slot (slot 0), all the stations under node 1 are allowed to compete for the channel. If there is a single station that is ready to transmit, it is allocated the channel. However, if there is a collision, stations under the node 2 try to seize the channel in slot 1. If some station under node 2 acquires the channel, the next slot after the successful transmission of frame is kept reserved for the stations under node 3. However, if collision occurs in slot 1, the stations under node 4 contend during the slot 2. In essence, in case of collision during slot 0, the search continues recursively in the left and right subtree of binary tree and it stops when a bit slot is idle or there is only one station that is ready to transmit the data.

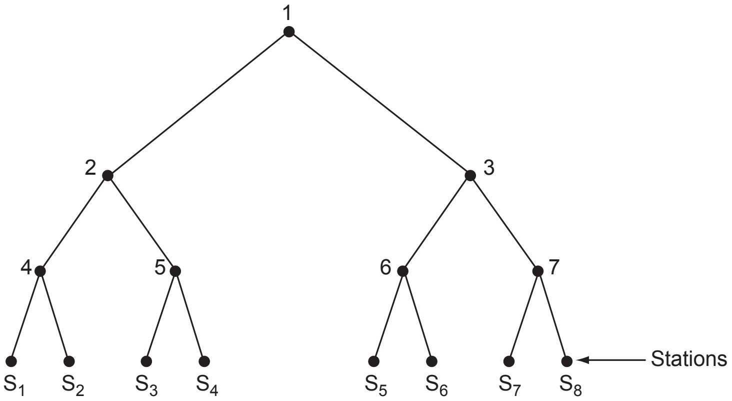


Figure 8.10 Adaptive Tree-walk Algorithm

14. Explain three controlled access methods.

Ans: In controlled access, stations refer each other to know which station has the right to transmit a frame. A station is allowed to transmit only if other stations authorize it do so. There are three controlled access methods, namely, *reservation*, *polling* and *token passing*.

Reservation

In this method, any station that wants to transmit a frame has to make a reservation before sending. During each time interval, the reservation frame precedes the data frames to be transmitted in that interval. A reservation frame consists of mini-slots with the number of mini-slots being equal to the number of stations in the network. Whenever, a station wants to transmit a data frame it makes a reservation by inserting a 1 bit into its corresponding mini-slot. After making reservations, the stations can transmit their data frames in the numerical order following the reservation frame.

Polling

In this method, two types of stations namely, *primary node* and *secondary node* exist. A **primary node** refers to the master station through which the exchange of the data takes place irrespective of whether the destination station is primary or secondary. **Secondary nodes** are the terminals that follow the commands of a primary node. Primary node decides which secondary node is allowed to use the channel and transmit at a particular time. Polling involves two operations, namely, *poll* and *select.*

- **Poll:** When the primary node is ready to receive data, it polls or asks all the secondary nodes in a round-robin fashion to determine if they have any data to transmit. The primary node sends a message to a secondary node by specifying the maximum number of frames the secondary node can send. The secondary node can respond with either negative acknowledgement (NAK) or positive acknowledgement (ACK). If the response is NAK, the primary node polls the next secondary node. This process goes on in a cyclic manner until any secondary node responds with an ACK. Once a positive response is received, the primary node also responds with an ACK to confirm the receipt
- **Select:** This operation is performed when primary node has some data to transmit. Before sending the data, it alerts the receiving secondary node about the transmission and does not transmit until it gets a ready acknowledgement from the receiving secondary node.

An advantage of polling is that it eliminates collision and results in better efficienc . However, it suffers from some limitations too. First, this protocol requires large amount of time in notifying secondary nodes and thus, introduces large amount of delay. Second, if the primary node fails, the entire network goes down.

Token Passing

In this method, all stations in the network are arranged in a logical ring manner (Figure 8.11). To allow stations to access the channel, a special packet known as **token** is circulated among the stations throughout the ring in a fixed order. Whenever a station receives the token from its predecessor and it has some data to send, it keeps the token with itself and transmits the data. After transmitting the data, it releases the token and passes it to its successor in the ring. In case a station receives the token but has no data to send, it immediately passes the token to its successor in the ring.

In this method, a priority can be assigned to each station in the ring such that whenever a high priority station wants to transmit, a low priority station has to release the token. In addition, type of data being transmitted from the stations can also be prioritized.

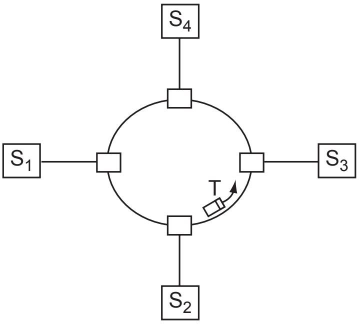


Figure 8.11 Token Passing

An advantage of token-passing method over polling is that there is no primary node present in the network, so this method is decentralized. However, it also suffers from some limitations. First, if any station goes down then entire network goes down. Second, if some problem such as failure of a station possessing the token occurs then token will vanish from the network.

15. What is the advantage of token-passing protocol over CSMA/CD protocol?

Ans: In CSMA/CD, a frame may be delivered at the destination either after many collisions or not delivered at all. Thus, CSMA/CD is not suitable for real-time applications. On the other hand, in token passing, a frame is delivered within the time. Also, the frames can be assigned priorities. This makes token passing suitable for real-time applications.

16. What is meant by the term channelization? Explain in detail various channelization protocols.

Ans: **Channelization** refers to a multiple-access method in which the bandwidth of a communication link is partitioned in time, frequency or using code among the stations that want to transmit data. Three channelization protocols, namely, *FDMA*, *TDMA* and *CDMA* are discussed as follows:

- **Frequency Division Multiple Access (FDMA):** This method involves partitioning the bandwidth of a channel into parts called **frequency bands**. Each frequency band is allocated to a particular station for transmitting its data and it remains fixed throughout the entire communication period. The frequency bands are kept well separated by placing guard bands in between to avoid the station interference. In case of higher load on the network, the performance of FDMA can be improved by allocating the frequency bands to the stations dynamically when they demand rather than keeping the frequency bands reserved for stations.

- ❑ **Time Division Multiple Access (TDMA):** In this method, the bandwidth of channel is time shared among the stations. The entire time is partitioned into slots and each slot is allocated to a particular station in which it can transmit data. The major limitation of TDMA is that synchronization is required between different stations so that every station could know the beginning as well as position of its respective slot. To achieve synchronization, **preamble bits** also known as **synchronization bits** are inserted at the start of each time slot.
- ❑ **Code Division Multiple Access (CDMA):** This method allows all the stations to send data through the same channel and at the same time. As compared to FDMA, in CDMA, the whole bandwidth of a link can be utilized by only one channel. Further, CDMA is also different from TDMA in the sense that in CDMA, all stations can transmit the data at the same time. All transmissions are separated using coding theory. Each station is assigned a code—a sequence of numbers called **chips**. These sequences are called **orthogonal sequences** and possess the following properties.
  - Each sequence contains a number of elements equal to the number of stations. For example, `(+1 -1 -1 +1)` is a sequence with four elements. Here, `-1` denotes the 0 bit while `+1` denotes the bit 1.
  - When a sequence is multiplied with a scalar quantity, every element of the sequence is multiplied with it. For example, on multiplying the sequence `(-1 -1 +1 +1 -1 -1)` with 5, we get `(-5 -5 +5 +5 -5 -5)`.
  - On multiplying two equal sequences, element by element with each other, and further adding the elements of resulting sequence, the final result obtained is equal to the number of elements in each sequence. This is also known as **inner product of two sequences**. For example, when `(-1 -1 +1 +1 -1 -1 +1 +1)` is multiplied with `(-1 -1 +1 +1 -1 -1 +1 +1)`, the resulting sequence is `(+1 +1 +1 +1 +1 +1 +1 +1)` whose sum of element is 8, equal to the number of elements in the sequence.
  - On multiplying two different sequences, element by element with each other, and then adding the elements of resulting sequence, the final result obtained is zero. This is called the **inner product of two different sequences**. For example when `(-1 -1 +1 +1 -1 -1 +1 +1)` is multiplied with `(+1 +1 +1 +1 +1 +1 +1 +1)`, the resulting sequence is `(-1 -1 +1 +1 -1 -1 +1 +1)` whose sum of elements is zero.
  - When two sequences are added, the corresponding elements of both sequences are added to each other. For example, on adding a sequence `(-1 -1 +1 +1 -1 -1 +1 +1)` with `(-1 -1 +1 +1 -1 -1 -1 -1)`, the resulting sequence is `(-2 -2 +2 +2 -2 -2 0 0)`.

To understand how CDMA works, consider four stations S_1, S_2, S_3 and S_4 with data d_1, d_2, d_3 and d_4 and codes c_1, c_2, c_3 and c_4, respectively. Each station multiplies its data by its code to get c_1*d_1, c_2*d_2, c_3*d_3 and c_4*d_4, respectively. The data that is sent to the channel is the sum of c_1*d_1, c_2*d_2, c_3*d_3 and c_4*d_4. Any station (say S_4) that wants to receive data from another station (say S_2) multiplies the data on the channel with the code of the sender (in our case c_2) to get the data as shown here

$$\begin{aligned}\text{Data} &= (c_1*d_1+c_2*d_2+c_3*d_3+c_4*d_4)*c_2\\ &= 4*d_2\end{aligned}$$

It is clear from the second and third property that `c2*c2` will result in four while other products `c1*c2`, `c3*c2` and `c4*c2` will result in zero. Thus, in order to receive data from `S2` (which is `d2`), the station `S4` has to divide the result by four.

Further, CDMA is widely used for cellular networks. The main advantage of CDMA is that it uses a larger bandwidth, so transmission of data is less affected by the transmission impairments. However, the limitation of CDMA is self-jamming and distance.

17. How FDM differs from FDMA?

Ans: Although FDM and FDMA employ the same concept, there are differences between the two. The FDM is a physical layer technique, which involves using a multiplexer to combine traffic from low bandwidth channels and transmitting them on a higher bandwidth channel. In this technique, channels are statically allocated to different stations, which is inefficie t in case of bursty traffic. In contrast, FDMA is an access method in the data link layer in which channels can be allocated on demand. In FDMA, the bandwidth is divided into frequency bands and each band is reserved for a specific station. The efficiency is improved in FDMA by using a dynamic-sharing technique to access a particular frequency band. No physical multiplexer is used at the physical layer in FDMA.

18. How TDM differs from TDMA?

Ans: TDM and TDMA have certain differences. The TDM is a physical layer technique, which uses a physical multiplexer to render data from slower channel, combine them and transmit using faster channel, whereas TDMA is a multiple-access method in the data link layer where the data link layer of each station tells the physical layer to use the specific slot allocated for it. No physical multiplexer is used at the physical layer in TDMA.

19. A slotted ALOHA channel has an average 10% of the slots idle. What is the offered traffic G? Calculate the throughput and determine whether the channel is overloaded or under loaded?

Ans: According to Poisson's distribution

$$P_0 = e^{-G}$$

$$\text{Also, } G = -\ln P_0$$

$$= -\ln 0.1$$

$$= 2.3$$

As we know that, throughput (S) of slotted ALOHA = Ge^{-G}

$$S = 2.3 \times 0.1 = 0.23$$

As $G > 1$, the channel is overloaded.

20. Consider a slotted ALOHA having fiv stations. If the offered load $G_1 = 0.1$, $G_2 = 0.15$, $G_3 = 0.2$, $G_4 = 0.25$ and $G_5 = 0.3$ packets, fin the individual throughput of each station and channel throughput.

Ans: In slotted ALOHA, individual throughput, $S_i = G_i\, e^{-G_i}$

Let the individual throughput of each station be S_1, S_2, S_3, S_4 and S_5.

Then,

$$S_1 = G_1 e^{-G_1} = 0.1e^{-0.1} = 0.0905$$
$$S_2 = G_2 e^{-G_2} = 0.15e^{-0.15} = 0.1291$$
$$S_3 = G_3 e^{-G_3} = 0.2e^{-0.2} = 0.1637$$
$$S_4 = G_4 e^{-G_4} = 0.25e^{-0.25} = 0.1947$$
$$S_5 = G_5 e^{-G_5} = 0.3e^{-0.3} = 0.2222$$

Thus, total channel throughput (S) can be determined as

$$\begin{aligned} S &= S_1 + S_2 + S_3 + S_4 + S_5 \\ &= 0.0905 + 0.1291 + 0.1637 + 0.1947 + 0.2222 \\ &= 0.8002 \end{aligned}$$

21. Consider a CSMA/CD LAN running at 1 Gbps over a 1 km long cable with no repeaters. The signal propagation speed is 200 m/µs. What is the minimum frame size?

Ans: Frame transmission time = 2 × propagation time

Here, propagation time = distance/propagation speed

That is, propagation time = 1000/200 = 1000/2 = 5 µs

So, frame transmission time = 2 × 5 = 10 µs

The minimum size of the frame is given as

$$\begin{aligned} &\text{data rate} \times \text{frame transmission time} \\ &= 1 \text{ Gbps} \times 10\ \mu\text{s} \\ &= 1 \times 10^9 \times 10 \times 10^{-6} \\ &= 10{,}000 \text{ bits} = 1{,}250 \text{ bytes} \end{aligned}$$

22. A 4 Mbps token ring has a token holding timer value of 10 ms. What is the longest frame that can be sent on this ring?

Ans: Here, token holding time = 10 ms

Thus, the longest frame that can be sent on this ring = data rate × token holding time

$$\begin{aligned} &= 4 \times 10^6 \times 10 \times 10^{-3} \\ &= 40 \times 10^3 \text{ bits} = 40{,}000 \text{ bits} \\ &= 5 \text{ KB (as 1 byte = 8 bits)} \end{aligned}$$

Multiple choice questions

1. In which of the following protocols, a station sends a frame whenever it wants?
   (a) pure ALOHA (b) slotted ALOHA
   (c) both (a) and (b) (d) none of these

2. In which of the following protocols, the station senses the channel before trying to use it?
   (a) ALOHA (b) CSMA
   (c) CDMA (d) none of these

3. The throughput of pure ALOHA is expressed as:
   (a) $S = Ge - 2G$ (b) $S = Ge - G$
   (c) $S = 2Ge - 2G$ (d) $S = 2Ge-^{G}$

4. Which of the following is true with reference to 1-persistent CSMA?
   (a) If the line is not idle, it continuously senses the line until it finds the line idle
   (b) If the line is not idle, it waits a random amount of time and then senses the line again.
   (c) If the station finds the line idle it sends or refrains from sending based on the outcome of a random number generator.
   (d) None of these

5. In which of the following methods, the stations refer each other to know which station has the right to transmit a frame?
   (a) random access
   (b) controlled access
   (c) channelization
   (d) none of these

6. Which of the following protocol involves division of time into intervals and at each interval reservation frame precedes the data frame?
   (a) reservation (b) polling
   (c) token passing (d) none of these

7. In which of the following methods, primary station controls the link?
   (a) reservation
   (b) polling
   (c) token passing
   (d) none of these

8. In which of the following methods, the stations are arranged in logical ring?
   (a) reservation (b) polling
   (c) token passing (d) none of these

9. Channelization involves:
   (a) FDMA (b) TDMA
   (c) CDMA (d) all of these

10. Which of the following is based on coding theory?
    (a) FDMA (b) TDMA
    (c) CDMA (d) none of these

Answers

1. (a) 2. (b) 3. (a) 4. (a) 5. (b) 6. (a) 7. (b) 8. (c) 9. (d) 10. (c)

9

Ethernet, Virtual Circuit Networks and SONET

1. Write a short note on IEEE 802 standards.

Ans: IEEE 802 standards were developed by IEEE in 1985 for local area networks (LANs). These standards are compatible with each other at data link layer and enable intercommunication between various devices developed by different manufacturers. These standards are classified into the following categories:

- ❑ **IEEE 802.1:** This category defines interface primitives for LAN. It deals with internetworking aspect, which seeks to settle down the conflicts between incompatible devices.
- ❑ **IEEE 802.2:** This category specifies the upper part of the data link layer and supports the logical link protocol.
- ❑ **IEEE 802.3:** This category supports Ethernet. Further, CSMA/CD protocol is used in the Ethernet to control simultaneous access to the channel by multiple media.
- ❑ **IEEE 802.4:** This category has been specified for LANs based on Token Bus architecture. It supports token passing access method and bus topology.
- ❑ **IEEE 802.5:** This category describes standards for LANs based on Token Ring. It supports token passing access method and ring topology.
- ❑ **IEEE 802.6:** This category is used for distributed queue dual bus (DQDB) architecture. It has been developed for usage in metropolitan area networks (MANs).
- ❑ **IEEE 802.11:** This category applies to wireless Ethernet or Bluetooth. Bluetooth is a technology that is used for small wireless LANs.

2. Explain IEEE 802 reference model.

Ans: IEEE 802 reference model was developed by IEEE and adopted by all the organizations for LAN standards. Initially, the American National Standards Institute (ANSI) adopted the standard and later in 1987, it was approved by the International Organization for Standards (ISO) as an international standard. The 802 reference model is related to the open systems interconnection (OSI) model as shown in Figure 9.1.

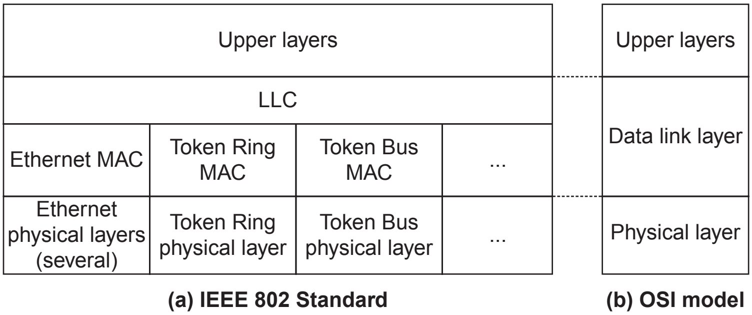


Figure 9.1 Relationship Between IEEE 802 Reference Model and OSI Model

Physical Layer

The lowest layer of IEEE 802 reference model is equivalent to the physical layer of the OSI model. It depends on the type and implementation of transmission media. It defines a specification for the medium of transmission and the topology. It deals with the following functions:

- encoding of signals at the sender's side and the decoding of signals at the receiver's side;
- transmission and reception of bits and
- preamble generation for synchronization.

Data Link Layer

The layer above the physical layer in the 802 reference model corresponds to the data link layer of the OSI model. Here, the data link layer is divided into two layers, namely, *logical link control* (*LLC*) and *media access control* (*MAC*).

- **LLC:** This layer is the upper part of the data link layer that provides an interface to upper layers and performs functions such as flow control and error control. It also performs a part of framing function. It provides single data link protocol for all IEEE LANs. In addition, it must support multi-access channels and multiple user networks.

  The LLC layer is concerned with the transmission of link-level protocol data unit (PDU) that is identical to high-level data link control (HDLC) and referred to as **LLC frame**. Each LLC frame consists of a header field followed by a data field. The header of LLC frame contains three subfields, namely, *destination service access point* (*DSAP*), *source service access point* (*SSAP*) and *control* (Figure 9.2) and the data field is used to hold data received from upper layers. The description of subfields in LLC frame header is as follows:

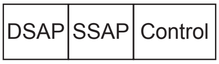


Figure 9.2 Format of LLC Frame Header

- **DSAP:** This field contains a 7-bit address that identifies a user of LLC at the destination. One bit of the address specifies whether it is a group or individual address. It specifies the upper-layer protocol at the destination.
- **SSAP:** This field contains a 7-bit address that identifies the user of LLC at the source. One bit of the address specifies whether it is a command or response PDU. It specifies the upper-layer protocol at the source.
- **Control Field:** This field is used to handle flow and error contro

- **MAC:** This layer forms the lower part of the data link layer that specifies the access control method used for each type of LAN. For example, CSMA/CD is specified for Ethernet LANs and the token passing method is specified for Token Ring and Token Bus LANs. It also handles a part of framing function for transmitting data. To implement all the specified functions, MAC also uses a PDU at its layer, which is referred to as **MAC frame**. The MAC frame consists of various fields (Figure 9.3) which are described as follows:
  - **MAC Control:** This field contains protocol control information such as priority level, which is required for the proper functioning of protocol.
  - **Destination MAC Address:** This field contains the address of the destination on the LAN for this frame.
  - **Source MAC Address:** This field contains the address of the source on the LAN for th s frame.
  - **LLC PDU:** This field contains the LLC data arriving from the immediate upper laye .
  - **Cyclic Redundancy Check (CRC):** This field contains the CRC code that is used for error detection. This field is also referred to as **frame check sequence** (**FCS**).

MAC control	Destination MAC address	Source MAC address	LLC PDU	CRC

Figure 9.3 Format of an MAC Frame

3. **Discuss frame format of IEEE 802.3 standards.**

Ans: IEEE 802.3 standard supports Ethernet which was developed in 1976 by Xerox Corporation. It was developed as an improvement over prior networks and is capable of controlling access to channel in case many stations attempt to transmit simultaneously. To control media access, it uses 1-persistent CSMA/CD protocol.

In standard Ethernet, the MAC layer is responsible for performing the operation of access method. Further, IEEE 802.3 has specified a type of an MAC frame for Ethernets. This frame consists of seven fields (Figure 9.4), which are described as follows

- **Preamble:** It is the first field of the Ethernet frame. It contains 7 bytes of alternating 0s and 1s such as 1010101 that are used to warn the receiver about the incoming frame so that the receiver may synchronize its timing with the input. In fact, this field is appended at the physical layer and is not a part of the frame.
- **Start Frame Delimiter (SFD):** It is a 1-byte long field that is used to determine the beginning of the frame. The last two bits of this field are set to 11 to indicate the receiver that the next field is destination address; also, it is the last chance for the receiver to synchronize its input timing.
- **Destination Address (DA):** It is a 6-byte long field that holds the physical address of the next receiving station(s) to which the frame is to be transmitted.
- **Source Address (SA):** It is a 6-byte long field that holds the physical address of the station that has sent the frame.

Preamble 7 bytes	SFD 1 byte	Destination address 6 bytes	Source address 6 bytes	Length or type 2 bytes	Data and padding 46-1500 bytes	CRC 4 bytes

Figure 9.4 Format of IEEE 802.3 MAC Frame

- **Length or Type:** It is a 2-byte-long field that defines either the length or type of data. The Ethernet originally used this field as a type field to define the total length of data in upper-layer protocols, while the IEEE standard used it as the length field to indicate total number of bytes in data field
- **Data:** This field carries data arriving from upper-layer protocols. The amount of data stored in this field can range between 46 and 1,500 bytes
- **CRC:** It is a 4-byte-long field that contains error detection information. In case of Ethernet MAC frame, it is the CRC that is computed over all the fields except preamble, SFD and CRC itself.

4. What are the four generations of Ethernet? Discuss Ethernet cabling in all the generations of Ethernet.

Ans: The Ethernet was developed in 1976 at the Xerox's Palo Alto Research Center (PARC). Since its development, the Ethernet has been evolving continuously. This evolution of Ethernet can be categorized under four generations, which include standard Ethernet, fast Ethernet, gigabit Ethernet and 10-gigabit Ethernet. These generations are discussed here.

Standard Ethernet

Standard Ethernet uses digital signals (baseband) at the data rate of 10 Mbps and follows 1-persistent CSMA/CD as access method. A digital signal is encoded/decoded by sender/receiver using the Manchester scheme. Standard Ethernet has defined several physical layer implementations, out of which the following four are commonly used.

- **10Base5:** It uses a thick coaxial cable of 50 ohm and is implemented in bus topology with an external transceiver connected to coaxial cable. The transceiver deals with transmitting, receiving and detecting collisions in the network. The cable used is too firm to bend with the hands. The maximum length of the cable should not be more than 500 m; otherwise, the signals may deteriorate. In case greater length of cable is required, the maximum five segments each of 500 m can be used and repeaters are used to connect the segments. Thus, the length of the cable can be extended up to 2,500 m. The 10Base5 Ethernet is also referred to by other names including **thick Ethernet** or **thicknet**.
- **10Base2:** It is also implemented in the bus topology but with a thinner coaxial cable. The transceiver in this Ethernet is a part of the NIC. The 10Base2 specification are cheaper than the 10Base5 as the cost of thin cable is less than that of the 10Base5 specifications. The thinner cable can easily be bent close to the nodes that results in flexibility and thus, making installation of the 10Base2 specification easier. The maximum length of the cable segment must not exceed 185 m. The 10Base2 Ethernet is also referred to as **thin Ethernet** or **Cheapernet**.
- **10Base-T:** It uses two pairs of twisted cable and is implemented in star topology. All nodes are connected to the hub via two pairs of cable and thus, creating a separate path for sending and receiving the data. The maximum length of the cable should not exceed 100 m; otherwise, the signals may attenuate. It is also referred to as **twisted-pair Ethernet**.
- **10Base-F:** It is the most common 10-Mbps Ethernet that is implemented in star topology. It uses a pair of fibre optic cables to connect the nodes to the central hub. The maximum length of cable should not exceed 2,000 m. It is also referred to as the **fib e Ethernet**.

Fast Ethernet

The IEEE 802.3 committee developed a set of specifications referred to as the fast Ethernet to provide low-cost data transfer at the rate of 100 Mbps. It was designed to compete with LAN protocols such as fibre distributed data interface (FDDI) and it was also compatible with the standard Ethernet. The fast Ethernet uses a new feature called **autonegotiation**, which enables two devices to negotiate on certain features such as data rate or mode of transmission. It also allows a station to determine the capability of hub and two incompatible devices can also be connected to one another using this feature. Like the standard Ethernet, various physical-layer implementations of the fast Ethernet have also been specified. Some of them are as follows:

- **100Base-TX:** It either uses two pairs of either cat5 UTP cable or STP cable. The maximum length of the cable should not exceed 100 m. This implementation uses MLT-3 line coding scheme due to its high bandwidth. However, since MLT-3 coding scheme is not self-synchronized, the 4B/5B block coding scheme is used to prevent long sequences of 0s and 1s. The block coding increases the data rate from 100 Mbps to 125 Mbps.
- **100Base-FX:** It uses two wires of fibre optic cable that can easily satisfy the high bandwidth requirements. The implementation uses NRZ-I coding scheme. As NRZ-I scheme suffers from synchronization problem in case of long sequence of 0s and 1s, 4B/5B block coding is used with NRZ-I to overcome this problem. The block coding results in increased data rate of 125 Mbps. The maximum cable length in 100Base-FX must not exceed 100 m.
- **100Base-T4:** It is the new standard that uses four pairs of cat3 or higher UTP cables. For this implementation, 8B/6T line coding scheme is used. The maximum length of cable must not exceed 100 m.

Gigabit Ethernet

Gigabit Ethernet was developed by the IEEE 802.3 committee to meet the higher data rate requirements. This standard provides a data rate of 1000 Mbps (1 Gbps). It is backward compatible with traditional and fast Ethernet and also supports autonegotiation feature. Various physical layer implementations of gigabit Ethernet are as follows:

- **1000Base-SX:** It is a two-wire implementation that uses short wave fibres. One wire is used for sending the data and other is used for receiving the data. The NRZ line coding scheme and 8B/10B block coding scheme is used for this implementation. The length of the cable should not exceed 550 m in the 1000Base-SX specifications
- **1000 Base-LX:** It is also a two-wire implementation that uses long wave fibres. One wire is used for sending the data and other is used for receiving the data. It is implemented by the NRZ line coding scheme and the 8B/10B block-coding scheme. The length of the cable should not exceed 5,000 m in the 1000Base-LX specifications
- **1000 Base-CX:** It uses two STP wires where one wire is used for sending the data and other is used for receiving the data. It is implemented by the NRZ line coding scheme and the 8B/10B block-coding scheme. The length of the cable should not exceed 25 m in the 1000Base-CX specifications
- **1000 Base-T:** It uses four cat5 UTP wires. It is implemented by the 4D-PAM5 line coding scheme. In this specification, the length of the cable should not exceed 100 m

Ten-Gigabit Ethernet

This standard was named as 802.3ae by the IEEE 802.3 committee. It was designed to increase the data rate to 1000 Mbps (10 Gbps). It is compatible with standard Ethernet, fast Ethernet and gigabit Ethernet. It enables the Ethernet to be used with technologies such as Frame Relay and ATM. Various physical-layer implementations of 10-gigabit Ethernet are as follows:

- **10GBase-S:** It uses short-waves fibres and is designed for 850 nm transmission on multimode fibre. The maximum length of the cable should not exceed 300 m.
- **10GBase-L:** It uses long-wave fibres and is designed for 1,310 nm transmission on single-mode fibre. The maximum length of the cable should not exceed 10 km.
- **10GBase-E:** It uses extended waves and is designed for 1,550 nm transmission on single-mode fibre. The maximum distance that can be achieved using this medium, is up to 40 km.

5. What is Token Ring (IEEE 802.5)? How is it different from Token Bus (IEEE 802.4)?

Ans: The IEEE 802.5 is a specification of standards for LANs that are based on Token Ring architecture. The Token Ring network was originally developed by IBM in the 1970s. It is the most commonly used MAC protocol that uses token passing mechanism with ring topology. In this protocol, the stations are connected via point-to-point links with the use of repeaters (Figure 9.5). To control the media access, a small frame called **token** (a 3-byte pattern of 0s and 1s) is allowed to move around the network and the station possessing the token can only transmit frames in the allotted time.

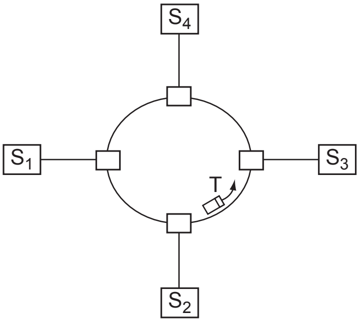


Figure 9.5 Token Ring LAN

Whenever a station wants to transmit a frame, it first needs to grab a token from the network before starting any transmission. Then, it appends the information with the token and sends it on the network. The information frame then circulates around the network and eventually, received by the intended destination. After receiving the information frame, the destination copies the information and sends the information frame back on the network with its two bits set to indicate that it is an acknowledgement. The information frame then moves around the ring and is finall , received by the sending station. The sending station checks the returned frame to determine whether it has been received with or without errors. If the sending station has now finished the transmission, it creates a new token and inserts it on the network. Notice that while one station is transmitting the data, no other station can grab a token. Thus, collisions cannot occur as only one station can transmit at a time. In addition, if a station does not have a frame to send or the time allotted to it passes away, the token is immediately passed to the next station.

In Token Ring networks, the ring topology is used in which the failure of any one station can bring the entire network down. Thus, another standard known as **Token Bus** (IEEE 802.4) was developed as an improvement over Token Ring networks. Like Token Ring, Token Bus is also based on token-passing mechanism. In Token Bus, the stations are logically organized into a ring but physically organized into a bus (Figure 9.6). Thus, each station knows the addresses of its adjacent (left and right) stations. After the logical ring has been initialized, the highest numbered station may transmit. The sending station broadcasts the frame in the network. Each station in the network receives the frame and discards if frame is not addressed to it. When a station finishes the transmission of data or the time allotted to it passes away, it inserts the address of its next neighbouring station (whether logical or physical) on the token and passes it to that station.

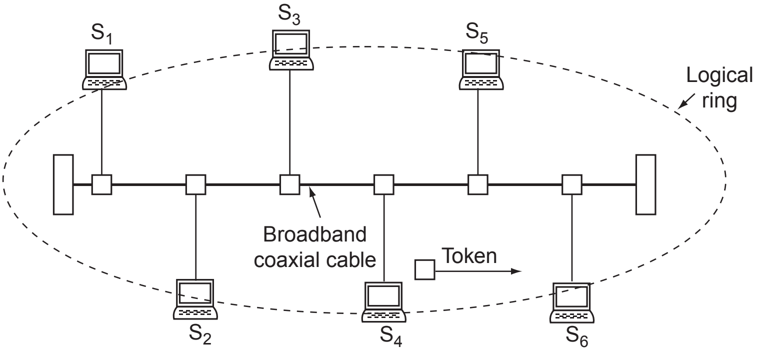


Figure 9.6 Token Bus LAN

6. **Compare IEEE 802.3, 802.4 and 802.5.**

Ans: There are certain differences among the IEEE 802.3, 802.4 and 802.5 standards that are listed in Table 9.1.

Table 9.1 Comparison among IEEE 802.3, 802.4 and 802.5

IEEE 802.3	IEEE 802.4	IEEE 802.5
• This standard uses 1- persistent CSMA/CD medium access protocol.	• This standard uses Token Bus medium access protocol.	• This standard uses Token Ring medium access protocol.
• The stations are logically connected to each other via a broadcast cable medium.	• The stations are logically connected to each other via a broadcast cable medium.	• The stations are physically connected to each other via point-to-point links.
• Frames are broadcasted to the destination.	• Frames are broadcasted to the destination.	• Frames are transmitted to the destination using point-to-point links.
• Transmission media used is generally coaxial cable, optical fibre or twisted pair.	• Transmission medium used is generally coaxial cable or twisted pair. It is not well suited to fibre cables.	• Transmission medium used is generally coaxial cable, optical fibre or twisted pair.
• There is no prioritization of stations for transmission of data.	• Stations are prioritized for transmission of data.	• Stations are prioritized for transmission of data.
• It cannot transmit short frames.	• It can handle transmission of short frames.	• It can handle transmission of short frames.
• It cannot be used for real-time applications.	• It is used for real-time applications.	• It is used for office automation.
• It applies Manchester encoding.	• It applies analog encoding.	• It applies differential Manchester encoding.
• At high loads, its efficiency is very low. However, at low loads, its efficiency is high due to less delay.	• At high loads, its efficiency is very high. However, at low loads, its efficiency is low due to more delay.	• At high loads, its efficiency is also high and at low loads, its efficiency is low similar to the Token Bus.

7. Write a short note on FDDI. Explain access method, time registers, timers and station procedure.

Ans: The **fib e distributed data interface** (**FDDI**) refers to the first high speed LAN protocol standardized by ANSI and ITU-T. It has also been approved by the ISO and resembles IEEE 802.5 standards. It uses fibre optic cable; thus, packet size, network segment length and number of stations increase. It offers a speed of 100 Mbps over the distance of up to 200 km and connects up to 1,000 stations. The distance between any two stations cannot be more than a few kilometers.

Access Method

The FDDI employs the token passing access method. A station possessing the token can transmit any number of frames within the allotted time. There are two types of frames provided by the FDDI: *synchronous* and *asynchronous*. **Synchronous frame** (also called **S-frame**) is used for real-time applications such as audio and video. The frame needs to be transmitted within a short period of time without much delay. **Asynchronous frame** (also called **A-frame**) is used for non-real-time applications (such as data traffic) that can tolerate large delays. If a station has both S-frames and A-frames to send, it must send S-frames first. After sending the S-frame, if the allotted time is still left then A-frames can be transmitted.

Time Registers

Three time registers are used to manage the movement of token around the ring, namely, *synchronous allocation* (*SA*), *target token rotation time* (*TTRT*) and *absolute maximum time* (*AMT*). The **SA** register specifies the time for transmitting synchronous data. Each station can have a different value for it. The **TTRT** register specifies the average time a token needs to move around the ring exactly once. The **AMT** register has a value two times the value of the TTRT. It specifies the maximum time that it can take for a station to receive a token. However, if a token takes more time than the AMT, then the reinitialization of the ring has to be done.

Timers

Each station maintains two types of timers to compare the actual time with the value present in time registers. These timers include *token rotation timer* (*TRT*) and *token holding timer* (*THT*). The **TRT** calculates the total time taken by the token to complete one cycle. This timer runs continuously. The **THT** starts when the token is received by a station. This timer indicates the time left for sending A-frames after the S-frames have been sent.

Station Procedure

When a station receives the token, it uses the following procedure:

1. It sets the THT to a value equal to (TTRT – TRT).
2. It sets TRT to zero.
3. It transmits synchronous frame. With each sent unit, the value of TRT is decremented by one.
4. It continues to send asynchronous data as long as the value of THT is positive.

8. What are the advantages of FDDI over a basic Token Ring?

Ans: Though FDDI, like Token Ring, is a token-passing protocol, it provides certain advantages over Token Ring. Some of these advantages are as follows:

- ❑ It provides a data rate of 100 Mbps as compared to the 10–16 Mbps in Token Ring.
- ❑ It supports large number of stations as compared to Token Ring.
- ❑ The access method used in FDDI is timed-token passing. It supports transmission of multiple frames at the same time after capturing a token that is not possible in Token Ring.
- ❑ In case of Token Ring, the transmitting station releases the token after it receives the acknowledgement of sent frames. On the other hand, in FDDI the station releases the token immediately after it has finished the transmission. This is known as **early token release**.
- ❑ It offers higher reliability than Token Ring by using dual counter ring topology. In this, two types of rings are used, namely, *primary* and *secondary* in contrast to Token Ring in which only one ring is present. Both rings are used to transmit data, however, in opposite directions to provide fault tolerance. Thus, in case one ring breaks or some station malfunctions, the load can be shifted to another ring. Moreover, if both rings break at the same point, two rings can be joined together to form a single ring. Reliability can be further increased by using **dual ring of trees** or **dual homing** that provides multiple paths. Thus, on failure of one path, another path can be chosen for passing a token or data.

9. What is meant by wireless LAN? Mention its advantages and disadvantages.

Ans: **Wireless LAN** (**WLAN**) refers to a network that uses wireless transmission medium. It is used to connect devices without using cables and introduces a higher flexibility for ad hoc communication. Some of the advantages of wireless LAN are as follows:

- ❑ It is difficult to design small-size devices such as PDA and laptop with the use of cables and thus, WLAN becomes an alternative to be used as a transmission media.
- ❑ In case of natural disasters, such as flood and earthquake, noise in the cable increases. Therefore, WLAN can be used where transmission rate is not affected by such natural calamities.
- ❑ It can cover large area and number of devices. In addition, new devices can be added easily without affecting the existing network design.
- ❑ The nodes can communicate without any restriction and from anywhere.

Some disadvantages of WLAN are as follows:

- ❑ It is an expensive medium of transmission as compared to cables. Certain wireless devices such as wireless LAN adaptor and PC card are quite expensive.
- ❑ Installation of WLANs is expensive.
- ❑ Radio waves used in WLAN might interfere with various devices and thus, are not secure to use.
- ❑ WLANs provide low quality of transmission because of high error rate due to interference.
- ❑ WLANs are restricted to only certain frequency bands in radio transmission.

10. Differentiate between wired and wireless LAN.

Ans: Both wired and wireless LANs are used for establishing a network within an organization but there are some differences between them. Table 9.2 lists these differences.

Table 9.2 Differences Between Wired and Wireless LAN

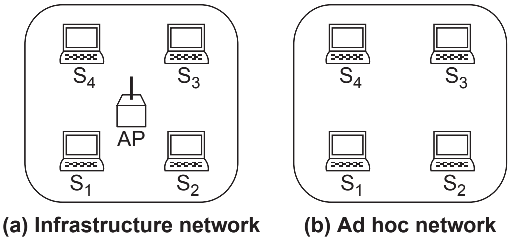
Wired LAN	Wireless LAN
• It is difficult to set up wired LANs, as it requires long and large number of wires to connect devices to each other or to the central device such as hub or switch.	• It is easier to set up WLANs as compared to wired LANs.
• The total cost required to set up these type of networks include cost of cable, hubs, switches and various software packages to install the network.	• Wireless adapters and access points are three to four times expensive as compared to components of wired LAN.
• It is more secure because firewalls can be installed on the computers.	• It is less secure because radio waves travel through air and can be easily intercepted.
• The components used in wired LANs including Ethernet cable, hub and switch are extremely reliable.	• It is less reliable as signals are easily interfered from home appliances, causing more problems.
• Wired LANs provide less flexibility, as one need to separate printers, modems and scanners on every computer.	• The use of WLANs provides flexibility as it is not required to separate CD-ROMs, colour printers and B/W printers.

11. Explain two types of services of IEEE 802.11.

Ans: The IEEE 802.11 is a standard specified for wireless LANs. Two types of services namely, *basic service set* (*BSS*) and *extended service set* (*ESS*) has been defined for IEEE 802.11. These two services are explained as follows:

Basic Service Set

The BSS acts as the main building block of a WLAN. It consists of many wireless stations (stationary or mobile) and an optional base station called **access point** (**AP**). If AP is present in the network, then BSS is referred to as the **infrastructure network** [Figure 9.7(a)]; otherwise, BSS is referred to as an **adhoc network** [Figure 9.7(b)], which cannot transmit data to any other BSS.



(a) Infrastructure network (b) Ad hoc network

Figure 9.7 Basic Service Set (BSS)

Extended Service Set

The ESS is formed by the combination of at least two BSSs with APs (Figure 9.8). All BSSs are connected via a **distribution system** that is generally a wired LAN such as Ethernet. The distribution system connects the APs of each BSS to one another and thus, enables the communication between BSSs. Each BSS can have two types of stations: *mobile* and *stationary*. The stations inside the BSS are mobile stations while AP of each BSS is a stationary station. The stations inside a BSS can communicate with one another without requiring the use of an AP. However, if communication is required between two stations of different BSSs, then it occurs via APs. The ESS is analogous to a cellular network in which each cell can be considered as a BSS and each base station as an AP.

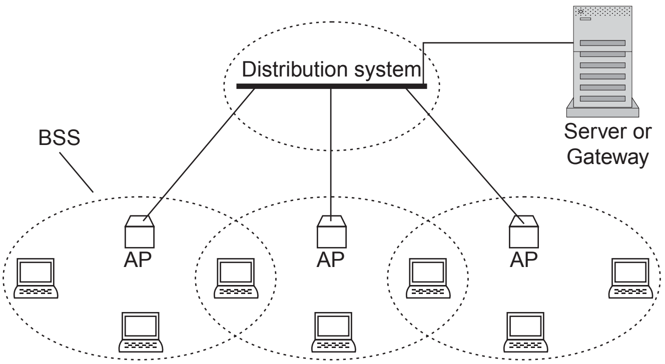


Figure 9.8 Extended Service Set (ESS)

12. **What are the types of frames specifie in IEEE 802.11?**

Ans: The IEEE 802.11 has specified three types of MAC frames for WLANs, which include *management frames*, *control frames* and *data frames*. All these three types are discussed as follows:

- ❑ **Management Frame:** This frame is used for managing communication between stations and APs. It manages request, response, reassociation, dissociation and authentication.
- ❑ **Control Frame:** This frame is used for accessing the channel and acknowledging frames. It ensures reliable delivery of data frames. There are six subtypes of a control frame which are as follows:
  - **Power Save-Poll (PS-Poll):** This frame is used by a station to send a request to an AP for the transmission of frames buffered by AP for that station while the station was in power saving mode.
  - **Request to Send (RTS):** Whenever a station wishes to send data to another station, it first sends an RTS frame to declare to the destination and other stations within its reception range that it is going to send data to that destination.
  - **Clear to Send (CTS):** This frame is sent by a station in response to an RTS frame. It indicates to the source station that the destination station has granted permission for sending data frames.
  - **Acknowledgement:** This frame is sent by the destination station to the source station to acknowledge the successful receipt of the previous frames.
  - **Contention-Free (CF)-end:** This frame is used to indicate the end of the contention-free period.
  - **CF-End + ACK:** This frame is used to acknowledge the CF-end frame. It ends the period and all the bound stations are freed from all the restrictions associated with that period.
- ❑ **Data Frame:** This frame is used for carrying data and control information from a source station to a destination station. Data frames are divided into eight subtypes, which are further organized under two groups. One group contains the data frames that are used to carry the user data (received from upper layers) from the source station to the destination station. The data frames included in this group are described as follows:
  - **Data:** This is the simplest data frame used to send data in both contention period and contention-free period.
  - **Data + CF-ACK:** This frame carries data and also acknowledges the data, which has been received previously. It can be used only in the contention-free period.

- **Data + CF-Poll:** This frame is used by a point coordinator to send data to a mobile station. It also requests the mobile station to send a data frame, which may have been buffered by the mobile station.
- **Data + CF-ACK + CF-Poll:** This frame combines the functionality of two frames Data + CF-ACK and Data + CF-Poll into a single frame.

Besides, there is another group that contains four more subtypes of data frames, which do not carry any user data. One of these frames is **null-function** data frame that carries the power management bit in the frame control field to the AP. It indicates that the station is moving to a low-power operating state. The remaining three frames (CF-ACK, CF-Poll, CF-ACK + CF-Poll) function in the same way as that of last three frames in the first group, the only difference being that they do not contain any data.

13. Explain the frame format of 802.11 standards.

Ans: The IEEE 802.11 has defined three MAC layer frames for WLANs including control, data, and management frames. Figure 9.9 shows the format of data frame of IEEE 802.11 that comprises nine fields. The format of management frames is also similar to data frames except that it does not include one of the base station addresses. The format of control frames does not include frame body and SC fields. It also includes one or two address fields

The description of fields included in the IEEE 802. 1 MAC frame is as follows:

FC	D	Address 1	Address 2	Address 3	SC	Address 4	Frame body	FCS
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0-2312 bytes	4 bytes

Figure 9.9 Frame Format of the IEEE 802.11 Standard

- **Frame Control (FC):** It is a 2-byte-long field in which the first byte indicates the type of frame (control, management, or data) and the second byte contains control information such as fragmentation information and privacy information.
- **Duration (D):** It is a 2-byte-long field that defines the channel allocation period for the transmission of a frame. However, in case of one control frame, this field stores the ID of the frame.
- **Addresses:** The IEEE 802.11 MAC frame contains four address fields and each field is 6-byte-long. In case of a data frame, two of the frame address fields store the MAC address of the original source and destination of the frame, while the other two store the MAC address of transmitting and receiving base stations that are transmitting and receiving frames respectively over the WLAN.
- **Sequence Control (SC):** It is a 2-byte (that is 16 bits) field, of which 12 bits specify the sequence number of a frame for flow control. The remaining 4 bits specify the fragment number required for reassembling at the receiver's end.
- **Frame Body:** It is a field that ranges between 0 and 2,312 bytes and contains payload information.
- **FCS:** It is a 4-byte-long field that comprises a 32-bit CRC

14. With reference to 802.11 wireless LAN, explain the following:

(a) Hidden terminal problem
(b) Exposed terminal problem
(c) Collision avoidance mechanisms

Ans:

(a) Hidden Terminal Problem The hidden terminal problem occurs during communication between two stations in wireless networks. It is the problem where a station is unable to detect another station while both of them are competing for the same data transfer medium. To understand how this problem occurs, consider three stations `X`, `Y` and `Z` situated in a network as shown in Figure 9.10. The transmission range of station `X` is represented by the left oval and that of `Z` is represented by the right oval. The stations falling in either of the ovals can hear the signal transmitted by the station situated in that oval. However, stations `X` and `Z` are outside the transmission range of each other, that is, they are hidden from each other. As the station Y is situated in the area common to `X` and `Z`, it can hear the signals transmitted by both `X` and `Z`. Now, suppose, while `X` is transmitting data to `Y`, `Z` also wants to send data to `Y`. As `Z` is unable to hear the transmission from `X` to `Y`, it assumes that the transmission medium is free and starts sending data frames to `Y`. This results in a collision at station `Y`, as it is receiving from both `X` and `Z`, which are hidden from each other with respect to `Y`.

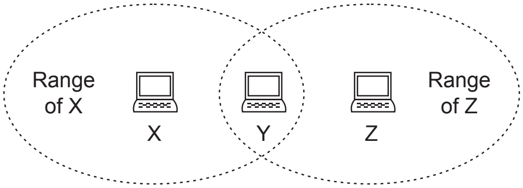


Figure 9.10 Hidden Terminal Problem

The hidden terminal problem can be solved by making use of the RTS and CTS frames before starting the transmission of data. Initially, station `X` sends an RTS frame to station `Y` to request for sending data. The transmission of RTS frame cannot be detected by `Z`. In response to RTS frame, station `Y` sends a CTS frame, which specifies the duration of transmission from `X` to `Y`. As `Y` in the transmission range of `Z`, `Z` can detect the transmission of CTS frame and knows that `Y` is busy with any other station and also for how long. Therefore, it does not initiate the transmission until that duration is finished.

(b) Exposed Terminal Problem This problem is the reverse of the hidden terminal problem. This problem arises when a station restricts itself from using another station that is in fact available for use. To understand how this problem occurs, consider four stations `P`, `Q`, `R` and `S` in a network as shown in Figure 9.11. Suppose that while the station `P` is sending data to station `Q`, there arises a need in station `R` to send data to `S`. The transmission from `R` to `S` can be done without disturbing the transmission from `P` to `Q`. However, as the station `R` is exposed to transmission range from `P`, it stops itself from transmitting to `S` after realizing that `P` is transmitting some data. Such a situation is known as exposed terminal problem.

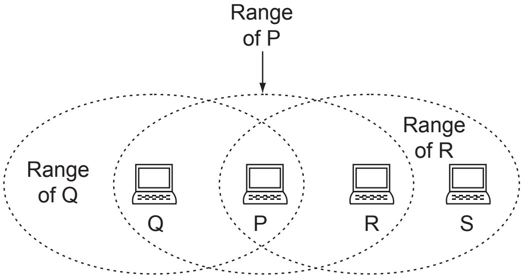


Figure 9.11 Exposed Terminal Problem

(c) Collision Avoidance Mechanisms To avoid the collisions in the wireless networks, a collision avoidance protocol named as multiple access with collision avoidance (MACA) has been designed. This protocol requires a sender to make the receiver send a short frame before starting the transmission of data frames. This frame is used as an announcement to the nearby frames that transmission is going on between sender and the receiver and no other station should interfere in between, thus, avoiding any collision.

To understand how MACA works, consider five stations `P`, `Q`, `R`, `S` and `T` as shown in Figure 9.12. Suppose `P` wants to send data to `Q`. Initially, `P` sends an RTS frame to `Q` specifying the length of the data frame. The station `Q` then responds with a CTS frame specifying the duration for transmission from `P` to `Q`. After receiving the CTS frame, `P` begins transmitting data to `Q`. Now, as the station `S` is in the transmission range of `Q`, it hears the CTS message from `Q` and thus, remains silent for the duration, `Q` is receiving from `P`. The station `R` is in the transmission range of `P` and hears the RTS message from `P` (but not the CTS message from `Q`). Thus, `R` can transmit to `P` without avoiding the collision as long as the data from R to P does not interfere with CTS from Q to P. The station T being in the transmission range of both P and Q hears RTS and CTS both and thus, remain silent until the transmission is over.

The disadvantage of the MACA protocol is that collision can still occur in case both Q and R transmit RTS frames to P simultaneously. The RTS from Q and R may collide at P; because of collision, neither Q nor R receives the CTS frame. Then both Q and R wait for a random amount of time using binary exponential back off algorithm (explained in Chapter 8) and again retry to transmit.

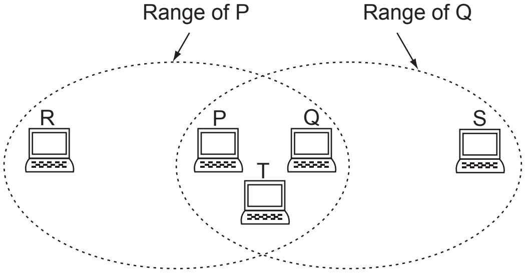


Figure 9.12 MACA Protocol

To overcome the disadvantage and improve the performance of MACA, it was enhanced in 1994 and renamed as **MACA for wireless** (**MACAW**). This newer version of MACA includes several enhancements, some of which are as follows:

- To identify the frames that have been lost during the transmission, the receiver must acknowledge each successfully received data frame by sending an ACK frame.
- CSMA protocol is used for carrier sensing so that no two stations could send an RTS frame at the same time to the same destination.
- Instead of running the binary back off exponential algorithm for each station, it is run for a pair of transmitting stations (source and destination).

15. What is meant by Bluetooth? Explain its architecture.

Ans: **Bluetooth** is a short-range wireless LAN technology through which many devices can be linked without using wires. It was originally started as a project by the Ericsson Company and then formalized by a consortium of companies (Ericsson, IBM, Intel, Nokia and Toshiba). Bluetooth is supposed to get its name from 10th century Danish king Harald Bluetooth who united Scandinavian Europe (Denmark and Norway) during an era when these areas were torn apart due to wars. The Bluetooth technology operates on the 2.4 GHz industrial, scientific and medical (ISM) band and can connect different devices such as computer, printer and telephone. The connections can be made up to 10 m or extended up to 100 m depending upon the Bluetooth version being used.

Bluetooth Architecture

A Bluetooth LAN is an ad hoc network, which means the network is formed by the devices themselves by detecting each other's presence. The number of devices connected in Bluetooth LAN should not be very large as it can support only a small number of devices. The Bluetooth LANs can be classified into two types of networks, namely, *piconet* and *scatternet* (Figure 9.13).

- **Piconet:** It refers to a small Bluetooth network in which the number of stations cannot exceed eight. It consists of only one primary station (known as **master**) and up to seven secondary stations (known as slaves). If number of secondary stations exceeds seven, then 8th secondary station is put in the **parked** state. A secondary station in the parked state cannot participate in communication in the network until it leaves the parked state. All stations within a piconet share the common channel (communication link) and only a master can establish the link. However, once a link has been established, the other stations (slaves) can also request to become master. Slaves within a piconet must also synchronize their internal clocks and frequency hops with that of the master.

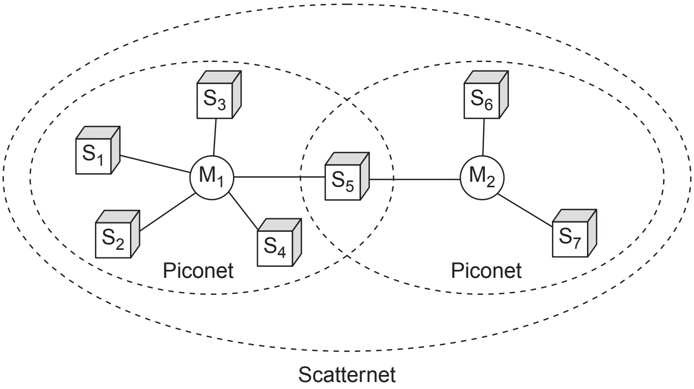


Figure 9.13 Bluetooth Piconets and Scatternets

- ❑ **Scatternet:** It refers to a Bluetooth network that is formed by the combination of piconets. A device may be a master in one piconet whiles a slave in another piconet or a slave in more than one piconet.

16. Discuss the Bluetooth protocol stack.

Ans: Bluetooth protocol stack is a combination of multiple protocols and layers (Figure 9.14). Bluetooth comprises several layers including radio layer, baseband layer, L2CAP layer and other upper layers. In addition, various protocols are also associated with Bluetooth protocol stack. The description of these layers and protocols is as follows:

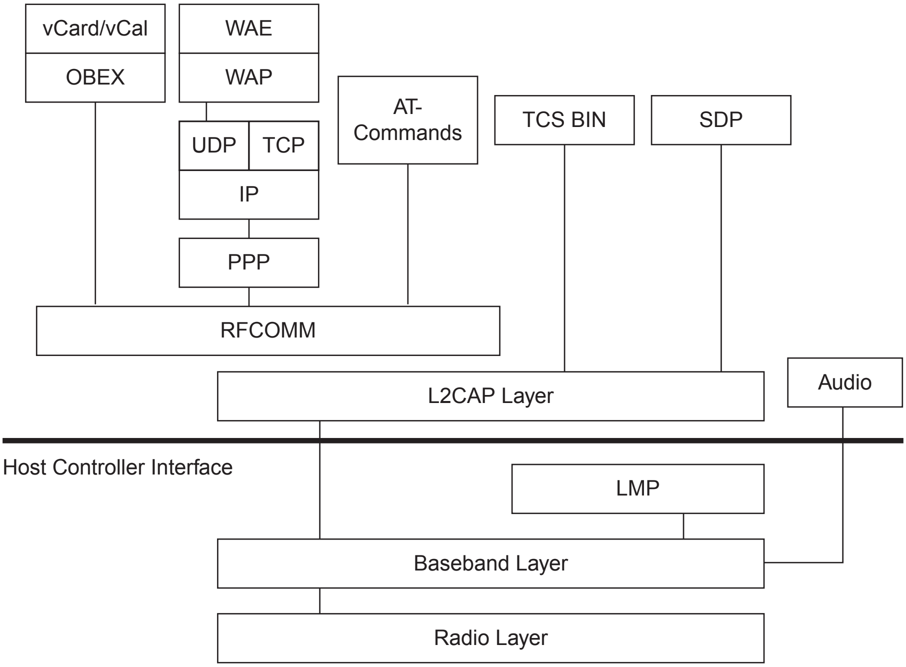


Figure 9.14 Bluetooth Protocol Stack

Radio Layer

This is the lowest layer in the Bluetooth protocol stack and is similar to a physical layer of transmission control protocol/Internet protocol (TCP/IP) model. The Bluetooth devices present in this layer have low power and a range of 10 m. This layer uses an ISM band of 2.4 GHz that is divided into 79 channels, each of 1 MHz. To avoid interference from other networks, the Bluetooth applies frequency-hopping spread spectrum (FHSS) technique. Here, a packet is divided into different parts and each part is transmitted at a different frequency. The bits are converted to signal using a variant of FSK, known as **Gaussian bandwidth filterin shift keying (GFSK)**. In GFSK, the bit 1 is represented by a frequency deviation above the carrier frequency used and bit 0 by a frequency deviation below the carrier frequency.

Baseband Layer

This layer is similar to MAC sublayer in LANs. It uses time division multiplexing (TDMA) and the primary and secondary stations communicate with each other using time slots. Bluetooth uses a form of TDMA known as **TDD-TDMA (time-division duplex TDMA)**—a sort of half-duplex communication, which uses different hops for each direction of communication (from primary to secondary or vice versa). If there is only one secondary station in the piconet, then the secondary station uses even numbered slots while the primary station using odd-numbered slots for communication. That is, in slot 0, data flows from primary to secondary while in slot 1 data flows from secondary to primary. This process continues until the end of frame transmission. Now, consider the case where there is more than one secondary station in the piconet. In this case also, primary station sends in even-numbered slots, however, only one secondary station (out of many) who had received the data in the previous slot transmits in the odd-numbered slot. For example, suppose in slot 0, the primary station (P) has sent data intended for a secondary station (S) then only S can transmit in slot 1.

L2CAP Layer

The logical link control and adaptation protocol (L2CAP) is similar to LLC sublayer in LANs. This layer is used for exchanging data packets. Each data packet comprises three fields (Figure 9.15), which are as follows:

Length 2 bytes	Channel ID 2 bytes	Data and control 0-65535 bytes

Figure 9.15 Format of Data Packet of L2CAP Layer

- ❑ **Length:** It is a 2-byte long field that is used to specify the size of data received from upper layers in bytes.
- ❑ **Channel ID (CID):** It is a 2-byte long field that uniquely identifies the virtual channel made at this level.
- ❑ **Data and Control:** This field contains data that can be up to 65,535 bytes as well as other control information.

The L2CAP layer performs many functions that are discussed as follows:

- ❑ **Segmentation and Reassembly:** Application layer sometimes delivers a packet that is very large in size, however, baseband layer supports only up to 2,774 bits or 343 bytes of data only in the payload field. Thus, the L2CAP layer divides large packets into segments at the source and these packets are reassembled again at the destination.

- **Multiplexing:** The L2CAP deals with multiplexing. At the sender's side, it acquires data from the upper layers, frames them and gives them to the baseband layer. At the receiver's station, it acquires frames from the baseband layer, extracts the data and gives them to the appropriate protocol layer.

Link Manager Protocol

The link manager protocol (LMP) helps a Bluetooth device to discover other devices when they come across within the radio range of each other. It uses peer-to-peer message exchange in order to perform various security functions such as authentication and encryption. The LMP layer performs the following functions:

- Generation and exchange of encryption keys.
- Link setup and negotiation of baseband packet size.
- Controlling the power modes, connection state and duty cycles of Bluetooth devices in a piconet.

Host Controller Interface

The host controller interface (HCI) provides command line access to LMP and the baseband layer in order to control and receive the status information. It consists of the following three parts:

- The **HCI firmwa e**, which is a part of the actual Bluetooth hardware.
- The **HCI driver**, which is present in the Bluetooth device software.
- The **host controller transport layer**, which is used to connect the firmware with the drive .

Radio Frequency Communication

Radio frequency communication (RFCOMM) is a serial line communication protocol. It communicates with other upper layer protocols and tells them that the current Bluetooth devices are working over a RS232 wired serial interface.

Service Discovery Protocol (SDP)

Service discovery protocol (SDP) allows a Bluetooth device to join a piconet. It also tells about the available services, their types and the mechanism to access these services.

Telephony Control Protocol Binary (TCS BIN)

Telephony control protocol binary (TCS BIN) is a bit-oriented protocol that helps to setup speech and data calls between Bluetooth devices by defining all essential call control signalling protocols. It also defines mobility management procedures to handle a group of Bluetooth telephony control services (TCS) devices.

AT-Commands

This protocol consists of a set of AT-commands (**attention commands**) which are used to configure and control a mobile phone to act as a modem for fax and data transfers.

Point-to-Point Bluetooth

This is a point-to-point protocol (PPP) that takes IP packets to/from the PPP layer and places them onto the LAN.

TCP/IP

This protocol is used for Internet communication.

Object Exchange Protocol

The Object Exchange (OBEX) is a session protocol, which is used to exchange objects. It works like the hypertext transfer protocol but with a much lighter fashion. It helps to browse the contents of a folder on some remote device.

vCard/vCal

These are the content formats supported by OBEX protocol. A vCard specifies the format for electronic business card while vCal specifies the format for entries in personal calendar, which are maintained by Internet mail consortium.

17. Write a short note on virtual circuit networks.

Ans: A virtual circuit network includes the characteristics of both circuit-switched and a datagram network and performs switching at the data link layer. Like circuit-switched networks, it requires a virtual connection to be established between the communicating nodes before any data can be transmitted. Data transmission in virtual circuit networks involves three phases: connection setup, data transfer and connection teardown phase. In connection setup phase, the resources are allocated and each switch creates an entry for a virtual circuit in its table. After establishment of virtual connection, data transfer phase begins in which packets are transmitted from source to destination; all packets of a single message take the same route to reach the destination. In connection teardown phase, the communicating nodes inform the switches to delete the corresponding entry.

In virtual circuit networks, data is transmitted in the form of packets, where each packet contains an address in its header. Each packet to be transmitted contains a virtual circuit identifier (VCI) along with the data. The **VCI** is a small number, which is used as an identifier of packets between two switches. When a packet arrives at a switch, its existing VCI is replaced with a new VCI when the frame leaves from the switch.

The main characteristic of virtual circuit networks is that nodes need not make any routing decision for the packets, which are to be transferred over the network. Decisions are made only once for all the packets using a specific virtual circuit. At any instance of time, each node can be connected via more than one virtual circuit to any other node. Thus, transmitted packets of a single message are buffered at each node and are queued for output while packets using another virtual circuit on the same node are using the line. Some of the advantages associated with virtual circuit approach are as follows:

- ❑ All packets belonging to the same message arrive in the same order to the destination as sent by the sender. This is because every packet follows the same route to reach the receiver.
- ❑ It ensures that all packets arriving at the destination are free from errors. For example, if any node receives a frame with an error, then a receiving node can request for retransmission of that frame.
- ❑ Packets transmit through the virtual circuit network more rapidly.

18. Write a short note on datagram networks.

Ans: **Datagram networks** are the connectionless networks used for packet switching at the network layer. Here, the packets are referred to as **datagrams**. No virtual connection exists between the source and the destination and each arriving datagram is treated independently by the switch regardless of the source and destination address provided in the datagram. Thus, the different datagram even if they belong to the same message may be forwarded through different paths to reach the destination. This results in the unordered arrival of datagrams at the receiver and with varying delay times. As switches are involved in processing datagrams belonging to other messages also, it might be possible that some datagrams are lost or dropped because of the unavailability of resources.

In datagram networks, there is no need of any connection setup or teardown phase. Each switch maintains a dynamic routing table that helps to deliver the datagrams to the intended receiver. This routing table contains the destination address of every node connected to the network and the corresponding forwarding output port. This approach provides better efficiency as compared to other networks such as circuit-switched networks because resources are allocated only when datagrams need to be transferred instead of setting a connection and reserving the resources in advance. However, datagrams may have to experience more delay as compared to packets in virtual circuit networks. This is because each datagram of a message can be forwarded through different switches and thus, may have to wait at a switch depending on the resources available at the switch at that instance of time.

19. Differentiate virtual circuits and datagram networks.

Ans: There are certain differences between virtual circuits and datagram networks that are listed in Table 9.3.

Table 9.3 Differences between Virtual Circuit Network and Datagram Networks

Virtual Circuit Networks	Datagram Networks
• It is a connection-oriented service. Thus, it requires setting up a circuit between the sender and receiver before transmission.	• It is a connectionless service.
• Each frame that is to be transmitted contains a virtual circuit identifier.	• Each frame that is to be transmitted contains source and destination address.
• All frames belonging to the same message follow the same route to a destination. The route is selected at the time when the virtual circuit is set up.	• The frames belonging to the same message can follow different routes to reach the destination.
• If a router fails then all virtual circuits passing through it are terminated.	• There is no effect on the datagram networks when the router fails. Only the loss of some packets takes place.
• Congestion control is easy as the virtual circuit is set up depending upon the available buffers.	• Congestion control is difficult.
• The delay associated with each packet is less.	• The delay associated with each packet is more.
• It provides less efficiency because resources remain allocated to stream of packets even if the connection is not been used.	• It provides more efficiency as resources are allocated only when required. If a packet of the message being transmitted fails due to some reason, the resources can be allocated to a packet of another message.

20. What is X.25? With reference to X.25, explain the following:

(a) Switched virtual circuit and permanent virtual circuit

(b) Protocols used at the link level

(c) State diagrams to explain call setup and call clearing.

Ans: X.25 is the first public network that was developed in 1976 by ITU-T. It specifies an interface for exchanging data packets between the packet mode end system called **data terminal equipment** (**DTE**) and the access node of switched packet data network called **data circuit terminating equipment** (**DCE**). The DTE is operated by the user, while the DCE is operated by the service provider.

X.25 is a virtual circuit-switching network, which requires the prior establishment of virtual connection between sender and receiver. Each connection is assigned a unique connection number that is included in each packet to be transmitted. Each packet comprises a 3-byte header followed by data up to 128 bytes. The header consists of 12-bit connection number packet sequence number and many other fields. X.25 provides flow and error control at both data link and network lay .

(a) Switched Virtual Circuit and Permanent Virtual Circuit X.25 offers end-to-end virtual communication path through the network for communication between two DTEs. This virtual path can be of two types: *switched virtual circuit* (*SVC*) and *permanent virtual circuit* (*PVC*). An **SVC** is a temporary switched connection that is established upon the request of a DTE and is terminated when data transmission is over. It involves three phases, namely, *call setup*, *data transfer* and *call clearing*. In the **call setup** phase, an entry for the virtual circuit (connection between a source and a destination) is made in each switch. The network resources are allocated for the entire duration of transmission. In **data transfer** phase, the data packets are exchanged between the communicating DTEs. The communication between DTEs is made via local and remote DCEs. The calling DTE sends the data packets to its local DCE, which forwards the packets to remote DCE through the virtual circuit, established between them. The remote DCE finally hands over the packets to the called DTE. In **call clearing** phase, the virtual connection is terminated and resources are deallocated.

On the other hand, **PVC** is a constant (fixed) connection established between two DTEs. It need not be established or terminated for every instance of communication between the DTEs. Thus, it does not require call setup and call clearing phases and always remains in the data transfer phase.

(b) Protocols used at the Link Level The interface of X.25 has been defined at three levels including level 1, level 2 and level 3 which correspond to physical, data link and network layer of OSI model, respectively. Various protocols are used at each level. The link level (level 2) uses data link protocols whose functionality is same as that of the HDLC. These protocols are as follows:

- **Link Access Protocol, Balanced (LAPB):** This protocol is the most common protocol and has been derived from HDLC. It supports all the characteristics of HDLC and can also form a logical link connection.
- **Link Access Protocol (LAP):** This protocol is the earlier version of the LAPB protocol and it is rarely used today.
- **Link Access Procedure, D Channel (LAPD):** This protocol has been derived from the LAPB protocol. It is mainly used in integrated services digital networks (ISDNs), supporting data transmission between DTE and ISDN node. The transmission is mainly done through channel D.
- **Logical Link Control (LLC):** This is an IEEE 802 protocol used in LANs. It allows transmission of X.25 packets through a LAN channel.

(c) State Diagrams to explain Call Setup and Call Clearing The communication between two DTEs initiates through the call setup phase. In this phase, initially, the calling DTE sends a *Call Request* packet to its local DCE. After receiving a *Call Request* packet, the local DCE forwards this packet to the next node thus, establishing the virtual connection up to the remote DCE, which serves the required DTE. The remote DCE then sends an *Incoming Call* packet to the called DTE to indicate the willingness of calling DTE to communicate with it. If the called DTE is ready to communicate, it sends a *Call Accepted* packet to the remote DCE, which then forwards this packet to the local DCE via the same virtual connection. After receiving the *Call Accepted* packet, the local DCE sends a *Call Connected* packet to the calling DTE to indicate the successful establishment of connection. Figure 9.16 depicts the whole process of call setup phase.

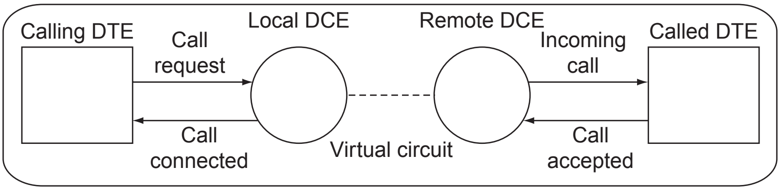


Figure 9.16 Call Setup Phase

Generally, the call-clearing phase is initiated after the completion of data transfer between calling and called DTEs. However, in certain situations, such as when call is not accepted by the called DTE or when a virtual circuit cannot be established, the call-clearing procedure is also initiated. The call can be terminated by either of the communicating parties or by the network. For example, if the calling DTE wants to clear the connection, it sends a *Clear Request* packet to the local DCE which forwards this packet to the remote DCE. To forward the call-clearing request to called DTE, the remote DCE sends a *Clear Indication* packet to it. In response, the called DTE sends a *Clear Confir* packet to the remote DCE, which then forwards this packet to local DCE. The local DCE passes this packet to the calling DTE, thus terminating the connection. Figure 9.17 depicts the whole process of call-clearing phase initiated by DTE.

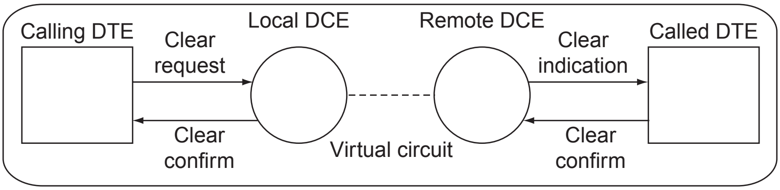


Figure 9.17 Call-clearing Phase

Now, consider the case where the call-clearing phase is initiated by the network. In this case, both the local and remote DCE send a *Clear Indication* packet to the calling and called DTE, respectively. On receiving the packets, the calling and called DTEs respond with a *Clear Confir* packet to the local and remote DCE respectively, thus, terminating the connection. The call clearing by the network may result in the loss of some data packets.

21. List some drawbacks of X.25.

Ans: X.25 is a virtual circuit network that was first developed in 1976 by ITU-T. It has some drawbacks, which are as follows:

- It provides a low data rate only up to 64 kbps. Thus, it cannot be used to transmit bursty data.
- The error and flow control is performed at both data link and network layer. This results in great overhead and reduced speed of transmission.
- It has its own network layer as it was designed for the private use. Thus, if X.25 is to be used with some network that has its own network layer such as Internet, the network layer packets of Internet have to be delivered to X.25, which then encapsulates them into X.25 packets. This increases the overhead.

22. What are T1/T3 lease lines? List some of their drawbacks.

Ans: Some organizations started working in separation from the X.25. They started using their own private wide area networks (WANs), where a line (T1 or T3) was leased from the private service providers. These lines (T1 or T3) are known as **leased lines**. Like X.25, the leased lines also have certain drawbacks, which are as follows:

- It was too costly, as organizations have to pay for them. The payment has to be made even if the lines are not in use.
- Only fixed rate data can be transmitted with T1/T3 lines. It was not possible to send different frames at different bandwidths.

23. Discuss Frame Relay in detail.

Ans: **Frame Relay** is a virtual circuit WAN that came into existence in the late 1980s to meet the demands of a new WAN with faster transmission capability. Prior to Frame Relay, some organizations were using virtual circuit network X.25 and some organizations were having their own private WANs using lease lines (T1 or T3) from public service providers. Both these technologies suffered from severe limitations and thus, were replaced by Frame Relay.

Frame Relay provides a higher transmission speed of 44.376 Mbps and allows sending a frame of size up to 9,000 bytes. It operates in physical and data link layer only and thus, can be easily used with networks having their own network layer such as Internet. It allows bursty data to send through it and is less expensive as compared to other WANs. It does not provide flow control; however, error detection is supported and that too only at the data link layer.

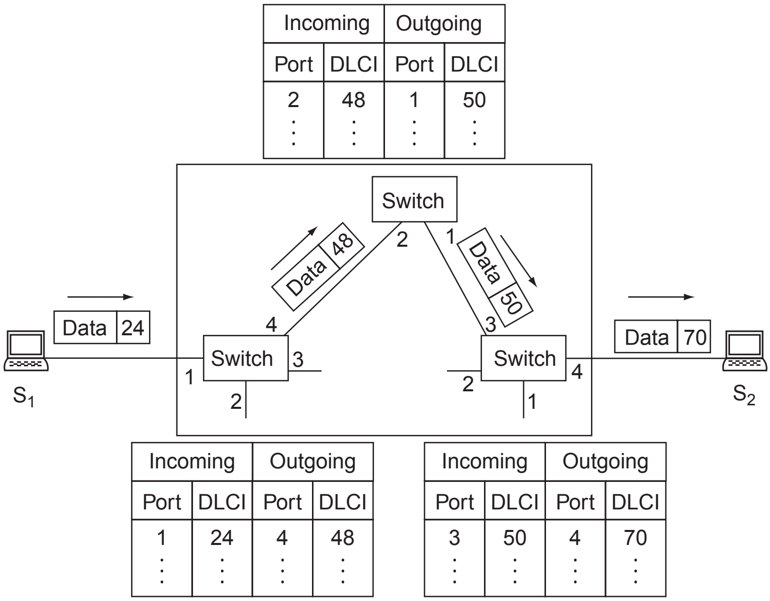
Architecture

Frame Relay is a virtual circuit network in which each virtual circuit is uniquely identified by a number known as **data link connection identifie** (**DLCI**). It provides two types of virtual circuits, which are as follows:

- **Permanent Virtual Circuit (PVC):** In this circuit, a permanent connection is created between a source and a destination and the administrator makes a corresponding entry for all the switches in a table. An outgoing DLCI is given to the source and an incoming DLCI is given to the destination. Using PVC connections is costly, as both source and destination have to pay for the connection even if it is not in use. Moreover, it connects a single source to a single destination. Thus, if source needs connection with another destination, then separate PVC is to be set up.

- **Switched Virtual Circuit (SVC):** In this circuit, a short temporary connection is created and that connection exists as long as data transmission is taking place between source and the destination. After the transmission of the data, the connection is terminated.

In a Frame Relay network, the frames are routed with the help of a table associated with each switch in the network. Each table contains an entry for every virtual circuit that has already been set up. The table contains four fields for each entry: incoming port, incoming DLCI, outgoing port and outgoing DLCI. Whenever a packet arrives in a switch, it searches the incoming port DLCI combination in the table to match with an entry. After a match has been found, the DLCI of the arrived packet is replaced with outgoing DLCI (found in table) and the packet is routed to the outgoing port. This way the packet travels from switch to switch and eventually, reaches the destination. Figure 9.18 depicts how data is transferred from a source to a destination in a Frame Relay network.



Incoming		Outgoing	
Port	DLCI	Port	DLCI
2	48	1	50
⋮	⋮	⋮	⋮

Incoming		Outgoing	
Port	DLCI	Port	DLCI
1	24	4	48
⋮	⋮	⋮	⋮

Incoming		Outgoing	
Port	DLCI	Port	DLCI
3	50	4	70
⋮	⋮	⋮	⋮

Figure 9.18 Data Transfer in a Frame Relay Network

Frame Relay Layers

Frame Relay comprises two layers: physical and data link layer. There is no specific protocol defined for the physical layer; the implementer can use any of ANSI-recognized protocols at this layer. In contrast, at the data link layer, a simple protocol is used, which does not offer any flow or error control. However, error detection is supported by this protocol. Frame Relay uses a frame at the data layer provides whose format is shown in Figure 9.19.

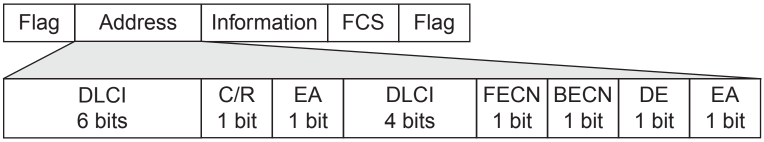


Figure 9.19 Format of Frame Relay Frame

The Frame Relay frame consists of five fields, which are described as follow

- **Flag:** It is an 8-bit long field, which is used at the start and end of the frame. The starting flag indicates the start of the frame, whereas the ending flag indicates the end of the frame.
- **Address:** This field has a default length of 16 bits (2 bytes), and may be extended up to 4 bytes. The address field is further divided into various subfields, which are described as follow
    - **DLCI:** This field is specified in the two parts in the frame as shown in Figure 9.19. The first part is 6 bits long while the second part is 4 bits long. These 10 bits together identify the data link connection defined by the standard
    - **Command/Response (C/R):** It is 1-bit long field that enables the upper layers to recognize whether a frame is a command or a response.
    - **Extended Address (EA):** This field is also specified in two parts in the frame, with each part of 1 bit. It indicates whether the current byte is final byte of the address. If the value is zero, then it indicates that another address byte is to follow; else, it means that the current byte is the final byte
    - **Forward Explicit Congestion Notification (FECN):** It is a 1-bit long field that informs the destination that congestion has occurred. It may lead to loss of data or delay.
    - **Backward Explicit Congestion Notification (BECN):** It is a 1-bit long field that informs the sender that congestion has occurred. The sender then slows down the speed of the transmission in order to prevent data.
    - **Discard Eligibility (DE):** It is a 1-bit long field that indicates the priority level of the frame. If its value is set to one, it indicates the network to discard the packet in case of congestion.
- **Information:** It is a variable-length field that carries higher-level data.
- **FCS:** It is a 16-bit long field, which is used for error detection.

24. Discuss congestion control in Frame Relay networks.

Ans: Frame Relay was designed to provide higher data rate and to achieve that congestion must be avoided. However, congestion control is difficult for a Frame Relay networks as it supports variable data rate. In addition, it does not have a network layer for flow control. To avoid congestion in the network Frame Relay uses two notification bits in the frame, namely, *forward explicit congestion notification* (*FECN*) and *backward explicit congestion notification* (*BECN*). The **FECN** bit is used to signal the receiver about the congestion in the network so that the receiver could control the transmitting of frames by delaying the acknowledgement to the higher layers. The **BECN** bit is used to signal the sender about the congestion in the network. To inform the source, the switch can either send response frame from the receiver or use a special connection having DLCI 1023 to send special frames. The sender then reduces the rate of data transmission to control congestion.

25. What is the limitation of using Frame Relay?

Ans: In Frame Relay, the length of frame is not fixed, that is, a user may transmit frames of different sizes. As all the frames are stored in the same queue, a small frame after a long frame in the queue experiences different delay than a small frame before the large frame in the queue. That is, delay varies from frame to frame. This makes the Frame Relay unsuitable for real-time applications such as audio and video as these applications are time sensitive.

26. What is ATM? Explain the architecture of ATM network?

Ans: Asynchronous transfer mode (**ATM**) is the standard specified by ITU-T for cell relay in which multiple service types including video and data are transferred in the form of fixed-size cells. A cell is the basic unit of data exchange in an ATM. Each ATM cell is 53 bytes long including 5 bytes of header and 48 bytes of payload or data. Further, ATM networks are connection-oriented though they employ packet-switching technique. They also allow bursty traffic to pass through as well as devices with different speeds can communicate with each other via ATM network. Thus, it combines the advantages of both packet switching and circuit switching.

Architecture of ATM Network

An ATM network is composed of ATM switches and ATM endpoints. An **ATM switch** deals with transmission of a cell through the network. It takes the cell from an ATM switch or ATM endpoint, reads the cell header information and updates it. After this, it switches the cell to an output interface towards its intended destination. An **ATM endpoint** is a user access device such as router, workstation and digital service unit (DSU) that consists of a network interface adapter.

Two types of interfaces, namely, *user-to-network interface* (*UNI*) and *network-to-network interface* (*NNI*) are used in an ATM network. The **UNI** connects the ATM endpoints to the ATM switches inside the network, whereas the **NNI** connects the switches within the network. Each UNI and NNI can also be classified into public or private UNIs and NNI. A **private UNI** connects an ATM endpoint and a private switch. However, the **public UNI** connects an ATM endpoint or private switch to a public switch. A **private NNI** connects two ATM switches located in the same private organization. However, the **public NNI** connects two ATM switches located in the same public organization. The architecture of an ATM network is shown in Figure 9.20.

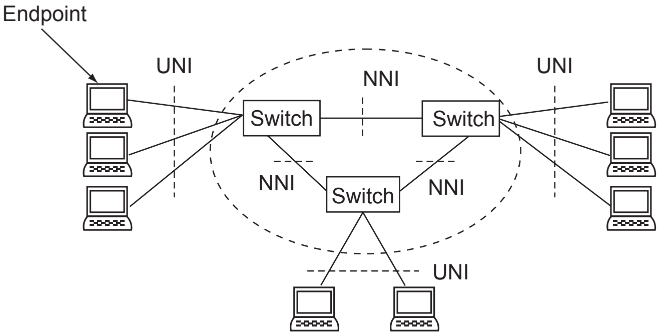


Figure 9.20 Architecture of an ATM Network

Two ATM endpoints are connected through transmission path (TP), virtual path (VP) and virtual circuits (VC). A **transmission path** such as wire or cable that links an ATM endpoint with an ATM switch or two ATM switches with one another. It consists of a set of virtual paths. A **virtual path** refers to the link (or a group of links) between two ATM switches. Each virtual path is a combination of virtual circuits having the similar path. A **virtual circuit** refers to the logical path that connects two points. All the cells corresponding to the same message pass through the same virtual circuit and in the same order until they reach the destination.

In order to route cells from one end ATM end point to another, the virtual connections must be uniquely identified. Each virtual connection is identified by the combination of virtual path identifier (VPI) and virtual circuit identifier (VCI). Further, VPI uniquely identifies the virtual path while VCI uniquely identifies the virtual circuit; both VPI and VCI are included in the ATM cell header. Notice that all the virtual circuits belonging to the same virtual path possess the same VPI. The length of VPI is different in UNI and NNI. It is of 8 bits in UNI but of 12 bits in NNI. On the other hand, the length of VCI is same in both UNI and NNI and is 16 bits. Thus, to identify a VC, a total of 24 bits are required in UNI while 28 bits are required in NNI.

The ATM also uses PVC and SVC connections like Frame Relay. However, the difference is that ATM was developed from the starting to support audio and video applications using SVCs while in a Frame Relay, PVC and SVC were added later.

27. How are ATM cells multiplexed?

Ans: In an ATM, asynchronous time division multiplexing technique is followed to multiplex the cells from different input sources. The size of each slot is fixed and is equal to the size of a cell. Each input source is assigned a slot when it has some cell to send. In case none of the sources has cell to send, the slots remain empty. Whenever any channel has a cell to send, the ATM multiplexer puts any of these cells into a particular slot. However, if all the cells have been multiplexed, the empty time slots are sent in the network.

Figure 9.21 shows the cell multiplexing from four input sources P, Q, R and S. At the first clock tick, as the input source Q has no cell to send, the multiplexer takes a cell from S and puts it into the slot. Similarly, at the second clock tick, Q has no data to send. Thus, the multiplexer fills the slot with a cell from R. This process continues until all the cells have been multiplexed. After all the cells from all the sources have been multiplexed, the output slots are empty.

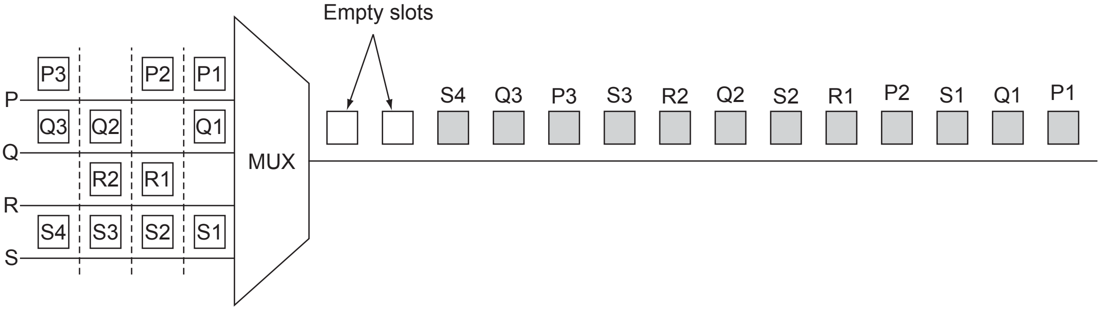


Figure 9.21 Multiplexing in ATM

28. Discuss ATM layers.

Ans: The ATM standard has defined three layers, namely, *physical layer*, *ATM layer* and *application adaptation layer* (AAL) as shown in Figure 9.22.

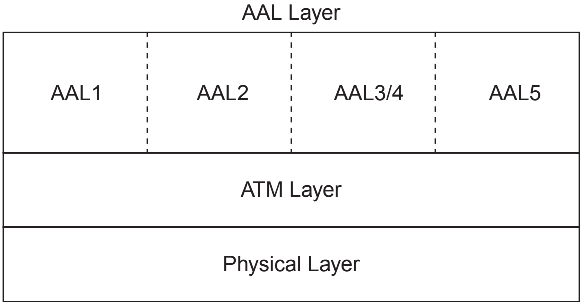


Figure 9.22 ATM Layers

Physical Layer

The physical layer is responsible for managing the medium-dependent transmission. It carries the ATM cells by converting them into bit streams. It is responsible for controlling the transmission and receipt of bits as well as maintaining the boundaries of an ATM cell. Originally, ATM was designed to use synchronous optical network (SONET) as the physical carrier. However, other physical technologies can also be used with ATM.

ATM Layer

An ATM layer is similar to the data link layer of the OSI model. It is responsible for cell multiplexing and passing cells through ATM network (called **cell relay**). Other services provided by the ATM layer include routing, traffic management and switching. It accepts a 48-byte segment from the AAL layer and adds a 5-byte header, transforming it into a 53-byte cell. Further, ATM uses a separate header for UNI and NNI cell (Figure 9.23). The header format of the UNI cell is similar to the NNI cell except the GFC field that is included in the UNI cell, but not in the NNI cell

GFC	VPI	VCI	PT	CLP	HEC	Payload
4 bits	8 bits	16 bits	3 bits	1 bit	8 bits	data

(a) UNI cell

VPI	VCI	PT	CLP	HEC	Payload
12 bits	16 bits	3 bits	1 bit	8 bits	data

(b) NNI cell

Figure 9.23 Format of an ATM Cell Header

The description of fields included in cell header is as follows

- **Generic Flow Control (GFC):** It is a 4-bit long field that is used for flow control in UNI. In NNI, this field is not required. Thus, all the bits are assigned to VPI. The longer is the VPI, the more number of virtual paths will be specified at NNI.
- **Virtual Path Identifier (VPI):** It is an 8-bit long field in UNI cell and 12-bit long field in NNI cell that identifies a specific virtual pat
- **Virtual Circuit Identifier (VCI):** It is 16-bit long field that identifies a specific virtual circuit inside the virtual path.
- **Payload Type (PT):** It is a 3-bit long field in which the first bit is used to define the type of information, that is, data or managerial information while the context of other two bits are based on the first bit
- **Cell Lost Priority (CLP):** It is a 1-bit long field that is used for congestion control
- **Header Error Correction (HEC):** It is the cyclic redundant code that is used for error correction. It is calculated over the first 4 bytes of header using a divisor $x^8 + x^2 + x + 1$ to correct single and multiple-bit errors.

Application Adaptation Layer

Application adaptation layer (AAL) accepts data frames or stream of bits from upper layers and divides them into fixed-size segments of 48 bytes. At the receiver's side, these data frames or stream of bits are again reassembled into their original form. An AAL layer is partitioned into two sublayers, namely, *segmentation and reassembly sublayer* (*SAR*) and *convergence sublayer* (*CS*). The **SAR** sublayer is responsible for segmentation of payload at the sender's side and reassembling the segments to create the original payload at the receiver's side. The **CS** sublayer is responsible for ensuring the integrity of data and preparing it for segmentation by the SAR sublayer. There are various types of AAL including AAL1, AAL2, AAL3/4 and AAL5. Out of these four versions, only AAL1 and AAL5 are commonly used.

29. Explain the structure of ATM adaptation layer.

Ans: The ATM standard has defined four versions of AAL, which include AAL1, AAL2, AAL3/4 and AAL5. All these versions are discussed as follows:

AAL1

It is a connection-oriented service that supports applications needing to transfer information at constant bit rates such as voice and video conferencing. The bit stream received from upper layer is divided into 47-byte segments by the CS sublayer and then segments are passed to SAR sublayers below it. The SAR sublayer appends a 1-byte header to each 47-byte segment and sends the 48-byte segments to the ATM layer below it. The header added by SAR sublayer consists of two fields (Figure 9.24) namely, *sequence number* (*SN*) and *sequence number protection* (*SNP*). The **SN** is a 4-bit field that specifies a sequence number for ordering the bits. Further, **SNP** is a 4-bit field that is used to protect the sequence number. It corrects the SN field by using first three bits and the last bit is used as a parity bit to discover error in all eight bits.

SN 4 bits	SNP 4 bits

Figure 9.24 SAR Header

AAL2

Initially, it was designed to support applications that require variable-data rate. However, now it has been redesigned to support low bit rate traffic and short-frame traffic such as audio, video or fax. The AAL2 multiplexes short frames into a single cell. Here, the CS sublayer appends a 3-byte header to the short packets received from the upper layers and then passes them to the SAR layer. The SAR layer combines the short frames to form 47-byte frames and adds a 1-byte header to each frame. Then, it passes the 48-byte frames to the ATM layer.

The header added by CS sublayer consists of five fields (Figure 9.25(a)) which are described as follows:

- ❑ **Channel Identifie (CID):** It is an 8-bit long field that specifies the channel user of the packe
- ❑ **Length Indicator (LI):** It is a 6-bit long field that indicates the length of data in a packet
- ❑ **Packet Payload Type (PPT):** It is a 2-bit long field that specifies the type of a packe
- ❑ **User-to-User Indicator (UUI):** It is a 3-bit long field that can be used by end-to-end use .
- ❑ **Header Error Control (HEC):** It is a 5-bit long field that is used to correct errors in the heade .

The header added by SAR consists of only one field [Figure 9.25(b)], **start fiel** (**SF**) that specifies an offset from the beginning of the packet.

CID 8 bits	LI 6 bits	PPT 2 bits	UUI 3 bits	HEC 5 bits

(a) CS header

SF 8 bits

(b) SAR header

Figure 9.25 CS and SAR Headers

AAL3/4

Originally, AAL3 and AAL4 were defined separately to support connection-oriented and connectionless services, respectively. However, later they were combined to form a single format AAL3/4. Thus, it supports both connection-oriented and connectionless services. Here, the CS sublayer forms a PDU by inserting a header at the beginning of a frame or appending a trailer. It passes the PDU to SAR sublayer, which partitions the PDU into segments and adds a 2-byte header to each segment. It also adds a trailer to each segment.

The header and trailer added by the CS layer together consist of six fields (Figure 9.26) that are described as follows:

- **Common Part Identifie (CPI):** It is an 8-bit long field that helps to interpret the subseque t fields
- **Begin Tag (Btag):** It is an 8-bit long field that indicates the beginning of a message. The value of this field is same for all the cells that correspond to a single message
- **Buffer Allocation Size (BAsize):** It is a 16-bit long field that specifies to the receiver buffer size needed to hold the incoming data that is to be transmitted.
- **Alignment (AL):** It is an 8-bit long field that is added to make the trailer 4 bytes long
- **Ending Tag (Etag):** It is a 16-bit long field that indicates the end of the message. It has the same value as that of Btag.
- **Length (L):** It is a 16-bit long field that specifies the length of the data uni

CPI 8 bits	Btag 8 bits	BAsize 16 bits

(a) CS header

AL 8 bits	Etag 8 bits	L 16 bits

(b) CS trailer

Figure 9.26 CS Header and Trailer

The header and trailer added by SAR layer together consists of five fields (Figure 9.27) that are described as follows:

- **Segment Type (ST):** It is a 2-bit long field that specifies the position of a segment corresponding to a message.
- **Sequence Number (SN):** It is a 4-bit long field that specifies the sequence numb .
- **Multiplexing Identifie (MID):** It is a 10-bit long field that identifies the flow of data to which the incoming cells belong.
- **Length Identifie (LI):** It is a 6-bit long field in the trailer that specifies the length of a data in the packet excluding padding.
- **CRC:** It is a 10-bit long field that contains CRC computed over the entire data unit

ST 2 bits	SN 4 bits	MID 10 bits

(a) SAR header

LI 6 bits	CRC 10 bits

(b) SAR trailer

Figure 9.27 SAR Header and Trailer

AAL5

This layer supports both connection-oriented and connectionless data services. It assumes that all cells corresponding to single message follow one another in a sequential order and the upper layers of the application provide the control functions. This layer is also known as **simple and efficient algorithm layer** (**SEAL**). Here, the CS sublayer appends a trailer to the packet taken from upper layers and then passes it to the SAR layer. The SAR layer forms 48-bytes frames from it and then passes them to the ATM layer.

The trailer added by CS layer consists of four fields (Figure 9.28) that are described as follows

- ❑ **User-to-User (UU):** It is an 8-bit-long field that is used by users
- ❑ **Common Part Identifier (CPI):** It is an 8-bit-long field that is used for the similar function as that in the CS layer of AAL3/4.
- ❑ **Length (L):** It is a 16-bit-long field that specifies the length of dat
- ❑ **CRC:** It is a 32-bit-long field, which is used for error correction

UU 8 bits	CPI 8 bits	L 16 bits	CRC 32 bits

Figure 9.28 CS Trailer

30. List some benefits of ATM.

Ans: An ATM is a cell-switched network that provides several benefits over its counterpart, the Frame Relay. Some of these benefits are as follows:

- ❑ It provides high bandwidth for applications that require bursty traffic. For example, applications such as video involve bursty data in which amount of motion in a video is not fixed and also in audio, conversation does not go the same way all the time. Thus, ATM can be used for these applications.
- ❑ Technologies such as Frame Relay use frames of different sizes. Thus, it is difficult to manage the traffic. In contrast, ATM was developed to carry audio and video using a cell-switched technology in which fixed-size frames are used. This improves the efficiency, as it is easier to quantify, predict and manage the network traffic.
- ❑ Further, ATM is a WAN technology but it can be used as both LAN and WAN technology. It can be used to cover large distances to link LANs or WANs.

31. What is the relationship between SONET and SDH?

Ans: Both Synchronous optical network (SONET) and synchronous digital hierarchy (SDH) are WANs that are used as transport networks to carry data at high rate from other WANs because of higher bandwidths of fibre optic cables as well as carrying vast amount of lower-rate data. The only difference is that ANSI of the United States has provided SONET while SDH has been provided by ITU-T of Europe. Both SONET and SDH are synchronous networks that use synchronous TDM multiplexing. A master clock controls all the clocks present in the system. Both SONET and SDH standards are independent of each other; however, they are functionally similar and compatible. It can be said that they are nearly identical.

32. How is an STS multiplexer different from an add/drop multiplexer since both can add signals together?

Ans: Both synchronous transport signal (STS) and add/drop multiplexer are the devices used in SONET. Further, STS is used as an interface between electrical and optical networks. At the sender's end, STS multiplexer is used that multiplexes the signals coming from various electrical sources into the corresponding optical carrier (OC) signal. This optical signal passes through the SONET link and finall , reaches the receiver. At the receiver's end, STS demultiplexer is used that demultiplexes the OC signals into the corresponding electrical signals.

Add/drop multiplexer is used in the SONET link to insert or remove signals. It can combine the STSs from several sources into a single path or extract some desired signal and send it to some other path without demultiplexing. In SONET, the signals multiplexed by the STS multiplexer (optical signals) are passed through regenerator, which regenerates the weak signals. The regenerated signals are then passed to add/drop multiplexer that transmits them in the directions as per the information available in data frames (Figure 9.29). The main difference between add/drop multiplexer and STS multiplexer is that it does not demultiplex the signals before delivering them.

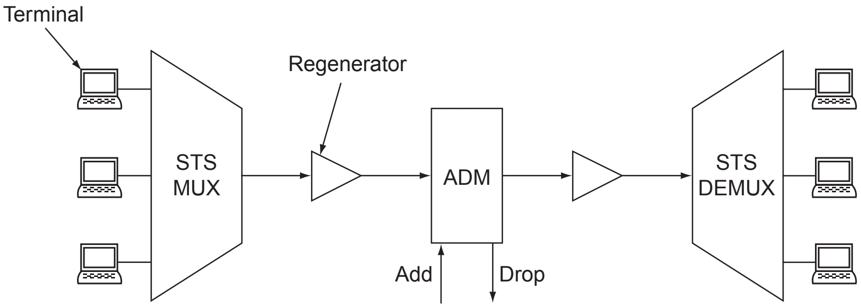


Figure 9.29 A Simple Network using SONET Equipment

33. What is the function of a SONET regenerator?

Ans: The **SONET regenerator** is a repeater that regenerates the weak signals. Sometimes, because of the long distances travelled from one multiplexer to another, the signals becomes weak and need to be regenerated. The regenerator receives an OC signal and demodulates it into the corresponding electrical signals. These electrical signals are then again regenerated and finall , modulated into OC signals. The regenerator functions at the data link layer.

34. What are the four SONET layers? Discuss the functions of each layer.

Ans: There are four functional layers included in the SONET standard, namely, *photonic*, *section*, *line* and *path* (Figure 9.30).

- **Photonic Layer:** It is the lowest layer whose functionalities are similar to that of the physical layer of the OSI model. This layer includes the physical specifications related to optical fibre, the multiplexing functionalities and the sensitivity of the receiver. Further, NRZ encoding is used by SONET where the presence of light shows bit 1 while absence of light shows 0.
- **Section Layer:** The function of section layer includes handling framing, scrambling and error control. It has the responsibility of moving a signal across a physical section. In addition, the section layer header is added to the frame at this layer.

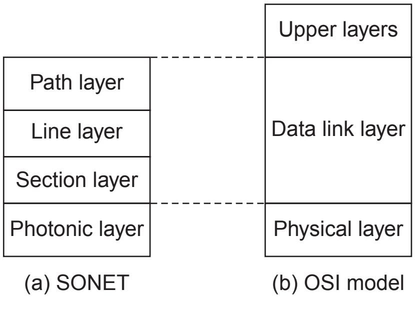


Figure 9.30 Relationship of SONET Layers with the OSI Model

- **Line Layer:** The line layer takes care of the movement of signal across a physical line. At this layer, the line layer overhead is added to the frame. The line layer functions are provided by STS multiplexers and add/drop multiplexers.
- **Path Layer:** The movement of a signal from the optical source to the optical destination is the responsibility of the path layer. The electronic signal is changed into the optical form from the electronic form at the optical source and then multiplexed with other signals, finally being encapsulated into a frame. The received frame is demultiplexed and the individual optical signals are changed into their electronic form at the optical destination. The STS multiplexers are used to provide path layer functionalities. At this layer, the path layer overhead is added to the signal.

35. What are virtual tributaries?

Ans: SONET was originally introduced to hold the broadband payloads. However, the data rates of the current digital hierarchy ranging from DS-1 to DS-3 are lower than STS-1. Thus, virtual tributary (VT) was introduced to make the SONET compatible with the present digital hierarchy. A VT is a partial payload, which can be filled into an STS-1 frame and combined with many other partial payloads to cover the entire frame. The VTs filled in the STS-1 frame are organized in form of rows and columns. There are four types of VTs, which have been defined to make SONET compatible with the existing digital hierarchies. These four categories are as follows:

- **VT1.5:** This VT adapts to the US DS-1 service and provides a bit rate of 1.544 Mbps. It gets three columns and nine rows.
- **VT2:** This VT adapts to the European CEPT-1 service and provides a bit rate of 2.048 Mbps. It gets four columns and nine rows.
- **VT-3:** This VT adapts to the DS-1C service and provides a bit rate of 3.152 Mbps. It gets six columns and nine rows.
- **VT 6:** This VT adapts to the DS-2 service and provides a bit rate of 6.312 Mbps. It gets 12 columns and nine rows.

Multiple Choice Questions

1. Fast Ethernet operates at
(a) 10 Mbps (b) 100 Mbps
(c) 1000 Mbps (d) none of these

2. 10-Base F uses
(a) optical fibr (b) coaxial cable
(c) twisted pair (d) none of these

3. IEEE 802.4 is used to describe
(a) Token Ring (b) Token Bus
(c) CSMA/CD (d) Ethernet

4. The access method used in FDDI is
(a) CSMA/CD (b) token passing
(c) timed token passing (d) none of these

5. Extended service set in IEEE 802.11 consists of
(a) only one basic service set with AP
(b) only one basic service set without AP
(c) at least two basic service sets without APs
(d) at least two basic service sets with APs

6. An example of wireless LAN is
(a) Bluetooth (b) Ethernet
(c) both (a) and (b) (d) none of these

7. Which of the following statements is false?
(a) Virtual circuit network provides less efficienc .
(b) Congestion control is easy in virtual circuit networks.

(c) Virtual circuit does not require set up of a connection before transmission.
(d) all of these

8. Which of the following statements is false?
(a) In Frame Relay, frame length is not fixed.
(b) Frame Relay was developed for real-time applications.
(c) ATM uses fixed-size cells
(d) none of these

9. Which of the following is a type of interface in an ATM network?
(a) user-to-network (b) network-to-network
(c) user-to-user (d) both (a) and (b)

10. AAL1 is a
(a) connection-less service
(b) connection-oriented service
(c) both (a) and (b)
(d) none of these

Answers

1. (b) 2. (a) 3. (b) 4. (c) 5. (d) 6. (a) 7. (c) 8. (b) 9. (d) 10. (b)

10

Routing and Congestion Control

1. Explain the various design issues of the network layer.

Ans: The network layer provides an end-to-end communication between two hosts. There are mainly four design issues in the network layer, which are discussed as follows:

- **Network l ayer i nterface:** The network layer can follow two methods, namely, *virtual circuit* (connection-oriented network service) and *datagram* (connectionless network service) for sending packets from node to node. In the **virtual circuit** method, first a logical connection is established between the two communicating users and then the quality of service to be used is decided. All the packets travel through the established path to reach the destination. On the other hand, the **datagram** method does not require to set up any fixed path before the transmission. Thus, each packet should contain sufficient information for routing from source to destination so that it need not depend upon previous exchanges. Each packet may follow a different path to reach the destination.
- **Routing issues:** It is the responsibility of the network layer to route packets from source to destination. For this, a piece of software, known as routing algorithm, is used which decides where the packets are to be sent. The routing algorithm has to deal with the following issues:
  - **Correctness and simplicity:** The networks should never go down; the links or routers may fail but the whole network should still function.
  - **s tability:** When a router fails, the time elapsed before other routers realize this change should be stable.
  - **Fairness and optimality:** Some aspects such as whether to maximize channel usage or minimize the average delay should be considered while making the routing decisions.
- **Congestion:** The network layer also deals with congestion issues, which are as follows:
  - The network should not be flooded with packets more than its capacity; otherwise, the delay increases and the performance degrades. If the situation does not improve then the packets have to be discarded.

  - If the delay increases, packets may be incorrectly transmitted by the sender making the situation worse.
  - If congestion is not controlled, the overall performance of the network degrades as the network resources would be used for processing the packets that have actually been discarded.
- **internetworking:** Internetworking is used to connect different network technologies together. Certain issues related to internetworking are as follows:
  - The packets should be able to pass through many different networks.
  - Different networks may have different frame formats. Thus, the network layer should support multiple frame formats.
  - The network layer should support both connectionless and connection-oriented networks.

2. Write a short note on iP addresses.

Ans: Each system (computer or router) that connects to the Internet is assigned a specific Internet address. This Internet address, referred to as **iP address**, uniquely identifies the connection of the system to the Internet. Here, uniquely means that no two systems can be assigned the same IP address at the same time. Moreover, IP addresses are universal which means each system wishing to connect to Internet must accept the addressing system.

Each protocol that defines the IP addresses has an **address space**—the total number of addresses that the protocol can use. If a protocol assigns n-bit addresses to machines, the address space of protocol will be 2^n. For example, traditional IP protocol, which is IPv4, defines 32-bit IP addresses and thus, its address space is 2^{32}. On the other hand, IPv6 protocol—the new generation of IP—defines 128-bit addresses and thus, its address space is 2^{128}.

3. Briefl describe the notations used to represent IPv4 addresses.

Ans: An IPv4 address is of 32 bits in length and can be represented using two notations, namely, *binary notation* and *dotted-decimal notation*.

In **binary notation**, the IP address is represented as 32 bits grouped into four octets. As each octet is one byte, an IPv4 address is sometimes also referred to as a **4-byte address**. The problem with this notation is that the binary address is too lengthy and difficult to read. To overcome this problem, dotted-decimal notation is used.

In **dotted–decimal notation**, each byte of an IPv4 address is represented by a decimal value ranging between 0 and 255 and different bytes are separated with a decimal point (.). Figure 10.1 shows a 32-bit IPv4 address written in binary as well as dotted decimal notation.

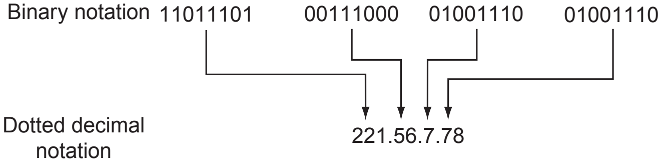


Figure 10.1 An IPv4 Address in Binary and Dotted–Decimal Notation

4. Explain classful and classless addressing.

Ans: IP addressing can be either classful or classless. Both classful and classless addressing are discussed as follows:

Classful Addressing

The traditional IP addressing used the concept of classes thereby named as classful addressing. IPv4 addressing is classful in which all the IP addresses (address space) are divided into five classes, namely, A, B, C, D and E with each class covering a specific portion of the address space. Each class is further divided into a fixed number of blocks with each block of fixed size. Given an IPv4 address, its class can be identified by looking at either few bits of first byte in case IP address is represented in binary notation or the first byte in case the I address is represented in dotted-decimal notation (Table 10.1).

Table 10.1 Determining Class of IP Address

Class	Binary notation (few bits of first byte)	Dotted-Decimal notation (first byte)
A	0	0–127
B	10	128–191
C	110	192–223
D	1110	224–239
E	1111	240–255

The blocks of class A, B and C addresses were granted to different organizations depending on their size. The large organizations using a vast number of hosts or routers were assigned class A addresses. The class B addresses were designed to be used by mid-size organizations having tens of thousands of hosts or routers while the class C addresses were designed for small organizations having small number of hosts or routers. The class D addresses were projected to be used for multicasting where each address identifies a specific group of hosts on the Internet. Only a few of class E addresses were used while rest were kept reserved for the future use. The main problem with classful addressing was that a large number of available addresses were left unused resulting in a lot of wastage.

Each IP address in class A, B and C is divided into two parts: **net iD** that identifies the network on the Internet and **host iD** that identifies the host on that network. The size of each part is different for the different classes. In a class A address, net ID is identified by one byte and host ID is identified by three bytes. In a class B address, net ID is identified by two bytes and host ID is also identified by two bytes and in a class C address, three bytes specify the net ID and one byte specifies the host ID

Classless Addressing

There were certain problems with classful addressing such as address depletion and less organization access to Internet. To overcome these problems, classful addressing is replaced with classless addressing. As the name of the addressing scheme implies, the addresses are not divided into classes; however, they are divided into blocks and the size of blocks varies according to the size of entity to which the addresses are to be allocated. For instance, only a few addresses may be allocated to a very small organization while a larger organization may obtain thousands of addresses. IPv6 addressing is a classless addressing.

The Internet authorities have enforced certain limitations on classless address blocks to make the handling of addresses easier. These limitations are as follows:

- ❑ The addresses of a block must be contiguous.
- ❑ Each block must have a power of 2 (that is, 1, 2, 4, 8…) number of addresses.
- ❑ The first address in a block must be evenly divisible by the total number of addresses in that block.

5. Describe the notation used to represent i Pv6 addresses.

Ans: An IPv6 address is of 128 bits (16 bytes) and is represented using **hexadecimal colon notation**. In this notation, the 128-bit address is divided into eight sections of two bytes each and each byte is represented by four hexadecimal digits. Thus, the address consists of 32 hexadecimal digits with each group of four hexadecimal digits separated by a colon. Figure 10.2 shows an IPv6 address written in hexadecimal colon notation.

FABD : 0037 : 0000 : 0000 : 0000 : ABCF : 0000 : FFFF

Figure 10.2 An IPv6 Address in Hexadecimal Colon Notation

Since many of the digits in the IP address represented in Figure 10.2 are zeros, the address even in hexadecimal format is still too long. However, it can be abbreviated by omitting leading (but not trailing) zeros of a section. For example, 0037 in the second section can be written as 37 and 0000 in third, fourth, fifth and seventh section can be written as 0. Figure 10.3 shows the abbreviated form of a hexadecimal address after omitting leading zeros of a section.

As still there are many consecutive sections containing zero only in the address shown in Figure 10.3, the address can be more abbreviated. The consecutive section of zeros can be eliminated and replaced with double semicolon (**::**) as shown in Figure 10.4. However, there is one limitation with this type of abbreviation that it can be applied only once per address. That is, if there are two or more runs of consecutive sections of zeros in a single address, only one run can be replaced with double semicolon but not others.

FABD : 37 : 0 : 0 : 0 : ABCF : 0 : FFFF

Figure 10.3 Abbreviated Form of IPv6 Address

FABD : 37 : : ABCF : 0 : FFFF

Figure 10.4 More Abbreviated Form of IPv6 Address

6. Defin network address. Is it different from net ID?

Ans: The address that defines the network itself is referred to as the **network address**. It cannot be assigned to a host. It is also different from a net ID. It comprises both net ID and host ID with all bits of host ID set to zero. The network address is required to route the packets to the destination. Table 10.2 lists examples of network addresses for classes A, B and C.

Table 10.2 Examples of Network Addresses

Class	Network address
A	112.0.0.0
B	155.7.0.0
C	229.48.57.0

7. l ist some special i P addresses.

Ans: Depending on their contents, some IP addresses have been designated as special IP addresses. These addresses are listed as follows:

- ❑ An IP address with all 0s (that is, 0.0.0.0) identifies this host. This address is used by the hosts at the time when they are being booted up but not afterwards.

- An IP address with all 1s (that is, 255.255.255.255) indicates broadcast on this network. This address is used for forwarding the packet to all the hosts on the local network.
- An IP address with net ID all 0s and a proper host ID (see diagram below) identifies a specific host on the local network.

000 0	Host ID

- An IP address with a proper net ID, and host ID containing all 1s (see diagram below) indicates broadcast to some distant LAN in the Internet.

Net ID	111 1

- An IP address of the form 127.aa.bb.cc (see diagram below) indicates reserved address used for loopback testing.

127	Anything

8. Write a short note on address masks.

Ans: An address mask, also referred to as **default mask**, is a string made up of contiguous 1s followed by contiguous 0s. Like IP address, it is of 32 bits, that is, four octets where each octet is equivalent to a decimal value in the range of 0–255. Table 10.3 lists the default masks used for classes A, B and C IP addresses.

Table 10.3 Default Masks for Classes A, B and C

Class	Address mask (in binary)	Address mask (in dotted–decimal)
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	225.255.255.0

The address mask (also simply called **mask**) identifies which part of an IP address defines the net ID and which part defines the host ID. To determine this, the IP address and mask are compared bit by bit. If a given mask bit is 1, its corresponding bit in IP address will form a part of net ID. On the other hand, if mask bit is 0, its corresponding bit in IP address will form a part of host ID. For example, consider an IP address 132.7.21.84 (that is, 10000100 00000111 00010101 01010100) that belongs to class B. It is clear from Table 10.3 that the mask for class B addresses is 255.255.0.0 (that is, 11111111 11111111 00000000 00000000). Now, if we compare given IP address with its corresponding mask, we can easily determine that 132.7 define the net ID and 21.84 define the host I

9. Explain the concept of subnetting in IP. What is subnet mask?

Ans: The subnetting was introduced at the time when classful addresses were being used. It means breaking large blocks of addresses into many contiguous groups, which are further assigned to smaller networks known as subnets. It came in use when a single network had to be subdivided internally to accommodate more computers, increasing the size of the whole network. It was impossible to acquire new network addresses every time a network is divided. Therefore, in such a situation, subnetting was used to split the network into many subnets. When subnetting is done, the network is divided internally, however, it appears as a single network to the outside world. For example, in a college campus network the main router may be connected to an Internet service provider (ISP) and different departments may use their own routers, which are connected to the main router. Here, each department with a router and some communication lines form a subnet, however to the outside world, the whole campus appears as a single network (Figure 10.5).

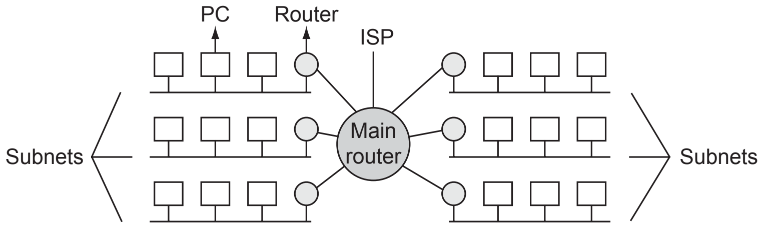


Figure 10.5 A Campus Network Divided into Subnets

Now, a problem arises when a packet comes to the main router; how does it know to which subnet the packet is to be delivered. One way is to maintain a table in the main router having an entry corresponding to each host in the network along with the router being used for that host. Though this scheme seems fine, it is not feasible as it requires a large table and many manual operations as hosts are added or deleted. Thus, a more feasible scheme was introduced, where a part of the host address is used to define a subnet number. For example, in a class B address where a host ID is of 16 bits, the six bits can be used to define the subnet number and the rest 10 bits can be used to define the host ID. This would lead to up to 64 subnetworks, each with a maximum of 1,022 hosts.

For the implementation of subnetting, the main router requires subnet mask that shows the division of addresses between network plus subnet number and host ID. For example, Figure 10.6 shows a subnet mask written in binary notation for a subnetted class B address, where six bits have been used to represent the subnet number and 10 bits for host ID. The subnet mask can also be written in dotted-decimal notation. For example, for the IP address shown in Figure 10.6, the subnet mask in dotted-decimal notation can be written as 255.255.192.0. Alternatively, **slash** (/) **notation**, also called **CiDR** (**classless interdomain routing**) notation can also be used to represent the subnet mask. In this notation, a slash followed by the number of bits in the network plus subnet number defines the subnet mask. For example, the IP address shown in Figure 10.6 can be defined in slash notation as /22 where 22 is the size of subnet mask. Notice that /22 indicates that the first 22 bits of subne mask are 1s while rest 10 bits are 0s.

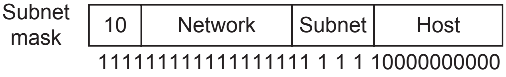


Figure 10.6 A Class B Network Address Subnetted into 64 Subnets

10. What is supernetting? Why it is needed?

Ans: Supernetting is just the opposite of subnetting. There was a time when all the class A and B addresses were used up but still there was a great demand of address blocks for mid-size organizations. The class C address blocks were also not suitable for serving needs of those organizations; more addresses were required. As a solution to this problem, supernetting was used. In this method, several class C blocks can be combined by an organization to create a large address space, that is, smaller networks can be combined to create a **super-network** or **supernet**. For example, an organization having the requirement of 1,000 addresses can be allocated four contiguous blocks of class C addresses.

11. What is IP spoofing

Ans: IP spoofin is a mechanism, which is used to hide the original IP address by replacing it with an arbitrary IP address. The IP datagrams, which are transferred over a network, carry the sender's IP address apart from the data from the upper layers. Any user having control over the operating system can place an arbitrary address into a datagram's source address field by modifying the device protocols. Thus, an IP packet may be made to appear as though it is originating from an arbitrary host. IP spoofing is generally used in denial of service attacks to hide the originator of attack.

If IP spoofing is destructive, it can be prevented through a mechanism known as ingress filtering. When it is implemented, the routers receiving the IP datagrams see their source addresses to check whether these addresses are in the range of network addresses known to the routers. This check is performed at the edge of a network such as a corporate gateway or a firewall

12. What is routing? Differentiate adaptive and non-adaptive routing algorithms.

Ans: Generally, in a network there exist multiple paths available for going from a source to destination. To forward the packets, one of the available routes is to be chosen by the network layer. This is called **routing**.

The part of the network layer software which is responsible for deciding which output line should be used to transmit an incoming packet is referred to as **routing algorithm**. The routing algorithms can be divided into two categories; namely, *non-adaptive* and *adaptive*. **Non-adaptive algorithms** are the algorithms, which make routing decisions regardless of the current status of the network such as current traffic or current topology. If a packet has to be transferred from A to B, then the route to get from A to B is traced in advance and is entered in the routing table. This is done at the time of booting of the network. This is also sometimes called as **static routing**. Some examples of non-adaptive routing algorithms include flooding, shortest path routing and flow-based routin

On the other hand, the **adaptive algorithms** change their decisions dynamically in coordination with the changes in the network attributes as topology, traffic and time delay. Whenever changes occur in the network attributes, the routes of the routers are also changed accordingly. That is why it is also referred to as **dynamic routing**. Some examples of the adaptive routing algorithms are distance vector routing and link state routing.

13. What is optimality principle?

Ans: o ptimality principle refers to a general statement about the optimal routes without taking into account the topology and the traffic load in the network. According to the principle, if an optimal path (say d_1) from router A to G goes through a router F, then the path from F to G (say, d_2) is also optimal. To prove this principle, let us assume that d_2 is not optimal. This means there exist some other path (say, d_3) from F to G that is more optimal than d_2. Thus, d_3 can be combined with d_1 to improve the path from A to G. This implies that d_1d_2 is not optimal which contradicts our statement that d_1d_2 is optimal.

14. What is routing table? What are its categories?

Ans: Each host or router in a network maintains a data structure, known as **routing table**, which contains an entry corresponding to each destination or a group of destinations to route the IP packets.

Whenever an IP packet arrives at a router, it sees the destination address of the packet. Then, it looks up in the routing table to check whether the destination address matches some existing entry. If so, the IP packet is forwarded through the interface specified in the routing table corresponding to that matching entry.

Routing tables are of two types: *static and dynamic routing table*. Both these types are discussed as follows:

- **s tatic Routing t able:** This routing table is created manually. The route of each of the destination is entered into the table by the administrator. If there is any change in the network, it is also done manually by the administrator. Any broken link in the network would require the routing tables to be manually reconfigured immediately so that alternate paths could be used. It is not possible to automatically update the table. Static routing tables are well suited for small networks. However, in large networks such as Internet, maintenance of static routing tables can be very tiresome.
- **Dynamic Routing t able:** This routing table is updated automatically by the dynamic routing protocols such as RIP, BGP and OSPF whenever there is a change in the network. Generally, each router periodically shares its routing information with adjacent or all routers using the routing protocols so that the information about the network could be obtained. If some change is found in the network, the routing protocols automatically update all the routing tables.

15. Differentiate between intradomain and interdomain routing.

Ans: Due to the ever-growing size of Internet, using only one routing protocol to update the routing tables of all routers is not sufficient. Therefore, the network is divided into various autonomous systems. An **autonomous system (As)** is a group consisting of networks and routers, which is controlled by a single administrator. Thus, a network can be seen as a large collection of autonomous system. The routing, which is done inside an autonomous system, is known as **intradomain routing**. One or more intradomain routing protocols may be used to handle the traffic inside an autonomous system. Two most commonly used intradomain routing protocols include *distance vector routing* and *link state routing*. On the other hand, routing which is done between different autonomous systems is known as **interdomain routing**. Only one interdomain routing protocol is used to handle the routing between autonomous systems. The most popular interdomain routing protocol is the *path vector routing*.

16. Explain the following algorithms in brief.

(a) Flooding

(b) Flow-based routing

Ans: (a) Flooding: Flooding is a static routing algorithm that works based on forwarding of packets. Here, every packet arriving in a router is forwarded (flooded) to all the outgoing lines from the router, except the one through which it has arrived. Due to bulk forwarding of packets, a large number of duplicate packets are generated. The flooding can be controlled by ignoring the flooded packets rather than resending them. Some preventive measures that can be used to control flooding are as follows

- A **hop counter** can be included in the header of each packet. Initially, the hop counter can be set to a value equal to the total distance from source to destination. If the distance is not known, then the counter can be initialized to the whole length of the subnet. As the packet reaches at every hop, the counter is decremented by one and finall , when it becomes zero the packet is discarded.
- Another technique to prevent duplication is to keep track of all those packets, which have already been flooded so that they could not be sent for the second time. This technique requires a sequence

number to be included in every packet that is to be forwarded. This sequence number is entered by the source router whenever it receives a packet from a host in its network. Every router maintains a list per each source router indicating the sequence numbers that have already been seen by that source router. The packet is not flooded if it is already on the list

- ❑ A variation of flooding known as **selective floodin** can be used to overcome the problem. In this algorithm, not every incoming packet is sent to every outgoing line, but only to those lines, which are going in the right direction.

Few applications where flooding is useful are as follows

- ❑ It is used in distributed database applications where the need arises to update all the databases at the same time and to choose the shortest path to the destination resulting in shorter delay.
- ❑ It is used in wireless networks where one station can transmit a message, which can be received by all other stations within the range of that network.
- ❑ It can be used as a metric in routing algorithms. This is because of the reason that flooding always gives a shorter delay which no other algorithm can.

(b) Flow-based Routing: This is also a static routing algorithm in which packets are forwarded by taking into account the traffic condition and the structure of the network. To understand, consider a network shown in Figure 10.7. Suppose there always remains a great traffic from node M to L. If node M has to send packets to node K, routing through node L would not be efficient because of the heavy load on path ML. Thus, another path MNJK is used even though it is a longer than the MLK path. This type of routing is known as **flow-base routing**. The optimal routes can be found by analyzing the flow of data mathematically. However, this is possible only if average traffic from a node to any other node is already known and it always remains constant. Once the average traffic and capacity of a line has been known, the mean delay for each packet can be calculated in advance.

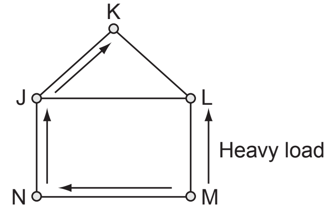


Figure 10.7 Flow-based Routing

17. What is shortest path routing? Explain with the help of a suitable example.

Ans: The **shortest path routing** is a static routing algorithm, which is based on the concept of graphs. Here, the whole subnet is depicted as a graph where the nodes of the graph represent the routers and the edges represent the links between two routers. The optimal route between two routers is determined by finding the shortest path between them. The metric used in shortest path routing can be number of hops, distance or the transmission delay. Any of the metrics used is represented as the weights assigned to the edges in the graph.

There are many algorithms for computing the shortest path between two nodes of a graph representing a network. However, the Dijkstra's algorithm is the most often used to calculate the shortest path. In this algorithm, each node is labelled with a value equal to its distance from the source node along the optimal path. Since no paths are known initially, all nodes are labelled with infinit . As the algorithm proceeds, paths are found and thus, label may change. The labels on the nodes are divided into two categories: *tentative* and *permanent.* Initially, and each label is tentative. However, as it is assured that the label presents the shortest distance, it is made permanent.

To understand the Dijkstra's algorithm, consider a sample subnet graph shown in Figure 10.8 where the weights on the edges represent the distance between nodes connected by that edge. Suppose the shortest path has to be calculated from node A to D.

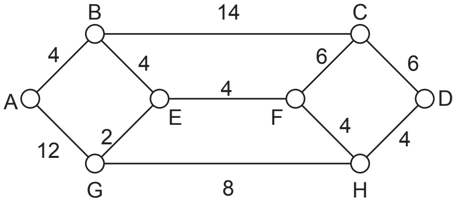


Figure 10.8 A Sample Subnet Graph

The steps involved in calculating the shortest path from A to D are as follows:

1. The node A is marked permanent (shown by the filled circle in Figure 10.9). Each adjacent neighbour of A is examined and is relabelled with distance from A. For example, B is relabelled as (4, A) which indicates that distance of B is 4 from A. Similarly, G is relabelled as (12, A). Rest of the nodes still remain labelled with infinit . Thus, the new tentative nodes are B and G.

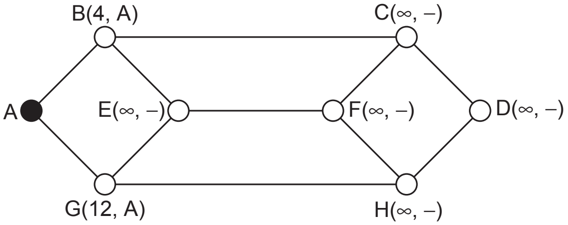


Figure 10.9 Node A Marked as Permanent

2. As out of nodes B and G, B has the shorter distance from A, it is selected and marked permanent as shown in Figure 10.10. Thus, now each adjacent neighbour of B is examined and relabelled with distance from B. Notice that a node is relabelled only if the existing label on it is greater than the sum of the label on the source node and the distance between that node and source node. For example, while examining the node C with respect to node B, we find that the sum of label on B (that is, 4) and the distance between B and C (that is, 14) is 18, which is far less than the existing label on C (that is, ∞). Thus, node C is relabelled as (18,B). Similarly, E is relabelled as (8,B).

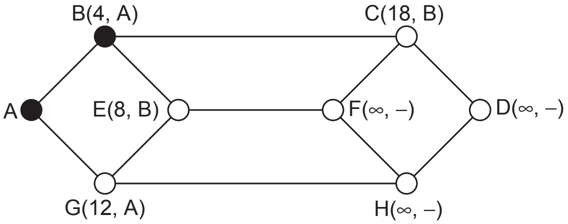


Figure 10.10 Node B Marked as Permanent

3. As out of nodes C and E, E has the shorter distance from B, it is selected and marked permanent as shown in Figure 10.11. Thus, now each adjacent neighbour of E is examined and relabelled with distance from E. As the node G can be reached via E with a shorter distance (that is, 10) than its previous distance (that is, 12), G is relabelled as (10,E). Similarly, F is relabelled as (12,E).

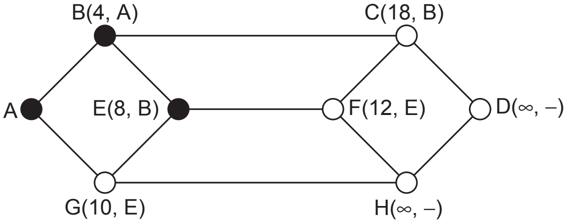


Figure 10.11 Node E Marked as Permanent

4. Though out of nodes `G` and `F`, `G` has the shorter distance from `E`, it cannot be selected as it will result in a loop. Therefore, node `F` is selected and marked permanent as shown in Figure 10.12 and its adjacent neighbours are examined. While examining the neighbouring nodes, the node `E` is not considered because we have reached `F` via `E` and thus, cannot go back. In addition, as the existing label on node `C` (that is, 18) is equal to the sum of distance between `F` and `C` (that is, 6) and label on `F` (that is, 12), node `C` is not relabelled. Contrastive to this, node `H` is relabelled as `(16,F)`.

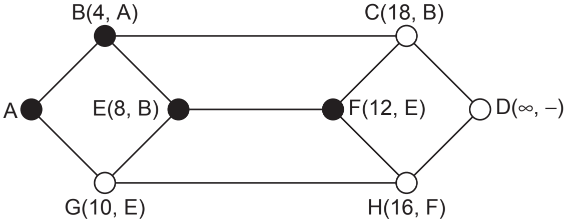


Figure 10.12 Node F Marked as Permanent

5. The node `H` is marked permanent as shown in Figure 10.13 and its adjacent neighbour `D` is examined. The node `D` is relabelled as `D(20,H)`. Since our intended destination `D` has been reached, the node `D` is also marked permanent. Thus, the shortest path from `A` to `D` is `ABEFHD` as shown in Figure 10.13 and the shortest distance from `A` to `D` is 20.

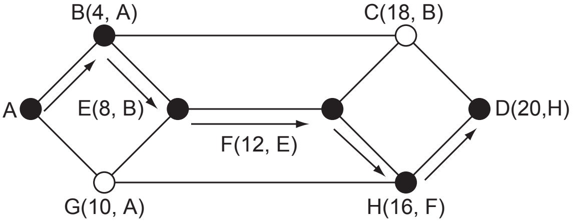
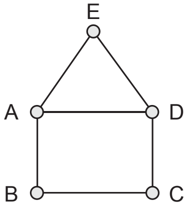


Figure 10.13 Shortest Path from A to D

18. Explain distance vector routing algorithm with the help of a suitable example.

Ans: The **distance vector routing** (also known as **Bellman–Ford routing**) is a dynamic routing algorithm. In this method, each router maintains a table (known as **vector**) in which routing information about the distance and route to each destination is stored. The table contains an entry per each router in the network, where the preferred outgoing line and the distance to that router are specified. Each router periodically exchanges its routing information with their neighbours and updates its table accordingly. Thus, each router knows the distance to each of its neighbours. To make the routing decisions, the metric used maybe the total number of packets queued along the path, number of hops, time delay in milliseconds, etc. For example, if delay is used as the metric for making routing decisions then after every t milliseconds, every router updates its neighbour with the estimated delays needed to reach each destination in the network. Suppose, one such table has just arrived to router J showing that its neighbour A can reach the router I in estimated time A_i. If now the router J knows that its delay time to A is n milliseconds, then it can reach to router I via A in $A_i + n$ milliseconds. By doing such calculation for each neighbour, the optimum estimate is found.

To understand how calculations are performed in distance vector routing, consider a subnet consisting of routers and networks as shown in Figure 10.14(a). Suppose at any instant the router D receives the delay vectors from its neighbours A, C, and E as shown in Figure 10.14(b). Further, assume that the estimated delay from D to its neighbours A, C, and E are 5, 8 and 6, respectively. The router D can now calculate the delays to all the other routers in the network. Suppose D wants to compute the route to B, using the available delay information. Now, D has a delay time of 5 ms to reach A while A takes 10 ms to reach B [Figure 10.14(b)], so D would take a total of 15 ms to reach B via A. In the same way, D can calculate the delays to reach B using the lines C and E as 18(11 + 7), 31(9 + 12 + 10) ms, respectively. Since, the optimum value is 15 ms, the router D updates its routing table mentioning that the delay to B is 15 ms via the route A. The same procedure can be followed by D to calculate the delays to all the other routers and then making entries in its routing table as shown in Figure 10.14(c).



(a)

Delays received by D

	A	C	E
A	0	20	10
B	10	7	22
C	17	0	20
D	9	11	9
E	12	20	0

DA DC DE
5 8 6

(b)

New routing table for D

		line
A	5	A
B	15	A
C	8	C
D	0	–
E	6	E

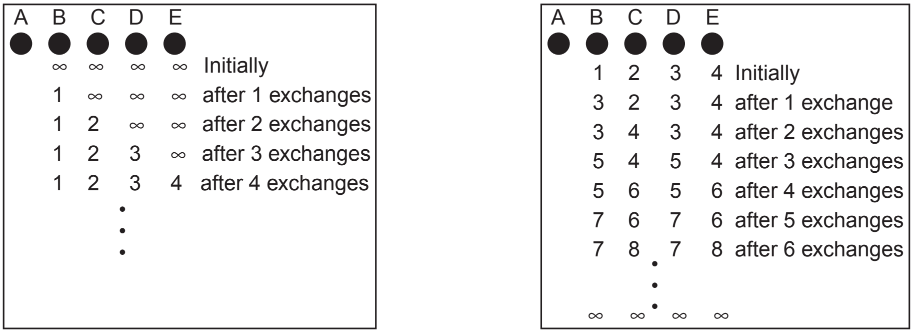
(c)

Figure 10.14 Distance Vector Routing

19. What is the count-to-infinity problem in the distance vector routing algorithm?

Ans: Theoretically, the distance vector routing algorithm works efficiently but practically, it has serious loopholes. Even though a correct answer is derived, it takes time. In practice, this algorithm acts quickly to good news but acts very late to bad news. For example, let us consider a router whose best route to destination X is large. If on the next neighbour exchange, one of its neighbours (say, A) declares a short delay to X, the router starts using the line through A to reach X. The good news is thus processed by B within a single vector exchange. The news spreads even faster as it is received by its neighbours.

To understand how fast good news spreads, consider a linear subnet consisting of five nodes [Figure 10.15(a)]. Suppose, the metric used in the subnet is the number of hops. In the beginning, the node A is down and therefore, all the routers have recorded their delay to A as infinity. When A becomes functional, the routers perceive it through the vector exchanges. At the first vector exchange, B realizes that its left neighbour has zero delay to A, so it makes an entry 1 in its routing table as A is just one hop away from it. At the second vector exchange, the router C comes to know that B is just one hop


A B C D E
∞ ∞ ∞ ∞ Initially
1 ∞ ∞ ∞ after 1 exchanges
1 2 ∞ ∞ after 2 exchanges
1 2 3 ∞ after 3 exchanges
1 2 3 4 after 4 exchanges
A B C D E
1 2 3 4 Initially
3 2 3 4 after 1 exchange
3 4 3 4 after 2 exchanges
5 4 5 4 after 3 exchanges
5 6 5 6 after 4 exchanges
7 6 7 6 after 5 exchanges
7 8 7 8 after 6 exchanges
∞ ∞ ∞ ∞

(a) (b)

Figure 10.15 The Count-to-Infinity Problem

away from A, so C updates its table making an entry of two hops to A. Similarly, D and E update their routing tables after the third and fourth exchanges, respectively. Thus, the news about the recovery of A propagates at a rate of one hop per exchange.

However, the situation is very different in the case of bad news propagation. To understand the propagation of bad news, consider the situation shown in Figure 10.15(b). Here, initially all routers are properly functioning and the routers B,C,D and E are 1, 2, 3 and 4 hops away from A, respectively. Now, if A goes down all of a sudden, the routers still think A to be functional. At the first vector exchange, no vector is received from A but the node B sees in the vector received from C that C has a path of length 2 to A. As B does not know that path from C to A goes through it, it updates its routing table with distance to A as 3 and via C. Now, at the second vector exchange, as C sees the distance of B to A as 3, it updates its distance to A as 4 and via B. Similarly, all the routers continue to update their routing tables and increase their distance to A after every vector exchange. Eventually, all routers update their routing tables with distance to A as infinity where infinity denotes the longest path plus one. This problem is known as the **count-to-infinit** problem.

20. Explain the link state routing protocol.

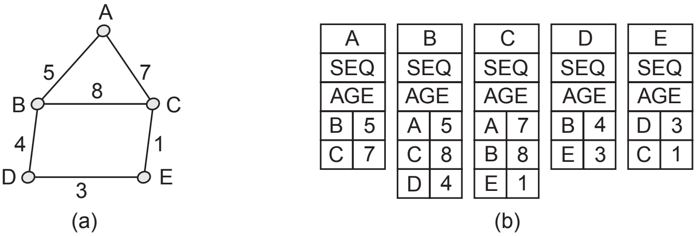
Ans: The link state routing is a dynamic routing algorithm that had been designed to replace its previous counterpart distance vector routing. The distance vector routing has certain limitations, as it does not take into account the line bandwidth while choosing among the routes. It also suffers from count-to-infinity problem. To overcome these limitations, link state routing algorithm was devised.

In link state routing, the information such as network topology, metric used and type and condition of links is available to each router (node). Therefore, each router can use the Dijkstra's algorithm to compute the shortest path to all the available routers and then build their routing tables. Link state routing involves the following phases:

- **Learning about the Neighbours:** Whenever a router boots up, the first step for it is to identify all its neighbours and get their network addresses. For this, the router sends a HELLO packet on each point-to-point line. Each router receiving the HELLO packet responds with its name (or network address) to the sending router. Similarly, all the routers in the network discover their neighbours. Notice that the name of the routers must be globally unique in order to avoid any ambiguity.
- **Measuring the l ine Cost:** After discovering all the neighbours, the next step for a router is to have an estimate of delay to reach every other router in the network. For this, the simplest method that a router can adopt is to send a special ECHO packet over the line and then start a timer. As soon as a router

receives an ECHO packet, it immediately sends the packet back to the sending router. After receiving the ECHO packet back, the sending router can determine the round-trip time of packet and then divide it by two to calculate the delay. To have better estimate of delay, the router can send ECHO packet several times and then use the average time as delay. While computing the delay, the traffic load in the network may or may not be taken into account. If the load is considered, the sending router starts the timer at the time the packet is queued up. On the other hand, if load is not taken into account, the sending router starts the timer at the time the packet reaches at the front of the queue.

- **Building l ink s tate Packets: t** he next step for a router is to package the collected information to form a link state packet (LSP). Each LSP comprises four fields: the identity of the sending router, sequence number, age and list of its neighbouring links. The first and fourth fields of LSP together determine the network topology. The second field indicates the sequence number assigned to the LSP packet; the sequence number is incremented by one each time the packet is created by the router. The third field indicates the duration for which the LSP has been residing in the domain. The LSP also includes delay to reach each adjacent neighbour. For example, Figure 10.16(b) shows the LSPs for each of the five routers of the subnet shown in Figure 10.16(a).



A	
SEQ	
AGE	
B	5
C	7

B	
SEQ	
AGE	
A	5
C	8
D	4

C	
SEQ	
AGE	
A	7
B	8
E	1

D	
SEQ	
AGE	
B	4
E	3

E	
SEQ	
AGE	
D	3
C	1

Figure 10.16 Subnet and Link State Packets

The LSPs are created by the routers periodically at regular intervals of time or at certain occasions such as when some changes occur in the topology or either when some router goes down or comes up.

- **Flooding of ls Ps:** After each router has created the LSP, it needs to distribute its LSP to its neighbours in the network. This process is referred to as **floodin** . The router forwards a copy of its LSP through each of its neighbouring interface. For example, the router A sends its LSP through lines AB and AC [Figure 10.16(a)]. Each receiving router compares the received LSP against the list of LSPs that it already has. If the sequence number of newly arrived LSP is found lower than the highest sequence number in the list, the packet is simply discarded. Otherwise, the receiving router stores the new LSP and also forwards a copy of it through its neighbouring interfaces except the one through which the LSP has arrived.
- **Computing New Routes:** After receiving all LSPs, the next step for a router is to compute the shortest path to every possible destination using the Dijkstra's algorithm (explained in **Q 17**) and build the routing table. The routing table of a router lists all the routers in the network, the minimum cost of reaching them and the next router in the path to which the packet should be forwarded.

21. Differentiate link state and distance routing vector algorithms.

Ans: The link state routing algorithm came after the distance vector routing algorithm and it offers many advantages over the previous one. Some of the differences between the two are as follows:

- The traffic generated due to routing process is less in link state routing as compared to the distance vector routing. The reasons for this difference are as follows:

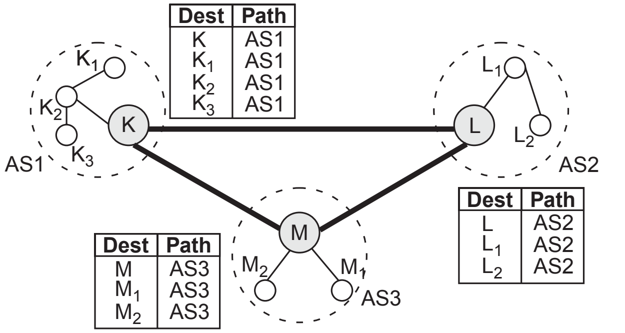
- The HELLO messages exchanged between adjacent routers are much smaller in size than the vectors in the distance vector routing. The LSPs of the link state routing contain information only about the neighbours, while the distance vectors include the net IDs of all the routers in the network.
- In link state routing, the LSPs are exchanged between neighbours after every 30 min, while in distance vector routing, the vectors are exchanged after a comparatively very small period (for example, 30 s in RIP).

- ❑ In link state routing, the optimal paths are calculated by each router independently. However, in distance vector routing each router depends on its neighbour for updating its distance vector resulting in slow processing.
- ❑ Alternate routes are also possible in link state routing but in distance vector routing only specific routes are used.
- ❑ Multiple cost metrics can be used in link state routing and the optimal paths can be computed with respect to each metric separately. Further, packets can be forwarded based on any one metric.

22. Explain the path vector routing protocol.

Ans: Path vector routing is an interdomain routing protocol, which is used between various autonomous systems (ASs). In every AS, there is one node (can be more, but only one is considered here) which acts on behalf of the whole system. This node is known as the **speaker node**. It creates the routing table for its AS and announces it with the speaker nodes residing in the neighbouring ASs. Path vector routing is similar to that of distance vector routing; however, here only the speaker nodes in ASs can communicate with each other. In the advertised tables, only the path is shown excluding the metric of the nodes.

To understand path vector routing, consider three ASs, AS1, AS2 and AS3 with K, L and M as the speaker nodes, respectively (Figure 10.17). The path vector routing works in various phases, which are as follows:



Dest	Path
K	AS1
K$_1$	AS1
K$_2$	AS1
K$_3$	AS1

Dest	Path
L	AS2
L$_1$	AS2
L$_2$	AS2

Dest	Path
M	AS3
M$_1$	AS3
M$_2$	AS3

Figure 10.17 Initial Routing Tables in Path Vector Routing

- ❑ **i nitialization:** Initially, the speaker nodes know only how to reach the nodes inside their own autonomous system. Thus, each speaker node initializes its routing table with an entry per each node that resides in its own network. For example, the routing table of node K shows that the nodes K$_1$, K$_2$ and K$_3$ are located in AS1 and can be reached through K. The routing tables of L and M are also initialized in the same way.
- ❑ **s haring:** After the routing tables have been initialized, they are shared between the speaker nodes of all ASs. For example, the node K shares its table with L and M providing the routing information inside AS1. Similarly, node L and M also share their routing tables.

- **Updating:** When a routing table is received by a speaker node, it updates its routing table by adding the nodes that are not present in its own routing table along with the path to reach them (Figure 10.18). After updating the table, each speaker node knows how to reach every node in other ASs. For example, if node K receives a packet for node K_2, it knows that the path is in AS1. However, if it receives a packet for M_2, it knows that it has to follow the path AS1-AS3.

K's routing table

Dest	Path
K	AS1
K_1	AS1
K_2	AS1
K_3	AS1
L	AS1-AS2
L_1	AS1-AS2
L_2	AS1-AS2
M	AS1-AS3
M_1	AS1-AS3
M_2	AS1-AS3

L's routing table

Dest	Path
K	AS2-AS1
K_1	AS2-AS1
K_2	AS2-AS1
K_3	AS2-AS1
L	AS2
L_1	AS2
L_2	AS2
M	AS2-AS3
M_1	AS2-AS3
M_2	AS2-AS3

M's routing table

Dest	Path
K	AS3-AS1
K_1	AS3-AS1
K_2	AS3-AS1
K_3	AS3-AS1
L	AS3-AS2
L_1	AS3-AS2
L_2	AS3-AS2
M	AS3
M_1	AS3
M_2	AS3

Figure 10.18 Routing Tables After Updating

23. l ist some advantages of path vector routing.

Ans: The path vector routing is an interdomain routing protocol that offers certain advantages. Some of these advantages are as follows:

- **l oop Prevention:** Path vector routing avoids the creation of loops in a path. Whenever a router receives a message, it determines whether or not its own AS is in the path list to destination. If so, looping tends to occur in which case the message is ignored.
- **Policy Routing:** The path vector routing can implement the policy routing easily. Whenever a router receives a message, the path of its AS is checked. If any of the ASs listed in the path is against its policy then that path and destination are ignored. This path is also not included in the routing table and the message is not forwarded.
- **o ptimum Path:** The optimum path is the path that is best for the organization. Path vector routing only shows the path and does not include the metrics involved in the path as different ASs may use different metrics. Optimal path does not mean only the shortest path, several other measures like security, safety and reliability are also taken into account while determining optimal path.

24. Explain in the following routing protocols.

(a) RiP

(b) os PF

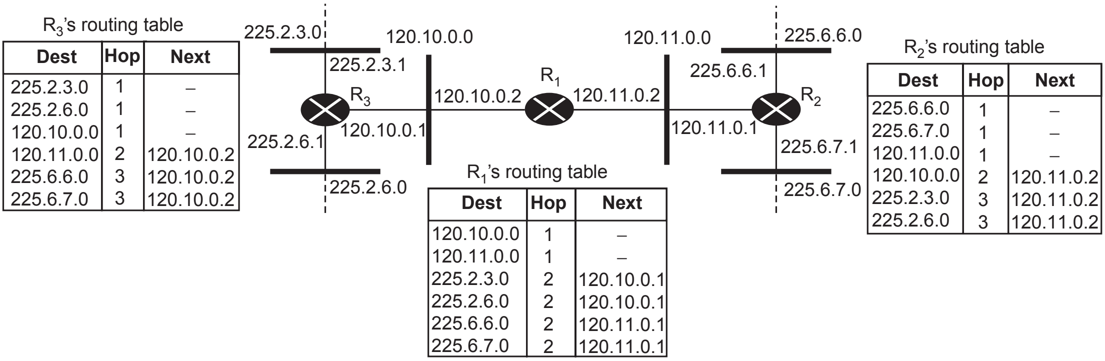
(c) BGP

Ans: (a) RiP: Routing information Protocol (**RiP**) is an intradomain routing protocol (also known as **interior gateway protocol**) which is used inside an autonomous system. It is a simple protocol whose operating procedures are similar to the widely used distance vector routing. The operation of RIP is based on certain considerations, which are as follows:

- RIP is used in autonomous systems, which consists of routers and networks (links). Routing tables are created for the routers but the networks do not implement any such table.

- As the first column of a routing table specifies a destination and in case of RIP, the destination is the network; therefore, a network address is defined in the first column of the R routing table.
- The metric used by RIP is the hop count where the term hop defines the number of subnets traversed from the source router to the destination subnet with including the destination subnet.
- The maximum cost of a path in RIP cannot be more than 15, that is, any route in an autonomous system cannot have more than 15 hops.
- The next-node column in the routing table of RIP contains the address of the router to which the packet is to be forwarded (the first hop to be done)

Consider an autonomous system consisting of six networks and three routers as shown in Figure 10.19. Each router has its own routing table showing how to reach each network existing in the AS. Let us study the routing table of one of the router, say R_1. The networks 120.10.0.0 and 120.11.0.0 are directly connected to the router R_1; therefore, R_1 need not make any hop count entries for these networks. The packets destined for both these networks can be sent directly by the router; however, such forwarding cannot be done in the case of the other networks. For example, if the router R_1 needs to send packets to the two networks to its left, then it has to forward the packets to the router R_3. Thus, for these two networks, the next-node column of the routing table stores the interface of router R_2 with the IP address 120.10.0.1. Similarly, if R_1 has to send packets to two networks to its right, then it has to forward packets to the router R_2. Thus, for these two networks, the next-node entry of routing table is the interface of router R_2 with IP address 120.11.0.1. The routing tables of other routers can also be explained in the same way.



R_3's routing table

Dest	Hop	Next
225.2.3.0	1	–
225.2.6.0	1	–
120.10.0.0	1	–
120.11.0.0	2	120.10.0.2
225.6.6.0	3	120.10.0.2
225.6.7.0	3	120.10.0.2

R_1's routing table

Dest	Hop	Next
120.10.0.0	1	–
120.11.0.0	1	–
225.2.3.0	2	120.10.0.1
225.2.6.0	2	120.10.0.1
225.6.6.0	2	120.11.0.1
225.6.7.0	2	120.11.0.1

R_2's routing table

Dest	Hop	Next
225.6.6.0	1	–
225.6.7.0	1	–
120.11.0.0	1	–
120.10.0.0	2	120.11.0.2
225.2.3.0	3	120.11.0.2
225.2.6.0	3	120.11.0.2

Figure 10.19 Example of a Domain Using RIP

(b) os PF: o pen s hortest Path First (**os PF**) is an intradomain routing protocol which works within an autonomous system. It is based on the link state routing algorithm. In OSPF, the autonomous system is divided into many areas so that the routing traffic can be handled easily. Each area is formed by the combination of networks, hosts and routers within an autonomous system and is assigned a unique identification number. The networks residing in an area must be connected to each other. The routers inside an area function normally, that is, periodically updating the area with routing information.

In OSPF, there are two types of routers, namely, *area border router* and *backbone router*. The **area border router** is situated at the boundary of each area and it shares the information about its area with the other areas. The **backbone router** is situated in a special area (called the **backbone area**) among all the areas inside an autonomous system. The backbone is considered as a primary area and all the other

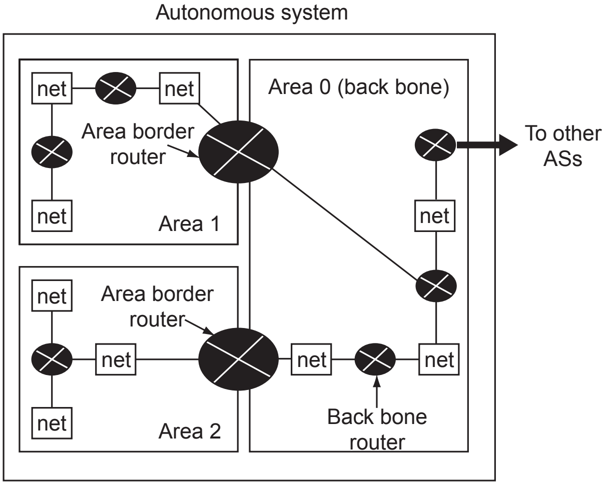


Figure 10.20 Areas in an Autonomous System

areas are connected to it. The backbone routers can also function as area border routers. Figure 10.20 depicts the idea of an OSPF protocol.

Like every other routing protocol, in OSPF also, there is a cost associated with each route known as **metric**. This metric may depend upon the type of service such as minimum delay, minimum hop count or maximum throughput and there may be multiple routing tables with each based on a different type of service.

The connections in OSPF are known as **links**. In OSPF, four types of links have been identified: *point-to-point*, *transient*, *stub* and *virtual*.

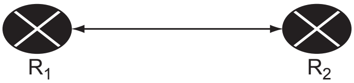


Figure 10.21 Point-to-Point Link

- **Point-to-Point link:** This link defines a direct connection between the routers. It can be represented as a graph where the nodes of the graph represent routers while the bidirectional arrows connecting the nodes represent the link between the routers (Figure 10.21).
- **t ransient link:** This link defines a network to which multiple routers are attached. In this type of network, each router has many neighbours all linked through a common network. The data can enter the network through any of the routers and leave the network through any of the routers. For example, consider an Ethernet network consisting of six routers R_1, R_2, R_3, R_4, R_5 and R_6 [Figure 10.22(a)]. To represent transient link graphically, the network is represented as a node, which is connected directly to all other nodes [Figure 10.22(b)].

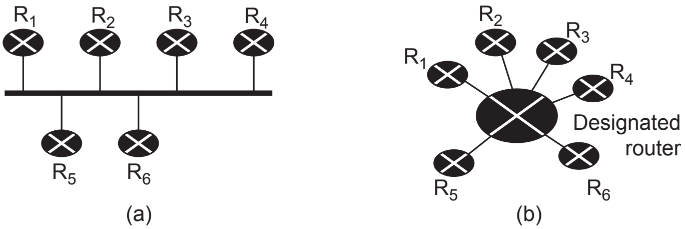


Figure 10.22 Transient Link and its Graphical Representation

- ❑ **s tub link:** This link is a special case of transient link, which defines a network with only one router connected to it [Figure 10.23(a)]. The packets enter and leave the network using this single router. Graphically, it can be represented using the designated router for the network and the router as a node [Figure 10.23(b)]. The link is only unidirectional from the router to the network.

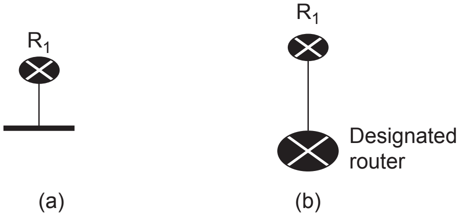


Figure 10.23 Stub Link and its Graphical Representation

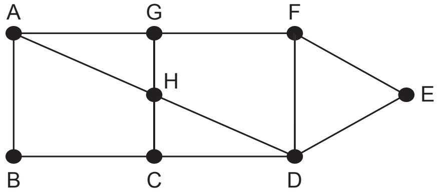
- ❑ **Virtual link:** When the link between two routers is broken, a new link has to be established by the administrator, which is known as virtual link. This link may use a longer path covering more number of routers.

(c) BGP: Border Gateway Protocol (**BGP**) is an interdomain routing protocol, which came into existence in 1989. It is implemented using the concept of path vector routing. As BGP works between the different ASs, it is an exterior gateway routing protocol. It follows certain policies to transfer packets between various types of ASs and these policies are to be configured manually in each BG router.

In BGP, the ASs are divided into three categories, namely, *stub AS*, *multihomed AS* and *transit AS*. The **stub As** has a single connection with any other AS. The data traffic can either originate or terminate at a stub AS, that is, a stub AS is either a source or a sink; however, data traffic cannot pass through it. The **multihomed As** can have multiple connections with other ASs, that is, it can send data to more than one AS and receive also from many. However, still it is a sink or source as it does not allow data traffic to pass through it. The **transit As** is also a multihomed AS except that it allows third-party traffic to pass through it.

Each BGP router maintains a routing table that keeps track of the path being used by the BGP router. The routing information is exchanged periodically between the routers in a session, referred to as **BGP session**. Whenever a BGP router needs to exchange the routing information with its neighbour, a transmission control protocol (TCP) connection is established between the two, which indicates the start of session. Using TCP connection provides a reliable communication between the routers. However, the TCP connection used for BGP is not permanent and it is terminated as soon as some unusual event occurs.

To understand the BGP operation, consider a set of BGP routers shown in Figure 10.24. Let the router `H` uses the path `HDE` to travel to `E`. When the neighbours of `H` provide routing information, they give their complete paths to reach `E`. After receiving all the paths, `H` examines which one will be the optimal path for going to `E`. The path originating from A is discarded as it passes through `H`. The choice now has to be made between `G`, `C` and `D`. To select from `G`, `C` and `D`, BGP uses a scoring function that is responsible for examining the available routes to a destination and scoring them, returning a number indicating the distance of each route to that destination. After the paths have been scored, the one with the shortest distance is selected. As the path `DE` has the shortest distance, it is selected.



Information received by H:

From C: “CDE”
From D: “DE”
From A: “AHDE”
From G: “GFE”

Figure 10.24 A Set of BGP Routers Along with Routing Information for H

BGP solves the count-to-infini y problem previously encountered in the distance vector routing algorithm. To understand how it happens, suppose D crashes and the line HD goes down. When H receives routing information from the remaining working neighbours A, C and G, it finds the new routes to E as GFE, AHGFE and CHGFE, respectively. The route GFE is selected as the other two pass through H itself. Thus, the new shortest path for H to reach E is HGFE via G.

25. Explain unicast and multicast routing.

Ans: Unicast and multicast routing are the techniques of routing based on the network structure. These are explained as follows:

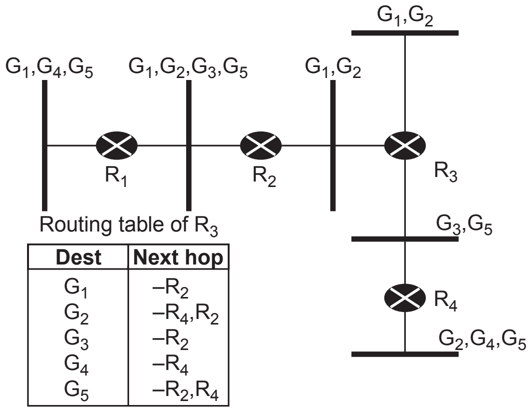
Unicast Routing

In unicast communication, there is only one source and one destination, that is, one-to-one connection. The data packets are transferred between the source and the destination using their unicast addresses. The packets go through various routers to arrive at their destination. Whenever a packet arrives at the router, the shortest path to the intended destination has to be found. For this, the router checks its routing table to find out the next hop to which the packet should be forwarded in order to reach the destination through the shortest path. If a path is not found in the table, the packet is discarded; otherwise, the packet is forwarded only through the interface specified in the routing table

Multicast Routing

In multicast communication, there is one source and many destinations. The communication is one-to-many communication, that is, the packets are forwarded to one or more destination addresses defined altogether by a group address. Whenever a router receives a packet destined for a group address, it forwards the packet through its many interfaces so that the packet could reach to all destinations belonging to that group. To forward a single packet to a group address, the router needs to create a shortest path tree per each group. This makes the multicast routing complex, as N shortest path tree need to be created for N groups. To resolve the complexity, two approaches including *source-based tree* and *group-shared tree* can be used to construct the shortest path tree.

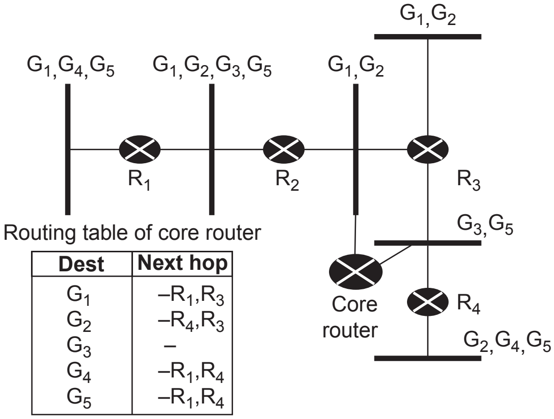
- **s ource-based t ree:** In this approach, each router constructs a shortest path tree for each group, which defines the next hop for each network containing the members for that group. For example, consider Figure 10.25 in which there are five groups G_1, G_2, G_3, G_4 and G_5 and four routers R_1, R_2, R_3 and R_4. The group G_1, G_2 and G_5 has its members in four networks while the group G_2 and G_3 in two networks. Each router is required to construct five shortest path trees, one per each group and having the shortest path entries in its routing table. Figure 10.25 shows a multicast routing table maintained by the router R_3. Now, suppose the router R_3 receives a packet destined for group G_5. Then, it forwards the copy of a packet to router R_2 and R_4. Further, router R_2 forwards the copy of a packet to router R_1. This process continues and eventually, the packet reaches each member of G_5 in the whole network. The problem with this approach is the complexity of routing table, which may have thousand of entries in case of large number of groups.



Dest	Next hop
G_1	$–R_2$
G_2	$–R_4,R_2$
G_3	$–R_2$
G_4	$–R_4$
G_5	$–R_2,R_4$

Figure 10.25 Source-based Tree Approach

- ❑ **Group-shared t ree:** This approach overcomes the problem of source-based approach, as each router is not required to construct shortest path for each group. Rather, one router is designated as the **core** (or **rendezvous**) and only it is responsible for having N shortest paths in its routing table for N groups, one per each group. Whenever a router receives a packet containing a group address, it encapsulates the packet into a unicast packet and forwards it to the core router. The core router then extracts the multicast packet and checks its routing table to determine the route for the packet. Figure 10.26 shows the core router and its routing table.



Dest	Next hop
G_1	$–R_1,R_3$
G_2	$–R_4,R_3$
G_3	–
G_4	$–R_1,R_4$
G_5	$–R_1,R_4$

Figure 10.26 Group-shared Tree Approach

26. Write a short note on internetworking.

Ans: internetworking refers to the interconnection of many different networks. There exist many different networks like LAN, MAN and WAN using different protocols and design. When users existing in these different networks need to communicate with each other, internetworking has to be implemented.

Internetworking not only allows these users to communicate with each other, but to access each other's data also. The communication between users is carried through transfer of packets. To transfer packets from one network to another, internetworking devices such as routers, transport gateways and application gateways are used at the junction between two networks. These devices help in converting the packets in a format accepted by the network to which the packets are to be transferred.

27. Explain the concept of tunnelling with respect to internetworking.

Ans: Consider two hosts A and B residing in the same type of networks (say, TCP/IP-based Ethernet LAN) and connected via a different type of network (say, a non-IP WAN) in between the two similar networks. Now, if A and B wish to communicate with each other, they can do so using the technique named as **tunnelling**, which implements internetworking.

To send a packet to host B, the host A creates an IP packet containing the IP address of the host B. The IP packet is then put in an Ethernet frame addressed to the multiprotocol router residing in A's network and eventually, put on the Ethernet. When the multiprotocol router on A's network receives the frame, it removes the IP packet and inserts it in the payload field of the WAN network layer packet. The packet is now addressed to the WAN address of the multiprotocol router residing in B's network. After the packet reaches to the multiprotocol router on B's network, it removes the IP packet from the Ethernet frame and sends to the host B in the local network inside an Ethernet frame. The host B then extracts the IP packet from the Ethernet frame and uses it. Figure 10.27 shows the communication between host A and B.

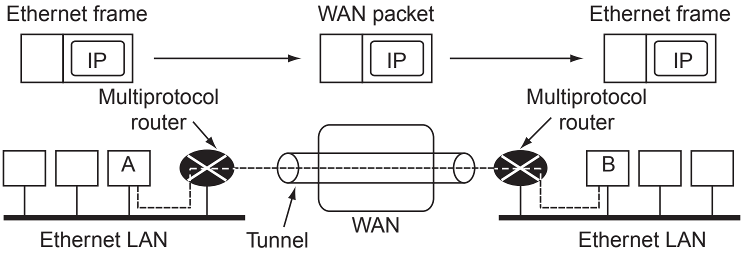


Figure 10.27 Tunnelling

Here, the WAN situated in between acts as a big tunnel connecting both the multiprotocol routers. The IP packet and the communicating hosts know nothing about the WAN architecture. Only the multiprotocol routers need to understand the IP and WAN packets. In effect, the distance from the middle of one multiprotocol router to another is like a tunnel that carries IP packets without any obstruction.

28. What is congestion? Why do we need congestion control?

Ans: **Congestion** is a situation that occurs in a network when the number of packets sent to the network is far more than its capacity. It results in increased traffic in the network layer and as a consequence, the TCP segments start getting lost as they pass through the network layer. Since TCP follows retransmission policy in case of lost or delayed segments, the congestion problem is further aggregated due to retransmission of segments. The situation becomes even worse and the performance of network degrades rapidly. That is why congestion needs to be controlled.

29. What is congestion control? What are its categories?

Ans: Congestion control refers to the techniques and mechanisms used to prevent or remove congestion from the network. There are various ways that can be used to control the congestion all these ways are divided into two categories, namely, *open-loop* and *closed-loop* congestion control. The **open-loop** congestion control aims to prevent the congestion from occurring by using some policies. Either the source or destination handles the congestion. On the other hand, the **closed-loop** congestion control attempts to remove congestion after it has occurred. The closed-loop congestion control is further divided into two categories, namely, *implicit feedback* closed-loop congestion control and *explicit feedback* closed-loop congestion control. In **implicit feedback** algorithms, the source is required to detect the congestion by making certain observations such as monitoring the time needed for acknowledgement to come back. In contrast, in **explicit feedback** algorithms, whenever congestion occurs, the packets are sent back to the source from the point of congestion to indicate the congestion.

30. What are the prevention policies used by the congestion?

Ans: The open-loop congestion control method adopts certain policies to prevent the congestion. Some of these policies are described as follows:

- **Retransmission Policy:** When the sent packets are damaged or lost then they need to be retransmitted; however, the retransmission usually results in more congestion in the network. Thus, a reliable retransmission policy needs to be implemented to prevent the congestion. The retransmission timers are introduced to check, how fast the sender sends the data at a particular time. Both the retransmission policy and timers are designed in such a way that efficiency is optimized with preventing the congestion.
- **Acknowledgement Policy:** Congestion may be affected by the acknowledgement policy used by the receiver, as acknowledgements are also a part of the network. Thus, if the receiver does not send an acknowledgement for every packet, it helps to reduce the congestion. Moreover, the receiver may decide to send acknowledgement only for specific packets or only when it is having packets to send or when the timer expires. All these factors result in less traffic in the network and thus, prevent congestion.
- **Discarding Policy:** A reliable discarding policy can be implemented to prevent the congestion. For instance, the routers may start to discard packets when the network is not able to handle more packets, thus, preserving the integrity of transmission. If discarding policy is implemented correctly, then it is the best method to prevent the congestion; otherwise, it will make the situation worse.
- **Admission Policy:** This policy is used to prevent congestion in virtual-circuit networks. According to this policy, whenever a request for virtual connection arrives to a router/switch, it first determines the flow of data and other resources in the network before admitting the incoming data into the network. If there is congestion or even the possibility of congestion in the network, the router/switch denies the connection request.

31. What are the different mechanisms carried out to remove congestion?

Ans: After congestion has occurred in the network, it can be removed by implementing various mechanisms, some of which are described here.

Backpressure

Backpressure is a node-to-node congestion control technique where each node knows its immediate upstream node from which it is receiving the flow of data. When congestion occurs, the congested node rejects to receive any more data from its upstream node. This makes the upstream node to become congested and thus, it also starts rejecting the data coming from its upstream node. Therefore, they drop all the data coming from the upper node. This procedure continues and eventually, the congestion information reaches the original source of flo , which may then slow down the flow of data. As backpressure begins with the node where congestion is detected first and propagates back to the source, this technique is a kind of explicit feedback algorithm.

Backpressure technique can be applied only in virtual circuit networks that support node-to-node connection. It was introduced in X.25, the first virtual-circuit network. However, this technique is not applicable for IP-based networks, as in such networks, a node does not know its upstream node.

Choke Packet

Choke packet is a control packet that is created by the congested node to inform the source about the congestion in the network. Unlike backpressure method, the choke packet is sent by the congested node directly to the source of flow rather than to the intermediate nodes. The source receiving the choke packet is required to reduce the rate of flow towards the router from where the choke packet has come.

An example of choke packet is the source quench message used in ICMP (discussed in **Chapter 11**). This message is sent by the router or destination node to ask the source to slow down the rate of sending traffic. The router sends a source quench message for every datagram it discards due to overloaded buffer.

Implicit Congestion Signalling

In this method, there is no communication between the source and the nodes where congestion has occurred. Rather, the source is required to determine the congestion in the network by observing certain things. For example, if the source after sending many packets still does not receive any acknowledgement, it may assume that there is congestion in the network and thus, reduce its rate of sending flo . This is called **implicit congestion signalling**. This method can be used in connection-oriented networks such as frame relay networks; however, it is more effective in connectionless networks such as packet-switching networks and IP-based networks.

Explicit Congestion Signalling

The explicit signalling method is used by a congested node to send information to the source or destination. It is different from the choke packet method. In the choke packet method, when congestion occurs, a separate packet signalling the congestion is sent to the source whereas in explicit signalling method, the signals are included in the packets carrying data. The explicit congestion signalling can work in two directions, namely, *backward signalling* and *forward signalling.* In **backward signalling**, a bit is set in the packet that is moving in a direction opposite to the congestion. This bit informs the source that there is congestion in the link and the traffic needs to be slow down to avoid the discarding of packets. In **forward signalling**, a bit is set in the packet that is moving in the direction of congestion. This bit informs the destination that there is congestion in the link and thus, the destination needs to adopt some policy such as reducing the speed of sending acknowledgements to remove the congestion.

32. Write a short note on load shedding.

Ans: It is one of the simple and effective closed-loop congestion control techniques. Whenever a router discovers congestion in the network, it starts dropping out the packets until the congestion disappears. To decide which packet to drop, it uses certain policies. The simplest but less efficient policy is to randomly pick up the packets to be dropped. Another complex but effective policy requires some cooperation from the sender side. This policy uses some kind of priorities among the packets. As some packets are more important than others, different priority classes are used to distinguish them from less important ones. At the time of congestion in the network, the packets from the lowest priority class are discarded first, then from the next lower class and so on. There is one more policy, which allows a host to break the agreement made when the network was set up. According to this policy, the host can use resources beyond its specified limit in order to deal with congestion. For example, host can increase its bandwidth more than the specified limit.

33. List the differences between congestion control and flo control.

Ans: The congestion control and flow control are distinct in some ways that are as follows:

- In congestion control, the whole network traffic (containing many nodes) is checked for congestion, while in flow control, the point-to-point traffic is checked for smooth functionin
- The congestion control involves many hosts, routers, connections while transferring the data, whereas in flow control only sender and receiver interact with each othe .
- In congestion control, when the network is unable to handle the load, packets are dropped to remove the congestion. However, in flow control, when the receiver is unable to absorb more data, it informs the sender to slow down the speed of sending data.

34. Write a short note on hop-by-hop choke packets.

Ans: The hop-by-hop choke packet method is an improvement over choke packet method. In choke packet method, at the time of congestion, the choke packets are sent directly to the source from congested node. However, until the time choke packets reach the source, many data packets will have already been sent out from the source and still have to be dealt with. Thus, the choke packet method is not desirable at high speeds or over long distances. In such cases, hop-by-hop choke packet method is preferred. In **hop-by-hop choke packet** method, not only the source node but also each intermediate node receiving the choke packet gets affected, thus, reducing the traffic between the intermediate nodes as well as the source.

To understand how hop-by-hop choke packet method works, consider the subnet shown in Figure 10.28(a). Here, the data is being sent from the node `P` to node `R` via path `PTSR` [Figure 10.28(b)]. Now, suppose the node `R` runs out of buffers and thus, sends a hop-by-hop choke packet to `P` via path `RSTP`. As the packet reaches from `R` to `S`, it informs the node `S` to slow down the speed of sending data packets to `R`. However, as `S` is still receiving the data packets, it has to include more buffers to accommodate the packets. This puts more demand on `S` but makes `R` congestion free [Figure 10.28(c)]. Thus, `S` forwards the choke packet to `T`, which informs `T` to reduce its speed of sending data packets to `S`. This puts more demand on `T` but makes `S` congestion free [Figure 10.28(d)]. Finally, the choke packet reaches `P` and the traffic flow is reduced [Figure 10.28(e)]. This mechanism makes all the nodes congestion free. Thus, the congestion is controlled and that too without losing any packets.

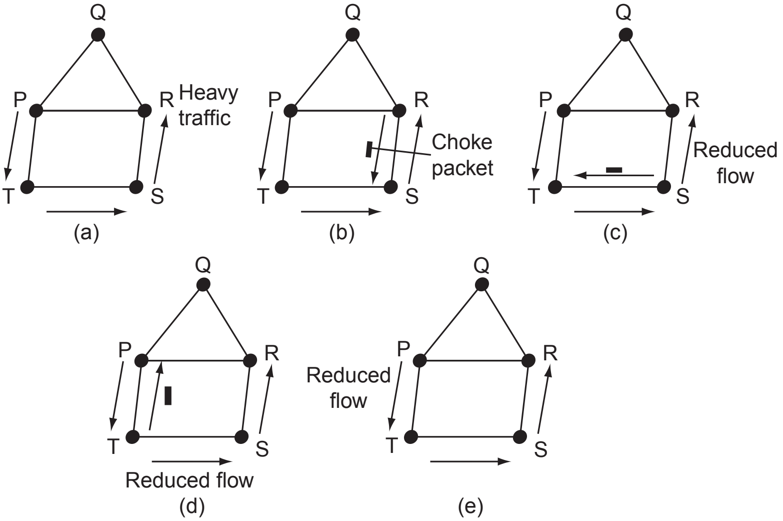


Figure 10.28 Hop-by-Hop Choke Packet Method

35. Find the class of each of the following address.

(a) 00000001 00001011 00001011 11101111

(b) 11000001 10000011 00011011 11111111

(c) 14.23.120.8

(d) 252.5.15.111

Ans: **(a)** As the first bit of the address is 0, it is a class A address.

(b) As the first two bits of the address are one and the third bit is zero, it is a class B address

(c) As the first byte of the address is 14 (between 0 and 127), it is a class A address.

(d) As the first byte of the address is 252 (between 240 and 255), it is a class E address

36. Why the largest octet in an Internet address is 255?

Ans: Each octet in an IP address consists of 8 bits, each of which can be either 0 or 1. The largest value that can be expressed in 8 bits is 11111111, that is, 255. That is why the largest octet in an IP address is 255.

37. Given the following i P addresses,

(a) 32.46.7.3

(b) 200.132.110.35

(c) 140.75.8.92

determine (i) class, (ii) network address, (iii) mask and (iv) broadcast address for each.

Ans: **(a)** Given IP address = 32.46.7.3

(i) As the first byte of this address is 32 (between 0 and 127), it is class A address.

- **(ii)** Since it is class A address, its first byte (that is, 32) denotes the net ID. To obtain the network address, the host ID bits are made zero. Thus, the network address is 32.0.0.0
- **(iii)** Being a class A address, the mask for this address is 255.0.0.0.
- **(iv)** The broadcast address is obtained by keeping the net ID of the address same and replacing each byte of host ID with 255. Thus, the broadcast address is 32.255.255.255.

(b) Given IP address = 200.132.110.35

- **(i)** As the first byte of this address is 200 (between 192 and 223), it a Class C address
- **(ii)** Since it is Class C address, its first three bytes (that is, 200.132.110) denote the net ID. To obtain the network address, the host ID bits are made zero. Thus, the network address is 200.132.110.0.
- **(iii)** Being a Class C address, the mask for this address is 255.255.255.0.
- **(iv)** The broadcast address is obtained by keeping the net ID of the address same and replacing each byte of host ID with 255. Thus, the broadcast address is 200.132.110.255.

(c) Given IP address = 140.75.8.92

- **(i)** As the first byte of this address is 140 (between 128 and 191), it a class B address
- **(ii)** Since it is class B address, its first two bytes (that is, 140.75) denote the net ID. To obtain the network address, the host ID bits are made zero. Thus, the network address is 140.75.0.0.
- **(iii)** Being a class B address, the mask for this address is 255.255.0.0.
- **(iv)** The broadcast address is obtained by keeping the net ID of the address same and replacing each byte of host ID with 255. Thus, the broadcast address is 140.75.255.255.

38. The IP network 192.168.130.0 is using the subnet mask 255.255.255.224. What subnets are the following hosts on?

(a) 192.168.130.10

(b) 192.168.130.67

(c) 192.168.130.93

(d) 192.168.130.199

(e) 192.168.130.222

(f) 192.168.130.250

Ans: To determine which host is lying on which subnet, we need to determine the total number of subnets in the network, number of hosts in each subnet and the range of IP addresses assigned to each subnet. For finding the number of subnets and the number of hosts in each subnet, we need to know the number of masked and unmasked bits in the subnet mask, which can be found as follows:

Given, subnet mask = 255.255.255.224

The binary equivalent of host ID byte (that is, 224) is 11100000. Here, three bits are 1s while five bits are 0s. Thus, the number of masked bits (m) is 3 and the number of unmasked bits (n) is 5. Now, the number of subnets and the number of hosts in each subnet can be determined using the following formulas.

Number of subnets = 2^m

$\Rightarrow 2^3$

$\Rightarrow 8$

Number of hosts in each subnet = $2^n - 2$

$\Rightarrow 2^5 - 2$

$\Rightarrow 30$

Thus, there are eight subnets in the network with each subnet comprising 30 hosts. As the given IP network is 192.168.130.0, the range of IP addresses assigned to each subnet can be given as follows:

Range of first subne = 192.168.130.0 – 192.168.130.31

Range of second subnet = 192.168.130.32 – 192.168.130.63

Range of third subnet = 192.168.130.64 – 192.168.130.95

Range of fourth subnet = 192.168.130.96 – 192.168.130.127

Range of fifth subne = 192.168.130.128 – 192.168.130.159

Range of sixth subnet = 192.168.130.160 – 192.168.130.191

Range of seventh subnet = 192.168.130.192 – 192.168.130.223

Range of eighth subnet = 192.168.130.224 – 192.168.130.255

Notice that the first and last address of each range cannot be assigned to hosts. For example, in the first subnet, the addresses 192.168.30.0 and 192.168.130.31 cannot be used for the hosts

Now, we can find which host lies on which network as given below

(a) The host 192.168.130.10 lies on the first subnet

(b) The host 192.168.130.67 lies on the third subnet.

(c) The host 192.168.130.93 lies on the third subnet.

(d) The host 192.168.130.199 lies on the seventh subnet.

(e) The host 192.168.130.222 lies on the seventh subnet.

(f) The host 192.168.130.250 lies on the eighth subnet.

39. What will be the subnet address if the destination address is 200.45.34.56 and subnet mask is 255.255.240.0?

Ans: Given, destination address = 200.45.34.56

Subnet mask = 255.255.240.0

Now, the subnet address can be determined by performing AND of destination address and the subnet mask.

The destination address and subnet mask can be written in binary notation as shown below:

11001000 00101101 00100010 00111000
11111111 11111111 11110000 00000000

On ANDing the both addresses, we get the following subnet address:

11001000 00101101 00100000 00000000

This subnet address can be written in dotted decimal notation as:

200.45.32.0.

40. Given an IP address 156.36.2.58 with default mask 255.255.0.0/23. Determine its subnet mask in the event of subnetting.

Ans: Given IP address = 156.36.2.58
Default mask = 255.255.0.0/22

Here, /22 indicates that the first 22 bits of the subnet mask are 1s while the rest are 0s. Thus, the subnet mask is:

11111111 11111111 11111100 00000000

This subnet mask can be written in dotted decimal notation as 255.255.252.0.

Multiple choice questions

1. How many bits are allocated for the host ID in an IP address of class A?
   (a) 8 (b) 24
   (c) 48 (d) 16

2. Which class of IP address is used for multicasting?
   (a) class E (b) class B
   (c) class D (d) class M

3. Which class address is used to implement supernetting?
   (a) class D (b) class A
   (c) class C (d) class B

4. What is the maximum limit for hop count in RIP protocol?
   (a) 15 (b) 12
   (c) 25 (d) 10

5. Which of the following metrics is used in RIP?
   (a) delay (b) hop count
   (c) throughput (d) bandwidth

6. Which of the following is an interdomain routing protocol?
   (a) RIP (b) OSPF
   (c) BGP (d) none of these

7. Which protocol uses backbone router?
   (a) OSPF
   (b) RIP
   (c) BGP
   (d) all of these

8. ________ is a node-to-node congestion control technique where the congested node stops receiving data from the upstream nodes.
   (a) backpressure
   (b) choke packet
   (c) implicit congestion
   (d) explicit congestion

9. Which of the following belongs to explicit feedback closed-loop congestion control?
   (a) choke packet
   (b) hop-by-hop choke packet
   (c) backpressure
   (d) all of these

10. Which of the following is not a prevention policy used for congestion?
    (a) retransmission policy
    (b) discarding policy
    (c) acknowledgement policy
    (d) error control policy

Answers

1. (b) 2. (c) 3. (c) 4. (a) 5. (b) 6. (c) 7. (a) 8. (a) 9. (d) 10. (d)

11

Quality of Service and Protocols

1. What is meant by quality of service? What are its characteristics?

Ans: A stream of packets being transmitted from the source node to destination node is referred to as the **flow**. Each flow is characterized by a certain set of performance parameters such as reliability, jitter, delay and bandwidth. The ability of a network to deliver the flow of packets to the destination node with the defined set of performance parameters is defined as its **quality of service** (**QoS**). The characteristics that a flow seeks to attain are as follows

- **Reliability:** This characteristic ensures that no packet is damaged or lost during the transmission and all packets are received at the destination correctly. If the flow does not attain reliability then retransmission needs to be done. Reliability can be achieved by applying checksum to each packet at the sender's end and then verifying it at the receiver's end. Some applications such as e-mail, remote login require high reliability while others such as telephony and video-on-demand are less sensitive to reliability.
- **Delay:** This characteristic slows down the flow of transmitted packets that are needed to be received by the destination node. Like reliability, delay requirements also depend on the type of the application used. In case of file transfer applications such as e-mail, if packets are delayed by a few seconds then it cannot cause any harm. However, if the delay occurs in real-time applications such as telephony, then the users will not be able to understand each other's conversation. Thus, for such applications, delay should be the least.
- **Jitter:** This characteristic defines the variation in delay of packets that correspond to the same flow. If the delay between successive packets is constant, then there is no harm but if the packets are received with irregular time intervals between them, the result may be unacceptable. Video and audio applications are highly sensitive to jitter while applications such as e-mail and file transfer have less stringent requirements with respect to jitter.
- **Bandwidth:** This characteristic defines the number of bits that can be delivered per second. Different applications have different bandwidth requirements. For example, in e-mail applications, bandwidth consumption is less as number of bits transmitted is not much but in the case of video conferencing, more bandwidth is utilized as number of bits to be transmitted is in millions.

2. What are the four general techniques to improve the QoS?

Ans: The QoS can be improved by using the four techniques, namely, *scheduling*, *traffic shaping*, *resource reservation* and *admission control*.

- **Scheduling:** This technique schedules the arrival of packets from different flows so that packets can be processed in an appropriate manner by the router or switch. Some scheduling techniques to improve the QoS are as follows:
  - **FIFO Queuing:** In this technique, packets are scheduled based on First-In-First-Out (FIFO) method. A queue is maintained by the router or switch in which packets wait for their turn to get processed. Each incoming packet is appended to the queue if there is space in the queue. The packet, which enters the queue, first, is processed first. If the queue is filled, then the new packets are discarded until some space is freed up in the queue.
  - **Priority Queuing:** In this scheduling, each packet is assigned a priority class and a separate queue is maintained for each priority class. The packets in the queue of the highest priority class are processed first while packets in the queue of the lowest priority class are processed last. Thus, this technique processes the higher-priority packets with less delay. However, the demerit of this technique is that low-priority queue packets will not be processed if there is a continuous flow of packets in high-priority queues. This situation is referred to as **starvation** of low-priority packets.
  - **Weighted Fair Queuing:** In this technique, weights are assigned to different priority classes such that higher-priority queues get higher weight and the lower-priority queues get the lower weight. The weight assigned to a queue indicates the number of packets that will be processed from the queue. For example, consider three queues Q_1, Q_2 and Q_3 with priorities 1, 2 and 3 and weights assigned are 4, 1 and 2, respectively. Initially, four packets will be processed from the Q_1; then, one packet will be processed from Q_2 and finally, two packets from Q_3.
- **Traffic Shaping:** It is a technique that improves the QoS by managing the amount of traffic, which is to be sent to the network. This technique tries to make the traffic flow at the uniform data rate, resulting in less congestion and improved QoS. The flow of traffic is regulated by monitoring the traffic flow during the connection period what is referred to as **traffic policing**. If a packet in a stream does not obey the policy, then it is penalized by either discarding it or by assigning low priority. There are two traffic-shaping techniques, namely, *leaky bucket* and *token bucket* (discussed later) used to improve the QoS.
- **Resource Reservation:** This technique reserves the resources required for a flow beforehand when a specific route to reach the destination node has been decided. The three kinds of resources that are normally reserved for the flow include bandwidth, buffer space and central processor unit (CPU) cycles. The reservation of bandwidth enables the flow to reach the destination node more effectively. For example, if a flow requires 2 Mbps and the capacity of outgoing line is 5 Mbps then reserving 2 Mbps for one flow will effectively work but trying to direct three flows through the line will lead to more congestion. The buffer space must be reserved at the destination side so that a specific flow does not compete with other flows for being placed in the queue. This is because if the buffer space is not available, then the packets have to be discarded which may degrade the QoS. The CPU cycles also need to be reserved, as the router takes some CPU time to process each packet and also, it can process only a few numbers of packets per second. Thus, for effective and timely processing of each packet, the CPU must not be overloaded.
- **Admission Control:** This technique is used by the router or switch to decide whether to accept or reject the incoming flow. The decision to accept or reject the flow is made based on certain parameters

such as bandwidth, buffer cycles, CPU cycles and packet size. The set of these parameters is referred to as **flow specification**. Whenever a flow comes to a router, the router checks the flow specification to determine whether it can handle the incoming flow. To determine this, the router checks its current buffer size, bandwidth and CPU usage. It also checks its prior commitments made to other flows. The flow is accepted only after the router becomes sure that it can handle the flow.

3. Explain the leaky bucket algorithm.

Ans: The leaky bucket algorithm is a traffic-shaping technique that is used to control the congestion in a network. It was proposed by Turner in 1986 that used the concept of a **leaky bucket**—a bucket with a hole at the bottom. The water is pouring into the bucket and it is leaking continuously. However, the rate of leakage is always constant irrespective of the rate of water pouring into the bucket. This process continues until the bucket is empty. If the bucket is overflowed, then additional water falls through the sides of bucket but leakage rate will always be constant. Turner applied the same idea to packets transmitted over the network and therefore, the algorithm was named as leaky bucket algorithm. This algorithm smooths out the bursty traffic by storing bursty chunks of packets in the leaky bucket so that they can be sent out at a constant rate.

To understand the leaky bucket algorithm, let us assume that network has allowed the hosts to transmit data at the rate of 5 Mbps and each host is connected to the network through an interface containing a leaky bucket. The leaky bucket enables to shape the incoming traffic in accordance with the data rate committed by the network. Suppose the source host transmits the bursts of data at the rate of 10 Mbps for the first three seconds, that is, a total of 30 Mbits of data. After resting for 3 s, the source host again transmits the bursts of data at the rate of 5 Mbps for 4 s, that is, a total of 20 Mbits. Thus, the total amount of data transmitted by the source host is 50 Mbits in 10 s. The leaky bucket sends the whole data at the constant rate of 5 Mbps (that is, within the bandwidth commitment of the network for that host) regardless of the rate arrived from the source node. If the concept of leaky bucket was not used, then more bandwidth would be consumed by the starting burst of data, leading to more congestion.

The leaky bucket algorithm is implemented by maintaining a FIFO queue to hold the arriving packets. The queue has a finite capacity. Whenever a packet arrives, it is appended at the end of queue if there is some space in queue; otherwise, the packet is discarded (Figure 11.1). If each packet is of fixed size, then a fixed number of packets are removed from the queue per each clock tick. However, if packets are of variable sizes, a fixed number of bytes (say, `p`) are removed from the queue per each clock tick. The algorithm for variable size packets is as follows:

1. A counter is initialized to `p` at the tick of the clock.
2. If packet size is smaller than or equal to `p`, the packet is sent and value of counter is decremented by the packet size.
3. Repeat step 2 until `p` becomes smaller than the packet size.
4. Reset the counter and go back to step 1.

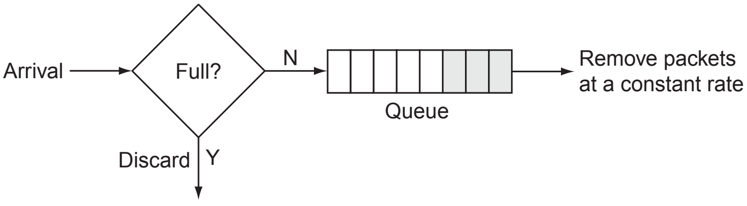


Figure 11.1 Leaky Bucket Implementation

4. Explain token bucket algorithm.

Ans: The token bucket algorithm is a traffic-shaping technique used to control the congestion in the network. Though it is a variation of leaky bucket algorithm, it is more flexible as it allows the output to go at the higher rate when a large burst of traffic arrives in the bucket rather than persisting with the constant output rate. Moreover, it takes into account the time for which a host remains idle so that the idle hosts could take benefit in the future. For this, the system generates many tokens (say, `n`) per each clock tick and these tokens are fed into the bucket. The token are added to the bucket as long as there is a space in the bucket. For transmitting each packet, one token is removed from the bucket and is destroyed. Now, if some host remains idle for 50 clock ticks and the system sends 20 tokens per each clock tick then there will be 1,000 (50*20) tokens in the bucket of idle host. When host becomes active, either it can transmit 1,000 packets (one per each token) in a single clock tick or it can transmit 100 packets per each clock tick up to 10 clock ticks or any other way thereby sending the bursty traffic

The token bucket algorithm is implemented by the counter to count tokens. The counter variable is incremented by one each time a token is added in the leaky bucket and is decremented by one each time a packet is transmitted. If the counter value becomes zero then the host cannot send any further packets.

The performance of token bucket algorithm is measured by the burst time (S) which is given as

$$S = C/(M - P)$$

where C is the token bucket capacity in bytes, M is the maximum output rate in bytes/s and P is the token arrival rate in bytes/s.

5. Distinguish between leaky bucket algorithm and token bucket algorithm.

Ans: Though both leaky bucket and token bucket are traffic-shaping techniques that smooth out the traffic between routers and regulate output from nodes, still there are some differences between the two. These differences are as follows:

- Token bucket algorithm stores tokens up to the maximum size of the bucket if the node is not sending packet for some period of time, whereas in leaky bucket algorithm no such storing of tokens happens.
- Token bucket algorithm can send large bursts of packets at once if needed but in leaky bucket algorithm, the output rate always remains constant.
- Token bucket algorithm never discards the packet but throws away the tokens not the packets if the bucket overflows, whereas in leaky bucket algorithm the packets are discarded when the bucket fills up
- Token bucket algorithm does not result in loss of data as node with the token bucket stops sending the packets if the router defines such a rule but in leaky bucket algorithm there is no such provision to prevent any data loss.

6. Write a short note on ARP.

Ans: **Address resolution protocol** (**ARP**) is a network layer protocol used to map an Internet protocol (IP) address (logical address) to its corresponding media access control (MAC) address (physical address). The mapping from logical to physical address can be of two types, namely, *static mapping* and *dynamic mapping*. In **static mapping**, each node on the network maintains a table that contains entries of IP addresses of all other nodes along with their corresponding MAC addresses. If any node knows the IP address of a particular node but does not know its MAC address then it can find the corresponding entry from the table. The disadvantage of static mapping is that as the physical address of a node may change, the table must be updated at regular intervals of time and thus, causing more overhead. On the other hand, in **dynamic mapping**, a protocol can be used by the node to find the other address if one is known. The ARP is based on dynamic mapping.

Whenever a host wishes to send IP packets to another host or router, it knows only the IP address of the receiver and needs to know the MAC address as the packet has to be passed through the physical network. For this, the host or router broadcasts an **ARP request packet** over the network. This packet consists of IP address and MAC address of the source node and the IP address of the receiver node. As the packet travels through the network, each node in between receives and processes the ARP request packet. If a node does not find its IP address in the request, it simply discards the packets. However, when an intended recipient recognizes its IP address in the ARP request packet, it sends back an **ARP response packet**. This packet contains the IP and MAC address of the receiver node and is delivered only to the source node, that is, ARP response packet is unicast instead of broadcast.

The performance of ARP decreases if every time the source node or router has to broadcast an ARP request packet to know the MAC address of the same destination node. Thus, to improve the efficienc , ARP response packets are stored in the cache memory of the source system. Before sending any ARP request packet, the system first checks its cache memory and if the system finds the desired mapping in it then the packet is unicasted to the intended receiver instead of broadcasting it over the network.

The format of ARP packet is shown in Figure 11.2.

The ARP packet comprises various fields, which are described as follows

- ❑ **Hardware Type:** It is a 16-bit long field that defines the type of the network on which ARP is running. For example, if ARP is running on Ethernet then the value of this field will be one. ARP can be used on physical network.
- ❑ **Protocol Type:** It is a 16-bit long field that defines the protocol used by ARP. For example, if ARP is using IPv4 protocol then the value of this field will be $(0800)_{16}$. ARP can be used with any protocol.
- ❑ **Hardware Length:** It is an 8-bit long field that defines the length of MAC address in byte

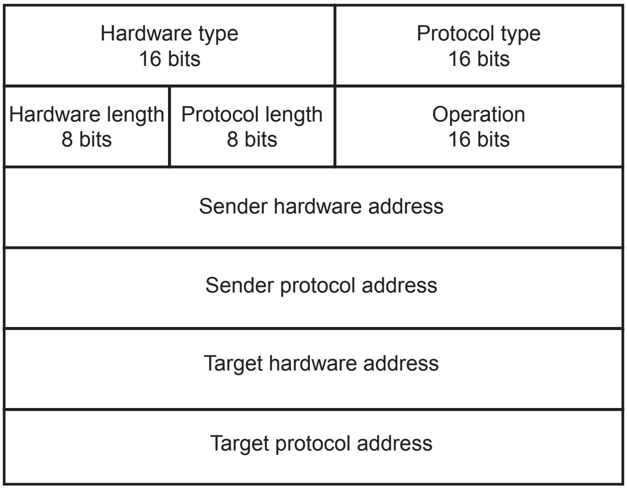


Figure 11.2 ARP Packet Format

- **Protocol Length:** It is an 8-bit long field that defines the length of address in bytes.
- **Operation:** It is a 16-bit long field that defines the type of packet being carried out. For ARP request packet, the value of this field will be one and for ARP response packet, the value will be two.
- **Sender Hardware Address:** It is a variable-length field that defines the MAC address of the sender node.
- **Sender Protocol Address:** It is a of variable-length field that defines the IP address of the sender node.
- **Target Hardware Address:** It is a variable-length field that defines the MAC address of the destination node. In case of an ARP request packet, the value of this field is 0s as the MAC address of the receiver node is not known to the sender node.
- **Target Protocol Address:** It is a variable-length field that defines the IP address of the destination node.

7. Write a short note on the following.

(a) RARP
(b) BOOTP
(c) DHCP

Ans:

(a) RARP: Reverse address resolution protocol, as the name implies, performs the opposite of ARP. That is, it helps a machine that knows only its MAC address (logical address) to find the IP address (logical address). This protocol is used in situations when a diskless machine is booted from read-only-memory (ROM). As ROM is installed by the manufacturer, it does not include the IP address in its booting information because IP addresses are assigned by the network administrator. However, MAC address of the machine can be identified by reading its NIC. Now, to get the IP address of the machine in a network, **RARP request packet** is broadcast to all machines on the local network. The RARP request packet contains the MAC address of the inquiring machine. The **RARP server** on the network that knows all the IP addresses sees this request and responds with a **RARP reply packet** containing the corresponding IP address to the sender machine.

The problem in using RARP protocol is that if there is more than one network or subnets then RARP server needs to be configured on each network as RARP requests are not forwarded by the routers and, thus, cannot go beyond the boundaries of a network.

(b) BOOTP: Bootstrap protocol is an application layer protocol designed to run in a client/server environment. The BOOTP client and BOOTP server can be on the same or different network. The BOOTP uses user datagram protocol (UDP) packets, which are encapsulated in an IP packet. A **BOOTP request packet** from a BOOTP client to BOOTP server is broadcast to all the nodes on the network. In case the BOOTP client is in one network and BOOTP server is on another network and two networks are separated by many other networks, the broadcast BOOTP request packet cannot be forwarded by the router. To solve this problem, one intermediary node or router, which is operational at the application layer, is used as a **relay agent**. The relay agent knows the IP address of the BOOTP server and when it receives a BOOTP request packet, it unicasts the BOOTP request packet to the BOOTP server by including the IP address of the server and of itself. On receiving the packet, the BOOTP server sends **BOOTP reply packet** to the relay agent, which further sends it to the BOOTP client.

A problem associated with BOOTP is that it is a static configuration protocol. The mapping table containing MAC and IP addresses is configured manually by the network administrator. Thus, a new node cannot use BOOTP until its IP and MAC address have been entered manually by the network administrator in the table.

(c) DHCP: Dynamic host control protocol supports both static and dynamic address allocation that can be done manually or automatically. Thus, it maintains two databases one for each allocation. In **static address allocation**, DHCP acts like BOOTP, which means that a BOOTP client can request for a permanent IP address from a DHCP server. In this type of allocation, DHCP server statically maps MAC address to IP address using its database. On the other hand, in **dynamic address allocation**, dynamic database is maintained by DHCP that contains the unused IP addresses. Whenever a request comes for an IP address, DHCP server assigns a temporary IP address to the node from the dynamic database using a technique called leasing. In this technique, the node requests the DHCP server to renew the IP address just before the time of using this IP address expires. If the request is denied by the DHCP server, then the node cannot use the same IP address that was assigned to it earlier.

Like BOOTP, DHCP also uses relay agent on each network to forward the DHCP requests. When a DHCP node requests for an IP address, the relay agent on network helps the request to unicast to the DHCP server. On receiving the request, the server checks its static database to find the entry of the requested physical address. If it finds the address, it returns the permanent IP address to the node; otherwise, it selects some temporary address from the available pool, returns this address to the host and also, adds this entry to the dynamic database.

8. Draw and discuss the IP datagram frame format. Discuss in detail the various fields

Ans: The Internet protocol version 4 (IPv4) is the most widely used internetworking protocol. In IPv4, the packets are termed as **datagrams** (a variable length packet). Further, IPv4 is a connectionless and unreliable datagram protocol; **connectionless** means each datagram is handled independently and can follow different paths to reach the destination; **unreliable** means it does not guarantee about the successfully delivery of the message. In addition, IPv4 does not provide flow control and error control except the error detection in the header of the datagram. To achieve reliability, the IP is paired with transmission control protocol (TCP), which is a reliable protocol. Thus, it is considered as a part of TCP/IP suite.

An IPv4 datagram consists of a header field followed by a data field. The header field is 20–60 bytes long and contains routing and delivery information. The header comprises various subfields (Figure 11.3), which are described as follows:

- **Version (VER):** It is a 4-bit long field, which indicates the version being used. The current version of IP is 4.
- **Header Length (HLEN):** It is a 4-bit long field, which defines the IPv4 header length in 32-bit words. The minimum length of IPv4 header is five 32-bit words
- **Service:** It is an 8-bit long field, which provides an indication of the desired QoS such as precedence, delay, throughput and reliability. This field is also called **type of service** (**ToS**) field
- **Total Length:** It is a 16-bit long field, which defines the total length (in bytes) of the datagram including header and data. The maximum permitted length is 65,535 (2^{16}–1) bytes with 20–60 bytes for header and rest for data.
- **Identification** It is a 16-bit long field, which uniquely identifies the datagram. The datagrams can be fragmented at the sender's end for transmission and then reassembled at the receiver's end.

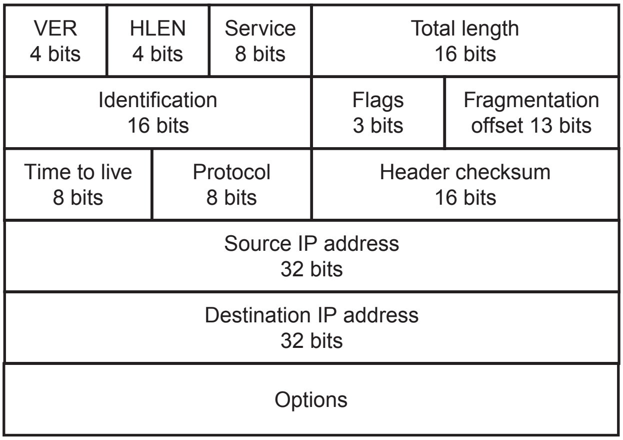


Figure 11.3 IPv4 Datagram Header Format

When a datagram is fragmented into multiple datagrams, all datagrams belonging to the same datagram are labelled with same identification number and the datagrams having same identification number are reassembled at the receiving side.

- **Flags:** It is a 3-bit long field in which the first bit is reserved and always zero, the second bit is do not fragment (DF) and the third bit is more fragment (MF). If DF bit is set to 1 then it means the datagram must not be fragmented while a value of zero indicates the fragmentation of the datagram. If MF bit is set to zero, then it means this fragment is the last fragment. However, if MF bit is zero then it means there are more fragments after this fragment.
- **Fragmentation Offset:** It is a 13-bit long field that indicates the relative position of this fragment with respect to the entire fragment. The fragmentation offset indicate the actual datagram to which the given fragment belongs. It is measured in units of eight octets (64 bits). The first fragment is set to the offset zero.
- **Time-to-Live (TTL):** It is an 8-bit long field, which indicates the total time (in seconds) or number of hops (routers) that an IPv4 datagram can survive before being discarded. As a router receives a datagram, it decrements the TTL value of datagram by one and then forwards that datagram to the next hop and so on. When the TTL value becomes zero, it is discarded. Generally, when a datagram is sent by the source node, its TTL value is set to the two times of the maximum number of routes between the sending and the receiving hosts. This field is needed to limit the lifetime of datagram because it may travel between two or more routers for a long time without ever being delivered to the destination host. Therefore, to avoid this, we discard the datagram when its TTL value becomes zero.
- **Protocol:** It is an 8-bit long field, which specifies the higher-level protocols that uses the services of IPv4.
- **Header Checksum:** It is a 16-bit long field that is used to verify the validity of the header and is recomputed each time when the TTL value is decremented.
- **Source IP Address:** It is a 32-bit long field, which holds the IPv4 address of the sending host. This field remains unchanged during the lifetime of the datagram

- **Destination IP Address:** It is a 32-bit long field, which holds the IPv4 address of the receiving host. This field remains unchanged during the lifetime of the datagram
- **Options:** These are included in the variable part of header and can be of maximum 40 bytes. These are optional fields, which are used for debugging and network testing. However, if they are present in the header then all implementations must able to handle these options. Options can be of single or multiple bytes. Some examples of single byte options are **no-operation** and **end of option** and of multiple bytes are **record route** and **strict source route**.

9. Explain in detail about IPv6.

Ans: The IP is the foundation for most Internet communications. Further, IPv6 is a version of IP that has been designed to overcome the deficiencies in IPv4 design. Some of the important issues that reflect IPv4 inadequacies include:

- The IPv4 has a two-level address structure (network number, host number), which is inconvenient and inadequate to meet the network prefixes requirements. In addition, IPv4 addresses need extra overhead like subnetting, classless addressing, NAT, address depletion, etc., which are still a big issue for efficient implementation
- Internet also deals with real-time audio and video transmission, which requires high speed with minimum delays and requires reservation schemes of resources. There is no such a procedure in IPv4 to deal with such kind of transmission.
- Some confident al applications need authentication and encryption to be performed during data transmission, However, IPv4 does not provide any authentication and encryption of the packets.

Thus, an Internetworking Protocol, version 6 (IPv6), also known as **Internetworking Protocol Next Generation** (**Ipng**) with enhanced functionality is proposed by the Internet Engineering Task Force (IETF) to accommodate the future growth of Internet.

Packet Format of IPv6

Figure 11.4 shows the format of IPv6 packet. An IPv6 packet consists of two fields: *base header* field of 40 bytes and a *payload* field of length up to 65,535 bytes. The payload field further consists of *optional extension headers* and *data packets* from upper layer.

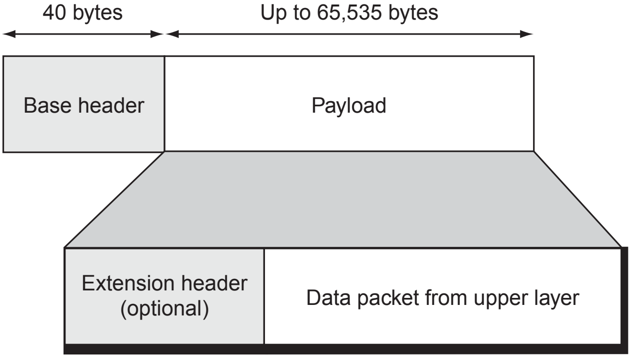


Figure 11.4 IPv6 Datagram Format

The format of IPv6 datagram header is shown in Figure 11.5.

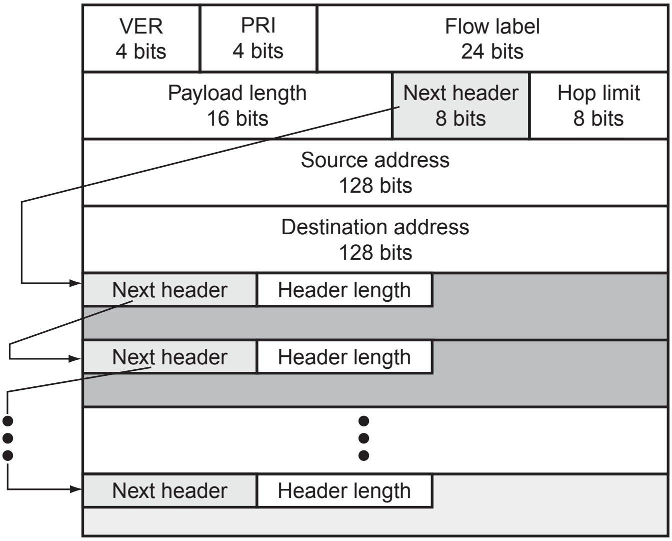


Figure 11.5 IPv6 Datagram Header Format

The description of various fields included in IPv6 header is as follows

- **Version (VER):** It is a 4-bit long field, which indicates the version being used. The current version of IPv6 is 6.
- **Priority (PRI):** It is a 4-bit long field, which indicates the transmission priority of the packet in accordance to traffic congestion
- **Flow Label:** It is a 24-bit (3-byte) long field which is used to provide special handling to some particular data packet flow like audio and video packets
- **Payload Length:** It is a 16-bit (2-byte) long field which defines the length of the remainder of the IPv6 packet following the header, in octets.
- **Next Header:** It is an 8-bit long field which identifies the first extension header (if extension header is available) following the base header or defines the protocol in the upper layer such as TCP, UDP or ICMPv6.
- **Hop Limit:** It is an 8-bit long field, which defines the maximum number of routers the IPv6 packet can travel during its lifetime. The purpose of this field is same as of TTL field in IPv4
- **Source Address:** It is a 128-bit long field, which holds the IPv6 address of the sending host. This field remains unchanged during the lifetime of the datagram
- **Destination Address:** It is a 128-bit long field, which holds the IPv6 address of the receiving host. It remains unchanged during the lifetime of the datagram.

10. Discuss the advantages of IPv6 over IPv4.

Ans: The IPv6 has the following advantages over IPv4:

- **Bigger Address Space:** IPv6 has 128-bit address, which can make 2^{128} addresses.
- **Improved Header Format:** In IPv6 header format, options are kept distinct from the base header and can be inserted when needed. These optional headers are not examined by any router during the datagram path thereby simplifying and speeding up the routing process.

- **Auto Configuratio of Addresses:** IPv6 protocol can provide dynamic assignment of IPv6 addresses.
- **Allow Future Extensions:** IPv6 design allows any future extensions, if needed, to meet the requirements of future technologies or applications.
- **Support for Resource Allocation:** In IPv6, a new mechanism called flo label has been introduced to replace TOS field. With this mechanism, a source can request special handling of the packet. This mechanism supports real-time audio and video transmission.
- **Enhanced Security:** Ipv6 includes encryption and authentication options, which provide integrity and confidentiality of the packet

11. Compare IPv4 header with IPv6 header.

Ans: Both IPv4 and IPv6 are the variants of IP, which have certain differences between them. These differences are listed in Table 11.1.

Table 11.1 Differences Between IPv4 and IPv6 Header

IPv4 Header	IPv6 Header
• IPv4 has header length (HLEN) field and it is variable in size.	• IPv6 does not have header length field because the length of the header is fixed.
• It has service field to provide desired QoS such as precedence, delay, throughput and reliability.	• The priority and flow label fields together provide the functionality provided by the service field.
• It has total length field, which shows the total length (header plus data) of the datagram.	• It has payload field that indicates the length of data but not the header.
• It has identification, flag, and offset fields in its base header.	• These fields have been removed from the base header and are included in the fragmentation extension header.
• In this, the TTL field specifies time to live in seconds.	• IPv6 uses a hop limit field, which serves the same purpose as TTL field in IPv4.
• There is a protocol field.	• There is a next header field in place of protocol field in IPv4.
• There is a header checksum field in IPv4, which is used to detect errors in the header of an IP packet and results into an extra overhead while processing an IP packet.	• There is no header checksum field needed because it is provided by the protocol in upper layer.
• There is an options field.	• There is an extension header field.
• The source and destination address fields are of 32 bits.	• The source and destination fields are of 128 bits.

12. Discuss some deficiencie of IP.

Ans: The IP is the best effort service to deliver a datagram from the original source to the final destination. However, it has certain deficiencies, which are as follows

- It does not support error control and assistance mechanism. Sometimes, unexpected errors may occur, such as a router may have to discard a datagram because it cannot find a route to the destination or TTL field has a zero value. In such a situation, the I protocol is unable to inform the source host.
- It does not provide any support for host and management queries. Sometimes, a host wants to know whether the router or another host is alive and sometimes, a network administrator may need information about another host or router.

13. Explain message types associated with ICMP.

Ans: Internet control message protocol (**ICMP**) has been designed to overcome the problems with IP. It provides a mechanism for error reporting and host and management queries. It addresses and reports these problems through ICMP messages. The ICMP messages are of two types, namely, *error-reporting messages* and *query messages*.

Error-reporting Messages

The ICMP facilitates for reporting error messages to the original source. It does not correct errors but only reports them. The error-reporting messages report problems that a router faces while processing an IP packet. The ICMP handles five types of errors, which are as follows

- ❑ **Destination Unreachable:** The destination-unreachable messages are used in case of routing or delivery error. It may happen that routers are unable to route the datagrams or a host is unable to deliver it. In such situations, destination-unreachable messages are sent back to the source host. It is to be noted that these messages cannot be created by the routers or destination host.
- ❑ **Time Exceeded:** The time-exceeded message is sent in two cases: first, when the packet is dropped because the value of TTL field reaches zero and second, when a destination does not receive all the fragments belonging to the same packet within a certain time limit.
- ❑ **Parameter Problem:** When a router or the destination host finds an illegal or missing value in any field of the datagram then it discards and sends a parameter problem message to the source
- ❑ **Source Quench:** If a router or host discards the datagram due to congestion in the network, then it sends a source quench message to the source host. There are two purposes of sending this message. First is to tell the source that the sending datagram has been discarded and second is to slow down the process of sending datagrams to prevent the congestion.
- ❑ **Redirection:** When a router finds that the packet has been sent to the wrong route because of some sudden change in the routing table or loss of a routing table update, then it sends a redirect message to the source host to notify the problem.

Query Messages

The ICMP allows sending query messages in addition to error-reporting messages. The query messages help a host or a network manager to receive specific information from a router or another host. For example, nodes can search their neighbours, hosts can search and know about routers on their network, and routers can help a node to redirect its messages. The query messages always occur in pairs. Different types of query messages are as follows:

- ❑ **Echo Request and Echo Reply:** The echo-request and echo-reply messages are used to determine whether there is communication between two systems at the IP level. If the machine that has sent the echo-request message, receives the echo-reply message, it is proved that these two machines are communicating with each other through IP datagrams. A **ping** command is used to determine the communication in which a series of echo-request and echo-reply messages are transferred between two hosts to check the connectivity.
- ❑ **Timestamp Request and Reply:** The timestamp request and timestamp reply messages are used by the hosts or routers to find out the round-trip time required for an IP datagram to reach from one to another. It is also used to synchronize the clocks.

- **Address Mask Request and Reply:** The address mask request is sent by a host to a router on a local area network (LAN) that knows its IP address but wants to know its corresponding mask. In response, the address mask reply messages are sent by the router to the host by providing it necessary mask.
- **Router Solicitation and Advertisement:** To send data to a host on another network, the source host needs to know the router address of its own network which connects it to other networks. Along with this, it needs to know whether neighbour's routers are alive and functioning. In these situations, the router solicitation and advertisement message helps the host to find out such information. The source host broadcasts a router-solicitation message. The router, which receives the router-solicitation message, broadcast their routing table information through router-advertisement message. The router-advertisement message includes an announcement about its presence as well as of other routers on the network.

14. In a leaky bucket, what should be the capacity of the bucket if the output rate is 5 gal/min and there is an input burst of 100 gal/min for 12 s and there is no input for 48 s?

Ans: Total input = 100*(12/60) + 0*48 = 20 gal/min
Given, output rate = 5 gal/min
Thus, the capacity of bucket = 20 – 5 = 15 gal.

15. Imagine a flo specificatio that has a maximum packet size of 1,000 bytes, a token bucket rate of 10 million bytes/s, a token bucket size of 1 million bytes and a maximum transmission rate of 50 million bytes/s. How long can a burst at maximum speed last?

Ans: Given that
Bucket size, C = 1 million bytes
Maximum transmission rate, M = 50 million bytes/s
Token bucket rate, P = 10 million bytes/s
Burst time, S = ?
We know that, $S = C/(M - P)$
Putting the respective values in the above formula, we get

$$S = 1/(50 - 10)$$
$$\Rightarrow S = 1/40$$
$$\Rightarrow S = 0.025 \text{ s}$$

Therefore, burst will last for 0.025 s.

Multiple Choice Questions

1. ________ defines the variation in the packet delay.
   (a) jitter (b) bandwidth
   (c) reliability (d) none of these

2. Which of the following are not the scheduling techniques used to improve the QoS?
   (a) FIFO queuing
   (b) LIFO queuing
   (c) priority queuing
   (d) weighted fair queuing

3. Which of the following ICMP messages is sent by the router to source host to inform that the packet has been discarded due to congestion?
   (a) redirection (b) parameter problem
   (c) time exceeded (d) source quench

4. In which of the following algorithms, the output rate of burst packets can be of variable rate?
   (a) token bucket (b) leaky bucket
   (c) both (a) and (b) (d) none of these

5. The protocol field in the ARP packet format is of ________bits.
   (a) 16 (b) 8
   (c) variable (d) 32

6. Mapping from MAC address to IP address is done by
   (a) RARP (b) BOOTP
   (c) DHCP (d) All of these

Answers

1. (a) 2. (b) 3. (d) 4. (a) 5. (b) 6. (d)

12

Internet Transport Protocols

1. **Explain the duties of transport layer.**

Ans: The transport layer ensures process-to-process delivery of message. As multiple processes may be running at the same time on the communicating hosts, it is the duty of the transport layer to communicate message from a specific process on sending host to the desired process on the receiving host. It also ensures that the receiving process receives the whole segment in the exact order as it was sent by the sending process. Some other responsibilities of transport layer are as follows:

❑ **Segmentation and Reassembly:** A message is divided into segments by the transport layer with each segment being given a sequence number. These sequence numbers enable the destination transport layer to reassemble the segments in exact order as they were sent by the sender and thus, help in identifying the segments that have been lost during the transmission.

❑ **Addressing:** As many processes may be running on the communicating hosts at the same time, it is necessary to identify the desired process out of many processes. For this, the transport layer header must include a service point address (port address) in each segment.

❑ **Connection Control:** The transport layer provides both connection-oriented and connectionless services. In connection-oriented service, a connection must be established first between two communicating processes before transmitting any segments. After transmitting the whole data, the connection is released. On the other hand, in connectionless service, no such connection is established and each segment takes different route to reach destination process.

❑ **Flow Control:** The transport layer is responsible for controlling the flow of data such that no sending process should send segments at a rate faster than the receiving process can process. The transport layer provides end-to-end flow control rather than across a single channel as provided by the data link layer.

❑ **Error Control:** The transport layer functions in such a way that the receiving process not only can detect the errors but also can determine the location of errors in the segment. The transport layer provides process-to-process error control rather than across a single link as provided by the data link layer.

2. In OSI model, both data link layer and transport layer are involved in error control. Why same activity twice? Justify.

Ans: Both data link layer and transport layer provide error control, but where the transport layer provides end-to-end error control and the data link control provides error control across a single link. The data link layer makes the physical link reliable by adding the mechanism for detecting the errors and retransmitting frames in case of lost and damaged frames. On the other hand, the transport layer ensures that the entire message is delivered to the receiving process without any error and in the same order as sent by the sending process. Retransmission is used in the transport layer to perform error correction.

3. Why do we need port addresses?

Ans: Usually, a machine provides a variety of services such as electronic mail, TELNET and FTP. To differentiate among these services, each service is assigned with a unique port number. To avail some specific service on a machine, first it is required to connect to machine and then connect to the port assigned for that service. The port numbers less than 1,024 are considered **well-known** and are reserved for standard services. For example, the port number used for TELNET is 23.

4. What is socket address? Explain socket addressing.

Ans: In transport layer, two processes communicate with each other via sockets. A **socket** acts as an end-point of the communication path between the processes. To ensure the process-to-process delivery, the transport layer needs the IP address and the port number at each communicating end. The IP address is used to identify the machine on the network and the port number is used to identify the specific process on that machine. The IP address and port address together define the **socket address**.

To enable the communication, each of the communicating processes (client and server) creates its own socket and these sockets are to be connected. The client socket address uniquely identifies the client process while the server socket address uniquely identifies the server process.

The server listens to a socket bound to a specific port for a client to make connection request. Whenever a client process requests for a connection, it is assigned a port number (greater than 1,024) by the host computer (say, `M`). Using this port number and the IP address of host `M`, the client socket is created. For example, if the client on host `M` having IP address (125.61.15.7) wants to connect to TELNET server (listening to port number 23) having IP address (112.56.71.8), it may be assigned a port number 1,345. Thus, the client socket and server socket used for the communication will be (125.61.15.7:1345) and (112.56.71.8:23), respectively as shown in Figure 12.1.

Each connection between client and server employs a unique pair of sockets. That is, if another client on host `M` wants to connect to TELNET server, it must be assigned a port number different from 1,345 (but greater than 1,024).

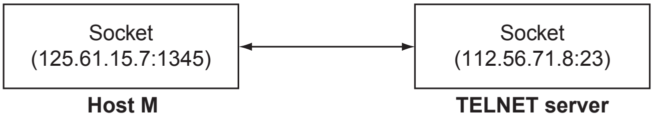


Figure 12.1 Communication Between Sockets

5. Write a short note on Berkeley sockets.

Ans: The transport layer offers certain operations called **transport service primitives** that enable the application programmes to use the transport services. Each transport service has its own access primitives. The set of transport service primitives used in Berkeley UNIX for transmission control protocol

(TCP) are referred to as **socket primitives**. These socket primitives are commonly used for Internet programming and also provide more flexibility. Various socket primitives used in Berkeley UNIX for TCP are described as follows:

- **SOCKET:** This primitive is used to create a new communication end point. It also allocates table space to the end point within the transport entity. This primitive is executed both by the client and by the server.
- **BIND:** This primitive is used to assign network addresses to newly created sockets. After the addresses have been attached with sockets, the remote systems can connect to them. This primitive is executed only at the server side and always after the SOCKET primitive. At the client side, there is no need to execute BIND primitive after the SOCKET primitive. This is because the server has nothing to do with the address used by the client.
- **LISTEN:** This primitive is used to indicate the willingness of a server to accept the incoming connection requests. If a number of clients attempt to make a connection with the server, it allocates space to queue up all the incoming requests. This primitive is executed only at the server side and always after the BIND primitive.
- **ACCEPT:** This primitive is used to make some incoming connection wait as long as a connection request does not arrive. This primitive is executed only at the server side and always after the LISTEN primitive.
- **CONNECT:** This primitive is executed by the client to attempt to establish a connection with the server. As the client executes the CONNECT primitive, it gets blocked. It remains blocked until it receives a transport packet data unit (TPDU) from the server, which indicates the completion of CONNECT primitive. Then, the client gets unblocked and a full-duplex connection is established between the client and the server.
- **SEND:** This primitive is used to send data over the full-duplex connection. Both client and server can execute this primitive.
- **RECEIVE:** This primitive is used to receive data from the full-duplex connection. Both client and server can execute this primitive.
- **CLOSE:** This primitive is used to release the connection between the client and the server. The connection is terminated only after both the communicating parties have executed the CLOSE primitive.

6. Explain various schemes used by the transport layer to find the transport service access point (TSAP) at a server.

Ans:- Whenever an application process (client) wishes to establish a connection with some application process running on the remote system (server), it needs to specify which one to connect to. For this, the transport layer specified transport addresses to which the process can listen for connection requests. In transport layer, these end points are termed as **TSAP**. Both client and server processes get attached to a TSAP for establishing a connection with remote TSAP. However, now the problem arises, how the client knows which TSAP a specific process on the server is listening to? To identify this, some scheme is needed.

One such scheme is the **initial connection protocol** scheme. In this scheme, not all the server processes are required to listen to well-known TSAPs; rather, each machine that wants to serve to remote users has a proxy server called **process server**. The process server can listen to a number of ports simultaneously. When a CONNECT request from a user specifying the TSAP address of a specific server process arrives, it gets connected to the process server in case no server process is waiting for it. After the desired server process gets available, the process server creates the requested server which then inherits the existing connection with the user. This way, the user gets connected to the desired server process. The newly created server then performs the requested job while the process server gets back to listening to ports. Though this scheme seems fine, it cannot be used for servers that cannot be created when required. To overcome this limitation, another scheme is used.

In the alternative scheme, there exists a process known as a **name server** or a **directory server** which listens to a well-known TSAP. The name server contains an internal database in which all the service names along with their TSAP addresses are stored. This scheme requires every newly created service to register itself with the name server. When a client needs to find the TSAP address corresponding to a service, it establishes a connection with the name server. After the connection has been established, the client sends a message including the requested service name to the name server. The name server searches through its database and sends the requested TSAP address back to the client. After receiving the TSAP address by the client, the connection between client and name server is released and a new connection is established between the client and the service requested by it.

7. What is meant by upward and downward multiplexings?

Ans: Multiplexing is a technique that allows the simultaneous transmission of multiple signals across a single data link. In transport layer, we may need multiplexing in the following two ways, which are as follows:

❑ **Upward Multiplexing:** When there is only one network address available on a host, then all the transport connections on that host use the same network connection. Whenever a TPDU is received, some means is required to indicate which process is to give the TPDU. This situation is known as **upward multiplexing**.

❑ **Downward Multiplexing:** The subnet uses virtual circuits with each virtual circuit having a fixed data rate. Now, if a user needs higher bandwidth than that of a single virtual circuit to transport the data, then the traffic from a single transport connection can be multiplexed to multiple network connections (virtual circuits) thereby increasing the bandwidth. This is what is called **downward multiplexing**.

8. Explain in detail user datagram protocol (UDP). Also list its uses.

Ans: UDP is a connectionless and unreliable transport protocol that offers process-to-process delivery with limited error checking. By **connectionless**, we mean that the segments are sent to the destination host without any prior establishment of the connection between communicating hosts. By **unreliable**, we mean that UDP does not perform error and flow control and thus, does not guarantee about the proper delivery of segments at the destination. As segments in UDP are not numbered, there is no means to identify the frames that have lost during the transmission.

Though UDP is considered powerless due to unreliable transport, it is a simple protocol that incurs a minimal overhead. It is generally used by a process that has only a small message to send and is not much concerned about the reliability. The applications such as speech and video for which instant delivery is more important than accurate delivery, prefer to adopt UDP for transport.

The UDP packets, known as **user datagrams**, have a fixed-size header of eight bytes, which is followed by the data. The header of UDP packet contains four fields of 16 bits each as shown in Figure 12.2.

Source port number 16 bits	Destination port number 16 bits
Total length 16 bits	Checksum 16 bits

Figure 12.2 UDP Packet Header Format

The-description-of-various-field -of-a-UDP-packet-header-is-as-follows:

- **Source Port Number:**-It-is-a-16-bit-long-fiel -that-define -the-process-running-on-the-source-host.-If the UDP packet is being sent from the client, that is, if the source host is client, then the source port number will be chosen randomly by the UDP software running on the client. However, if the UDP packet is sent by the server, the source port number will be a well-known port used with UDP. Some of the well-known ports used with UDP are listed in Table 12.1.

Table 12.1 Some Well-known Ports Used with UDP

Port	Protocol	Description
13	Daytime	Returns the date and the time
53	Name server	Domain name service
111	RPC	Remote procedure call
123	NTP	Network time protocol

- **Destination Port Number:**-It-is-a-16-bit-long-fiel -that-define -the-process-running-on-the-destination host. If the destination host is the client, the destination port number will be an ephemeral port number. However, if the destination host is the server, the destination port number will be a well-known port used with UDP.
- **Total Length:**-It-is-a-16-bit-long-fiel -that-specifie -the-total-length-of-the-UDP-packet-including-header-as-well-as-data.-The-size-of-this-fiel -can-range-from-0-to-65,535-(that-is,-2^{16}–1) bytes but the size-of-UDP-packet-must-be-much-less,-as-it-is-to-be-encapsulated-in-an-IP-datagram-having-a-total-length of 65,535 bytes.
- **Checksum:**-It-is-a-16-bit-long-fiel -that-is-used-for-error-detection-over-both-the-header-and-the data.

Uses of UDP

- It is suitable for multicasting.
- It is used for management processes such as SNMP.
- It is used for the route updating protocols such as routing information protocol (RIP).

9. What is transmission control protocol (TCP)? What are the services provided by it?

Ans: **TCP** is a connection-oriented and reliable transport layer protocol. By **connection-oriented**, we mean that a virtual connection must be established between the sending and the receiving processes-before-any-data-can-be-transferred.-Whenever-a-process-on-source-host-wishes-to-communicate-with-a-specific-process-on-destination-host,-first-a-virtual-connection-is-established-between-the-TCPs-of the sending and receiving processes. Then, the data can be transferred in both directions. After the completion of data transfer, the connection is released. TCP accepts a stream of bytes from the upper layer and divides it into a sequence of segments which are then sent to the destination. By **reliable**, we mean that TCP provides error and flow control and thus, ensures the delivery of segments to the destination. Each segment sent from the source needs to be acknowledged by the receiver on its receipt.

TCP provides a variety of services to the processes at the application layer. Some of these services are described as follows:

- **Process-to-Process Communication:** Like UDP, TCP is also a process-to-process protocol that connects-a-process-on-a-source-host-to-a-specific-process-on-the-destination-host-using-the-port-numbers. Some of the well-known ports used with TCP are listed in Table 12.2.

Table 12.2 Some Well-known Ports Used with TCP

Port	Protocol	Description
9	Discard	Discards any datagram that is received
13	Daytime	Returns the date and the time
19	Charg en	Returns a string of characters
23	SMTP	Simple mail transfer protocol

- **Stream Delivery Service:** TCP is a byte-oriented protocol that allows the sending process to send the stream of bytes and the receiving process to receive the stream of bytes. Since the speed of sending and receiving processes may differ, buffers need to be maintained at both ends to store the bytes. The buffer at the sender's end is divided into three sections: empty slots to hold the bytes produced by the sending process, slots containing bytes that have been sent but not yet acknowledged and the slots containing bytes that are to be sent. On the other hand, the buffer at the receiver's end is divided into two sections: empty slots to hold the bytes received from the sending process and the slots containing bytes that are to be read by the receiving process.
- **Segments:** The communication between sending and receiving TCPs takes places through the IP layer, which supports data in packets rather than a stream of bytes. Therefore, before sending the bytes (stored in the sending buffer), the sending TCP groups multiple bytes together into a packet called **segment**; different segments may or may not contain equal number of bytes. TCP header is attached with each segment and then the segment is delivered to IP layer. The IP layer encapsulates the segment into IP datagram and sends the IP datagrams. The IP layer at the receiving machine processes the header of IP datagrams and passes the segments to the receiving TCP. The receiving TCP stores the bytes of segments in the receiving buffer.
- **Full-Duplex Communication:** TCP provides full-duplex connection, that is, both the sender and the receiver processes can simultaneously transmit and receive the data.
- **Reliable Service:** TCP provides a reliable service, that is, every received byte of data is acknowledged to the sending process. This helps in detecting the lost data. To ensure reliability, TCP uses *byte number*, *sequence number* and *acknowledgement number*.
    - **Byte Number:** Each of the bytes that are transmitted in a connection is numbered by TCP. The numbering-does-not-start-necessarily-with-zero.-As-TCP-receives-the-first-byte-from-the-sending-process, it chooses a random number between 0 and 2^{32}—1-and-assigns-that-number-to-the-first-byte.-The-subsequent-bytes-are-numbered-accordingly.-For-example,-if-the-first-byte-is-numbered-as 330 and total 1,000 bytes are to be transmitted, then byte numbers will be from 330 to 1,330.
    - **Sequence Number:** After numbering the individual bytes, the groups of bytes, that is, segments are numbered. Each segment is assigned a sequence number by TCP, which is same as the-number-of-first-byte-carried-by-that-segment.

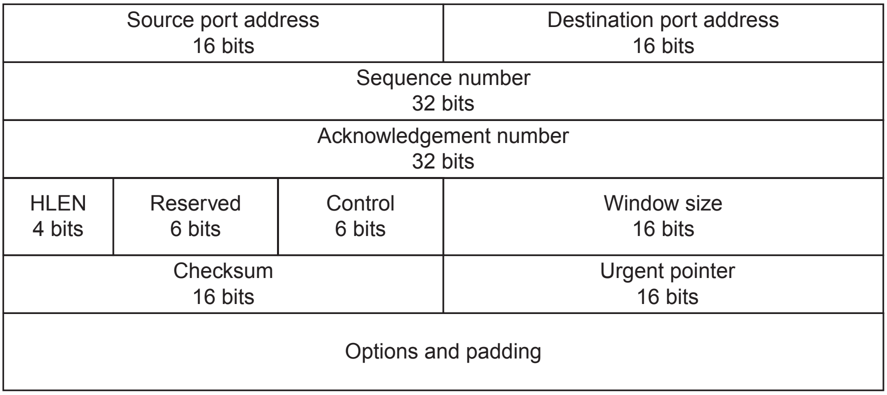
- **Acknowledgement Number:** The communicating parties send acknowledgement to each other to confirm the receipt of bytes. TCP numbers acknowledgement and the acknowledgement number indicate the number of byte expected to be received next. Moreover, the acknowledgement number is cumulative. For example, if one of the communicating devices sends an acknowledgement number 540 to the other, then it means that the bytes from the beginning up to 539 have been received and the byte number 540 is expected to be received next.

❑ **Flow Control:** TCP implements a byte oriented flow control mechanism to prevent the receiving TCP from being overloaded with data from the sending TCP.

❑ **Error Control:** To ensure reliability, byte-oriented error control mechanism is implemented by TCP.

10. Give the segment format of TCP.

Ans: TCP allows exchange of data in the form of segments, where each segment consists of header and data. The size of segment header varies from 20 to 60 bytes, depending on whether or not the header contains *Options* field If the header does not contain *Options* field then it is of 20 bytes else it can be up to 60 bytes. Figure 12.3 shows the format of a TCP segment header.



Source port address 16 bits		Destination port address 16 bits	
Sequence number 32 bits			
Acknowledgement number 32 bits			
HLEN 4 bits	Reserved 6 bits	Control 6 bits	Window size 16 bits
Checksum 16 bits		Urgent pointer 16 bits	
Options and padding			

Figure 12.3 TCP Segment Header Format

The TCP segment header comprises various fields which are described as follows:

❑ **Source Port Address:** It is a 16-bit long field that defines the port number of the application programme running on the source host.

❑ **Destination Port Address:** It is a 16-bit long field that defines the port number of the application programme running on the destination host.

❑ **Sequence Number:** It is a 32-bit long field that indicates to the receiving process the number of first byte contained in the received segment. While the connection is established, both the communicating processes make use of random number generator to generate the **initial sequence number** (**ISN**), which is different in each direction.

❑ **Acknowledgement Number:** It is a 32-bit long field that defines the byte number the receiving process is expecting to receive from the sending process. If the sending process sends the byte number `x` to the receiver, then the receiving process adds one to that byte number to create an acknowledgement number that is, `x+1`. The acknowledgement number `x+1` means that the receiving process has successfully received all bytes up to `x` and now, it is expecting to receive byte number `x+1`.

- **HLEN:** It is a 4-bit long field that defines the length of segment header in terms of 32-bit words. This field can take value between 5 (for 20 byte header) and 15 (for 60 byte header).
- **Reserved:** It is a 6-bit long field which has been kept reserved for the future use.
- **Control:** It is a 6-bit long field consisting of six flags each of one bit. These flag bits help in flow control, establishment of connection, termination of connection and the mode of transferring data in TCP. The description of flag bits are as follows:
  - **URG:** This bit is set to 1 if the Urgent pointer field is in use else it is set to 0.
  - **ACK:** This bit is set to 1 to indicate the valid acknowledgement number. If ACK bit is set to 0, then it indicates that the segment does not carry the acknowledgement and thus, the *Acknowledgement number* field is ignored.
  - **PSH:** This bit indicates the pushed data. The receiver is asked to deliver the data to the application immediately as it arrives and not buffer the data until a full buffer has been received.
  - **RST:** This bit is used to reset the data connection in case the connection has been distorted. It also rejects an invalid segment and denies making another connection.
  - **SYN:** This bit is used to synchronize the sequence numbers during the connection establishment. If the piggyback *Acknowledgement number* field is not in use, then SYN bit is set to 1 and ACK bit is set to 0. If the connection uses an acknowledgement, then SYN bit is set to 1 and ACK bit is also set to 1.
  - **FIN:** This bit is used to terminate the connection. If this bit is set to 1, then it means the sending process has transmitted all data and has no more data to transmit.
- **Window Size:** It is a 16-bit long field that describes the size of the window (in bytes) the receiving process should maintain. The maximum size of window is 65,535 bytes. This value is regulated by the receiver and is usually known as the **receiving window**.
- **Checksum:** It is a16-bit long field that is used to detect the errors. The checksum in TCP is necessary, unlike UDP. The same psuedoheader as that of UDP is added to the segment and for the TCP psuedoheader, the value of *Protocol* field is set to 6.
- **Urgent Pointer:** It is a 16-bit long field which is used only when segment contains the urgent data.
- **Options:** This field is up to 40 bytes that is used to contain additional or optional information in the TCP header.

11. Describe three phases of connection-oriented transmission in TCP.

Ans: The connection-oriented transmission in TCP needs three phases, which are described as follows:

- **Connection Establishment:** This is the first phase of connection-oriented transmission in TCP. In this phase, the TCPs in the machines that wish to communicate need to be first connected. Each of the communicating parties must initialize communication and take permission from the other party before transferring any data. In TCP, connection is established using **three-way handshaking** (discussed in **Q12**).
- **Data Transfer:** After the TCPs of the communicating machines are connected, the data transfer phase begins. In this phase, both the parties can send segments to each other at the same time as the connection established between TCPs is full-duplex. After receiving a segment, the receiving party is also required to send an acknowledgement number to the sending party to confirm the receipt of segment. An acknowledgement from either side (client to server or server to client) can also be piggybacked on the segment (containing data) that is travelling in the same direction. That is, a single segment may contain both data and acknowledgement.

- **Connection Termination:** This is the last phase of connection-oriented transmission that commences after the data have been transferred. Though either of the communicating parties can close the connection, generally the client initiates the connection close command. In TCP, connection is terminated using three-way handshaking mechanism (discussed in **Q14**).

12. Explain how connection is established in TCP using three-way handshaking mechanism.

Ans: TCP is a connection-oriented protocol that allows full-duplex transmission. In TCP, the connection is established using **three-way handshaking** mechanism.

Three-Way Handshaking

The server starts the mechanism. The server process informs its TCP that it is ready to accept an incoming connection by executing the LISTEN and ACCEPT primitives. This is called a request for a **passive open**. The client process then sends the request for an **active open** to its TCP by executing the CONNECT-primitive.-This-primitive-specifie -the-IP-address-and-port-number-that-the-TCP-on-client-could-identify-the-specifi -server-process-to-which-the-client-process-wants-to-connect.-Now,-TCP-starts-the three-way handshaking process, which involves the following steps (Figure 12.4).

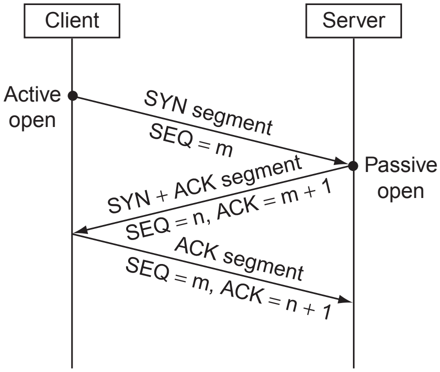


Figure 12.4 Connection Establishment Using Three-way Handshaking

1. The-client-sends-a-TCP-segment-with-SYN-bit-set-to-1-and-ACK-bit-set-to-0.-This-SYN-segment-is-used-for-synchronization-of-sequence-numbers-between-client-and-server.-The-SYN-segment-does-not actually contain any data; however, it consumes one byte space and is assigned a sequence number (say, `m`), so that it can be acknowledged unambiguously.
2. If-the-server-accepts-the-connection,-it-sends-a-TCP-segment-with-both-SYN-and-ACK-bits-set-to-1.-This-SYN+ACK-segment-serves-the-purpose-of-acknowledgement-to-the-SYN-segment-sent-by the client and does not carry any data. It also consumes a sequence number (say, `n`) and the acknowledgement-number-of-this-segment-is-set-to-sequence-number-of-SYN-segment-plus-one-(that is, `m+1`).
3. The client sends a TCP segment with ACK bit set to 1 and a valid Acknowledgement number. This-ACK-segment-does-not-carry-any-data;-it-just-confirm -the-receipt-of-SYN+ACK segment from-the-server.-The-sequence-number-of-ACK-segment-is-same-as-that-of-the-firs -segment-(SYN-segment) sent by the client while the acknowledgement number is set to sequence number of (SYN+ACK) segment plus one (that is, `n+1`).

13. Write a short note on SYN flooding attack.

Ans: The SYN flooding attack is a type of security attack that can occur during the connection establishment process in TCP. In this attack, an attacker sends a large number of SYN segments to the server with each segment carrying a fake source IP address. As the server believes that an *active open* request is being issued from different clients, it allocates the required resources to each client. It then sends SYN+ ACK segment to each fake client, which are lost. This results in a lot of server resources allocated but not used. Now, during this time, if more requests arrive to server, then it is quite possible that the server may not have enough resources to grant their requests and thus, server may crash.

To handle SYN flooding attacks, some strategies have been imposed by TCP. First, the number of requests during a specified period of time can be limited. Second, **filtering** strategy can be implemented in which datagrams are filtered out if they arrive from unwanted source addresses. Third, some other transport layer protocols such as SCTP have adopted a new strategy called **cookie** in which the allocation of resources to clients is delayed until the entire connection has been set up.

14. Discuss three-way handshaking mechanism for connection termination in TCP.

Ans: The connection termination in TCP is easier than the connection establishment. After the communicating processes have finished with exchanging data, any one of them can terminate the connection. In TCP, the connection is terminated with the help of three-way handshaking mechanism which involves the following steps (Figure 12.5).

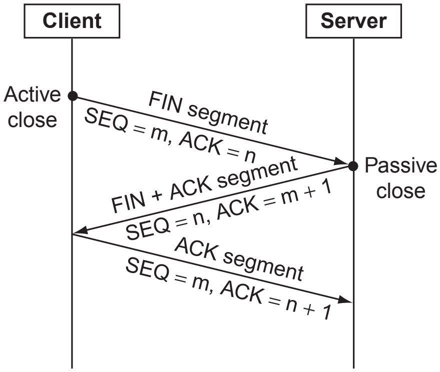


Figure 12.5 Connection Termination Using Three-way Handshaking

1. The client TCP initiates the termination process by sending a TCP segment with FIN bit set to 1 to the server. This FIN segment may also include the last chunk of data byte that needs to be sent to the server process. If the FIN segment does not contain any data, then it consumes only one sequence number (say, `m`). The FIN segment may also contain a valid acknowledgement number (say, `n`) to confirm the receipt of the latest bytes from the server.
2. On receiving the FIN segment, the server TCP sends the FIN+ACK segment to the client. This segment indicates the receipt of FIN segment by the server as well as closing of connection from the server side. This segment may also include last chunk of data byte to be sent by the server. However, if it does not contain data, it is assigned only one sequence number which is same as the acknowledgement number of FIN segment (that is, `n`). The acknowledgement number of this segment is equal to the sequence number of FIN segment plus one (that is, `m+1`).
3. The client TCP sends the last segment, an ACK segment, to acknowledge the FIN+ACK segment from the server TCP. This segment does not carry any data and thus, takes no new

sequence-number.-The-sequence-number-of-this-segment-is-same-as-that-of-firs -FIN-segment-sent by the client (that is, `m`). It includes an acknowledgement number equal to sequence number received in FIN+ACK segment plus one (that is, `n+1`).

15. Compare UDP with TCP.

Ans: Both UDP and TCP are transport layer protocols that provide process-to-process delivery of packets. Some differences between UDP and TCP are listed in Table 12.3.

Table 12.3 Comparison Between UDP and TCP

UDP	TCP
• It is simple and unreliable protocol.	• It is high featured and reliable protocol.
• It is a connectionless protocol, which means an establishment of connection between client and server is not required before starting the transfer of data.	• TCP is a connection-oriented protocol, which means a virtual connection needs to be established between client and server before initiating the data transfer.
• UDP application sends message-based data in discrete packages.	• TCP application sends stream-based data with no specific structure.
• No acknowledgement of data takes place.	• Each received byte of data needs to be acknowledged.
• Retransmission is not performed automatically. Applications must detect the lost data by themselves and retransmit if required.	• The lost data is retransmitted automatically by TCP.
• It does not provide any flow control mechanism.	• It offers flow control the sliding window mechanism.
• Its transmission speed is very high.	• Its transmission speed is high but lower than UDP.
• It is suitable for transferring small amount of data up to hundreds of bytes.	• It is suitable for small as well as large amount of data up to a few gigabytes.
• Some protocols and well-known applications of UDP include DNS, BOOTP, TFTP and SNMP.	• Some protocols and well-known applications of TCP include FTP, NNTP, DNS, SMTP, IRC and HTTP.
• Its header is shorter than that of TCP and thus it incurs less overhead.	• It incurs more overhead than UDP.

16. What is meant by remote procedure call (RPC)? Explain its mechanism.

Ans: RPC, as the name implies, is a communication mechanism that allows a process to call a procedure on a remote system connected via network. It was introduced by Birrell and Nelson in 1984. This method is implemented to allow programmes to call procedures located on remote host. The calling process (client) can call the procedure on the remote host (server) in the same way as it would call the local procedure. The syntax of RPC call is very similar to conventional procedure call as given below:

```
Call <Procedure_id>(<List of parameters>);
```

The RPC system facilitates the communication between client and server by providing a stub on both client and server. For each remote procedure, the RPC system provides a separate stub on the client side.-When-the-client-process-wants-to-invoke-a-remote-procedure,-the-RPC-call-is-implemented-in-the-following steps.

1. The RPC system invokes the stub for the remote procedure on the client, passing to it the parameters that are to be passed further to the remote procedure. The client process is suspended from execution until completion of the call.

2. The client stub performs **parameter marshalling**, which involves packaging the parameters into a machine-independent form, so that they can be transmitted over the network. It now prepares a message-containing-the-identifier-of-the-procedure-to-be-executed-and-the-marshalled-parameters.
3. The client stub sends the message to the server. After the message has been sent, the client stub blocks until it gets reply to its message.
4. The corresponding stub on the server side receives the message and converts the parameters into a-machine-specific-form-suitable-for-the-server.
5. The server stub invokes the desired procedure, passing parameters to it. The server stub is suspended from execution until completion of the call.
6. The procedure executes and the results are returned to the server stub.
7. The server stub converts the results into a machine-independent form and prepares a message.
8. The server stub sends the message containing the results to the client stub.
9. The-client-stub-converts-the-results-into-machine-specific-form-suitable-for-client.
10. The-client-stub-forwards-the-results-to-the-client-process.-With-this,-the-execution-of-RPC-is-completed, and now, the client process can continue its execution.

Figure 12.6 depicts all the steps involved in execution of RPC.

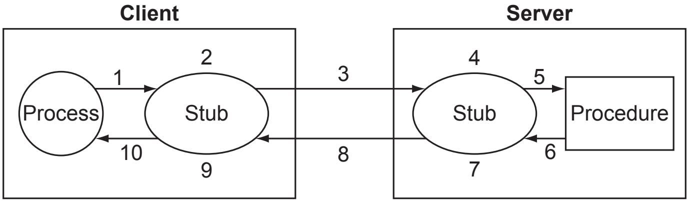


Figure 12.6 Implementation of RPC

Multiple Choice Questions

1. The main function of transport layer is:
   (a) Node-to-node delivery
   (b) Process-to-process delivery
   (c)- Synchronization
   (d) Source-to-destination delivery.

2. IP is responsible for _______communication while TCP is responsible for_____ communication.
   (a) Process-to-process, Host-to-host
   (b) Node-to-node, Process-to-process
   (c) Node-to-node, Host-to-host
   (d) Host-to-host, Process-to-process

- 3.-Which-of-the-following-is-true-for-UDP?
   (a) It is connection oriented.
   (b)- It-provides-flow-control.
   (c) It offers reliable service.
   (d) It performs error control.

4. TCP exchanges data in the form of:
   (a) Datagrams (b) Packets
   (c) Segments (d) Frames

5.- In-TCP,-control-fiel -consists-of:
(a)- Six-flag ----------------(b)--Three-flag
(c)- Five-flag ---------------(d)- Seven-flag

6. In TCP, the connection establishment uses:
(a)- FIN-and-SYN-bits
(b)- SYN-and-ACK-bits
(c) PSH and URG bits
(d) None of these

7. During connection establishment in TCP, the mode of data transmission is:
(a) Full-duplex (b) Half-duplex
(c) Simplex (d) None of these

Answers

1. (b) 2. (d) 3. (c) 4. (c) 5. (a) 6. (b) 7. (a)

13

Application Layer Protocols

1. Explain how TELNET helps in remote login.

Ans: The word "TELNET" is derived from **telecommunications** and **network** and is a protocol that allows a user to log on to a remote computer. Further, TELNET is also known as **remote login**, which means connecting one machine to another in such a way that a person may interact with another machine as if it is being used locally. It means that someone in New Delhi could connect to a computer in the New York City Public Library and search the card catalogue the same way as someone located at a terminal in the library. Once connected, the user's computer emulates the remote computer. When the user types in commands, they are executed on the remote computer. The user's monitor displays what is taking place on the remote computer during the TELNET session.

The user's computer, which initiates the connection, is referred to as the **local computer** or **TELNET client**, and the machine being connected to, which accepts the connection, is referred to as the **remote computer** or **TELNET server**. The transmission control protocol/Internet protocol (TCP/IP) protocol is used to transmit information between the TELNET client and the TELNET server. In addition, TELNET is text based and only the keyboard can be used for navigation. For this reason, it is widely used in UNIX-based systems. Further, TELNET creates a standard and a fictional terminal called the **network virtual terminal** (**NVT**) that is used for communication by all the computers on the network. The following steps are performed while conducting a TELNET session.

- ❑ The inputs from the user are taken and translated by the TELNET client to the NVT form.
- ❑ This input is send to a TELNET server running on a remote computer.
- ❑ The server translates the NVT form to whatever representation the computer being accessed requires.

The same steps are repeated when data are sent from the remote computer back to the user. This system allows clients and servers to communicate even if they use entirely different hardware and internal data representations.

2. What is a domain name system?

Ans: The TCP/IP protocol identifies entities that are connected on the Internet using their unique IP addresses. These addresses being numeric are difficult to remember for the users as compared to their names, therefore, a system was needed that can change a name to an address and vice versa. **Domain name system** (**DNS**) is such a system that is used to map the user friendly host names to their IP addresses and vice versa. This system is used extensively over the Internet and other private businesses.

3. What is a resolver? What is its role in DNS?

Ans: A **resolver** is a library procedure used by the DNS during mapping of a host name to its corresponding IP address. Whenever an application program requires mapping of a host name to IP address, or IP address to host name it invokes the resolver, passing the host name or IP address to it as a parameter. The resolver passes this parameter to a local DNS server, which searches the name or address in its database. After the name or address has been found, the DNS server returns the result back to the resolver. Then, the resolver passes on the result to the calling application program so that a connection could be established with the destination.

4. Explain the DNS in terms of name space, resource record and name server.

Ans: The DNS is used to map host names to their corresponding IP addresses or vice versa. Various components of DNS include *name space*, *resource record* and *name server*.

Name Space

It is a representation of the domains of the Internet as a tree structure. Each domain can be subdivided into many other domains, which are further partitioned thereby creating a hierarchy. The leaf nodes of the tree cannot be subdivided and each leaf node may contain only a single host or several hosts. The top-level domains are classified into two groups, namely, *generic* and *country.* The **generic** group contains domain names such as com (commercial), edu (educational institutions), gov (governments), int (international organizations), mil (armed forces), net (network providers) and org (organizations). The **country** domains contain one entry for every country, as per ISO 3166 specification. The tree structure of the name space is shown in Figure 13.1.

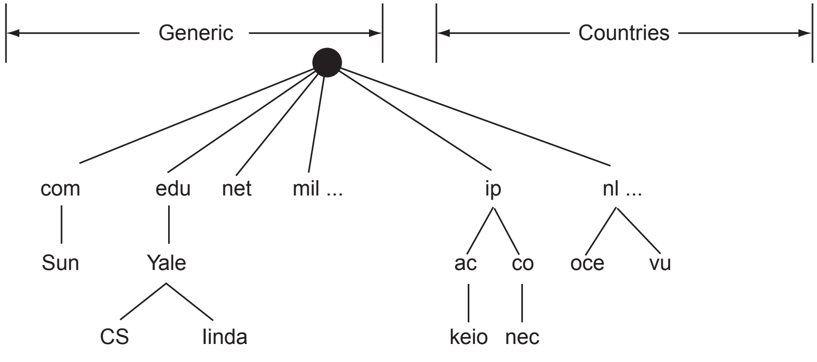


Figure 13.1 A Portion of Internet Domain Name Space

A label is included in each node of the tree (Figure 13.2). The label is a string, which has a maximum size of 63 characters. The label at the root node is just an empty string. The child nodes, which have the same parent, are not allowed to have the same label name as it may cause ambiguity. Each node in the

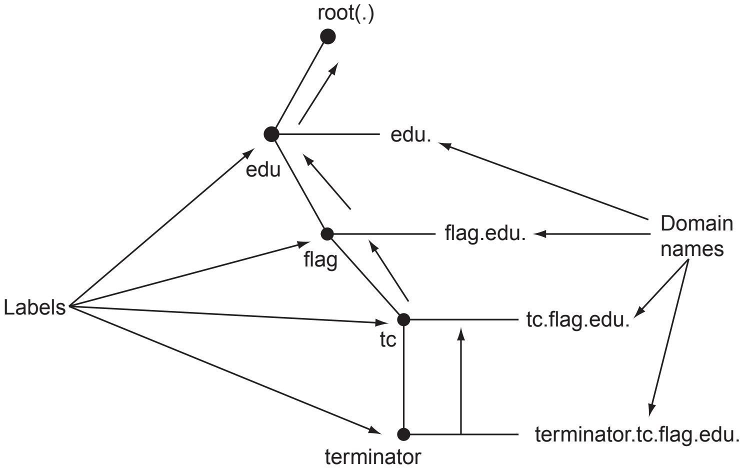


Figure 13.2 Labels and Domain Names

tree has a **domain name**, which is formed by a sequence of labels separated by dots (.). The domain names are again divided into two types, namely, *fully qualifie domain name* (*FQDN*) and *partially qualified domain name* (*PQDN*).

- **FQDN:** If the domain name ends with a dot (.), that is, null string, it is said to be an FQDN. It is the full name of a host, which includes all labels, starting from the host label toward the root label, which is a dot (.). For example, in Figure 13.2, the FQDN of a host named *terminator* installed at the technology centre *tc* is terminator.tc.flag.ed .
- **PQDN:** If a domain name does not end with a null string, then it is said to be a PQDN. This means a PQDN starts with the host label but does not end with the root node. A partial domain name address is used when the domain name and the client reside in the same site. The PQDN can take help of the resolver to convert it to an FQDN. For example, if a person at the *flag.ed* site wants to get the IP address of the *terminator* computer, he/she defines only the partial name *terminator*. The rest of the part (called **suffi**), that is, *tc.flag.ed* , is added by the resolver and then the address is passed to the DNS server.

Resource Records

Every domain is associated with a set of information known as **resource records** (**RRs**). The most common RR is the IP address for a single host, although many other kinds of resource records are also found. A RR is a five-tuple set, which is mostly represented as ASCII text, but for better efficienc , it can also be encoded in binary form. The different fields of the five-tuple set are described as follow

- **Domain_Name:** This field identifies the domain with which this record is associated. Usually, many records related to a single domain exist in the databases and the database contains RRs for multiple domains. Thus, this field is used for search operations so that queries an be executed efficientl .
- **Time_to_Live:** This field indicates the stability of the record. It specifies the time interval within which a RR may be cached by the receiver so that the server need not be consulted for RR repeatedly. A zero value in this field indicates that the RR is to be used for a single transaction and therefore, should not be cached. The highly stable records are given large values while less stable records are given small values.

- **Class:** This field identifies the protocol family. It is set to *IN* for Internet information; otherwise, some other codes are used.
- **Type:** This field specifies the type of the recor
- **Value:** This field depends on the *Type* field and can be a domain name, a number or an ASCII character.

Name Servers

As DNS database is very vast, it is impossible for a single server to hold information about the complete database and respond to all queries. Even if it is done, then a failure in the single name server would bring the whole network down. To avoid such a situation, the DNS name space is divided into many non-overlapping zones (represented by dotted areas in Figure 13.3) with each zone containing name servers holding information about that zone. Each zone covers some nodes of the tree and contains a group of one or more subdomains and their associated RRs that exist within that domain. The name server creates a zone file, which holds all the information of the nodes under it. Each zone has a primary name server and one or more secondary name servers. The **primary name server** of a zone obtains the information from a file on the disk, whereas the **secondary name servers** obtain information from the primary name server. Some servers can also be located outside the zone to improve the reliability.

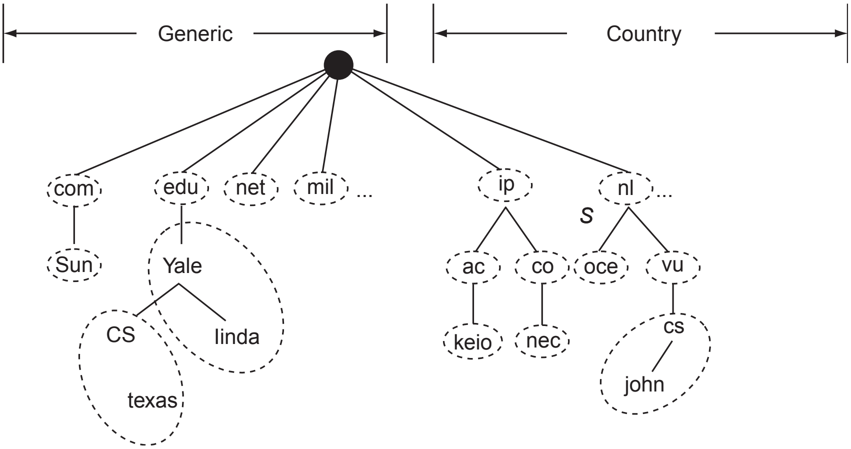


Figure 13.3 Division of DNS Name Space into Zones

Whenever a query from a resolver for a domain name arrives at a local name server, it checks whether that information falls under its zone. If so, then the domain name is provided; otherwise, the query is forwarded to the upper-level name servers. For example, consider a resolver *john.cs.vu.nl* wants to query about the IP address of the host *texas.cs.yale.edu* (Figure 13.3). To handle this query, firstly the resolver sends a query to the local name server *cs.vu.nl* to check whether it already has the IP address. If the local name server has the IP address in its cache, it returns the address to the resolver; else, it forwards the query to the root server. The root server then forwards the UDP packet to *yale.edu*, which is further forwarded to *cs.yale.edu* because this name server has the IP address of the host *texas.cs.yale.edu*. The whole process is repeated in the reverse order in order to reach to the client who had sent the original request. Once the client has been reached, the local name server stores this IP address in its cache so that it may be used later when required.

5. Why was there a need of dynamic domain name system (DDNS)?

Ans: The DNS database contains large number of addresses that need to be changed very often due to addition of a new host, removal of some existing host or change in the IP address of some host. All these changes must be updated in the DNS master file, which leads to lot of manual work consuming a lot of time. To overcome this problem, DDNS was devised that updates the master fil automatically. In DDNS, whenever a binding of name and address is found, the information is passed to a primary DNS server by dynamic host control protocol (DHCP). After receiving the information, the primary server updates its zone and the secondary servers are informed about the change using one of the two modes: *active* and *passive*. In the **active mode**, the primary name server itself informs about the change to the secondary servers by sending the message while in the **passive mode**, the secondary name server checks for any change at regular intervals of time. However, in both modes, the secondary server requests information about the entire zone after being notified about the change. Further, DDNS also secures DNS database from unauthorized changes by using an authentication mechanism.

6. What is e-mail? State its advantages and disadvantages.

Ans: **E-mail** (or **electronic mail**) is the process of exchanging messages electronically via a communications network using the computer. E-mail allows users to communicate with each other in less time and at nominal cost as compared to traditional phone or mail services. Apart from the textual message, e-mails can also consist of other data formats such as pictures, sound and video. E-mails can be sent anywhere in the world using the computer and a modem. Its delivery is almost instant and is very economical to use. One may send many messages at a time or just one to a designated location.

In order to use e-mail, one must have access to the Internet and an e-mail account. An **e-mail account** is a service that allows the user to send and receive e-mails through the Internet. The e-mail account provides a unique e-mail address and a mailbox where the user can save all his/her mails. The e-mail address is made up of two parts, namely, *the logon identity* and the *identity of the e-mail server*. Both these parts are separated by the symbol @ (pronounced as at the rate). A typical e-mail address is *username@website.com*. The first part of the address indicates name of the user. The symbol @ in the address is used to separate the user name from the rest of the address. Next comes the host name (*website.com*), also called the domain name.

E-mail consists of two fields: *envelope* and *message* (Figure 13.4). The **envelope** field defines the address of the sender and the receiver. The **message** field is again subdivided into parts, namely, *header* and the *body*. The **header** of the message specifies the sender and the receiver while the **body** contains the information that needs to be transmitted.

Though e-mail is quite popular and efficient but it has some disadvantages along with its advantages. The advantages and disadvantages are discussed in Table 13.1.

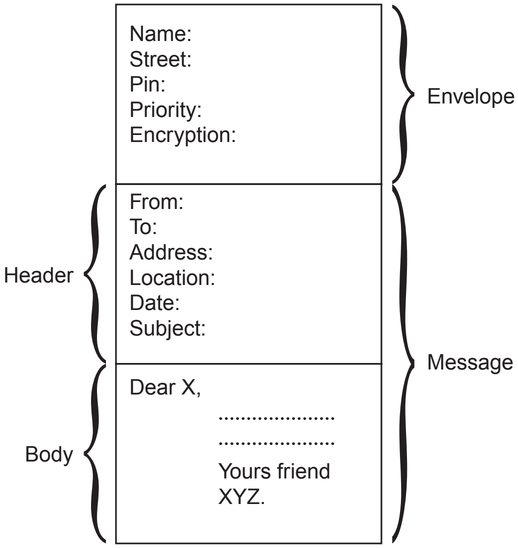


Figure 13.4 Format of an E-mail

Table 13.1 Advantages and Disadvantages of E-mail

Advantages	Disadvantages
• The delivery of messages is very fast, sometimes almost instantaneous, even though the message is meant for overseas or just to a friend next door.	• Although e-mail is delivered instantly, the recipient may or may not read his/her mail on time. That defeats the quickness of electronic mailing.
• The cost of e-mailing is almost free as it involves negligible amount of telephone and ISP charges.	• The user must stay online to read and write more than one mail. In addition, most webmail either display advertisements during use or append them to mails sent. It results in increased size of the original mail, which brings a significant decrease in speed of use.
• Multiple copies of the same message can be sent to a group of people at the same time and can be sent as easily to a single person.	• Since e-mail passes through a network, therefore, it may be intercepted in between. Moreover, viruses can enter the system while downloading the e-mails.
• Pictures, documents and other files can also be attached to messages.	• The slightest error in the address or a failure in one of the links between sender and receiver is enough to prevent a delivery.

7. Describe the architecture of e-mail.

Ans: The architecture of e-mail includes three components, namely, the *user agent* (*UA*), *message transfer agent* (*MTA*) and *message access agent* (*MAA*). The **UA** is a program that helps the user in reading, writing, replying and forwarding message. It also handles the user's mailboxes. The **MTA** is a client/server program where the MTA client can push messages to the MTA server. The **MAA** is a client/server program where the MAA client pulls (retrieves) messages from the MAA server.

To understand how e-mail system works, consider two users A and B on two different systems. Further, assume that both A and B are connected to their respective mail servers by local area network (LAN) or wide area network (WAN). When A wishes to send a message to B, it executes the UA program to prepare the message. Now, as the message is to be sent to A's mail server through LAN/WAN, a pair of MTAs (MTA client and MTA server) is used. The UA after preparing the message sends it to an MTA client, which then sets up a connection with MTA server on the mail server. At A's mail server, the message waiting to be sent is kept in a queue maintained by the mail server. Then, the mail server calls its MTA client to send the message to MTA server at B's mail server connected via Internet. At B's mail server, the received message for B is kept in his/her mailbox. To retrieve the message from mailbox at mail server, B calls the MAA client, which then establishes a connection with MAA server at the mail server. This way B can receive the message sent by A. Figure 13.5 depicts the whole mechanism.

8. What are the services offered by user agent? Also, discuss its types.

Ans: The UA offers various services to the user to make the process of sending and receiving messages easier. These services are discussed as follows:

- **Composing Messages:** This service helps the user in composing the messages that are to be sent. A template is provided by UA, which can be filled by the user to create the messages. Some UAs provide users with built-in editor to perform functions like spelling and grammar checking, emphasizing text by making it bold, italic, etc.

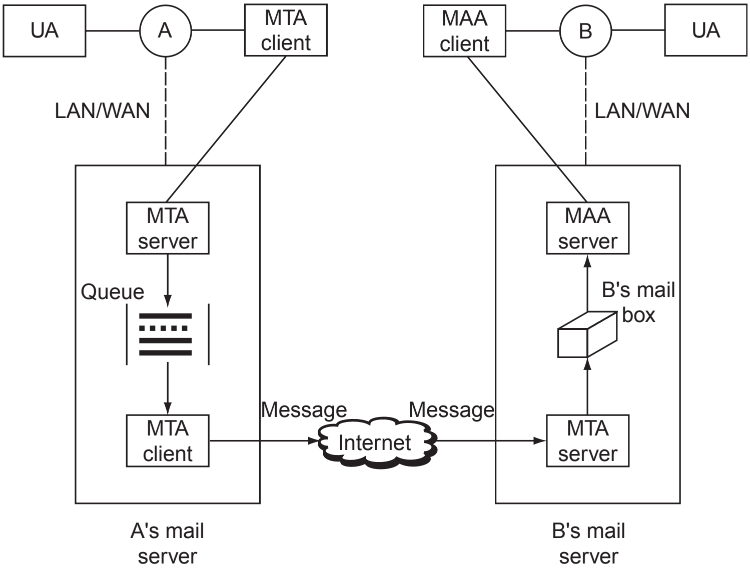


Figure 13.5 Mechanism of E-mail Transfer

- **Reading Messages:** This service helps the user to read the messages, which are in its inbox. Most user agents show a one-line description of each received mail.
- **Replying to Messages:** This service is used to reply to the messages that have been received by the user. While replying, a user can send a new reply or may include the original message sent by the sender along with the new one. Moreover, the user can reply either to the original sender or to all the recipients of message.
- **Forwarding of Messages:** This service helps the user to forward the message to the third party instead of sending it to the original sender. The user can also add some more content in the message to be forwarded.
- **Handling Mailboxes:** The user agent is responsible for maintaining all the mailboxes in e-mail system. Basically, it creates two types of mailboxes, namely, *inbox* and *outbox*. The **inbox** contains all the messages received by a user and the **outbox** contains all the messages sent by the user. The messages are kept in both mailboxes until the user deletes them.

There are two types of UAs namely, *command-driven* and *graphical-user-interface* (*GUI*)*-based UAs*. These types are described as follows:

- **Command-driven UA:** This UA was used in the early days in e-mail. In this type, the user can type one character at a time at the command prompt while replying to the sender. A few command-driven UAs include pine, elm and mail.
- **GUI-based UA:** This UA being used nowadays allows the user to use both mouse and keyboard to interact with the software. As the name of this UA suggests, it provides GUI components such as menus and icons that help the users to access the services more easily. Thus, GUI-based UAs are more user friendly.

9. Write a short note on MIME.

Ans: Multipurpose Internet mail extensions (MIME) is a protocol that enables the transfer of non-ASCII data through e-mails and thus, overcome the limitation of simple e-mail format. It converts non-ASCII messages to a 7-bit NVT ASCII format at the sender's side. The converted message is then forwarded to the MTA client so that it can be sent over the Internet to the receiver. At receiver's side, the message is converted to its original format. Further, MIME can also be used to send messages in different languages such as French, German, Chinese, etc. The structure of MIME defines five new headers that were included in the original e-mail header section. These headers are described as follows:

- **MIME Version:** This header specifies the MIME version and tells the receiver that the sender is using MIME message format. The version number 1.1 is being used nowadays.
- **Content Type:** This header defines the type and subtype of the data used in the message body. The type of the data is followed by its subtype, separated by a slash, that is, type/subtype. Some of the types and their subtypes used by MIME are listed in Table 13.2.

Table 13.2 Data Types and Subtypes in MIME

Type	Subtype	Description
Text	Plain	Unformatted
	HTML	HTML format
Image	JPEG	Image is in JPEG format
	GIF	Image is in GIF format
Video	MPEG	Video is in MPEG format
Audio	Basic	Single-channel encoding of voice at 8 kHz

- **Content Transfer Encoding:** This header defines the different methods used for encoding the messages into various formats, so that it can be transmitted over the network. Some schemes used for encoding the message body are listed in Table 13.3.

Table 13.3 Content Transfer Encoding

Type	Description
7 bit	NVT ASCII characters and short lines
8 bit	Non-ASCII characters and short lines
Binary	Non-ASCII characters with unlimited length

- **Content Id:** This header uniquely identifies the message content
- **Content Description:** This header tells what the body of message contains, that is, whether it contains picture, audio or video. It is an ASCII string that helps the receiver decide whether the message needs to be decoded.

10. Explain SMTP.

Ans: Simple mail transfer protocol (SMTP) is a TCP/IP application protocol that supports e-mail service. It handles the transfer of messages between the sender and receiver. It is based on the client-server model and defines the MTA client and server in the Internet. During the exchange of message between the sender and the receiver, SMTP is used twice. Once, it is used to transfer the mail from sender's end to sender's mail server, and then to transfer the mail from sender's mail server to receiver's mail server. To retrieve the mail from receiver's mail server at the receiver's end, a different mail protocol such as POP3 and IMAP (discussed in the next question) is used. While transferring mails, SMTP uses commands and responses between MTA client and MTA server.

- **Commands:** They are sent from the client machine to the server machine. The syntax of a command consists of a keyword followed by zero or more arguments. There are total 14 commands defined by SMT some of which are listed in Table 13.4.

Table 13.4 SMTP Commands

Keyword	Arguments	Description
HELO<domain>	Sender's host name	It is used for sending sender's identification.
MAIL FROM: <...>	Sender of the message	It specifies the sender's name.
RCPT TO: <...>	Intended recipient of the message	It specifies the receiver's name.
DATA	Body of the mail	It indicates the beginning of mail transmission.
RSET	No arguments	It ends the current mail transaction.
SEND FROM: <...>	Intended recipient of the message	It specifies that this mail should be sent directly to the user's terminal.
SOML FROM: <...>	Intended recipient of the message	It is used to specify that the mail should be sent to user's terminal if possible; otherwise to mailbox.
VRFY	Name of the recipient to be verified	It is used to confirm the user name.

- **Responses:** They are just the opposite of commands, that is, they are sent from a server machine to a client machine. A response consists of a three-digit code, which may be followed by additional textual information. Some of the SMTP responses are shown in Table 13.5.

Table 13.5 SMTP Responses

Code	Information
221	Service closing transmission channel
354	Start mail input
500	Syntax error, unrecognized command
503	Bad sequence or commands

11. Explain in brief the following:

(a) POP3
(b) IMAP4

Ans:

(a) POP3: It stands for **post office protocol** and the number 3 is its version number. It is a simple MAA protocol that has the limited functionality. To use POP3, the client POP3 software and server

POP3 software must be installed on the recipient's machine and on its mail server, respectively. Further, POP3 works in two modes: *delete mode* and *keep mode*. In the **delete mode**, as a message has been pulled from the mail server, it is deleted from the mailbox on the mail server. On the other hand, in the **keep mode** the message remains in the mailbox even after it has been pulled from the mail server. This mail can be read later from any other computer or location.

Whenever a recipient (client) needs to retrieve mails from the mail server, it establishes a TCP connection to the server on the port 110. Then, it passes its username as well as the password to the mail server to get access to the mailbox on the mail server. After the server has verified the client, the client can list and download the messages one at a time.

POP3 has some disadvantages, which are as follows:

- ❑ POP3 does not support mail organization on the server, that is, a user cannot have different folders on the mail server.
- ❑ POP3 does not allow the contents of the mail to be checked in parts while the mail is being downloaded. The mail can be checked after it has been completely downloaded.

(b) IMAP4: It stands for **Internet mail access protocol** and the number 4 denotes its version number. Like POP3, it is also an MAA protocol but it provides more functionality and is more complex than POP3. Some of the additional features provided by IMAP4 are as follows:

- ❑ A user can create folders on the mail server and can delete or rename the mailboxes.
- ❑ IMAP enables the user to partially download the mails. This is especially useful in cases where a message contains large audio and video files, which may take a lot of time to download because of slow Internet connection. In such cases, the user can download only the text part of message if required using IMAP4.
- ❑ A user can search through the contents of the messages while the messages are still on the mail server.
- ❑ IMAP allows the user to check the contents of the e-mail before it has been downloaded.
- ❑ A user can selectively retrieve the attributes of messages such as body, header, etc.

12. What is FTP? How the files a e transferred using FTP?

Ans: File transfer protocol (FTP) is a mechanism provided by TCP/IP to transfer the files between hosts connected via Internet. Further, FTP allows access to the files stored in the directory of a remote computer that is connected to the Internet. In order to access a remote system by FTP, you need to know either the uniform resource locator (URL) or the IP address of the FTP site such as *ftp: ftp.microsoft.com*.

Unlike other client-server applications, FTP establishes two TCP connections between the hosts, namely, *control connection* and *data connection.* The **control connection** is established over well-known TCP port 21 and it remains active throughout the session. This connection is used for transferring control information such as commands and responses. Only one line of command or response can be transferred at one time through the control connection. On the other hand, the **data connection** is established over the well-known TCP port 20 and it is established only after the control connection has established. In addition, it needs to be established and released for each file to be transferred while the control connection is open.

Figure 13.6 shows the FTP file transfer procedure. At the client side, there are three components, namely, *user interface*, *control process* and the *data transfer process* while the server side uses only two components, namely, *control process* and the *data transfer process.* The control processes of client

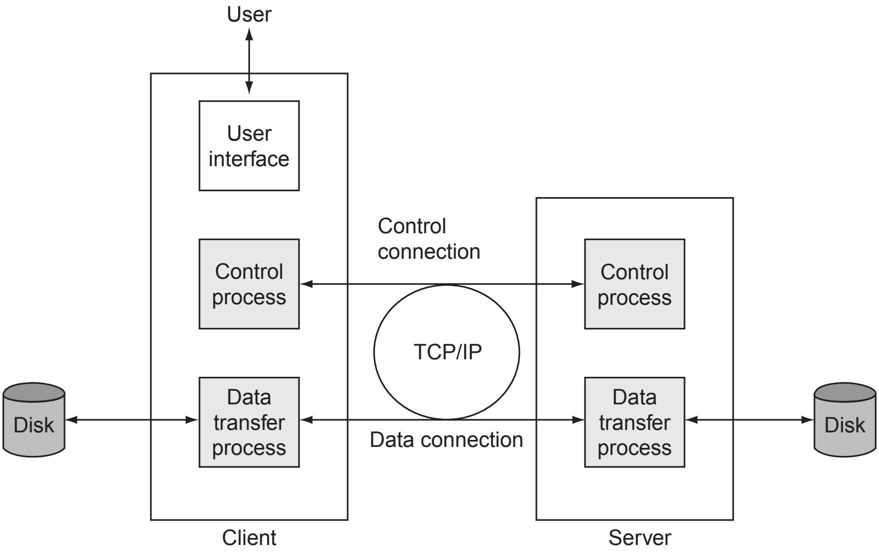


Figure 13.6 Mechanism of File Transfer in FTP

and server are connected via control connection, whereas the data transfer process of client and server are connected via data connection. The control processes of client and server communicate using NVT format. They are responsible for converting from their local syntax such as DOS or UNIX to NVT format and vice versa. The data transfer processes of client and server communicate under the control of commands transferred through the control connection.

13. Explain the following with respect to FTP:

- **File Type**
- **Data Structure**
- **Transmission Mode**

Ans: To transfer a file through the data connection in FTP, the user (client) has to specify certain attributes to the server including type of file to be transferred, the data structure and the transmission mode so that the control connection could be prepared accordingly. These attributes are described as follows:

- **File Type:** FTP supports three types of files for transmission over the data connection, namely, an *ASCII file*, *EBCDIC file* or *image file*. The **ASCII file** is the default format used for text files. It uses the 7-bit ASCII format to encode each character of text file. The sender converts the file from its original form to ASCII characters, while the receiver converts the ASCII characters back to the original form. If **EBCDIC** encoding (file format used by IBM) is supported at the sender or receiver side, then files can be transmitted using the EBCDIC encoding. The **image file** is the default format used in the transmission of binary files. Binary files are sent as continuous stream of bits without using any encoding method. Usually, the compiled programs are transferred using the image file
- **Data Structure:** FTP uses three data structures to transfer a file, namely, *file structure*, *record structure* and *page structure*. When **file structure** format is used, the file is sent as a continuous stream of bytes. The **record structure** can be used only with text files and the file is divided into many records.

In **page structure**, each file is divided into a number of pages where each page contains a page number and a page header. These pages can be accessed sequentially as well as randomly.

- **Transmission Mode:** FTP uses three types of transmission modes, namely, *stream mode*, *block mode* and *compressed mode.* The default mode of transmission is the **stream mode**, which sends the data as a continuous pattern of bytes. In case the data contains only a stream of bytes, then no end-of-file (closing of data connection) is required; the end of file is simply indicated by closing of connection by the sender. In the **block mode**, data is sent in blocks, where each block is preceded by a 3-byte header. The first byte is just a description about the block and the next two bytes define the size of the block in bytes. The **compressed mode** is used in case of large files to reduce their size so that they can be transmitted conveniently. The size of file is reduced by replacing multiple consecutive occurrences of characters with a single character or reducing the number of repetitions. For example, in text files blank spaces can be compressed

14. What is anonymous FTP access?

Ans: Generally, in FTP a user needs an account (username) and password to login to a particular site for accessing the file. However, some sites provide public access to a set of files; the user can access these files without having any account or password. The users can type "anonymous" in the username part and "guest" in the password part. Using FTP in this way is known as anonymous FTP access. With an anonymous FTP, users have restricted access rights and usually, can only list, view or copy files to and from a public directory on the remote system.

15. Define WWW. Explain its architecture.

Ans: The **World Wide Web** (abbreviated as the **Web** or **WWW**) is a collection of linked documents or pages, stored on millions of computers and distributed across the world. The concept of the Web began at CERN (the European Center for Nuclear Research) Geneva, Switzerland in the year 1989. Since then, WWW is the most popularly used Internet subnetwork. One of the main reasons that led to its popularity is that it provides information in multimedia form, that is, in more than one medium such as, text, graphics, video and audio. Further, it provides a simple and consistent way of accessing the information available on the Internet by using hypertext system. In the **hypertext system**, the documents are connected to other related documents on the Internet through links. The Web uses a specific Internet protocol called **hypertext transfer protocol** (**HTTP**) to support hypertext documents.

Further, WWW is based on a distributed client/server architecture in which the services provided by the server are distributed over various locations termed as **sites** and the client can access these services. Each site contains one or more documents, which are known as **web pages**. A web page contains hyperlinks that enable the user to jump on other web pages on the same site or on the different sites. The client can access the web pages through the **browser**—the software that enables a user to read/view web pages. Whenever a user needs to access some web page stored on some site, it sends a request including the address of the site and the web page (known as the **URL**) through its browser to the server. On receiving the request, the server searches the required document and returns it to the client.

The WWW includes many components, which are discussed as follows:

Client (Browser)

Browser is a program which accesses and displays the web pages. It consists of three components, namely, *controller*, *interpreter* and *client protocol*. The user provides inputs (request for a web document) to the controller through a keyboard or a mouse. After receiving the input, the controller uses client protocols such as FTP or HTTP to access the web document. Once the controller has accessed the desired web document, it selects an appropriate interpreter such as hypertext markup language (HTML) or JavaScript depending on the type of the web document accessed. The interpreters help the controller to display the web document. A few of the web browsers used today include Microsoft Internet Explorer, Opera and Google chrome.

To understand how a browser works, consider a user who wants to access the link http://www.ipl.com/home/teams.html. When the user provides this link (URL) to the browser, the browser goes through the following steps:

1. The browser determines the given URL and sends a query to the DNS server asking for the IP address of *www.ipl.com*.
2. The DNS sends a reply to the browser, providing the desired IP address.
3. A TCP connection to port 80 on the received IP address is made by the browser.
4. The browser then sends a request for the file *home/teams.html*.
5. The file *home/teams.html* is sent by the *www.ipl.com server*.
6. The TCP connection is ended.
7. The browser displays the text in the file */home/teams.html*. It also fetches and displays the images in the file

Server

Server is the place where web pages are stored. On a request from the client, the server searches the desired document from the disk and returns the document to the browser through a TCP connection. The steps performed by a server are as follows:

1. The server accepts the TCP connection request arriving from the client.
2. It then acquires the name of the file requested by the client
3. The server retrieves the file from the disk
4. The file is sent back to the client
5. The TCP connection is released.

The efficiency of a server can be improved by caching the recently accessed pages so that those pages could be directly accessed from memory and need not be accessed from the disk. Moreover, server can support multithreading, that is, serving multiple clients at the same time to increase the efficienc .

Uniform Resource Locator

Each web page has a unique address, called the URL that identifies its location on the Internet. This address can be used to locate that page all over the world by millions of people. Usually, the format of an URL consists of four parts: *protocol*, *name of the web server* (or *domain name*), *path* and *filenam* . Here is an example: *http://www.xyz.com/tutor/start/main.htm*. The structure of this URL is:

- **Protocol**: http
- **Web server name/domain name**: www.xyz.com
- **Path**: tutor/start/
- **File name**: main.htm

The first part of the address, the part before the colon, is the protocol. Most of the time *http* is used for accessing a web page. After the protocol, comes the domain name. Colons and slashes respectively separate the protocol and the domain name. Then comes the last part of a URL, namely, the path and the file name. The path name specifies the hierarchical location of the said file on the computer. For instance, in *http://www.xyz.com/tutor/start/main.htm*, the file *main.htm* is located in *start*, which is a subdirectory of *tutor*.

Cookies

Cookies are the small files or strings, which are used to store information about the users. This stored information may be later used by the server while responding to the requests of the client(s). For some particular sites, only registered users are permitted to access the information. In such a case, the server stores the user's registration information in the form of cookies on the client's machine. The size of a cookie file cannot exceed 4 KB. A user can disable the cookies in the browser or can even delete them.

16. What is HTTP? Describe the format of HTTP request and response message.

Ans: Hypertext transfer protocol (**HTTP**) is the most common protocol that is used to access information from the Web. It manages the transfer of data between the client and the server. The older version of HTTP was 1.0, in which TCP connection was released after serving a single request. This was not adequate as every time a new connection had to be established. This led to the development of HTTP version 1.1 that supports persistent connection, that is, it is meant for multiple request–response operations.

Further, HTTP is a stateless protocol and all the transactions between the server and client are carried out in the form of messages. The client sends a **request messag**e to the server and the server replies with a **response message**. The HTTP request and response messages have a similar format (Figure 13.7) except that in request message, the first line is the request line while in response message, and the first line is the status line. The remaining part of both the messages consists of a header and sometimes, a body.

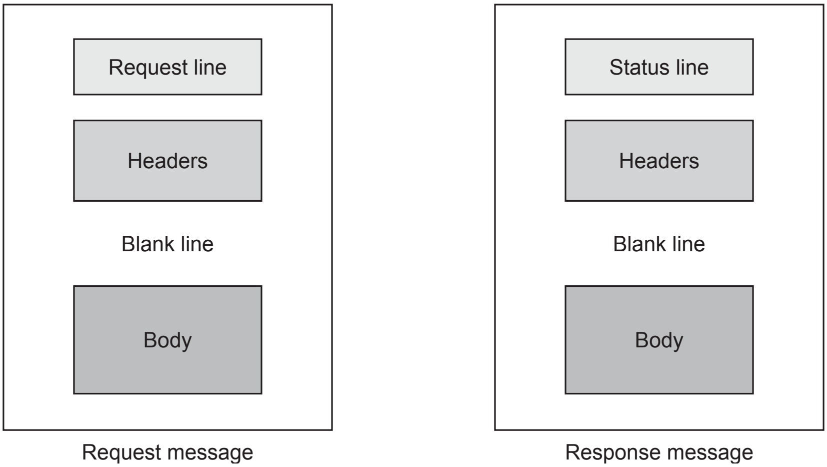


Figure 13.7 Format of HTTP Request and Response Message

The HTTP request messages are of different types, which are categorized into various methods as shown in Table 13.6.

For each HTTP request message, the server sends an HTTP response that consists of status line and some additional information. The status line comprises a three digit status code, similar to the response message of FTP and SMTP. The status code indicates whether the client request is satisfied or if there is some error. The first digit of the status code can be 1, 2, 3, 4 or 5 and it indicates one of the five groups

Table 13.6 The Built-in HTTP Request Methods

Method	Description
GET	Request to access a web page from the server.
HEAD	Request to get the header of a web page
PUT	Request to store a web page
POST	Append to a named resource
DELETE	Remove the web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Enquire about certain options

into which response messages have been divided. Codes falling in the 100 range are only informational and thus, rarely used. The codes falling in the 200 range indicate a successful request, codes in the 300 range redirect the client to some other site, the codes in the 400 range indicate an error in the client side and the codes in the 500 range indicate an error at the server site.

Further, HTTP also contains various headers, which are used to transfer additional information other than the normal message between the client and the server. For example, the request header can ask for a message to be delivered in some particular format while a response header can contain a description of the message. The additional information can be included in one or more header lines within the header. Each header line has a format as shown in Figure 13.8.

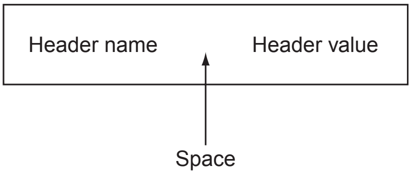


Figure 13.8 HTTP Header Format

Each header line may belong to one of the four types of HTTP headers, which are discussed as follows:

- **General Header:** This header can be included in both request and response message. It contains general information about the sent or received messages. An example of a general header is Date that is used to display the current date.
- **Request Header:** This header can be used only in the request messages from the client. The details about the client setup and the preference of the client for any particular format are included in this header. An example of a request header is the From header, which shows the e-mail address of the user.
- **Response Header:** This header is part of the response messages only. It contains the server's setup information. An example of a response header is the Age header, which shows the age of the document.
- **Entity Header:** This header includes information about the body of a document. It is mostly present in the request or response messages. An example of entity header is the Allow header, which lists the valid methods that can be used with a URL.

17. Compare HTTP with FTP and SMTP.

Ans: Functionally, HTTP works as a combination of FTP and SMTP. It is similar to FTP as it is also used to transfer files over the TCP connection. However, it differs from FTP in the respect that it can transfer only data and thus, no separate control connection is needed. It uses only one TCP connection over port number 80.

Further, HTTP is similar to SMTP because in both protocols, the client initiates a request and the server responds to that particular request. However, HTTP messages can only be read by HTTP server and HTTP client, whereas in SMTP, messages can be read by humans also. Moreover, HTTP messages are forwarded immediately unlike in SMTP, where messages are first stored and then forwarded

18. What is a proxy server and how it is related to HTTP?

Ans: A **proxy server** is a computer, which stores the copies of responses to most recently requests in its cache so that further requests for these pages need not be sent to the original server. The proxy server helps to reduce the load on the original server as well as decrease the network traffic thereby improving the latency. To use the proxy server, the client must be configured to send HTTP requests to proxy server instead of the original server. Whenever a HTTP client wishes to access a page, it sends HTTP request to a proxy server. On receiving a request, the proxy server looks up in the cache for the desired web page. If the page is found, the stored copy of response is sent back to the client; otherwise, the HTTP request is forwarded to the target server. Similarly, the proxy server receives responses from the target server. The proxy server stores these responses in the cache and then sends it to the client.

19. Explain SNMP and mention the two protocols used by it for managing tasks.

Ans: **Simple network management protocol** (**SNMP**) is an operational framework, which helps in the maintenance of the devices used in the Internet. In addition, SNMP comprises two components, namely, *manager* and *agent*. A station (host) which manages another station is called the **manager**. It runs the SNMP client program. The **agent** is the station (router) which runs the server program and is managed by the manager. Both the stations interact with each other to carry out the management. The manager can access all the information stored in the agent station. This information can be used by the manager to check the overall performance. The manager can also perform some remote operation on the agent station such as rebooting the remote station. On the other hand, the agent can also perform some management operations, such as informing the manager about the occurrence of any unusual situation, which may hamper the performance.

In order to manage tasks efficiently, SNMP uses two protocols: *structure of management information* (SMI) and *management information base* (MIB).These two protocols function together with the SNMP. The role of SMI and MIB protocols is discussed as follows:

- **SMI:** It generally deals with the naming of objects and defining their range and length. However, it does not specify the number of objects maintained by an entity, the relationship between objects, and their corresponding values.
- **MIB:** MIB basically performs the work that SMI has left behind. It defines the object name as per the conventions specified by SMI. It also states the number of objects and their types

Multiple Choice Questions

1. Which of the following is/are an application layer service?
   (a) remote login
   (b) file transfer and acces
   (c) domain name service
   (d) all of these

2. Which port number is used by the DNS server for both TCP and UDP connections?
   (a) 54 (b) 53
   (c) 51 (d) 50

3. The client TELNET translates characters that come from the local terminal into_____ character form and delivers them to the network.
   (a) ASCII (b) BCD
   (c) NVT (d) EBCDIC

4. The well-known port _____ is used for the control connection and the well-known port ______ is used for the data connection.
   (a) 20, 21   (b) 21, 20
   (c) 21, 22   (d) 20, 22

5. Which is the default format used by FTP for transferring text files
   (a) EBCDIC   (b) binary fil
   (c) ASCII fil   (d) bytes

6. Which port is used by SMTP for TCP connection?
   (a) 25   (b) 26
   (c) 21   (d) 20

7. Which protocol uses the GET and POST methods?
   (a) SMTP   (b) MIME
   (c) IMAP4   (d) HTTP

8. Which of the following supports a persistent connection?
   (a) FTP   (b) SMTP
   (c) HTTP   (d) MIME

9. Which of the following are MAA protocols?
   (a) SMTP and MIME
   (b) FTP and HTTP
   (c) SMTP and FTP
   (d) POP3 and IMAP4

10. Which of the following is the protocol used for network management?
   (a) SNMP   (b) POP3
   (c) FTP   (d) IMAP4

Answers

1. (d)   2. (b)   3. (c)   4. (b)   5. (c)   6. (a)   7. (d)   8. (c)   9. (d)   10. (a)

14

Multimedia

1. Defin multimedia.

Ans: The word multimedia is made up of two separate words, **multi** means many and **media** means the ways through which information may be transmitted. Therefore, **multimedia** can be described as an integration of multiple media elements (such as text, graphics, audio, video and animation) together to influence the given information, so that it can be presented in an attractive and interactive manner. In simple words, multimedia means being able to communicate in more than one way.

2. What are the different categories of Internet audio/video services?

Ans: Earlier, the use of Internet was limited for only sending/receiving text and images; however, nowadays, it is vastly being used for audio and video services. These audio and video services are broadly classified into three categories, namely, *streaming stored audio/video*, *streaming live audio/video* and *real-time interactive audio/video*. Here, the term **streaming** implies that the user can listen to or view the audio/video file after its downloading has begun

- **Streaming Stored Audio/Video:** In this category, the audio/video files are kept stored on a server in a compressed form. The users can download these stored files whenever required using the Internet; that is why this category is also termed as **on-demand audio/video**. Some examples of stored audio/video include songs, movies and video clips.
- **Streaming Live Audio/Video:** In this category, as the term **live** implies, the users can listen to or view audio/video that are broadcast through the Internet. Some examples of live audio/video applications include Internet radio and Internet TV.
- **Real Time (Interactive) Audio/Video:** In this category, users can communicate with each other in an interactive manner using the Internet. This category of Internet audio/video is used for real-time interactive audio/video applications such as Internet telephony, online video chatting and Internet teleconferencing.

3. How does streaming live audio/video differ from streaming stored audio/video?

Ans: The major difference between streaming live audio/video and streaming stored audio/video is that in the former, the communication is meant for a single user (unicast) and occurs on demand when the user downloads the file whereas in the latter, the communication is live instead of on demand and file is broadcast to multiple users at the same time

4. Explain the approaches that can be used to download streaming stored audio/video files

Ans: The streaming stored audio/video files are stored on a server in compressed form. In order to listen to or view these files, one needs to download them. There are mainly four approaches that can be used to download streaming audio/video files. These approaches are discussed as follows:

Using a Web Server

This is the simplest approach that allows the compressed audio/video file stored on a Web server to be downloaded as a text file. Following steps are involved in downloading file from th Web server.

1. The browser on the client machine establishes a TCP connection with the Web server on which the desired audio/video file is stored
2. After the connection has been established, the browser requests for desired file by sending a `GET` message to the Web server using the HTTP services.
3. The Web server in response retrieves the desired compressed file from the disk and sends it to the browser on the client machine.
4. The browser writes the received audio/video file to the disk
5. The browser uses some helper application such as Windows Media Player that retrieves the contents of file from the disk block by block and plays back the fil

This approach does not require streaming. Thus, the file cannot be played black on the media player until it gets downloaded entirely.

Using a Web Server with Metafile

This approach overcomes the limitation of first approach by allowing the media player on client machine to directly connect with the Web server, so that file can be played back as its downloading starts. There are two files stored on the Web server, one is the original audio/video file and the other is a **metafil** that contains the link (URL) to the desired file. Following are the steps for this approach. Following steps are involved in this approach.

1. The browser on the client machine sends the `GET` message using the HTTP services to access the Web server.
2. The Web server in response sends back the metafile
3. The browser passes the metafile to the media playe .
4. The media player reads the URL in the metafile and sends `GET` message using the HTTP services to access the audio/video file
5. The Web server responds now to the media player and not to the browser.
6. The file is played back on the media playe , as it is being fetched by the Web server.

Using a Media Server

In the second approach, both the browser and the media player access the Web server using the HTTP services. However, in certain cases, it may happen that the server mentioned in URL stored in metafile is different from the Web server. Moreover, it may not be even an HTTP server, but some specialized media server. In such cases, the audio/video files cannot be downloaded using HTTP; rather any protocol that runs over UDP can be used to download the file. Following are the steps invo ved in this approach.

1. The browser on the client machine uses the HTTP services and sends the `GET` message to access the Web server.
2. The Web server in response sends back the metafile
3. The browser passes the metafile to the media playe .
4. The media player reads the URL in the metafile and sends `GET` message to the media server to download the audio/video file from it
5. The media server responds to the media player.
6. The file is played back on the media playe , as it is being fetched by the media server.

Using a Media Server and Real Time Streaming Protocol (RTSP)

In this approach, the media server uses RTSP that offers additional functionalities to the streaming of media files such as pla , record and pause. The steps involved in this approach are as follows:

1. The browser on the client machine uses the HTTP services and sends the `GET` message to access the Web server.
2. The Web server in response sends back the metafile
3. The browser passes the metafile to the media playe .
4. The media player reads the URL in the metafile and sends a `SETUP` message to the media server to establish a connection between them.
5. The media sever responds to the media player.
6. The media player forwards a PLAY message to the media server to start downloading of file
7. The downloading of file gets started using a protocol that runs over UDP. The file is played back on the media player, as it is being fetched by the media server. Notice that while the file is being downloaded, the media player can send a PAUSE message to the media server to temporarily stop the downloading which can later be resumed by sending PLAY message.
8. After the file has been downloaded completely, the media player sends a TEARDOWN message to the media server to release the connection between them.
9. The media server in response releases the connection.

5. Write a short note on real-time transport protocol (RTP)?

Ans: **RTP** is a transport layer protocol designed for interactive (real-time) multimedia applications on the Internet such as Internet telephony, video-on-demand and video conferencing. These applications involve multiple streams of multimedia data including text, audio, video and graphics, being transmitted in real time over the Internet and RTP is responsible for managing these streams. RTP has been placed above UDP in the protocol hierarchy and is implemented in the user space (application layer); however, it must be used with UDP.

The basic function of RTP is to multiplex multiple real-time data streams of multimedia data onto single stream of UDP packets. To do this, different streams of multimedia data are first sent to RTP library that is implemented in the user space along with the multimedia application. The RTP library multiplexes these streams and encodes them in RTP packets, which are then stuffed into a socket. At the other end of the socket, the UDP packets are created and embedded in IP packets. Now, depending on the physical media say Ethernet, the IP packets are further embedded in Ethernet frames for transmission. Besides, some other functions of RTP include sequencing, time-stamping and mixing.

6. Explain the RTP packet header format.

Ans: The RTP is a transport layer protocol that has been designed to handle real-time traffic on the Internet. Figure 14.1 shows the format of an RTP packet header, which consists of various fields. Each field of TP packer header is described as follows:

- **Ver.:** It is a 2-bit long field that indicates the version number of RTP. The current version of RTP is 2.
- **P:** It is a 1-bit long field that indicates the presence of padding (if set to 1) or absence of padding (if set to 0) at the end of the packet. Usually, the packet is padded if it has been encrypted. The number of padding bytes added to the data is indicated by the last byte in padding.
- **X:** It is a 1-bit long field that is set to 1 if an extra extension header is present between the basic header and the data; otherwise, its value is 0.
- **Contributor Count (CC):** It is a 4-bit long field that signifies the total number of contributing sources participating in the session. Since this field is of four bits, its value can range from 0 to 15, that is, the maximum of 15 contributing sources can participate in the same session.
- **M:** It is a 1-bit marker field that is specific to the application being used. The application uses this marker to indicate certain things such as the start of a video frame and the end of a video frame.
- **Payload Type:** It is a 7-bit long field that indicates the type of encoding algorithm used such as MP3, delta encoding and predictive encoding.
- **Sequence Number:** It is a 16-bit long field that indicates the sequence number of the RTP packet. Each packet that is sent in an RTP stream during a session is assigned a specific sequence number. The sequence number for the first packet during a session is selected randomly and it is increased by one for every subsequent packet. The purpose of assigning sequence number to packets is to enable the receiver to detect the missing packets (if any).
- **Timestamp:** It is a 32-bit long field that is set by the source of stream to indicate when the first sample in the packet was produced. Generally, the first packet is assigned a timestamp value at random while the timestamp value of each subsequent packet is assigned relative to that of the first (or previous) packet. For example, consider there are four packets with each packet containing 15 s of information. This implies, if the first packet starts at `t` = 0, then second packet should start at `t` = 15, the third packet at `t` = 30 and the fourth at `t` = 45. This time relationship between the packets must be preserved at the playback time on the receiver to avoid the jitter problem. For this, timestamp values are assigned to receiver. Suppose the first packet is assigned a timestamp value 0, then the timestamp value for the second, third and fourth packets should be 15, 30 and 45, respectively. Now, the receiver on receiving a packet can add its timestamp to the time at which it starts playback. Thus, by separating the playback time of packets from their arrival time, the jitter problem is prevented at the receiver.

- **Synchronization Source Identifier** It is a 32-bit long field that indicates the source stream of the packet. In case of a single source, this field identifies that source. However, in case of multiple sources, this field identifies the **mixer**—the synchronization source—and the rest of the sources are the **contributors** identified by the contributing source identifiers. The role of mixer is to combine the streams of RTP packets from multiple sources and forward a new RTP packet stream to one or more destinations.
- **Contributing Source Identifier** It is a 32-bit long field that identifies a contributing source in the session. There can be maximum 15 contributing sources in a session and accordingly, 15 contributing source identifiers

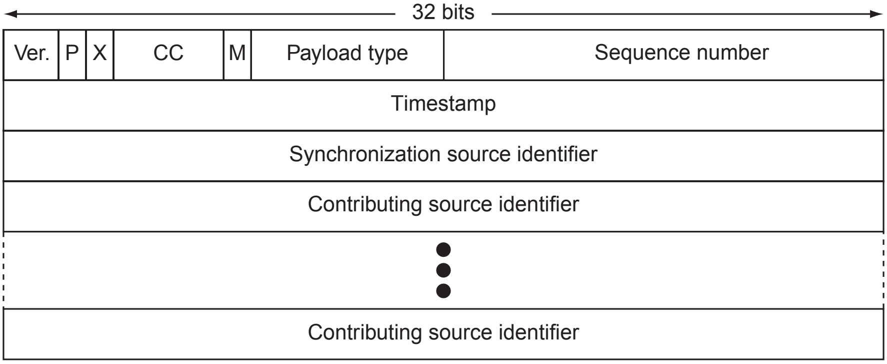

32 bits
Ver.
P
X
CC
M
Payload type
Sequence number
Timestamp
Synchronization source identifier
Contributing source identifier
Contributing source identifier

Figure 14.1 RTP Packet Header Format

7. What is RTCP? Describe the packet types define by it?

Ans: RTCP (stands for **real time transport control protocol**) is called a sibling protocol of RTP. RTP enables to transport messages containing only data; however, at certain times, some different types of messages that control the flow and quality of data are required to be sent. For example, a receiver may send a feedback on received quality of service to the source as well as other participants in the session, so that better quality could be achieved in future. To send such messages, RTCP is used. RTCP transmission contains five types of packets (containing messages) encapsulated into a single-UDP datagram. These packet types are described as follows:

- **Sender Report (SR):** This packet is used by RTCP receivers to provide feedback about the quality aspects of data transmission and reception from active senders. It may contain information regarding jitter, delay, congestion, bandwidth and other network properties. Absolute time stamp, that is, the number of seconds elapsed since midnight on January 1, 1970 is included in the sender's report. This helps the receiver in synchronizing multiple RTP packets.
- **Receiver Report (RR):** This packet is used for passive participants that do not transmit any RTP packets. The RR packet communicates the information related to quality of service to the senders as well as other receivers.
- **Source Description (SDES):** This packet is transmitted periodically by a source to give more information about itself such as its user name, e-mail address, geographical location and telephone number.
- **BYE:** This packet is a direct announcement sent by a source to indicate its exit from a session. Whenever a mixer receives a Bye message, it forwards this message along with list of sources still participating in the session to all the stations in session. A Bye packet can also contain the reason for exit as a description in text format.

- **Application-define Packet:** This packet is an experimental packet for applications that wish to use new applications that have not been defined in the RTCP standard. Eventually, if an experimental packet type is found useful, it may be assigned a packet type number and included in RTCP standards.

8. How is SIP used in the transmission of multimedia?

Ans: SIP, which stands for **session initiation protocol**, is designed by IETF to handle communication in real-time (interactive) audio/video applications such as Internet telephony, also called voice over IP (VoIP). It is a text-based application layer protocol that is used for establishing, managing and terminating a multimedia session. This protocol can be used for establishing two-party, multiparty or multicast sessions during which audio, video or text data may be exchanged between the parties. The sender and receiver participating in the session can be identified through various means such as e-mail addresses, telephone numbers or IP addresses provided all these are in SIP format. That is why SIP is considered very flexible

Some of the services provided by SIP include defining telephone numbers as URLs in Web pages, initiating a telephone call by clicking a link in a Web page, establishing a session from a caller to a callee and locating the callee. Some other features of SIP include call waiting, encryption and authentication.

SIP defines six messages that are used while establishing a session, communicating and terminating a session. Each of these messages is described as follows:

- **INVITE:** This message is used by the caller to start a session.
- **ACK:** This message is sent by the caller to callee to indicate that the caller has received callee's reply.
- **BYE:** This message is used by either caller or callee to request for terminating a session.
- **OPTIONS:** This message can be sent to any system to query about its capabilities.
- **CANCEL:** This message is used to cancel the session initialization process that has already started.
- **REGISTER:** This message is sent by a caller to the registrar server to track the callee in case the callee is not available at its terminal, so that the caller can establish a connection with the callee. SIP designates some of the servers on the network as **registrar server** that knows the IP addresses of the terminals registered with it. At any moment, each user (terminal) must be registered with at least one registrar server on the network.

Before starting transmission of audio/video between the caller and callee, a session needs to be started. A simple SIP session has three phases (see Figure 14.2), which are as follows:

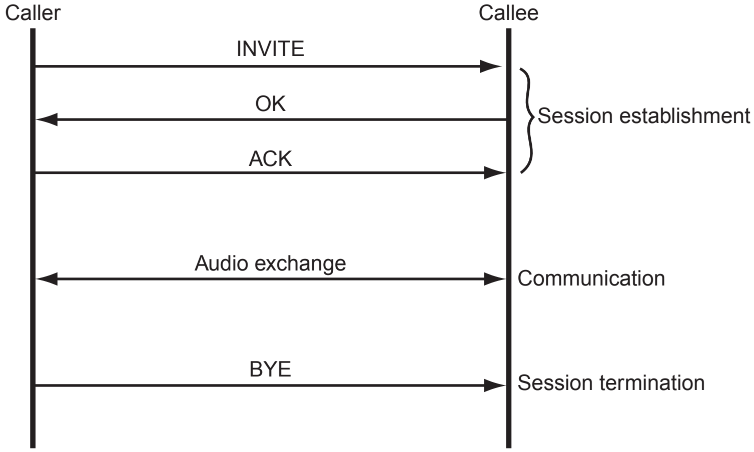


Figure 14.2 Phases in Session Using SIP

1. **Session Establishment:** The session between the caller and callee is established using the three-way handshake. Initially, the caller invites the callee to begin a session by sending it an INVITE message. If the callee is ready for communication, it responds to the caller with a reply message (OK). On receiving the reply message, the caller sends the ACK message to callee to confirm the session initialization.
2. **Communication:** Once the session has been established, the communication phase commences during which the caller and callee exchange audio data using temporary port numbers.
3. **Session Termination:** After the data has been exchanged, either the caller or the callee can request for the termination of session by sending a BYE message. Once the other side acknowledges the BYE message, the session is terminated.

9. Explain the H.323 standard.

Ans: H.323 is an ITU standard that allows communication between the telephones connected to a public telephone network and the computers (called **terminals**) connected to the Internet. Like SIP, H.323 also allows two-party and multiparty calls using a telephone and a computer. The general architecture of this standard is shown in Figure 14.3.

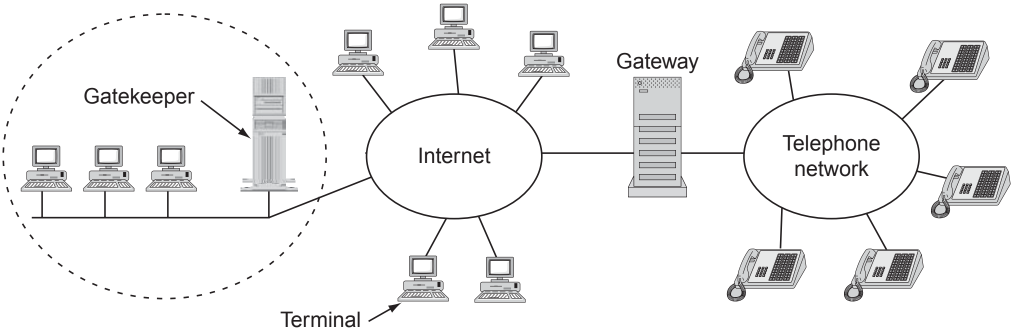


Figure 14.3 H.323 Architecture

As shown in Figure 14.3, the two networks, Internet and telephone networks, are interconnected via a **gateway** between them. As we know that a gateway is a five-layer device that translates messages from a given protocol stack to different protocol stack. In H.323 architecture, the role of gateway is to convert between the H.323 protocols on the Internet side and PSTN protocols on the telephone side. The **gatekeeper** on the local area network serves as the registrar server and knows the IP addresses of the terminals registered with it.

H.323 comprises many protocols which are used to initiate and manage the audio/video communication between the caller and the callee. The **G.71** or **G.723.1** protocols are used for compression and encoding/decoding speech. The **H.245** protocol is used between the caller and the callee to negotiate on a common compression algorithm that will be used by the terminals. The **H.225** or **RAS** (**Registration/Administration/Status**) protocol is used for communicating and registering with the gatekeeper. The **Q.931** protocol is used for performing functions of the standard telephone system such as providing dial tones and establishing and releasing connections.

Following are the steps involved in communication between a terminal and a telephone using H.323.

1. The terminal on a LAN that wishes to communicate with a remote telephone broadcasts a UDP packet to discover the gatekeeper. In response, the gatekeeper sends its IP address to the terminal.
2. The terminal sends a RAS message in a UDP packet to the gatekeeper to register itself with the gatekeeper.
3. The terminal communicates with the gatekeeper using the H.225 protocol to negotiate on bandwidth allocation.
4. After the bandwidth has been allocated, the process of call setup begins. The terminal sends a SETUP message to the gatekeeper, which describes the telephone number of the callee or the IP address of a terminal if a computer is to be called. In response to receipt of SETUP message, the gatekeeper sends CALL PROCEEDING message to the terminal. The SETUP message is then forwarded to the gateway, which then makes a call to the desired telephone. As the telephone starts ringing up, an ALERT message is sent to the calling terminal by the end office to which the desired telephone is connected. After someone picks up the telephone, a CONNECT message is sent by the end office to the calling terminal to indicate the establishment of connection. Notice that during call setup, all entities including terminal, gatekeeper, gateway and telephone communicate using the Q.931 protocol. After the connection establishment, the gatekeeper is no longer involved.
5. The terminal, gateway and telephone communicate using the H.245 protocol to negotiate on the compression method.
6. The audio/video in form of RTP packets is exchanged between the terminal and telephone via gateway. For controlling the transmission, RTCP is used.
7. Once either of the communicating parties hangs up, the connection is to be terminated. For this, the terminal, gatekeeper, gateway and telephone communicate using Q.931 protocol.
8. The terminal communicates with the gatekeeper using the H.225 protocol to release the allocated bandwidth.

10. Define compression. What is the difference between lossy and lossless compression?

Ans: The components of multimedia such as audio and video cannot be transmitted over the Internet until they are compressed. **Compression** of a file refers to the process of cutting down the size of the file by using special compression algorithms. There are two types of compression techniques: *lossy* and *lossless*.

In **lossy** compression technique, some data is deliberately discarded in order to achieve massive reductions in the size of the compressed file. In this compression format, we cannot recover all of its original data from the compressed version. JPEG image files and MPEG video files are the examples of lossy compressed files. On the other hand, in **lossless** compression technique, the size of the file is reduced without permanently discarding any information of the original data. If an image that has undergone lossless compression is decompressed, the original data can be reconstructed exactly, bit-for-bit, that is, it will be identical to the digital image before compression. PNG image file formats use lossless compression

11. Write a short note on audio compression.

Ans: Before the audio data can be transmitted over the Internet, it needs to be compressed. Audio compression can be applied on speech or music. There are two categories of techniques that can be used to compress audio, namely, *predictive encoding* and *perceptual encoding*.

- **Predictive Encoding:** In digital audio or video, successive samples are usually similar to each other. Considering this fact, the initial frame and the difference values in the successive samples for all the samples are stored in the compressed form. As the size of the difference values between two samples is much smaller than the size of sample itself, this encoding technique saves much space. While decompressing, the previous sample and the difference value are used to reproduce the next sample. Predictive encoding is generally used for speech.

- **Perceptual Encoding:** The human auditory system suffers from certain flaws. Exploiting this fact, the perceptual encoding technique encodes the audio signals in such a manner that they sound similar to human listeners, even they are different. This technique is generally used for compressing music, as it can create CD-quality audio. MP3, a part of MPEG standard, is the most common compression technique based on perceptual encoding.

12. How does frequency masking differ from temporal masking?

Ans: Effective audio compression takes into account the physiology of human hearing. The compression algorithm used is based on the phenomenon named **simultaneous auditory masking**—an effect that is produced due to the way the nervous system of human beings perceives sound. Masking can occur in frequency or time, accordingly named as *frequency masking* and *temporal masking*.

In **frequency masking**, a loud sound in a frequency range can partially or completely mask (hide) a low or softer sound in another frequency band. For example, in a room with loud noise, we are unable to hear properly the sound of a person who is talking to us.

In **temporal masking**, a loud sound can make our ears insensitive to any other sound for a few milliseconds. For example, on hearing a loud noise such as a gunshot or explosion, it makes our ears numb for a very short time before we are actually able to start hearing again properly.

13. Explain the JPEG process.

Ans: **JPEG**, which stands for **joint photographic experts group**, is the standard compression technique used to compress still images. It can compress images in lossy and lossless modes and produces high-quality compressed images. Following are the steps involved in the JPEG image compression (lossy) process.

1. **Colour Sub-Sampling:** This step is performed only if the image to be compressed is coloured; for gray-scale images, this step is not required. The RGB colour space of the image is changed to YUV colour space and its chrominance component is down-sampled.
2. **Blocking:** The image is divided into a series of 8 × 8-pixel blocks. Blocking also reduces the number of calculations needed for an image.
3. **Discrete Cosine Transformation (DCT):** Each block of 8 × 8 pixels goes through the DCT transformation to identify the spatial redundancy in an image. The result of DCT transformation for each 8 × 8 block of pixels is 8 × 8 block of DCT coefficients (that is, 64 frequency components in each block).
4. **Quantization:** In this phase, the DCT coefficients in each block are scalar quantized with the help of a quantization table (Q-table) in order to wipe out the less important DCT coefficients. Each value in the block is divided by a weight taken from the corresponding position in Q-table by ignoring the fractional part. The changes made in this phase cannot be undone. That is why this JPEG method is considered lossy.
5. **Ordering:** The output of quantization is then ordered in a zigzag manner to distinguish the low-frequency components (usually, non-zero) from the high-frequency components (usually, zero). Ordering results in bit stream in which zero-frequency components are placed close to the end.
6. **Run-Length Encoding:** The run-length encoding is applied to zeros of zigzag sequence to eliminate the redundancy. This encoding replaces each repeated symbol in a given sequence with the

symbol itself and the number of times it is repeated. For example, the text "ccccccbbbbuffffff" is compressed as "c7b4u1f6". Thus, redundant zeros are removed after this phase.

7. **Variable-length Encoding:** The variable-length encoding is applied on the output of the previous phase to get the compressed JPEG bit stream. In variable-length encoding, a variable number of bits are used to represent each character rather than a fixed number of bits for each character. Fewer bits are used to represent the more frequently used character; the most frequently used character can be represented by one bit only. This helps in reducing the length of compressed data.

14. What is MPEG? Describe spatial and temporal compressions?

Ans: MPEG, which stands for **moving picture experts group**, is a method devised for the compression of a wide range of video and motion pictures. It is available in two versions: MPEG1 and MPEG2. The former version has been designed for CD-ROM with a data arête of 1.5 Mbps while the latter version has been designed for DVD with a data rate of 3–6 Mbps.

Each video is composed of a set of frames where each frame is actually a still image. The frames in a video flow so rapidly (for example, 50 frames per second in TV) that the human eye cannot notice the discrete images. This property of human eye forms the basis of motion pictures. Video compression using MPEG involves *spatial compression* of each frame and *temporal compression* of a set of frames.

- **Spatial Compression:** Each frame in the video is spatially compressed with JPEG. Since each frame is an image, it can be separately compressed. Spatial compression is used for the purposes such as video editing where frames need to be randomly accessed.
- **Temporal Compression:** In this compression, the redundancy is removed among the consecutive frames that are almost similar. For example, in a movie, there are certain scenes where the background is same and stationary and only some portion such as hand movement is changing. In such cases, the most consecutive frames will be almost similar except the portion of frame covering the hand movements. That is, the consecutive frames will be containing redundant information. The temporal redundancy can be eliminated using the differential encoding approach, which encodes the differences between adjacent frames and sends them. An alternative approach is motion compensation that compares each frame with its predecessor and records the changes in the coordinate values due to motion as well as the differences in pixels after motion.

15. Differentiate among the different types of encoded frames used in MPEG video compression.

Ans: In MPEG video compression, the encoded frames fall under three categories, namely, *intracoded* (*I*) *frames*, *predicted* (*P*) *frames* and *bidirectional* (*B*) *frames*. These frames are described as follows:

- **I-frame:** This frame is not associated with any other frame (previous or next). It is encoded independently of other frames in the video and contains all the necessary information that is needed to recreate the entire frame. Thus, I-frames cannot be constructed from any other frames. I-frames must appear in a movie at regular intervals to indicate the sudden changes in the frame.
- **P-frame:** This frame relates to the frame preceding to it whether it is an I-frame or a P-frame. It contains small differences related to its preceding I-frame or P-frame; however, it is not useful for recording major modifications; for example, in case of fast-moving objects. Thus, P-frames carry only a small amount of information as compared to other frames and even more less number of bits after compression. Unlike I-frames, a P-frame can be constructed only from its preceding frame.

- **B-frame:** This frame, as the name implies, relates to its preceding as well as succeeding I-frame or P-frame. However, a B-frame cannot relate to any other B-frame. B-frames provide improved motion compensation and the best compression.

Multiple Choice Questions

1. Which of the following services is provided by RTP?
   (a) Time-stamping (b) Sequencing
   (c) Mixing (d) All of these

2. In __________, the user can listen to or watch the file only after the file has bee downloaded.
   (a) Streaming stored audio/video
   (b) Streaming live audio/video
   (c) Interactive audio/video
   (d) None of these

3. MP3 audio compression uses two phenomena, namely, __________.
   (a) Spatial compression and temporal compression
   (b) DCT and quantization
   (c) Frequency masking and temporal masking
   (d) None of these

4. Which step of the JPEG image compression is not needed for grey-scale images?
   (a) Quantization
   (b) Colour sub-sampling
   (c) Blocking
   (d) Discrete cosine transformation

5. Which of the following approaches that is used to download streaming stored audio/video does not involve streaming?
   (a) Using a Web server
   (b) Using a media server
   (c) Using a Web server with a metafil
   (d) Using a media server and RTSP

6. Which of the following is a characteristic of real-time interactive audio/video?
   (a) Time relationship (b) Mixing
   (c) Ordering (d) All of these

7. Which of the following message types is provided by both RTCP and SIP?
   (a) INVITE (b) BYE
   (c) Sender report (d) None of these

8. In H.323 architecture, __________ serves as the registrar server.
   (a) Gateway (b) Terminal
   (c) Gatekeeper (d) Telephone network

Answers

1. (d) 2. (a) 3. (c) 4. (b) 5. (a) 6. (d) 7. (b) 8. (c)

15

Network Security

1. What are the desirable requirements for a secure communication?

Ans: Nowadays, the computer network is used by most people for performing their tasks such as shopping, bill payment and banking. Thus, it becomes important to secure the network, so that unauthorized people could not access the information. For secured communication, there are some basic requirements that must be met. These are as follows:

- **Confidentiality** It refers to maintaining secrecy of the message being transmitted over the network. Only the sender and the intended receiver should be able to understand and read the message and no eavesdropper should be able to read or modify the contents of the message. Therefore, the users want their message to be transmitted over network in encrypted form.
- **Authentication:** It is concerned with determining whom you are communicating with. Authentication is must to ensure the receiver that the message has been received from the actual sender and not from the attacker. That is, the receiver should be able to authenticate the sender, which can be achieved by sharing a common secret code word, by sending the digital signatures or by the use of digital certificates
- **Integrity:** Any message sent over the network must reach to its intended receiver without any modification made to it. If any changes have been made, the receiver must be able to detect that alteration has happened. Integrity can be achieved by attaching a checksum to the message. This checksum ensures that an attacker cannot alter the message; therefore, integrity can be preserved.
- **Non-repudiation:** After a message has been sent and received, the sender and the receiver should not be able to deny about the sending and receiving of the message. The receiver should be able to prove that the message has come from the intended sender and not from anyone else. In addition, the receiver should be able to prove that the contents of the received messages are same as sent by the sender.

2. What do you understand by network security attack? Describe active and passive attacks.

Ans: A **network security attack** refers to an act of breaching the security provisions of a network. Such an act is a threat to the basic goals of secure communication such as confidentiality, integrity and authenticity. Network security attacks can be classified under two categories, namely, *passive attack* and *active attack*.

- **Passive Attack:** In a passive attack, an opponent is indulged in eavesdropping, that is, listening to and monitoring the message contents over the communication channel. The term **passive** indicates that the main goal of the opponent is just to get the information and not to do any alteration in the message or harm the system resources. A passive attack is hard to recognize, as the message is not tampered or altered; therefore, the sender or receiver remains unaware of the message contents been read by some other party. However, some measures such as encryption are available to prevent their success. Two types of passive attacks are as follows:
    - **Release of Message Contents:** This type of passive attack involves the learning of the sensitive information that is sent via e-mail or tapping a conversation being carried over a telephone line.
    - **Traffic Analysis:** In this type of attack, an opponent observes the frequency and the length of messages being exchanged between the communicating nodes. This type of passive attack is more elusive, as location and identity of communicating nodes can be determined.
- **Active Attack:** In active attack, an opponent either alters the original message or creates a fake message. This attack tries to affect the operation of system resources. It is easier to recognize an active attack but hard to prevent it. Active attacks can be classified into four different categories which are as follows:
    - **Masquerade:** In computer terms, masquerading is said to happen when an entity impersonates another entity. In such an attack, an unauthorized entity tries to gain more privileges than it is authorized for. Masquerading is generally done by using stolen IDs and passwords or through bypassing authentication mechanisms.
    - **Replay:** This active attack involves capturing a copy of message sent by the original sender and retransmitting it later to bring out an unauthorized result.
    - **Modification of Messages:** This attack involves making certain modifications in the captured message or delaying or reordering the messages to cause an unauthorized effect.
    - **Denial of Service (DoS):** This attack prevents the normal functioning or proper management of communication facilities. For example, network server can be overloaded by unwanted packets, thus, resulting in performance degradation. DoS attack can interrupt and slow down the services of a network or may completely jam a network.

3. What is meant by cryptography?

Ans: The term cryptography is derived from a Greek word *kryptos* which means "secret writing". In simple terms, **cryptography** is the process of altering messages to hide their meaning from adversaries who might intercept them. In data and telecommunications, cryptography is an essential technique required for communicating over any untrusted medium, which includes any network, such as Internet. Cryptography provides an important tool for protecting information and is used in many aspects of computer security. By using cryptography techniques, the sender can first encrypt a message and then transmit it through the network. The receiver on the other hand, must be able to decrypt the message and recover the original contents of message.

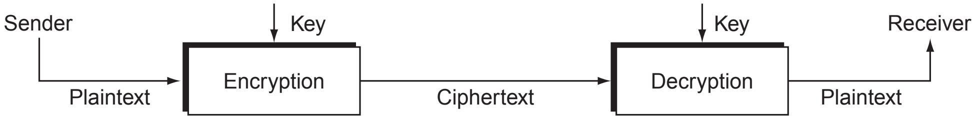


Figure 15.1 Cryptography Components

4. What are the various cryptography components? Show with the help of a diagram.

Ans: Cryptography allows a sender to disguise a message to prevent it from being read or altered by intruder as well as it enables receiver to recover the original message from disguised one. Various components are involved in cryptography (see Figure 15.1), which are described as follows:

- **Plaintext:** It refers to the original unencrypted message that the sender wishes to send.
- **Ciphertext:** It refers to the encrypted message that is received by the receiver.
- **Encryption:** It is the process of encrypting the plaintext, so that ciphertext can be produced. The plaintext is transformed to ciphertext using the encryption algorithm.
- **Decryption:** It is opposite of the encryption process. In this process, the ciphertext is converted back to plaintext using a decryption algorithm.
- **Ciphers:** The encryption and decryption algorithms are together known as ciphers. Ciphers need not necessarily be unique for each communicating pair; rather a single cipher can be used for communication between multiple pairs of sender and receiver.
- **Key:** A key is usually a number or a set of numbers on which the cipher operates. Encryption and decryption algorithms make use of a key to encrypt or decrypt messages respectively. At the sender's end, the encryption algorithm and encryption key are required to convert the plaintext to ciphertext. At the receiver's end, the decryption algorithm uses the decryption key to convert the ciphertext back to the plaintext. The longer the key is, the harder it is for an intruder to decrypt the message.

5. Defin the term cryptanalysis.

Ans: **Cryptanalysis** is the science and art of breaking the encrypted codes that are created by applying some cryptography algorithm. The person who performs cryptanalysis is known as **cryptanalyst**. Cryptanalysis attack is done by cryptanalyst so as to obtain the plaintext or key that was used to encrypt the message.

6. Explain the categories of cryptography algorithms.

Ans: Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a key. Algorithms are the complex mathematical formulae and keys are strings of bits. For two parties to communicate over a network (Internet), they must use the same algorithm (or algorithms that are designed to work together). In some cases, they must also use the same key. The cryptography algorithms are broadly classified into two categories, namel , *secret key cryptography* and *public key cryptography*.

Secret Key Cryptography

The secret key cryptography also called **symmetric key cryptography** uses a single key (shared secret key) for both encryption and decryption of data. Thus, it is obvious that the key must be known to both the sender and the receiver. As shown in Figure 15.2, the sender uses this key and the encryption algorithm to transform the plaintext into ciphertext. The ciphertext is then sent to the receiver via a communication network. The receiver applies the same key and the decryption algorithm to decrypt the ciphertext and recover the plaintext. Some examples of secret key cryptography algorithms include data encryption standard (DES), triple DES and advanced encryption standard (AES).

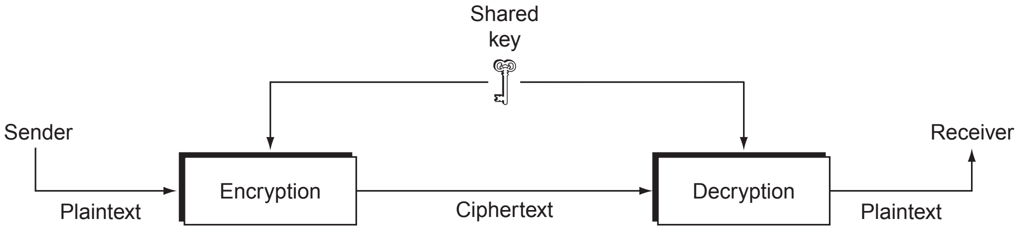


Figure 15.2 Message Exchange Using Secret Key

The main problem in secret key cryptography is getting the sender and receiver to agree on the secret key without anyone else finding out. If the key is compromised, the security offered by secret key cryptography is severely reduced or eliminated. Secret key cryptography assumes that the parties who share a key rely upon each other not to disclose the key and protect it against modification. If they are in separate physical locations, they must trust on a medium such as courier, or a phone system, to prevent the disclosure of the secret key. Anyone who overhears or intercepts the key in transit can later read, modify and forge all messages encrypted or authenticated using that key.

Public Key Cryptography

The public key cryptography also known as **asymmetric key cryptography** solves the problem found in secret key cryptography by involving two different keys for encryption and decryption. These two keys are referred to as the **public key** (used for encryption) and the **private key** (used for decryption). Each authorized user has a pair of public key and private key. The public key of each user is known to everyone, whereas, the private key is known to its owner only.

Now suppose that user A wants to transfer some information to user B securely. The user A encrypts the data by using public key of user B and sends the encrypted message to user B. On receiving encrypted message, user B decrypts it by using his or her private key. Since decryption process requires the private key of user B, which is only known to user B, the information is transferred securely. Figure 15.3 illustrates the whole process. RSA is a well-known example of public key encryption algorithm.

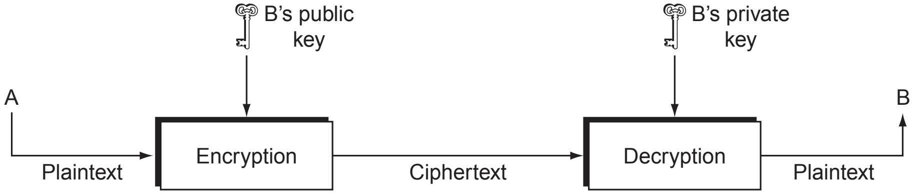


Figure 15.3 Message Exchange Using Public Key

The main advantage of public key cryptography is that the need for the sender and receiver to share secret key is eliminated and all communications involve only public keys. Thus, no private key is ever transmitted or shared. Anyone can send a confidential message using the public key, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient.

7. Explain substitution ciphers and transposition ciphers.

Ans: All encryption and decryption methods have been divided into two categories, namely, *substitution ciphers* and *transposition ciphers*. Both are the character-oriented ciphers.

Substitution Cipher

This cipher replaces a symbol (a single letter or group of letters) of the plaintext with another symbol. An example of substitution cipher is the **Caesar cipher** in which each alphabet of plaintext is replaced by an alphabet obtained by shifting three letters from it. That is, `A` is replaced by `D`, `B` is replaced by `E`, `Z` is replaced by `C` and so on. For example, cipher formed from the plaintext `TACKLE` will be `WDFNOH`**.** A slight generalization of Caesar cipher is **shift cipher** in which the ciphertext alphabet can be obtained by shifting `n` letters instead of 3; thus, `n` becomes the key. Substitution ciphers are further categorized into two types, which are as follows.

- ❑ **Monoalphabetic Cipher:** In monoalphabetic cipher, the characters in the plaintext have a one-to-one relationship with the characters in the ciphertext. It means that a character in the plaintext will always be replaced by the same character in the ciphertext. For example, if it is decided that a ciphertext character will be obtained by shifting two positions from the character in the plaintext and the given plaintext is `HAPPY`, then its ciphertext will be `JCRRA`.
- ❑ **Polyalphabetic Cipher:** In polyalphabetic cipher, the characters in the plaintext may have a one-to-many relationship with the characters in the ciphertext. It means that the same character appearing in plaintext can be replaced by a different character in the ciphertext. For example, the plaintext `HELLO` can be encrypted to `ARHIF` using a polyalphabetic cipher. Due to one-to-many relationship between the characters of plaintext and ciphertext, the key used must indicate which of the possible characters can be used for replacing a character in the plaintext. For this, the plaintext is divided into groups of characters and a set of keys is used for encrypting the groups.

Transposition Cipher

This cipher changes the location of characters in plaintext to form the ciphertext. In this cipher, there is no substitution of characters and thus, the order of characters in the plaintext is no longer preserved in the ciphertext. Transposition cipher uses a key that maps the position of characters in the plaintext to that of characters in the ciphertext. One of the commonly used transposition ciphers is **columnar transposition** in which a word or phrase without containing any repeated letters is chosen as a key. Each letter of the key is numbered to form the columns and the numbering is done in such a way that column 1 is one under the key letter closest to the start of the 26-alphabet set. Then, the plaintext is arranged horizontally under the columns forming the rows. The rows are padded with extra characters to fill the matrix, if required. The ciphertext is then read out column-wise starting from the first column to the last column. For example, if the key is `BACKIN` and the plaintext is given as `hellohowareyou`, then ciphertext will be formed as follows:

B	A	C	K	I	N
2	1	3	5	4	6
h	e	l	l	o	h
o	w	a	r	e	y
o	u	a	b	c	d

Thus, the ciphertext will be `ewuhoolaaoeclrbhyd`.

8. What is the difference between stream cipher and block cipher?

Ans: The stream cipher and block cipher are the categories of **symmetric cipher**—the ciphers that use the same key for both encryption and decryption.

The **stream cipher** operates on one symbol of plaintext at a time and using the key applied it produces a symbol of ciphertext one at a time. The stream ciphers implement a feedback mechanism so that the key is constantly changing. Thus, the same character in plaintext may be encrypted to different characters in ciphertext. However, each character is encrypted and decrypted using the same key regardless of the fact that multiple keys are being used. For example, consider the plaintext is *user* and three different keys (K_1, K_2 and K_3) are used to produce ciphertext, such that the characters u and r are encrypted using key K_1, the characters s is encrypted using key K_2 and the character e is encrypted using K_3. Then, during decryption also, the same set of keys (K_1, K_2 and K_3) are used, such that the characters u and r are decrypted using key K_1, the character s is decrypted using key K_2 and the character e is decrypted using the key K_3.

On the other hand, in **block ciphers**, an n-bit block of plaintext is encrypted together to produce an n-bit block of ciphertext. Similarly, during decryption, n-bit block of ciphertext is converted back to n-bit block of plaintext, one block at a time. Each block of bits is encrypted or decrypted using the same key. Thus, the same block of plaintext will always be encrypted to same block of ciphertext.

9. Describe S-box and P-box.

Ans: S-box (substitution box) and P-box (permutation box) are used to perform substitution and transposition function respectively. These are described as follows.

- **S-box:** This is a substitution box having same characteristics as that of substitution cipher except that the substitution of several bits is performed in parallel. It takes n bits of plaintext at a time as input and produces m bits of ciphertext as output where the value of n and m may be same or different. An S-box can be *keyed* or *keyless*. In a **keyed** S-box, the mapping of n inputs to m outputs is decided with the help of a key, while in **keyless** S-box, the mapping from inputs to outputs is predetermined.
- **P-box:** This is a permutation box having same characteristics as that of traditional transposition cipher except that it performs transposition at bit-level and transposition of several bits is performed at the same time. The input bits are permutated to produce the output bits. For example, the first input bit can be the second output bit, second input bit can be the third output bit and so on. P-box is normally keyless and can be classified into the following three types based on the length of input and output.
  - **Straight P-box:** This P-box takes n bits as input, permutes them and produces n bits as output. As the number of inputs and outputs is the same, there are total n! ways to map n inputs to n outputs.
  - **Compression P-box:** This P-box takes n bits as input and permutes them in such a way that an output of m bits is produced where $m < n$. This implies that two or more inputs are mapped to the same output.
  - **Expansion P-box:** This P-box takes n bits as input and permutes them in such a way that an output of m bits is produced where $m > n$. This implies that a single input is mapped to more than one output.

10. Explain DES in detail.

Ans: DES is a symmetric-key cipher that was developed by IBM. This encryption standard was adopted by the U.S. government for non-classified information and by various industries for the use in security products. It is also called a block cipher, as it divides plaintext into blocks and same key is used for encryption and decryption of blocks. DES involves multiple rounds to produce the ciphertext and the key used in each round is the subset of the general key called **round key** produced by the round key generator. That is, if there are P rounds in cipher, then P number of keys ($K_1, K_2 ... K_P$) will be generated where K_1 will be used in first round, K_2 in second round and so on.

At the sender's end, the DES takes 64-bit block of plaintext, encrypts it using the 56-bit round key and produces 64-bit ciphertext. Originally, the round key is of 64 bits including eight parity bits, thus, the usable bits in key are only 56. The whole process of producing ciphertext from plaintext comprises 19 stages (see Figure 15.4). The first stage is the keyless transposition on the 64-bit plaintext. Next, 16 stages are the rounds that are functionally similar and in each round, a different key K_i of 48 bits derived from the original key of 56 bits is used. The second last stage performs a swap function in which leftmost 32 bits are exchanged with the rightmost 32 bits. The last stage is simply the opposite of the first stage, that is, it performs inverse transposition on 64 bits. At the receiver's end, the decryption is performed using the same key as in encryption; however, now, the steps are performed in the reverse order.

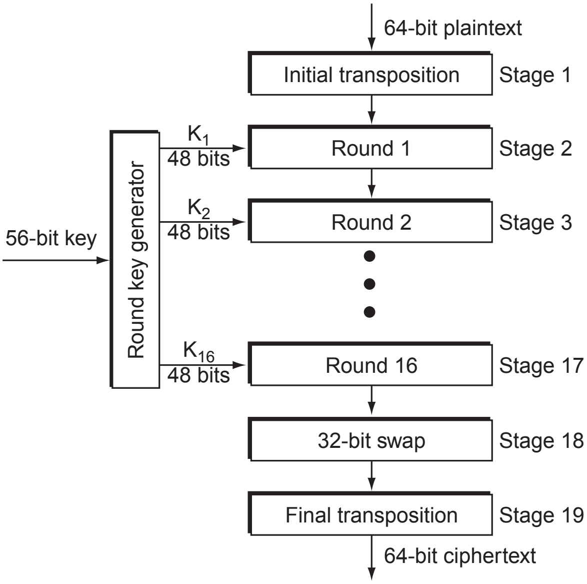


Figure 15.4 Stages Involved in the DES

The structure of one of the 16 rounds (say, i^{th} round) during the encryption in DES is shown in Figure 15.5. It takes two inputs: the leftmost 32 bits as left input (L_i) and the rightmost 32 bits as right input (R_i) and produces two outputs: left output (L_{i+1}) and right output (R_{i+1}), each of 32 bits. The left

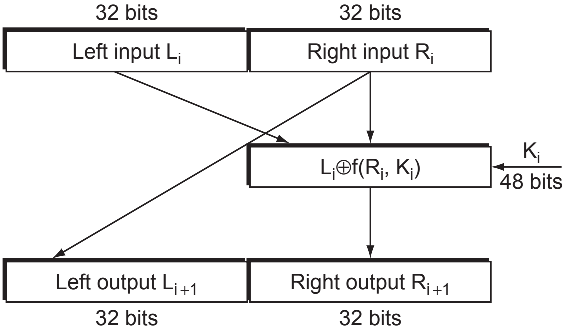


Figure 15.5 Structure of Encryption Round

output (L_{i+1}) is just the right input (R_i). The right output (R_{i+1}) is obtained by first applying the DES function (f) on the right input (R_i) and the 48-bit key (K_i) being used in the i^{th} round, denoted as $f(R_i, K_i)$, and then performing the bitwise XOR of the result of DES function and the left input (L_i). The structure of decryption round in DES is simply the opposite of the encryption round.

The essence of DES is the DES function. The function $f(R_i, K_i)$ comprises four steps (see Figure 15.6), which need to be carried out sequentially. These steps are as follows:

1. The right output (R_i) of 32 bits is fed into the expansion P-box which produces an output (say, E) of 48 bits.
2. A bitwise XOR is performed on 48-bit E and 48-bit key K_i generated for that round, resulting in 48 bits.
3. The 48-bit output of XOR operation is broken down into eight groups with each group consisting of six bits. Each group of six bits is then fed to one of eight S-boxes. Each S-box maps six inputs to four outputs and thus, total 32 bits are obtained from eight S-boxes.
4. The 32 bits obtained from S-boxes are input to a straight P-box, which permutes them and produces 32 bits as output.

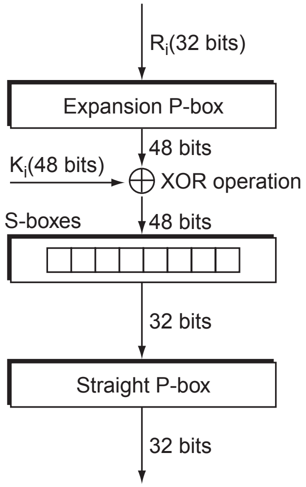


Figure 15.6 DES Function

11. Write a short note on triple DES.

Ans: The length of the key used in DES was too short. Therefore, triple DES (3DES) was developed to increase the key length, thereby making the DES more secure. The encryption and decryption in 3DES are performed in three stages with the help of two keys, say K_1 and K_2 of 56 bits each. During encryption, the plaintext is encrypted using DES with key K_1 in the first stage, then the output of first stage is decrypted using DES with key K_2 in the second stage and finall , the output of second stage is encrypted using DES with key K_1 in the third stage thereby producing the ciphertext. On the other hand, during decryption, the ciphertext is decrypted using DES with key K_1 in the first stage, then the output of first stage is encrypted using DES with key K_2 in the second stage and finall , the output of second stage is decrypted using DES with key K_1 in the third stage thereby producing the plaintext. The use of two keys and three stages in 3DES increased the key size to 112 bits and provides more secured communication.

Another version of 3DES uses three keys of 56 bits each and a different key is used for encryption/decryption in each stage. The use of three different keys further increases the key length to 168 bits; however, it results in an increased overhead due to managing and transporting one more key.

12. Explain the RSA algorithm.

Ans: In 1978, a group at M.I.T. discovered a strong method for public key encryption. It is known as **RSA**, the name derived from the initials of the three discoverers Ron **R**ivest, Adi **S**hamir and Len **A**dleman. It is the most widely accepted public key scheme, in fact most of the practically implemented security is based on RSA. The algorithm requires keys of at least 1024 bits for good security. This algorithm is based on some principles from number theory, which states that determining the prime factors of a number is extremely difficult. The algorithm follows the following steps to determine the encryption and decryption keys.

1. Take two large distinct prime numbers, say m and n (about 1024 bits).
2. Calculate $p = m*n$ and $q = (m-1)*(n-1)$.
3. Find a number which is relatively prime to q, say D. That number is the decryption key.
4. Find encryption key E such that $E*D = 1 \bmod q$.

Using these calculated keys, a block B of plaintext is encrypted as $T_e = B^E \bmod p$. To recover the original data, compute $B = T_e)^D \bmod p$. Note that E and p are needed to perform encryption whereas D and p are needed to perform decryption. Thus, the public key consists of (E,p) and the private key consists of (D, p). An important property of RSA algorithm is that the roles of E and D can be interchanged. As the number theory suggests that it is very hard to find prime factors of p, it is extremely difficult for an intruder to determine decryption key D using just E and p, because it requires factoring p which is very hard.

13. What is digital signature? How it works?

Ans: The historical legal concept of "signature" is defined as any mark made with the intention of authenticating the marked document. **Digital signature** refers to the digitized images of paper signature used to verify the authenticity of an electronic document. In other words, digital signatures play the role of physical handwritten signatures in verifying electronic documents. Digital signatures use public key cryptography technique, which employs an algorithm using two different but mathematically related keys: private and public keys. Both public and private keys have an important property that permits the reversal of their roles; the encryption key (E) can be used for decryption and the decryption key (D) can be used for encryption, that is, E(D(P)) = D(E(P)) where P denotes the plaintext. This property is used for creating messages with digital signature.

The private key is known only to the signer who uses it for creating a digital signature or transforming data into a seemingly unintelligible form and the signed document can be made public. The public key is used for verifying the digital signature or returning the message to its original form. Any user can easily verify the authenticity of the document by using the public key that means it can be easily verified that the data is originated by the person who claims for it. However, no one can sign the document without having the private key.

To have a clear understanding of how digital signature is used, refer Figure 15.7. Suppose A wants to send his or her signed message (message with digital signature) to B through network. For this, A encrypts the message (M) using his or her private key (E_A) and this process results in an encrypted message [E_A(M)] bearing A's signature on it. The signed message is then sent through the network to B. Now, B attempts to decrypt the received message using A's public key (D_A) in order to verify that the received message has really come from A. If the message gets decrypted {that is, $D_A[E_A(M)] = M$}, B can believe that the message has come from A. However, if the message or the digital signature has been modified during the transmission, it cannot be decrypted using A's public key. From here, B can conclude that either the message transmission has tampered or the message has not been generated by A.

Digital signatures also ensure non-repudiation. For example, on receiving the encrypted message, B can keep a copy of that message, so that A cannot later deny of sending of message. Moreover, as B is unaware of A's private key (E_A), he or she cannot alter the contents of the encrypted message. However, the only problem with this mechanism is that the message can be tapped by anyone (other than the intended user B) who knows the A's public key (D_A) thereby breaching confidentialit .

To ensure message confidentiali y, encryption and decryption are performed twice at A's end and B's end respectively. At A's end, first the message is encrypted using A's private key (E_A) and then a second

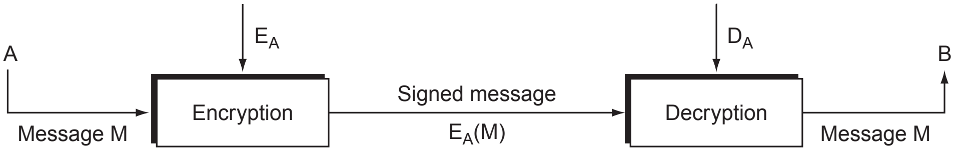


Figure 15.7 Digital Signature Using Private Key

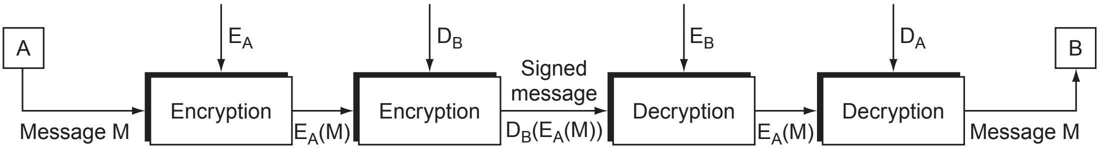


Figure 15.8 Digital Signature Using Public and Private Keys

encryption is performed using the B's public key (D_B) as shown in Figure 15.8. Similarly, at B's end, first, the message is decrypted using B's private key (E_B) and then a second decryption is performed using A's public key (D_A). With this mechanism, only B can decrypt the encrypted message received from A because only he or she knows his or her own private key.

14. Defin hash function. What are its properties?

Ans: A hash function is a cryptographic algorithm that transforms the given input (such as a message) into a fixed-length string, referred to as the **hash value**. Formally, the hash value (h) can be expressed as:

$$h = H(M),$$

where M = message (string) of any length, H = hash function and H(M) = a fixed-length string

The hash value plays the role of a "signature" for the data being sent from the sender to receiver through the network. Sometimes, the hash value is also referred to as message digest or simply digest, or electronic form of fingerprint

An ideal hash function is characterized by the following properties:

- For any given message, the hash value can be computed very easily and efficientl .
- Given a hash value, it is difficult, nearly impossible, to dete mine the message having that hash value.
- No two messages, even being almost similar, are likely to have the same hash value.

15. What do you understand by the term fi ewall? Explain its use with the help of an example?

Ans: The ongoing occurrences of incidents pertaining to network security caused a great concern to the people, using computers as their medium to exchange data across the country. A need was felt for a method of controlling the traffic, which allows access of information to computers. Organizations required an application that could protect and isolate their internal systems from the Internet. This application is called **fi ewall**. Simply put, a firewall prevents certain outside connections from entering into the network. It traps inbound or outbound packets, analyzes them and then permits access or discards them.

Generally, firewall system comprises software (embedded in a router), computer, host or a collection of hosts set up specifically to shield a site or subnet from protocols and services that can be a threat from hosts outside the subnet. It serves as the gatekeeper between an untrusted network (Internet) and the more trusted internal networks. If a remote user tries to access the internal networks without going through the firewall, its effectiveness is diluted. For example, if a travelling manager has an office computer that he or she can dial into while travelling, and his or her computer is on the protected internal network, then an attacker who can dial into that computer has circumvented the firewall. Similarly, if a user has a dial-up Internet account, and sometimes connects to the Internet from his or her office computer, he or she opens an unsecured connection to the Internet that circumvents the fi ewall.

To understand the use of firewall, consider an example where an organization is having hundreds of computers on the network. In addition, the organization will have one or more connections to the Internet lines. Now, without a firewall in place, all the computers are directly accessible to anyone on the Internet. A person who knows what other people are doing can probe those computers; try to make FTP (file transfer protocol) connections to them, or telnet connections and so on. If one employee makes a mistake and leaves a security hole, hackers can get to the machine and exploit that hole.

With a firewall in place, the network landscape becomes much different. An organization will place a firewall at every connection to the Internet (for example, at every T1 line coming into the company). The firewall can implement security rules. For example, one of the security rules may be: out of the 300 computers inside an organization, only one is permitted to receive public FTP traffic. A company can set up rules like this for FTP servers, web servers, telnet servers and so on. In addition, an organization can have control on how employees connect to websites, whether or not files can be sent as attachments outside the company over the network and so on. Firewall provides incredible control over how people use the network.

16. What is the role of packet filtering in the firewall?

Ans: A firewall intercepts the data between the Internet and the computer. All data traffic passes through it and it allows only authorized data to pass into the corporate network. Firewalls are typically implemented using **packet filtering**.

Packet filtering is the most basic firewall protection technique used in an organization. It operates at the network layer to examine incoming and outgoing packets and applies a fixed set of rules to the packets to determine whether or not they will be allowed to pass. The packet filter firewall is typically very fast because it does not examine any of the data in the packet. It simply examines the IP packet header, the source and destination IP addresses and the port combinations and then it applies filtering rules. For example, it is easy to filter out all packets destined for Port 80, which might be the port for a web server. The administrator may decide that Port 80 is off limits except for specific IP subnets and a packet filter would suffice for this. Packet filtering is fast, flexible, transparent (no changes are required at the client) and cheap. This type of filter is commonly used in small to medium businesses that require control over users to use the Internet.

17. Define identification and authentication. Explain how users can be authenticated?

Ans: Often people confuse identification from authentication, as both have similar aspects. **Identification** is the means through which a user provides a claimed identity to the system. On the other hand, **authentication** refers to establishing the validity of the claim. Computer systems make use of data authentication for recognizing people, which the systems receive. Authentication presents several challenges such as collecting authentication data, transmitting the data securely and identifying the same person who was earlier authenticated and is still using the computer system.

Various methods can be used to authenticate a user, such as a secret password, some physical characteristics of the user, a smart card or a key given to the user.

Password Authentication

It is the simplest and most commonly used authentication scheme. In this scheme, the user is asked to enter the user name and password to log in into the database. The DBMS then verifies the combination of user name and password to authenticate the user and allows him or her to access the database if he or she is the legitimate user, otherwise access is denied. Generally, password is asked once when a user log in into the database; however, this process can be repeated for each operation when the user is trying to access sensitive data.

Though the password scheme is widely used by database systems, this scheme has some limitations. In this method, the security of database completely relies on the password. Thus, the password itself needs to be secured from unauthorized access. One simple way to secure the password is to store it in an encrypted form. Further, care should be taken to ensure that password would never be displayed on the screen in its decrypted (non-encrypted) form.

Physical Characteristics of User

In this method, the physical characteristics, such as fingerprints, voice, length of fingers of hand, and face structure of the users are used for the identification purpose. These characteristics of users are known to be unique and have a very low probability of duplication. Thus, the security of the database is relatively high in this scheme as compared to the password scheme. However, this method requires the use of some special hardware and software to identify physical characteristics of the user, which incurs extra cost to the organization.

Smart Card

In this method, a database user is provided with a smart card that is used for identification. The smart card has a key stored on an embedded chip and the operating system of smart card ensures that the key can never be read. Instead, it allows data to be sent to the card for encryption or decryption using that private key. The smart card is programmed in such a way that it is extremely difficult to extract the values from smart card; thus, it is considered as a secure device.

18. Write a short note on message authentication.

Ans: Message authentication is a means to verify that the message received by the receiver is from the intended sender and not from the intruder. The sender needs to send some proof along the message, so that the receiver can authenticate the message. To authenticate a message, the message authentication code (MAC) is used. MAC uses a hash function (MAC algorithm) that generates a MAC (a tag-like) with the help of a secret key shared between the sender and the receiver. Figure 15.9 depicts the use of MAC to authenticate a message at the sender's end and to verify the authenticity of message at the receiver's end.

At the sender's end, the original message that is to be authenticated along with the secret key are given as input to the MAC algorithm that produces a MAC as output. The MAC is attached with the original message and both are sent to the receiver through the network. To verify the authenticity of message at the receiver's end, the message is distinguished from MAC and the MAC algorithm is again applied on the message using the secret key to generate a new MAC. Then, the newly generated MAC is compared

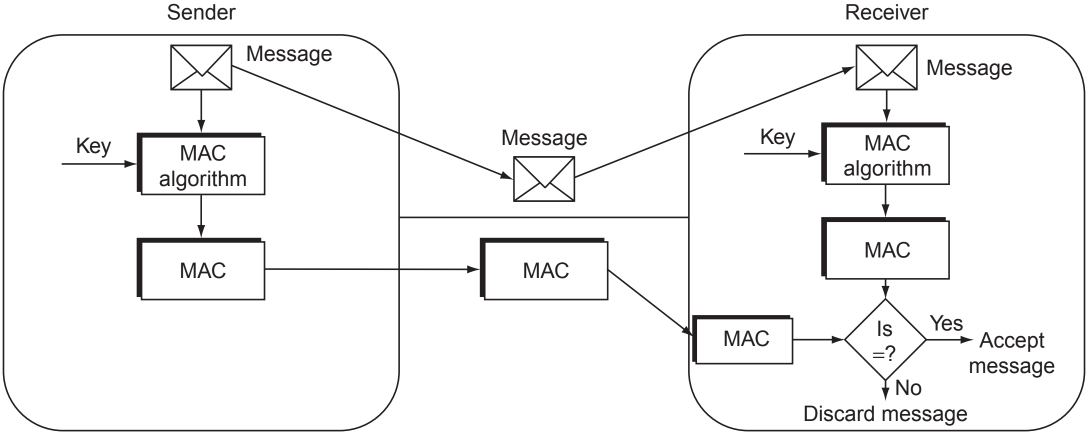


Figure 15.9 Message Authentication Using MAC

with the received MAC to determine whether they are same or not. If so, the receiver knows that the message has not been changed and is actually from the intended sender and thus, accepts the message. Otherwise, the message is discarded.

19. Encrypt the plaintext 6 using RSA public key encryption algorithm. Use prime numbers 11 and 3 to compute the public and private keys. Moreover, decrypt the ciphertext using the private key.

Ans: Here, $m = 11$ and $n = 3$

According to RSA algorithm (as explained in **Q12**)

$$p = m * n = 11 * 3 = 33$$
$$q = (m - 1) * (n - 1) = (11 - 1) * (3 - 1) = 10 * 2 = 20$$

We choose D = 3 (a number relatively prime to 20, that is, gcd (20, 3) = 1).

Now,

$$\mathrm{E} * \mathrm{D} = 1 \bmod \mathrm{q}$$
$$\Rightarrow \mathrm{E} * 3 = 1 \bmod 20$$
$$\Rightarrow \mathrm{E} = 7$$

As we know, the public key consists of (E, p) and the private key consists of (D, p). Therefore, the public key is (7, 33) and the private key is (3, 33).

The plaintext 6 can be converted to ciphertext using the public key (7, 33) as follows.

$$\mathrm{T}_e = \mathrm{B}^{\mathrm{E}} \bmod \mathrm{p}$$
$$\Rightarrow 6^7 \bmod 33$$
$$\Rightarrow 30$$

On applying the private key to the ciphertext 30 to get original plaintext, we get

$$\mathrm{B} = (\mathrm{T}_e)^{\mathrm{D}} \bmod \mathrm{p}$$
$$\Rightarrow (30)^3 \bmod 33$$
$$\Rightarrow 6$$

Multiple Choice Questions

1. Which of the following are necessary for secured communication?
   (a) Authentication (b) Confidentialit
   (c) Integrity (d) All of these

2. In ______ attack, an opponent either alters the original message or creates a fake message.
   (a) Passive (b) Inactive
   (c) Active (d) Access

3. __________ is a type of passive attack.
   (a) Replay (b) Traffic analysi
   (c) Masquerade (d) Denial of service

4. Which of the following is not a component of cryptography?
   (a) Ciphertext (b) Ciphers
   (c) Key (d) None of these

5. In public key cryptography, ________ key is used for encryption.
   (a) Public (b) Private
   (c) Both (a) and (b) (d) Shared

6. _________ is the means through which a user provides a claimed identity to the system.
   (a) Authentication (b) Identificatio
   (c) Encryption (d) Decryption

7. In __________cipher, characters in the plaintext and ciphertext are related to each other by one-to-many relationship.

(a) Monoalphabetic (b) XOR
(c) Polyalphabetic (d) Rotation

8. DES takes _____-bit key as an input for encrypting the text.
(a) 128 (b) 64
(c) 56 (d) 168

9. Which of the following applications traps inbound or outbound packets, analyze them and then permits access or discards them?
(a) Digital signature
(b) Authentication
(c) Identificatio
(d) Firewall

10. MDC stands for
(a) Message detection code
(b) Modification detection cod
(c) Masquerade detection code
(d) None of these

Answers

1. (d) 2. (c) 3. (b) 4. (d) 5. (a) 6. (b) 7. (c) 8. (c) 9. (d) 10. (b)

This page is intentionally left blank.

Index